

Novosit®

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

OnBase™
by Hyland

ProDactivity
Digital All

Microsoft Partner
Gold Independent Software Vendor (ISV)

PARASCRIP™

NovoSign

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1.1
Fecha edición:	06/02/2024
Fichero:	NOVOSIT_DPC_ES_v1

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Alejandro Grande Fecha: 06/02/2024	Nombre: Ramón E. Sarante Fecha: 12/02/2024	Nombre: Francis Ant. Reyes Fecha: 12/02/2024

Control de versiones

Versión	Partes que cambian	Descripción cambio	Autor cambio	Fecha cambio
1.0	Original	Creación del documento	Alejandro Grande	19/10/2020
1.1	1.1 ,1.2, 1.4, 3.1.1	Añadidos los perfiles de certificado cualificado de Persona Física para Procedimientos Tributarios	Alejandro Grande	06/02/2024

Índice

INFORMACIÓN GENERAL	2
CONTROL DOCUMENTAL	2
ESTADO FORMAL	2
CONTROL DE VERSIONES.....	3
ÍNDICE.....	4
1. INTRODUCCIÓN	11
1.1. PRESENTACIÓN	11
1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN	11
1.2.1. <i>Identificadores de certificados</i>	12
1.3. PARTICIPANTES EN LOS SERVICIOS DE CERTIFICACIÓN	12
1.3.1. <i>Entidad de Certificación Acreditada</i>	12
1.3.1.1. UANATACA ROOT 2016	13
1.3.1.2. NOVOSIT CA 1	13
1.3.2. <i>Unidad de Registro</i>	14
1.3.3. <i>Entidades finales</i>	15
1.3.3.1. Suscriptores del servicio de certificación	15
1.3.3.2. Firmantes	16
1.3.3.3. Partes usuarias	17
1.3.4. <i>Proveedor de Servicios de Infraestructura de Clave Pública</i>	17
1.4. USO DE LOS CERTIFICADOS	18
1.4.1. <i>Usos permitidos para los certificados</i>	18
1.4.1.1. Certificado cualificado de persona física en P12	18
1.4.1.2. Certificado cualificado de persona física en QSCD centralizado	19
1.4.1.3. Certificado cualificado de persona física representante en p12	20
1.4.1.4. Certificado cualificado persona física representante en QSCD centralizado.....	21
1.4.1.5. Certificado cualificado de persona física para Procedimientos Tributarios en P12	22
1.4.1.6. Certificado cualificado de persona física para Procedimientos Tributarios en QSCD.....	23
1.4.1.7. Certificado cualificado de Sello Electrónico en p12	23
1.4.1.8. Certificado cualificado de Sello Electrónico en QSCD centralizado	24
1.4.1.9. Certificado de sello de tiempo electrónico	25
1.4.2. <i>Límites y prohibiciones de uso de los certificados</i>	25
1.5. ADMINISTRACIÓN DE LA POLÍTICA	27
1.5.1. <i>Organización que administra el documento</i>	27
1.5.2. <i>Datos de contacto de la organización</i>	27
1.5.3. <i>Procedimientos de gestión del documento</i>	27
2. PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS.....	28

2.1.	DEPÓSITO(S) DE CERTIFICADOS.....	28
2.2.	PUBLICACIÓN DE INFORMACIÓN DEL PRESTADOR DE SERVICIOS DE CERTIFICACIÓN	28
2.3.	FRECUENCIA DE PUBLICACIÓN	28
2.4.	CONTROL DE ACCESO	29
3.	IDENTIFICACIÓN Y AUTENTICACIÓN.....	30
3.1.	REGISTRO INICIAL	30
3.1.1.	<i>Tipos de nombres.....</i>	<i>30</i>
3.1.1.1.	Certificado cualificado de Persona Física ciudadano en p12.....	30
3.1.1.2.	Certificado cualificado de Persona Física en QSCD centralizado	31
3.1.1.3.	Certificado cualificado de Persona Física Representante en p12	32
3.1.1.4.	Certificado cualificado de firma de Persona Física Representante en QSCD centralizado	32
3.1.1.5.	Certificado cualificado de Sello Electrónico en p12	33
3.1.1.6.	Certificado cualificado de Sello Electrónico en QSCD Centralizado	33
3.1.1.7.	Certificado de sello de tiempo electrónico	35
3.1.2.	<i>Significado de los nombres.....</i>	<i>35</i>
3.1.2.1.	Emisión de certificados del set de pruebas y certificados de pruebas en general	35
3.1.3.	<i>Empleo de anónimos y seudónimos.....</i>	<i>35</i>
3.1.4.	<i>Interpretación de formatos de nombres.....</i>	<i>36</i>
3.1.5.	<i>Unicidad de los nombres.....</i>	<i>36</i>
3.1.6.	<i>Resolución de conflictos relativos a nombres.....</i>	<i>37</i>
3.2.	VALIDACIÓN INICIAL DE LA IDENTIDAD	38
3.2.1.	<i>Prueba de posesión de clave privada.....</i>	<i>38</i>
3.2.2.	<i>Autenticación de la identidad de una organización, empresa o entidad mediante representante.....</i>	<i>38</i>
3.2.3.	<i>Autenticación de la identidad de una persona física</i>	<i>41</i>
3.2.3.1.	En los certificados	41
3.2.3.2.	Validación de la Identidad.....	42
3.2.3.3.	Vinculación de la persona física	43
3.2.4.	<i>Información de suscriptor no verificada</i>	<i>44</i>
3.2.5.	<i>Autenticación de la identidad de una RA y sus operadores.....</i>	<i>44</i>
3.3.	IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN.....	45
3.3.1.	<i>Validación para la renovación rutinaria de certificados</i>	<i>45</i>
3.3.2.	<i>Identificación y autenticación de la solicitud de renovación</i>	<i>45</i>
3.4.	IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SOLICITUD DE REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN	46
4.	REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS	47
4.1.	SOLICITUD DE EMISIÓN DE CERTIFICADO	47
4.1.1.	<i>Legitimación para solicitar la emisión</i>	<i>47</i>
4.1.2.	<i>Procedimiento de alta y responsabilidades</i>	<i>47</i>
4.2.	PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN	48
4.2.1.	<i>Ejecución de las funciones de identificación y autenticación.....</i>	<i>48</i>
4.2.2.	<i>Aprobación o rechazo de la solicitud</i>	<i>49</i>
4.2.3.	<i>Plazo para resolver la solicitud</i>	<i>49</i>

4.3.	EMISIÓN DEL CERTIFICADO	49
4.3.1.	<i>Acciones de la CA durante el proceso de emisión</i>	<i>49</i>
4.3.2.	<i>Notificación de la emisión al suscriptor</i>	<i>50</i>
4.4.	ENTREGA Y ACEPTACIÓN DEL CERTIFICADO	51
4.4.1.	<i>Responsabilidades de la CA</i>	<i>51</i>
4.4.2.	<i>Conducta que constituye aceptación del certificado</i>	<i>52</i>
4.4.3.	<i>Publicación del certificado</i>	<i>52</i>
4.4.4.	<i>Notificación de la emisión a terceros</i>	<i>52</i>
4.5.	USO DEL PAR DE CLAVES Y DEL CERTIFICADO	53
4.5.1.	<i>Uso por el firmante</i>	<i>53</i>
4.5.2.	<i>Uso por el suscriptor</i>	<i>54</i>
4.5.2.1.	Obligaciones del suscriptor del certificado	54
4.5.2.2.	Responsabilidad civil del suscriptor de certificado	55
4.5.3.	<i>Uso por el tercero que confía en certificados</i>	<i>55</i>
4.5.3.1.	Obligaciones del tercero que confía en certificados	55
4.5.3.2.	Responsabilidad civil del tercero que confía en certificados	56
4.6.	RENOVACIÓN DE CERTIFICADOS	56
4.7.	RENOVACIÓN DE CLAVES Y CERTIFICADOS	57
4.7.1.	<i>Causas de renovación de claves y certificados</i>	<i>57</i>
4.7.2.	<i>Procedimiento de renovación online de certificados</i>	<i>57</i>
4.7.2.1.	Circunstancias para la renovación online	57
4.7.2.2.	Quién puede solicitar la renovación online de un certificado	57
4.7.2.3.	Aprobación o rechazo de la solicitud	58
4.7.2.4.	Tramitación de las peticiones de renovación online	58
4.7.2.5.	Notificación de la emisión del certificado renovado	59
4.7.2.6.	Conducta que constituye aceptación del certificado renovado	59
4.7.2.7.	Publicación del certificado renovado	59
4.7.2.8.	Notificación de la emisión a terceros	59
4.8.	MODIFICACIÓN DE CERTIFICADOS	60
4.9.	REVOCACIÓN, SUSPENSIÓN O REACTIVACIÓN DE CERTIFICADOS	60
4.9.1.	<i>Causas de revocación de certificados</i>	<i>60</i>
4.9.2.	<i>Causas de suspensión de un certificado</i>	<i>62</i>
4.9.3.	<i>Causas de reactivación de un certificado</i>	<i>62</i>
4.9.4.	<i>Quién puede solicitar la revocación, suspensión o reactivación</i>	<i>62</i>
4.9.5.	<i>Procedimientos de solicitud de revocación, suspensión o reactivación</i>	<i>63</i>
4.9.6.	<i>Plazo temporal de solicitud de revocación, suspensión o reactivación</i>	<i>64</i>
4.9.7.	<i>Plazo temporal de procesamiento de la solicitud de revocación, suspensión o reactivación</i>	<i>64</i>
4.9.8.	<i>Obligación de consulta de información de revocación o suspensión de certificados</i>	<i>64</i>
4.9.9.	<i>Frecuencia de emisión de listas de revocación de certificados (LRCs)</i>	<i>65</i>
4.9.10.	<i>Plazo máximo de publicación de LRCs</i>	<i>65</i>
4.9.11.	<i>Disponibilidad de servicios de comprobación en línea de estado de certificados</i>	<i>65</i>
4.9.12.	<i>Obligación de consulta de servicios de comprobación de estado de certificados</i>	<i>66</i>
4.9.13.	<i>Requisitos especiales en caso de compromiso de la clave privada</i>	<i>66</i>

4.9.14.	<i>Período máximo de un certificado digital en estado suspendido</i>	66
4.10.	FINALIZACIÓN DE LA SUSCRIPCIÓN	66
4.11.	DEPÓSITO Y RECUPERACIÓN DE CLAVES	67
4.11.1.	<i>Política y prácticas de depósito y recuperación de claves</i>	67
4.11.2.	<i>Política y prácticas de encapsulado y recuperación de claves de sesión</i>	67
5.	CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES	68
5.1.	CONTROLES DE SEGURIDAD FÍSICA	68
5.1.1.	<i>Localización y construcción de las instalaciones</i>	69
5.1.2.	<i>Acceso físico</i>	70
5.1.3.	<i>Electricidad y aire acondicionado</i>	70
5.1.4.	<i>Exposición al agua</i>	70
5.1.5.	<i>Prevención y protección de incendios</i>	71
5.1.6.	<i>Almacenamiento de soportes</i>	71
5.1.7.	<i>Tratamiento de residuos</i>	71
5.1.8.	<i>Copia de respaldo fuera de las instalaciones</i>	71
5.2.	CONTROLES DE PROCEDIMIENTOS	71
5.2.1.	<i>Funciones fiables</i>	72
5.2.2.	<i>Número de personas por tarea</i>	73
5.2.3.	<i>Identificación y autenticación para cada función</i>	73
5.2.4.	<i>Roles que requieren separación de tareas</i>	73
5.2.5.	<i>Sistema de gestión PKI</i>	74
5.3.	CONTROLES DE PERSONAL	74
5.3.1.	<i>Requisitos de historial, calificaciones, experiencia y autorización</i>	74
5.3.2.	<i>Procedimientos de investigación de historial</i>	75
5.3.3.	<i>Requisitos de formación</i>	75
5.3.4.	<i>Requisitos y frecuencia de actualización formativa</i>	76
5.3.5.	<i>Secuencia y frecuencia de rotación laboral</i>	76
5.3.6.	<i>Sanciones para acciones no autorizadas</i>	76
5.3.7.	<i>Requisitos de contratación de profesionales</i>	77
5.3.8.	<i>Suministro de documentación al personal</i>	77
5.4.	PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	77
5.4.1.	<i>Tipos de eventos registrados</i>	77
5.4.2.	<i>Frecuencia de tratamiento de registros de auditoría</i>	79
5.4.3.	<i>Período de conservación de registros de auditoría</i>	79
5.4.4.	<i>Protección de los registros de auditoría</i>	79
5.4.5.	<i>Procedimientos de copia de respaldo</i>	80
5.4.6.	<i>Localización del sistema de acumulación de registros de auditoría</i>	80
5.4.7.	<i>Notificación del evento de auditoría al causante del evento</i>	80
5.4.8.	<i>Análisis de vulnerabilidades</i>	80
5.5.	ARCHIVOS DE INFORMACIONES	81
5.5.1.	<i>Tipos de registros archivados</i>	81

5.5.2.	<i>Período de conservación de registros</i>	82
5.5.3.	<i>Protección del archivo</i>	82
5.5.4.	<i>Procedimientos de copia de respaldo</i>	82
5.5.5.	<i>Requisitos de sellado de fecha y hora</i>	83
5.5.6.	<i>Localización del sistema de archivo</i>	83
5.5.7.	<i>Procedimientos de obtención y verificación de información de archivo</i>	83
5.6.	RENOVACIÓN DE CLAVES	83
5.7.	COMPROMISO DE CLAVES Y RECUPERACIÓN DE DESASTRE	84
5.7.1.	<i>Procedimientos de gestión de incidencias y compromisos</i>	84
5.7.2.	<i>Corrupción de recursos, aplicaciones o datos</i>	84
5.7.3.	<i>Compromiso de la clave privada de la entidad</i>	84
5.7.4.	<i>Continuidad del negocio después de un desastre</i>	84
5.8.	TERMINACIÓN DEL SERVICIO	85
6.	CONTROLES DE SEGURIDAD TÉCNICA	87
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES	87
6.1.1.	<i>Generación del par de claves</i>	87
6.1.1.1.	<i>Generación del par de claves del firmante</i>	88
6.1.2.	<i>Envío de la clave privada al firmante</i>	88
6.1.3.	<i>Envío de la clave pública al emisor del certificado</i>	88
6.1.4.	<i>Distribución de la clave pública del prestador de servicios de certificación</i>	89
6.1.5.	<i>Tamaños de claves</i>	89
6.1.6.	<i>Generación de parámetros de clave pública</i>	89
6.1.7.	<i>Comprobación de calidad de parámetros de clave pública</i>	89
6.1.8.	<i>Generación de claves en aplicaciones informáticas o en bienes de equipo</i>	89
6.1.9.	<i>Propósitos de uso de claves</i>	90
6.2.	PROTECCIÓN DE LA CLAVE PRIVADA	90
6.2.1.	<i>Estándares de módulos criptográficos</i>	90
6.2.2.	<i>Control por más de una persona (n de m) sobre la clave privada</i>	90
6.2.3.	<i>Depósito de la clave privada</i>	90
6.2.4.	<i>Copia de respaldo de la clave privada</i>	90
6.2.5.	<i>Archivo de la clave privada</i>	91
6.2.6.	<i>Introducción de la clave privada en el módulo criptográfico</i>	91
6.2.7.	<i>Método de activación de la clave privada</i>	92
6.2.8.	<i>Método de desactivación de la clave privada</i>	92
6.2.9.	<i>Método de destrucción de la clave privada</i>	92
6.2.10.	<i>Clasificación de módulos criptográficos</i>	93
6.3.	OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES	93
6.3.1.	<i>Archivo de la clave pública</i>	93
6.3.2.	<i>Períodos de utilización de las claves pública y privada</i>	93
6.4.	DATOS DE ACTIVACIÓN	93
6.4.1.	<i>Generación e instalación de datos de activación</i>	93

6.4.2.	Protección de datos de activación	93
6.5.	CONTROLES DE SEGURIDAD INFORMÁTICA	94
6.5.1.	Requisitos técnicos específicos de seguridad informática	94
6.5.2.	Evaluación del nivel de seguridad informática	95
6.6.	CONTROLES TÉCNICOS DEL CICLO DE VIDA	95
6.6.1.	Controles de desarrollo de sistemas	95
6.6.2.	Controles de gestión de seguridad.....	95
6.6.2.1.	Clasificación y gestión de información y bienes.....	96
6.6.2.2.	Operaciones de gestión.....	96
6.6.2.3.	Tratamiento de los soportes y seguridad.....	96
6.6.2.3.1	Planificación del sistema	97
6.6.2.3.2	Reportes de incidencias y respuesta.....	97
6.6.2.3.3	Procedimientos operacionales y responsabilidades	97
6.6.2.4.	Gestión del sistema de acceso	97
6.6.2.4.1	AC General	97
6.6.2.4.2	Generación del certificado.....	98
6.6.2.4.3	Gestión de la revocación.....	98
6.6.2.4.4	Estado de la revocación	98
6.6.2.5.	Gestión del ciclo de vida del hardware criptográfico	98
6.7.	CONTROLES DE SEGURIDAD DE RED	99
6.8.	CONTROLES DE INGENIERÍA DE MÓDULOS CRIPTOGRÁFICOS.....	99
6.9.	FUENTES DE TIEMPO	100
6.10.	CAMBIO DE ESTADO DE UN DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA (QSCD).....	100
7.	PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS	101
7.1.	PERFIL DE CERTIFICADO.....	101
7.1.1.	Número de versión.....	101
7.1.2.	Extensiones del certificado	101
7.1.3.	Identificadores de objeto (OID) de los algoritmos	101
7.1.4.	Formato de Nombres.....	102
7.1.5.	Restricción de los nombres	102
7.1.6.	Identificador de objeto (OID) de los tipos de certificados.....	102
7.2.	PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS	102
7.2.1.	Número de versión.....	102
7.2.2.	Perfil de OCSP	102
8.	AUDITORÍA DE CONFORMIDAD	103
8.1.	FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD	103
8.2.	IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR	103
8.3.	RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA.....	103
8.4.	LISTADO DE ELEMENTOS OBJETO DE AUDITORÍA	103
8.5.	ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD	104
8.6.	TRATAMIENTO DE LOS INFORMES DE AUDITORÍA	105

9.	REQUISITOS COMERCIALES Y LEGALES	106
9.1.	TARIFAS.....	106
9.1.1.	<i>Tarifa de emisión o renovación de certificados</i>	<i>106</i>
9.1.2.	<i>Tarifa de acceso a certificados</i>	<i>106</i>
9.1.3.	<i>Tarifa de acceso a información de estado de certificado</i>	<i>106</i>
9.1.4.	<i>Tarifas de otros servicios</i>	<i>106</i>
9.1.5.	<i>Política de reintegro.....</i>	<i>106</i>
9.2.	CAPACIDAD FINANCIERA.....	106
9.2.1.	<i>Cobertura de seguro</i>	<i>107</i>
9.2.2.	<i>Otros activos.....</i>	<i>107</i>
9.2.3.	<i>Cobertura de seguro para suscriptores y terceros que confían en certificados.....</i>	<i>107</i>
9.3.	CONFIDENCIALIDAD	107
9.3.1.	<i>Informaciones confidenciales</i>	<i>107</i>
9.3.2.	<i>Informaciones no confidenciales</i>	<i>108</i>
9.3.3.	<i>Divulgación de información de suspensión y revocación.....</i>	<i>108</i>
9.3.4.	<i>Divulgación legal de información</i>	<i>108</i>
9.3.5.	<i>Divulgación de información por petición de su titular.....</i>	<i>109</i>
9.3.6.	<i>Otras circunstancias de divulgación de información</i>	<i>109</i>
9.4.	PROTECCIÓN DE DATOS PERSONALES	109
9.5.	DERECHOS DE PROPIEDAD INTELECTUAL	110
9.5.1.	<i>Propiedad de los certificados e información de revocación.....</i>	<i>110</i>
9.5.2.	<i>Propiedad de la Declaración de Prácticas de Certificación.....</i>	<i>110</i>
9.5.3.	<i>Propiedad de la información relativa a nombres.....</i>	<i>110</i>
9.5.4.	<i>Propiedad de claves.....</i>	<i>111</i>
9.6.	OBLIGACIONES Y RESPONSABILIDAD CIVIL	111
9.6.1.	<i>Obligaciones de NOVOSIT.....</i>	<i>111</i>
9.6.2.	<i>Garantías ofrecidas a suscriptores y terceros que confían en certificados.....</i>	<i>112</i>
9.6.3.	<i>Rechazo de otras garantías</i>	<i>114</i>
9.6.4.	<i>Limitación de responsabilidades.....</i>	<i>114</i>
9.6.5.	<i>Cláusulas de indemnidad.....</i>	<i>114</i>
9.6.5.1.	<i>Cláusula de indemnidad de suscriptor</i>	<i>114</i>
9.6.5.2.	<i>Cláusula de indemnidad de tercero que confía en el certificado</i>	<i>115</i>
9.6.6.	<i>Caso fortuito y fuerza mayor</i>	<i>115</i>
9.6.7.	<i>Ley aplicable</i>	<i>115</i>
9.6.8.	<i>Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación.....</i>	<i>115</i>
9.6.9.	<i>Cláusula de jurisdicción competente</i>	<i>116</i>
9.6.10.	<i>Resolución de conflictos.....</i>	<i>116</i>
10.	ANEXO I - ACRÓNIMOS	117

1. Introducción

1.1. Presentación

Este documento declara las prácticas de certificación de firma electrónica Novosit, S.R.L, en adelante NOVOSIT.

Los certificados que se emiten son los siguientes:

De Persona Física

- Certificado cualificado de Persona Física en p12
- Certificado cualificado de Persona Física en QSCD centralizado
- Certificado cualificado de Persona Física para Procedimientos Tributarios en p12
- Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD

De Persona Física Representante

- Certificado cualificado de Persona Física Representante en p12
- Certificado cualificado de Persona Física Representante en QSCD centralizado

De Sello de Empresa

- Certificado cualificado de Sello Electrónico en p12
- Certificado cualificado de Sello Electrónico en QSCD centralizado

De Sello de Tiempo

- Certificado de Sello Electrónico en QSCD centralizado

1.2. Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación de NOVOSIT".

1.2.1. Identificadores de certificados

NOVOSIT ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

Número OID	Tipo de certificados
	Persona Física
1.3.6.1.4.1.56483.1.1.1	<i>Certificado cualificado de Persona Física en p12</i>
1.3.6.1.4.1.56483.1.1.2	<i>Certificado cualificado de Persona Física en QSCD centralizado</i>
1.3.6.1.4.1.56483.1.4.1	<i>Certificado cualificado de Persona Física para Procedimientos Tributarios en p12</i>
1.3.6.1.4.1.56483.1.4.2	<i>Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD</i>
	Representante de entidad
1.3.6.1.4.1.56483.1.2.1	<i>de Persona Física de firma Representante en p12</i>
1.3.6.1.4.1.56483.1.2.2	<i>de Persona Física de firma Representante en QSCD centralizado</i>
	Sello Electrónico
1.3.6.1.4.1.56483.1.3.1	<i>de Sello Electrónico en p12</i>
1.3.6.1.4.1.56483.1.3.2	<i>de Sello Electrónico en QSCD centralizado</i>
	Sello de tiempo
1.3.6.1.4.1.56483.2.10	<i>de Sello de Tiempo Electrónico</i>

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas de Certificación.

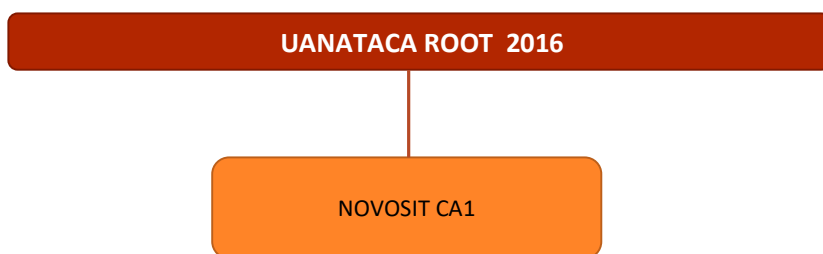
1.3. Participantes en los servicios de certificación

1.3.1. Entidad de Certificación Acreditada

La Entidad de Certificación acreditada es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Autoridad de Certificación, o presta otros servicios relacionados con la firma electrónica.

NOVOSIT es una Entidad de Certificación acreditada o Prestador de Servicios de Confianza, que actúa de acuerdo con lo dispuesto en la Ley nº 126-02 sobre comercio electrónico, documentos y firmas digitales, su reglamento general de aplicación, junto con las normas complementarias aplicables, así como las normas técnicas del ETSI aplicables a la expedición y gestión de certificados, principalmente EN 319 411-1 y EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, NOVOSIT ha establecido una jerarquía de Autoridades de certificación:



1.3.1.1. UANATACA ROOT 2016

Se trata de la Entidad de Certificación raíz de la jerarquía que emite certificados a otras Autoridades de certificación, y cuyo certificado de clave público ha sido auto firmado.

Datos de identificación:

CN:	UANATACA ROOT 2016
Huella digital:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce 23 0d 74 66 ad
Válido desde:	Viernes, 11 de marzo de 2016
Válido hasta:	Lunes, 11 de marzo de 2041
Longitud de clave RSA:	4.096 bits

1.3.1.2. NOVOSIT CA 1

Se trata de la Entidad de Certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la UANATACA ROOT 2016.

Datos de identificación:

CN:	NOVOSIT CA 1
Huella digital:	07bd82b88674979abfb78069a2dfd149e371d945
Válido desde:	viernes, 16 de octubre de 2020 10:43:03
Válido hasta:	domingo, 16 de octubre de 2033
Longitud de clave RSA:	4.096 bits

1.3.2. Unidad de Registro

Una Unidad de Registro de NOVOSIT es la entidad encargada de:

- Tramitar las solicitudes de certificados.
- Identificar al solicitante y comprobar que cumple con los requisitos necesarios para la solicitud de los certificados.
- Validar las circunstancias personales de la persona que constará como firmante del certificado.
- Gestionar la generación de claves y la emisión del certificado
- Hacer entrega del certificado al suscriptor o de los medios para su generación.
- Custodiar la documentación relativa a la identificación y registro de los firmantes y/o suscriptores y gestión del ciclo de vida de los certificados.

Podrán actuar como Unidad de Registro de NOVOSIT:

- Cualquier entidad que conste acreditada como Unidad de Registro y previa autorización por NOVOSIT.
- NOVOSIT directamente como Unidad de Registro acreditada.

Serán formalizadas contractualmente las relaciones entre ella misma y cada una de las entidades que actúen como Unidad de Registro de NOVOSIT.

La entidad que actúe como Unidad de Registro de NOVOSIT podrá autorizar a una o varias personas como Operador de la RA para operar con el sistema de emisión de certificados de NOVOSIT en nombre de la Unidad de Registro.

La Unidad de Registro podrá delegar las funciones de identificación de los suscriptores y/o firmantes, previo acuerdo de colaboración en el que se acepte la delegación de

estas funciones. NOVOSIT deberá autorizar de manera expresa dicho acuerdo de colaboración.

También podrán ser Unidades de Registro sujetas a esta Declaración de Prácticas de Certificación, las unidades designadas para esta función por los suscriptores de los certificados, como un departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

1.3.3. Entidades finales

Las entidades finales son las personas u organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de autenticación y firma electrónica.

Serán entidades finales de los servicios de certificación de NOVOSIT las siguientes:

1. Suscriptores del servicio de certificación
2. Firmantes
3. Partes usuarias

1.3.3.1. Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- Las empresas, entidades, corporaciones u organizaciones que los adquieren a NOVOSIT (directamente o a través de un tercero) para su uso en su ámbito corporativo empresarial, corporativo u organizativo, y se encuentran identificados en los certificados.
- Las personas físicas que adquieren los certificados para sí mismas, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio – certificados de sello electrónico –, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado.

El suscriptor del servicio electrónico de confianza es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación privada, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas aplicables a la expedición de certificados electrónicos, en especial ETSI EN 319 411.

1.3.3.2. Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma electrónica para autenticación y/o firma avanzada o cualificada, de acuerdo con los perfiles de este documento; siendo típicamente los empleados, representantes legales o voluntarios, así como otras personas vinculadas a los suscriptores; incluyendo las personas al servicio de las Administraciones Públicas, en los certificados de empleado público.

De acuerdo con la norma por la que se establece la equivalencia regulatoria del sistema dominicano de infraestructuras de claves públicas y de confianza con los marcos regulatorios internacionales de servicios de confianza, la equivalencia de las firmas es la siguiente:

- Se consideran equivalentes la firma digital y la firma electrónica avanzada.
- Se consideran equivalentes la firma digital segura y la firma electrónica cualificada.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre, apellidos, dirección y número de identificación inequívoco, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante no puede ser recuperada o deducida por el prestador de servicios electrónicos de confianza, por lo que las personas físicas identificadas en los correspondientes certificados son las únicas responsables de su protección y deberían considerar las implicaciones de perder una clave privada.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la autenticación, también se emplea el término más genérico de “persona física

identificada en el certificado”, siempre con pleno respeto al cumplimiento de la regulación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.3.3. Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas electrónicas y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones disponibles en la página web de la Autoridad de Certificación.

1.3.4. Proveedor de Servicios de Infraestructura de Clave Pública

NOVOSIT y UANATACA, S.A. han suscrito un contrato de prestación de servicios de tecnología en el que UANATACA, S.A., proveerá la infraestructura de clave pública (PKI) que sustenta el servicio de certificación de NOVOSIT. Así mismo UANATACA, S.A., pone a disposición de NOVOSIT el personal técnico necesario para correcto desempeño de las funciones fiables propias de un Entidad de Certificación acreditada.

Dicho lo cual, UANATACA, S.A., se configura como el proveedor de servicios de Infraestructura para servicios de certificación, provee sus servicios tecnológicos a NOVOSIT para que éste pueda llevar a cabo los servicios inherentes a un Entidad de Certificación acreditada, garantizando en todo momento la continuidad de los servicios en las condiciones y bajo los requisitos exigidos por la normativa.

La PKI de UANATACA, S.A., se somete a auditorías anuales para la evaluación de la conformidad de prestadores cualificados de servicios de confianza de acuerdo con la normativa aplicable, bajo las normas:

- a. ISO/IEC 17065:2012
- b. ETSI EN 319 403
- c. ETSI EN 319 421
- d. ETSI EN 319 401
- e. ETSI EN 319 411-2

- f. ETSI EN 319 411-1

Asimismo, la PKI de UANATACA se somete a auditorías anuales bajo los estándares de seguridad:

- a. ISO 9001:2015
- b. ISO/IEC 27001:2014

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1. Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, disponibles en el web <https://novofirma.com/>

1.4.1.1. Certificado cualificado de persona física en P12

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.1.1. Es un certificado cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de persona física se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Los certificados se pueden utilizar en aplicaciones como las que se indican a continuación:

- a) Autenticación en sistemas de control de acceso.
- b) Firma de correo electrónico seguro.
- c) Otras aplicaciones de firma electrónica, de acuerdo con lo que acuerden las partes o con las normas jurídicas aplicables en cada caso.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación)
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c. Key Encipherment

1.4.1.2. Certificado cualificado de persona física en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.1.2. Es un certificado cualificado que se emite para la firma electrónica y autenticación, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de persona física emitido en QSCD remoto de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de confianza, y permite la generación de la “firma electrónica cualificada”;

por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación)
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c. Key Encipherment

1.4.1.3. Certificado cualificado de persona física representante en p12

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.2.1. Es un certificado cualificado que se emite para la firma electrónica avanzada, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de representante se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo “O” (Organization), y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Por otra parte, los certificados de representante emitido en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

- a) Firma de correo electrónico seguro.

- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

1.4.1.4. Certificado cualificado persona física representante en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.2.2. Es un certificado cualificado que se emite para la firma electrónica cualificada, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de representante emitido en QSCD, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento entre el firmante y una entidad, empresa u organización descrita en el campo “O” (Organization), y permite la generación de la “firma electrónica cualificada”, por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

- a) Firma de correo electrónico seguro.
- b) Otras aplicaciones de firma electrónica.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)

1.4.1.5. Certificado cualificado de persona física para Procedimientos Tributarios en P12

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.4.1. Es un certificado cualificado que se emite para la firma electrónica avanzada y autenticación, de acuerdo con la política de certificación QCP-n con el OID 0.4.0.194112.1.0. Este certificado de persona física para Procedimientos Tributarios se emite en archivo p12, de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica avanzada basada en certificado electrónico cualificado”.

Este certificado solo podrá ser utilizado para procedimientos tributarios del suscriptor identificado en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.6. Certificado cualificado de persona física para Procedimientos Tributarios en QSCD

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.4.2. Es un certificado cualificado que se emite para la firma electrónica cualificada y autenticación, de acuerdo con la política de certificación QCP-n-qscd con el OID 0.4.0.194112.1.2. Este certificado de persona física para Procedimientos Tributarios se emite en QSCD de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Garantiza la identidad del firmante y su vinculación con el suscriptor del servicio electrónico de confianza, y permite la generación de la “firma electrónica cualificada”; por lo cual se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Este certificado solo podrá ser utilizado para procedimientos tributarios del suscriptor identificado en el certificado y por tanto cualquier otra operación no autorizada tendrá la consideración de usos indebidos.

La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación).
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica).
- c. Key Encipherment.

1.4.1.7. Certificado cualificado de Sello Electrónico en p12

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.3.1, y es un certificado que se emite de acuerdo con la política de certificación QCP-I con el OID 0.4.0.194112.1.1. Los certificados de sello electrónico son certificados cualificados emitidos de acuerdo con lo

dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Los certificados de persona física emitidos en software no garantizan su funcionamiento con dispositivos cualificados de creación de firma.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación)
- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c. Key Encipherment

1.4.1.8. Certificado cualificado de Sello Electrónico en QSCD centralizado

Este certificado dispone del OID 1.3.6.1.4.1.56483.1.3.2, y es un certificado cualificado que se emite de acuerdo con la política de certificación QCP-I-qscd con el OID 0.4.0.194112.1.3. Los certificados de sello electrónico son cualificados y emitidos de acuerdo con lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Funciona con dispositivos cualificados de creación de firma, dando cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia EN 319 411-2.

Estos certificados garantizan la identidad de la entidad suscriptora vinculada, y en su caso la del responsable de gestionar el sello identificado en el mismo. La información de usos en el perfil de certificado indica lo siguiente:

El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

- a. Firma digital (Digital Signature, para realizar la función de autenticación)

- b. Compromiso con el contenido (Content commitment, para realizar la función de firma electrónica)
- c. Key Encipherment

1.4.1.9. Certificado de sello de tiempo electrónico

Este certificado dispone del OID 1.3.6.1.4.1.56483.2.10, y se emite de acuerdo con la política de certificación NCP+ con el OID 0.4.0.2042.1.2.

Los certificados de sello de tiempo electrónico se tratan de certificados emitidos para la operación de autoridades de sellado de tiempo y hora, para la firma de los sellos de tiempo que estas producen.

Estos certificados permiten la firma de los sellos de tiempo que se emiten, desde el momento que hayan obtenido un certificado de sello de tiempo electrónico válido y mientras éste se encuentre vigente.

La sincronización de los tiempos se realiza mediante un servicio servidor de tiempo NTP Stratum 3.

Este servidor, un Meinberg Lantime M300/GPS, con oscilador TCXO de alta estabilidad, receptor GPS, formado por una tarjeta GPS interna para sincronizarse simultáneamente con los satélites con los que tiene visibilidad en cada momento (entre 3 y 8), y protección anti-rayos.

1.4.2. Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la regulación aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, disponibles en la web de NOVOSIT.

El empleo de los certificados digitales en operaciones que contravienen esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos con las Unidades de Registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a NOVOSIT, en función de la legislación vigente, de responsabilidades que provengan del uso indebido de los certificados ya sea realizado el uso por el firmante o por tercero.

NOVOSIT no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, y por ello no es posible emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta Declaración de Prácticas de Certificación, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las Unidades de Registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5. Administración de la política

1.5.1. Organización que administra el documento

Novosit SRL

Calle Pedro A. Bobea no. 1, Edif. Curvo 495, Bella Vista,
Santo Domingo, República Dominicana
809-482-6287- ext. 102
info@novofirma.com

1.5.2. Datos de contacto de la organización

Novosit SRL

Calle Pedro A. Bobea no. 1, Edif. Curvo 495, Bella Vista,
Santo Domingo, República Dominicana
809-482-6287- ext. 102
info@novofirma.com

1.5.3. Procedimientos de gestión del documento

El sistema documental y de organización de NOVOSIT garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

2. Publicación de información y depósito de certificados

2.1. Depósito(s) de certificados

Se dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema se realizarán sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en esta Declaración de Prácticas de Certificación.

2.2. Publicación de información del prestador de servicios de certificación

Serán publicadas las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona física identificada en el certificado.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación.
- Los textos de divulgación (Policy Disclosure Statements - PDS), como mínimo en español.

2.3. Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.9 y 4.9.10 de esta Declaración de Prácticas de Certificación.

2.4. Control de acceso

NOVOSIT no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

Se emplean sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación

3.1. Registro inicial

3.1.1. Tipos de nombres

Todos los certificados contienen un nombre distintivo (DN o *distinguished name*) conforme al estándar X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1. Certificado cualificado de Persona Física ciudadano en p12

Country Name	País de residencia o nacionalidad del firmante.
Organization Name	Organización a la que pertenece el firmante. • PF en calidad de ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Se especificará el nombre de la Empresa o Entidad. En caso de que el suscriptor sea un autónomo, se puede incluir el nombre comercial de su establecimiento. • PF Colegiada: Se especificará el nombre del Colegio Oficial.
Organizational Unit Name	Departamento o Área dentro de la Organización: • PF en calidad de ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la organización. • PF Colegiada: Se especificará en general “Colegiado”
Organization Identifier	• PF ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: “VATES-Q0000000”). • PF Colegiada: Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: “VATES-Q0000000”).
Title	Título o especialidad del firmante • PF en calidad de ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Se especificará el nombre del título o puesto que la persona ocupa en la Empresa o Entidad. • PF Colegiada: Se especificará el título o especialidad del firmante.
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 (“IDCES-12345678Z”)
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE

Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante y/o de la organización
----------------	--

3.1.1.2. Certificado cualificado de Persona Física en QSCD centralizado

Country Name	País de residencia o nacionalidad del firmante.
Organization Name	Organización a la que pertenece el firmante. • PF en calidad de ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Se especificará el nombre de la Empresa o Entidad. En caso de que el suscriptor sea un autónomo, se puede incluir el nombre comercial de su establecimiento. • PF Colegiada: Se especificará el nombre del Colegio Oficial.
Organizational Unit Name	Departamento o Área dentro de la Organización: • PF en calidad de ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Se especificará el Departamento al que pertenece el firmante o el tipo de vinculación con la organización. • PF Colegiada: Se especificará en general "Colegiado"
Organization Identifier	• PF ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q00000000"). • PF Colegiada: Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q00000000").
Title	Título o especialidad del firmante • PF en calidad de ciudadano: Este campo no tendrá que rellenarse. • PF perteneciente a Empresa o Entidad: Se especificará el nombre del título o puesto que la persona ocupa en la Empresa o Entidad. • PF Colegiada: Se especificará el título o especialidad del firmante.
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante y/o de la organización

3.1.1.3. Certificado cualificado de Persona Física Representante en p12

Country Name	País de residencia o nacionalidad del representante
Organization Name	Organización de la que el firmante es representante
Organizational Unit Name	Departamento al que pertenece representante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")
Title	Nombre del título o puesto del Representante
Surname	Apellidos del representante (como consta en el documento oficial)
Given Name	Nombre del representante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización

3.1.1.4. Certificado cualificado de firma de Persona Física Representante en QSCD centralizado

Country Name	País de residencia o nacionalidad del representante
Organization Name	Organización de la que el firmante es representante
Organizational Unit Name	Departamento al que pertenece representante
Organization Identifier	Número oficial de identificación de la persona jurídica a la que está vinculado el firmante, en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")
Title	Nombre del título o puesto del Representante
Surname	Apellidos del representante (como consta en el documento oficial)
Given Name	Nombre del representante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCES-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL REPRESENTANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la organización

3.1.1.5. Certificado cualificado de Persona Física para Procedimientos Tributarios en p12

Country Name	Estado
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")

Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante

3.1.1.6. Certificado cualificado de Persona Física para Procedimientos Tributarios en QSCD

Country Name	Estado
Surname	Apellidos del firmante (como consta en el documento oficial)
Given Name	Nombre del firmante (como consta en el documento oficial)
Serial Number	Número de documento oficial codificado acorde a ETSI EN 319 412-1 ("IDCDO-12345678Z")
Common Name	NOMBRE Y APELLIDOS DEL FIRMANTE
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad del firmante

3.1.1.7. Certificado cualificado de Sello Electrónico en p12

Country Name	País donde la entidad está registrada
Organization Name	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)
Organizational Unit Name	Denominación de la unidad
Organization Identifier	Número oficial de identificación de la Persona Jurídica a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")
Surname	Apellidos del responsable del sello (como consta en el documento oficial)
Given Name	Nombre del responsable del sello (como consta en el documento oficial)
Serial Number	Número oficial de identificación de la Persona Jurídica
Common Name	Nombre descriptivo del creador del sello. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la entidad

3.1.1.8. Certificado cualificado de Sello Electrónico en QSCD Centralizado

Country Name	País donde la entidad está registrada
Organization Name	Denominación (nombre "oficial" de la persona jurídica) del creador del sello (Empresa, Organización, Entidad)
Organizational Unit Name	Denominación de la unidad
Organization Identifier	Número oficial de identificación de la Persona Jurídica a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: "VATES-Q0000000J")
Surname	Apellidos del responsable del sello (como consta en el

	documento oficial)
Given Name	Nombre del responsable del sello (como consta en el documento oficial)
Serial Number	Número oficial de identificación de la Persona Jurídica
Common Name	Nombre descriptivo del creador del sello. Asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades.
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la entidad

3.1.1.9. Certificado de sello de tiempo electrónico

Country Name	País donde la entidad está registrada
Organization Name (O)	Denominación (nombre “oficial” de la persona jurídica) del creador del sello de tiempo (Empresa, Organización, Entidad)
Locality Name (L)	Nombre de la localidad
Organization Identifier	Número oficial de identificación de la Persona Jurídica a la que está vinculado el sello en formato ETSI EN 319412-1 (Ejemplo: VATES-Q0000000J)
Common Name	Nombre descriptivo del creador del sello de tiempo
Organizational Unit (OU)	Denominación de la unidad / encargado
Address	Se especificará la Dirección, Código Postal y Ciudad/Municipio/Localidad de la entidad

3.1.2. Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.2.1. Emisión de certificados del set de pruebas y certificados de pruebas en general

En el caso que los datos indicados en el DN o Subject fueran ficticios (ej. “Test Organization”, “Test Nombre”, “Apellido1”) o se indique expresamente palabras que denoten su invalidez (ej. “TEST”, “PRUEBA” o “INVALIDO”), se considerará al certificado sin validez legal y por lo tanto sin responsabilidad alguna sobre NOVOSIT. Estos certificados se emiten para realizar pruebas técnicas de interoperabilidad y permitir al ente regulador su evaluación.

3.1.3. Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad, empresa u organización, ni a un firmante. Así mismo, en ningún caso se emiten certificados anónimos.

3.1.4. Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” o “estado” será el del suscriptor del certificado.

Los certificados cuyos suscriptores sean personas jurídicas, entidades u organismos de la administración pública, muestran la relación entre estas y una persona física, con independencia de la nacionalidad de la persona física.

En el campo “número de serie” se incluye el número del documento oficial de identidad, de acuerdo con un documento de identidad reconocido en derecho.

3.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del documento oficial de identidad, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación u otro identificador legalmente válido de la persona física.
- Número de Identificación u otro identificador legalmente válido del suscriptor.
- Tipo de certificado (OID de identificador de política de certificación).
- Soporte del certificado (software o QSCD Centralizado)

Como excepción esta DPC permite emitir un certificado cuando coincidan el número de identificación del suscriptor, el número de identificación del firmante, Tipo de certificado, Soporte del certificado, con un certificado activo, siempre que exista algún

elemento diferenciador entre ambos, en los campos cargo (Title) y/o departamento (Organizational Unit).

3.1.6. Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

No existirá ninguna obligación de determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de electrónicos de confianza se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte en el documento contractual que formaliza el servicio.

3.2. Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre NOVOSIT y el suscriptor, previa verificación de la existencia del suscriptor a través de los procedimientos de reconocimiento establecidos y mediante la comprobación de su documento oficial de identidad o las escrituras correspondientes, al igual que los poderes de actuación de la persona que presente como representante si fuese el caso. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de personas naturales identificadas en certificados cuyo suscriptor sea una persona jurídica, sus identidades se validarán mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una certificación de los datos necesarios, y la remitirá a NOVOSIT, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

3.2.1. Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello, o por el firmante, en certificados de firma.

3.2.2. Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas físicas con capacidad de actuar en nombre de las personas jurídicas o entidades sin personalidad jurídica, públicas o privadas, que sean suscriptoras de certificados, podrán actuar como representantes de estas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la organización de la que se trate, que exige su reconocimiento por NOVOSIT, la cual se realizará mediante el siguiente procedimiento:

1. El representante del suscriptor deberá acreditar su identidad por uno de los siguientes métodos:

- (i) Identificándose presencialmente ante un operador o persona autorizada de una Unidad de Registro de NOVOSIT:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
 - Acreditando el carácter y facultades que alegue poseer.
 - (ii) Identificándose electrónicamente a través del sistema de video identificación remota de NOVOSIT:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
 - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.
 - Acreditando el carácter y facultades que alegue poseer.
2. El representante proporcionará la siguiente información y sus correspondientes soportes acreditativos:
- Sus datos de identificación, como representante:
 - Nombre y apellidos
 - Lugar y fecha de nacimiento
 - Documento de identidad reconocido en derecho para la identificación del representante,
 - Domicilio o dirección del firmante.
 - Los datos de identificación del suscriptor al que representa:
 - Denominación o razón social.
 - Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
 - Documento de Identificación o documento acreditativo de la identificación fiscal de la entidad.

- Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.
 - Los datos relativos a la representación o la capacidad de actuación que ostenta:
 - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin) si resulta aplicable.
 - El ámbito y los límites, en su caso, de la representación o de la capacidad de actuación:
 - TOTAL. Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.
 - PARCIAL. Representación o capacidad parcial. Esta comprobación se podrá realizar mediante copia auténtica electrónica de la escritura notarial de apoderamiento, en los términos de la normativa notarial.
3. El operador o personal autorizado de la Unidad de Registro de NOVOSIT comprobará la identidad del representante actuando del siguiente modo:
- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
 - Documento de identidad aportado.
 - Documentación que acredite su representación.
 - Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de NOVOSIT mediante:
 - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.

Comentado [ABD1]: Describir mínimamente el sistema acreditado de NOVOSIT.

En amarillo encontrarán un ejemplo de descripción de un sistema de video identificación basado en biometría facial e inteligencia artificial.

- Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.
- Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
- Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.
- Documentación que acredite su representación.

4. Alternativamente, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar al operador o personal autorizado de la Unidad de Registro por correo postal certificado, en cuyo caso los pasos 3 y 4 anteriores no serán necesarios.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre NOVOSIT y el suscriptor, debidamente representado.

3.2.3. Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1. En los certificados

La identidad de las personas naturales firmantes identificados en los certificados, se valida a través de uno de los siguientes métodos:

- (i) Identificándose presencialmente ante un operador o persona autorizada de una Unidad de Registro de NOVOSIT:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.

- (ii) Identificándose electrónicamente a través del sistema de video identificación remota de NOVOSIT:
 - Mostrando su Documento de Identidad, pasaporte u otro medio idóneo reconocido en derecho para la identificación del representante.
 - Proveyendo prueba de vida mediante el uso de medios técnicos de captación de imágenes y vídeo utilizando algoritmos de criptografía biométrica facial e inteligencia artificial para el cotejo inequívoco de la identidad del solicitante y la verificación de la prueba de vida de éste, así como de la autenticidad del documento de identidad exhibido.

Comentado [ABD2]: Describir mínimamente el sistema acreditado de NOVOSIT.

En amarillo encontrarán un ejemplo de descripción de un sistema de video identificación basado en biometría facial e inteligencia artificial.

La información de identificación de las personas naturales identificadas en los certificados (i) cuyo suscriptor sea una entidad con o sin personalidad jurídica o (ii) ya constase la misma en virtud de una relación previa, la información podrá ser validada comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, o bien con la documentación que esta haya suministrado sobre la persona natural que identifica como firmante, asegurando la corrección de la información a certificar.

3.2.3.2. Validación de la Identidad

El operador o personal autorizado de la Entidad de Registro de UANATACA comprobará la identidad de la persona natural identificada en la solicitud del certificado, actuando del siguiente modo:

- Cuando la identificación se haya realizado presencialmente, a través de la revisión de:
 - Documento de identidad aportado.
- Cuando la identificación se haya realizado a través del método de identificación electrónica a través de video identificación de UANATACA mediante:
 - Revisión de los vídeos e imágenes captadas del documento de identificación aportado y del propio solicitante.
 - Revisión de la prueba de vida del solicitante, a través de los resultados facilitados por el sistema de video identificación remota.

Comentado [ABD3]: Describir mínimamente el sistema acreditado de NOVOSIT.

En amarillo encontrarán un ejemplo de descripción de un sistema de video identificación basado en biometría facial e inteligencia artificial.

- Revisión del cotejo producido por el sistema de video identificación remota de la fotografía del documento de identidad con las imágenes y vídeo obtenido durante el registro del solicitante.
- Revisión producida por el sistema de video identificación remota, a través de inteligencia artificial para la detección de documentos de identidad falsos.

Para la solicitud de los certificados cuyo suscriptor sea una persona jurídica no se requiere identificación expresa, debido a la relación ya acreditada entre la persona natural y entidad, empresa u organización de derecho público o privado a la que está vinculada. Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona natural identificada en el certificado mediante su presencia física o siguiendo el procedimiento de video identificación remota establecido por UANATACA.

Durante este trámite se confirma rigurosamente la identidad de la persona física identificada en el certificado. Por este motivo, en todos los casos en que se expide un certificado se acredita ante un operador de registro la identidad de la persona física firmante.

La Unidad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de los datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

3.2.3.3. Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización...) de cada una de las personas públicas y privadas a las que están vinculadas.

3.2.4. Información de suscriptor no verificada

Bajo ningún concepto se incluirá información de suscriptor no verificada en los certificados.

3.2.5. Autenticación de la identidad de una RA y sus operadores

Para la constitución de una nueva Unidad de Registro, NOVOSIT realiza las verificaciones necesarias para confirmar la existencia de la entidad u organización de la que se trate, así como la debida acreditación ante el Organismo Supervisor Nacional. Para ello, podrá utilizar exhibición de documentos o utilizar sus propias fuentes de información.

Igualmente, de forma directa o a través de su Unidad de Registro, se verifica y valida la identidad de los operadores de las Unidades de Registro, para lo cual estas últimas envían a NOVOSIT la documentación referente a la identificación del nuevo operador, juntamente con su autorización para actuar como tal.

Debe asegurarse que los operadores de la Unidad de Registro reciben la formación suficiente para el desarrollo de sus funciones, lo cual verifica con la evaluación correspondiente. Dicha formación y evaluación puede ser ejecutada por la Unidad de Registro previamente autorizada por NOVOSIT.

Para la prestación de los servicios debe asegurarse de que los operadores de Unidad de Registro acceden al sistema mediante autenticación fuerte con certificado digital.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, el operador o personal autorizado de la Unidad de Registro comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son:

- El uso del código “CRE” o “ERC” relativo al certificado anterior, o de otros métodos de autenticación personal, que consiste en información que sólo conoce la persona física identificada en el certificado, y que le permite renovar de forma automática su certificado, siempre que no se haya superado el plazo máximo legalmente establecido.
- El empleo del certificado vigente para su renovación y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2. Identificación y autenticación de la solicitud de renovación

Antes de renovar un certificado, el operador o personal autorizado de la Unidad de Registro comprobará que la información empleada en su día para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúa siendo válida, en cuyo caso se aplicará lo dispuesto en la sección anterior.

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado.

- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una identificación completa, de acuerdo con lo establecido en la sección 3.2.

3.4. Identificación y autenticación de la solicitud de revocación, suspensión o reactivación

NOVOSIT o un operador o personal autorizado de la Unidad de Registro autentica las peticiones e informes relativos a la revocación, suspensión o reactivación de un certificado, comprobando que provienen de una persona autorizada.

La identificación de los suscriptores y/o firmantes en el proceso de revocación, suspensión o reactivación de certificados podrá ser realizada por:

- El suscriptor y/o firmante:
 - Identificándose y autenticándose mediante el uso del Código de Revocación (ERC o ERC) a través de la página web de NOVOSIT en horario 24 horas al día 7 días a la semana.
 - Otros medios de comunicación, como el teléfono, correo electrónico, etc. cuando existan garantías razonables de la identidad del solicitante de la suspensión o revocación, a juicio de NOVOSIT y/o Unidades de Registro.
- Las Unidades de Registro deberán identificar al firmante ante una petición de revocación, suspensión o reactivación según los propios medios que considere necesarios.

Cuando en horario de oficina el suscriptor desee iniciar una petición de revocación y existan dudas para su identificación, su certificado pasa a estado de suspensión.

4. Requisitos de operación del ciclo de vida de los certificados

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

El solicitante del certificado sea persona física o jurídica, debe firmar un contrato de prestación de servicios de certificación con NOVOSIT.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados ya sea en el mismo contrato, en un documento específico de hoja de solicitud de certificados o ante la Unidad de Registro.

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre propio en el caso de certificados para persona física, o bien en nombre del suscriptor en el caso de que el suscriptor sea la por entidad, empresa u organización de derecho público o privado.

4.1.2. Procedimiento de alta y responsabilidades

NOVOSIT recibe solicitudes de certificados, realizadas por personas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un formulario en formato papel o electrónico, de manera individual o por lotes, o mediante la conexión con bases de datos externas, o a través de una capa de *Web Services* cuyo destinatario es NOVOSIT. En el caso de certificados cuyo suscriptor sea una entidad, empresa u organización de derecho público o privado que actúe como una Unidad de Registro de NOVOSIT, podrá gestionar directamente las solicitudes accediendo a los sistemas informáticos de NOVOSIT y generar los certificados correspondientes para la propia entidad, empresa u organización o para sus miembros.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

4.2. Procesamiento de la solicitud de certificación

4.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, NOVOSIT se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, se verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2.

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante el plazo de 20 años desde la expiración del certificado, incluso en caso de pérdida anticipada de vigencia por revocación.

NOVOSIT, como entidad de certificación, lleva un registro de todos los certificados emitidos, que se encontrará a disposición del público, debiendo indicar las fechas de emisión, expiración y registros de suspensión, revocación o reactivación de estos. En este sentido, los registros de certificados expedidos por una entidad de certificación deben ser conservados por 40 años desde la fecha de revocación o expiración del certificado.

4.2.2. Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la solicitud queda aprobada, y como consecuencia se aprueba la solicitud del certificado y se procede a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Autoridad de Certificación, de las Unidades de Registro o de los suscriptores, deberá denegarse la petición, o detener su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que observadas las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, la solicitud quedará denegada definitivamente.

En cualquier caso, debe realizarse la notificación correspondiente sobre la aprobación o denegación de la solicitud.

NOVOSIT podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.2.3. Plazo para resolver la solicitud

Las solicitudes de certificados serán atendidas por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3. Emisión del certificado

4.3.1. Acciones de la CA durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, NOVOSIT:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo de las claves por parte del usuario, no pudiendo la propia NOVOSIT o sus Unidades de Registro deducirlas o utilizarlas en ningún modo.

4.3.2. Notificación de la emisión al suscriptor

Deberá ser notificada la emisión del certificado al suscriptor y/o a la persona física identificada en el certificado y el método de generación/descarga.

4.4. Entrega y aceptación del certificado

4.4.1. Responsabilidades de la CA

Durante este proceso, el operador o personal autorizado de la Unidad de Registro debe realizar las siguientes actuaciones:

- Acreditar definitivamente la identidad de la persona física identificada en el certificado, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Disponer del Contrato de Prestación de Servicios de Confianza debidamente firmado por el Suscriptor.
- Entregar la hoja de entrega y aceptación del certificado a la persona física identificada en el certificado con los siguientes contenidos mínimos:
 - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades.
 - Información acerca del certificado.
 - Reconocimiento, por parte del firmante, de recibir el certificado y/o los mecanismos para su generación/descarga y la aceptación de los citados elementos.
 - Régimen de obligaciones del firmante.
 - Responsabilidad del firmante.
 - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
 - La fecha del acto de entrega y aceptación.

Toda esta información podrá incluirse en el propio Contrato de Prestación de Servicios de Confianza. Dicho lo cual, cuando se produzca la firma del Contrato de Prestación de Servicios de Confianza por el Suscriptor, se entenderá perfeccionada la entrega y aceptación del certificado.

- Obtener la firma de la persona identificada en el certificado.

Las Unidades de Registro son las encargadas de realizar estos procesos, debiendo registrar documentalmente los anteriores actos y conservar los citados documentos originales (hojas de entrega y aceptación), remitiendo copia electrónica a NOVOSIT, así como los originales cuando se precise acceso a los mismos.

4.4.2. Conducta que constituye aceptación del certificado

Cuando se haga entrega de la hoja de aceptación, la aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación.

Cuando la generación y entrega del certificado se lleve a cabo a través del procedimiento automatizado definido por NOVOSIT, la aceptación del certificado por la persona física identificada en el mismo se produce mediante la firma del contrato de Prestación de Servicios de Confianza utilizando el propio certificado.

4.4.3. Publicación del certificado

Deberá publicarse el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que NOVOSIT disponga de la autorización de la persona física identificada en el certificado.

4.4.4. Notificación de la emisión a terceros

NOVOSIT no realiza ninguna notificación de la emisión a terceras entidades.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por el firmante

El firmante queda obligado a:

- Facilitar a NOVOSIT información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección **¡Error! No se encuentra el origen de la referencia..**
- Cuando el certificado funcione juntamente con un Dispositivo Cualificado de Creación de Firma (DCCF), reconocer su capacidad de producción de firmas electrónicas digitales; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6, 6.2.
- Comunicar a NOVOSIT , Unidades de Registro y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida, el robo o el compromiso potencial de su clave privada.
 - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.

El firmante queda obligado a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.

- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2. Uso por el suscriptor

4.5.2.1. Obligaciones del suscriptor del certificado

El suscriptor queda obligado contractualmente a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4. **¡Error! No se encuentra el origen de la referencia..**
- Comunicar a NOVOSIT, Unidades de Registro y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
 - La pérdida, el robo o el compromiso potencial de su clave privada.
 - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
 - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
 - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de estas.

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación.

4.5.2.2. Responsabilidad civil del suscriptor de certificado

NOVOSIT obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3. Uso por el tercero que confía en certificados

4.5.3.1. Obligaciones del tercero que confía en certificados

Se informa al tercero que confía en certificados de que el mismo debe asumir las siguientes obligaciones:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.

- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo cualificado de creación de firma tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación.

4.5.3.2. Responsabilidad civil del tercero que confía en certificados

NOVOSIT informa al tercero que confía en certificados de que el mismo debe asumir las siguientes responsabilidades:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6. Renovación de certificados

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 4.7.

4.7. Renovación de claves y certificados

4.7.1. Causas de renovación de claves y certificados

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

Se consideran al menos dos posibilidades para la renovación de certificados:

- Proceso de renovación presencial, que se efectuará del mismo modo que la emisión de un nuevo certificado.
- Proceso de renovación online (a través de internet), que se detalla a continuación.

4.7.2. Procedimiento de renovación online de certificados

4.7.2.1. Circunstancias para la renovación online

Solamente se podrá proceder a la renovación online del certificado si se cumplen las condiciones siguientes:

- La Unidad de Registro y/o NOVOSIT dispone del servicio de renovación online.
- El certificado con el que se firma la renovación esté vigente, es decir, no haya caducado, no esté revocado ni suspendido.

4.7.2.2. Quién puede solicitar la renovación online de un certificado

Cualquier firmante podrá pedir la renovación online de su certificado si se cumplen las circunstancias descritas en el punto anterior.

El firmante podrá formalizar su solicitud accediendo al servicio de renovación online de certificados en la página web de NOVOSIT.

4.7.2.3. Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, NOVOSIT aprobará la solicitud de renovación del certificado y proceder a su emisión y entrega, siendo notificada al solicitante la aprobación o denegación de la solicitud.

NOVOSIT podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes.

4.7.2.4. Tramitación de las peticiones de renovación online

La solicitud de una renovación del certificado se realizará de acuerdo con lo siguiente:

- Cuando el certificado digital de un usuario esté próximo a caducar, podrá enviarse una o más notificaciones distribuidas en el tiempo, invitándole a su renovación.
- El firmante se conectará al servicio de renovación de la página web de NOVOSIT y procederá a la solicitud de renovación.
- El firmante firmará la renovación de su certificado válido.
- Se procederá a la generación del nuevo par de claves y generación e importación del certificado, respetando los siguientes condicionantes:
 - Protege la confidencialidad e integridad de los datos de registro de que dispone.
 - Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
 - Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
 - Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
 - Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.

- Indica la fecha y la hora en que se expidió un certificado.
- Garantiza el control exclusivo del usuario sobre sus propias claves, no pudiendo la propia NOVOSIT o sus Unidades de Registro deducirlas o utilizarlas.

4.7.2.5. Notificación de la emisión del certificado renovado

NOVOSIT notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.7.2.6. Conducta que constituye aceptación del certificado renovado

El certificado se considerará aceptado al firmar electrónicamente la renovación.

4.7.2.7. Publicación del certificado renovado

NOVOSIT publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.2.8. Notificación de la emisión a terceros

NOVOSIT no realiza notificación alguna de la emisión a terceras entidades.

4.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4, 4.2, 4.3 y 4.4.

4.9. Revocación, suspensión o reactivación de certificados

La revocación de un certificado supone la pérdida de validez definitiva del mismo, y es irreversible.

La suspensión (o revocación temporal) de un certificado supone la pérdida de validez temporal del mismo, y es reversible. Sólo los certificados de entidad final podrán ser suspendidos.

La reactivación de un certificado supone su paso de estado suspendido a estado activo.

4.9.1. Causas de revocación de certificados

Un certificado será revocado cuando concurra alguna de las siguientes causas:

- 1) Circunstancias que afectan a la información contenida en el certificado:
 - a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
 - b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
 - c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
- 2) Circunstancias que afectan a la seguridad de la clave o del certificado:
 - a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

- b) Infracción, por NOVOSIT de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.
 - c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
 - d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
 - e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
- 3) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:
- a) Finalización de la relación jurídica de prestación de servicios entre el prestador y el suscriptor.
 - b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.
 - c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud de este.
 - d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.
 - e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.
 - f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.
 - g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.
- 4) Otras circunstancias:
- a) La terminación del servicio de certificación de la Entidad de Certificación de NOVOSIT.
 - b) El uso del certificado que sea dañino y continuado para NOVOSIT. En este caso, se considera que un uso es dañino en función de los siguientes criterios:
 - o La naturaleza y el número de quejas recibidas.

- La identidad de las entidades que presentan las quejas.
- La legislación relevante vigente en cada momento.
- La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.9.2. Causas de suspensión de un certificado

Los certificados pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona física identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la persona física identificada en el certificado.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, NOVOSIT tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.9.3. Causas de reactivación de un certificado

Los certificados pueden ser reactivados a partir de las siguientes causas:

- Cuando el certificado se encuentre en un estado de suspendido.
- Cuando así sea solicitado por el suscriptor o la persona física identificada en el certificado.

4.9.4. Quién puede solicitar la revocación, suspensión o reactivación

Pueden solicitar la revocación, suspensión o reactivación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio responsable del servicio de certificación.

4.9.5. Procedimientos de solicitud de revocación, suspensión o reactivación

La entidad que precise revocación, suspensión o reactivación un certificado puede solicitarlo directamente a NOVOSIT o a la Unidad de Registro del suscriptor o realizarlo él mismo a través del servicio online disponible en la página web de NOVOSIT. La solicitud de revocación, suspensión o reactivación deberá incorporar la siguiente información:

- Fecha de solicitud de la revocación, suspensión o reactivación.
- Identidad del suscriptor.
- Nombre y título de la persona que pide la revocación, suspensión o reactivación.
- Información de contacto de la persona que pide la revocación, suspensión o reactivación.
- Razón detallada para la petición de revocación.

La solicitud debe ser autenticada, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación, suspensión o reactivación.

El servicio de revocación, suspensión o reactivación se encuentra en la página web de NOVOSIT en la dirección: <https://novofirma.com/>.

En caso de que el destinatario de una solicitud de revocación, suspensión o reactivación por parte de una persona física identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a NOVOSIT.

La solicitud de revocación, suspensión o reactivación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado.

Tanto el servicio de gestión de revocación, suspensión o reactivación como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencia y el plan de continuidad de negocio de NOVOSIT.

4.9.6. Plazo temporal de solicitud de revocación, suspensión o reactivación

Las solicitudes de revocación, suspensión o reactivación se remitirán de forma inmediata en cuanto se tenga conocimiento.

4.9.7. Plazo temporal de procesamiento de la solicitud de revocación, suspensión o reactivación

La revocación, suspensión o reactivación se producirá inmediatamente cuando sea recibida. Si se realiza a través de un operador, se ejecutará dentro del horario ordinario de operación o en su caso de la Unidad de Registro. Si se realiza a través del servicio online, será inmediata.

4.9.8. Obligación de consulta de información de revocación o suspensión de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación de NOVOSIT.

Las Listas de Revocación de Certificados se publican en el Depósito de la Autoridad de Certificación, así como en las siguientes direcciones web, indicadas dentro de los certificados:

- <http://crl1.uanataca.com/public/pki/crl/novosit.crl>
- <http://crl2.uanataca.com/public/pki/crl/novosit.crl>

El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

- <http://ocsp1.uanataca.com/public/pki/ocsp/>
- <http://ocsp2.uanataca.com/public/pki/ocsp/>

4.9.9. Frecuencia de emisión de listas de revocación de certificados (LRCs)

NOVOSIT emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

4.9.10. Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

4.9.11. Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de NOVOSIT, que se encuentra disponible las 24 horas de los 7 días de la semana en el web: <https://novofirma.com/>.

Para comprobar la última CRL emitida en cada CA se debe descargar:

- *Autoridad de Certificación Raíz (UANATACA ROOT 2016):*
 - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
 - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl
- *Autoridad de Certificación Intermedia de Novosit (NOVOSIT CA1):*
 - <http://crl1.uanataca.com/public/pki/crl/Novosit.crl>
 - <http://crl2.uanataca.com/public/pki/crl/Novosit.crl>

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de NOVOSIT, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

Se suministrará información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

4.9.12. Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

4.9.13. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de NOVOSIT, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.14. Período máximo de un certificado digital en estado suspendido

El plazo máximo de un certificado digital en estado suspendido es indefinido hasta su caducidad.

4.10. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

NOVOSIT puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.11. Depósito y recuperación de claves

4.11.1. Política y prácticas de depósito y recuperación de claves

NOVOSIT no presta servicios de depósito y recuperación de claves.

4.11.2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5. Controles de seguridad física, de gestión y de operaciones

NOVOSIT y UANATACA, S.A., han suscrito un contrato de prestación de servicios de tecnología en el que UANATACA, S.A., provee la infraestructura de clave pública (PKI) que sustenta el servicio de confianza de NOVOSIT.

En el presente apartado, se describen los sistemas de seguridad con que cuenta el Centro de Procesamiento de Datos donde se aloja el sistema que contiene la infraestructura de clave pública PKI del servicio de la Entidad de Certificación de Información de NOVOSIT.

La Infraestructura de Clave Pública PKI de la Entidad de Certificación de NOVOSIT, está ubicada en un rack / armario aislado físicamente del resto de infraestructuras hospedados en el Centro de Procesamiento de Datos del proveedor de servicios de tecnología ADAM Ecotech (en lo sucesivo ADAM).

El Centro de Procesamiento de Datos de producción y contingencia se encuentra ubicado en una instalación segura dentro del edificio de ADAM. El mismo ha sido diseñado con tecnología TIER 3, el cual permite tener un esquema redundante para garantizar la continuidad en la operación y disponibilidad de los sistemas y cuenta con los controles de seguridad que se definen a continuación.

5.1. Controles de seguridad física

Se han establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de confianza.

En concreto, la política de seguridad aplicable a los servicios electrónicos de confianza establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de confianza, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1. Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

NOVOSIT dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

5.1.2. Acceso físico

Se dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al Rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

5.1.3. Electricidad y aire acondicionado

Las instalaciones disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4. Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5. Prevención y protección de incendios

Las instalaciones y activos de se encuentran dotados de sistemas automáticos de detección y extinción de incendios.

5.1.6. Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7. Tratamiento de residuos

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

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8. Copia de respaldo fuera de las instalaciones

Se realiza el uso de un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones.

5.2. Controles de procedimientos

Se garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de NOVOSIT ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1. Funciones fiables

NOVOSIT ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas:** Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación.
- **Administrador de CA:** Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de copia de respaldo y mantenimiento de la AC.
- **Operador de Registro:** Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor y emitir certificados digitales.
- **Oficial de Revocación:** Persona responsable de realizar los cambios en el estado de un certificado, principalmente proceder con la suspensión y revocación de estos.
- **Responsable de Seguridad:** Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de NOVOSIT. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, implementa criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

5.2.2. Número de personas por tarea

Deben garantizarse al menos dos personas para realizar las tareas relativas a la generación, recuperación y back-up de la clave privada de las Autoridades de Certificación. Igual criterio se aplica para la ejecución de tareas de emisión y activación de certificados y claves privadas de las Autoridades de Certificación, y en general cualquier manipulación del dispositivo de custodia de las claves de la Entidad de Certificación raíz e intermedias.

5.2.3. Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.2.4. Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Las tareas propias del rol de Auditor serán incompatibles con la operación y administración de sistemas, y en general aquellas dedicadas a la prestación directa de los servicios electrónicos de confianza.
- Emisión y revocación de certificados, serán tareas incompatibles con la Administración y operación de los sistemas.
- La administración y operación de los sistemas y las CAs, serán incompatibles entre sí.

5.2.5. Sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada.
- Componente/módulo de gestión de la Autoridad de Registro.
- Componente/módulo de gestión de solicitudes.
- Componente/módulo de gestión de claves (HSM).
- Componente/módulo de bases de datos.
- Componente/módulo de gestión de CRL.
- Componente/módulo de gestión de la Autoridad de Validación (servicios de OCSP).

5.3. Controles de personal

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

NOVOSIT se asegura de que el personal de registro es confiable para realizar las tareas de registro. El Administrador de Registro recibe formación para realizar las tareas de validación de las peticiones.

En general, retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones. Además de ello, no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

En todo caso, las Unidades de Registro podrán establecer procesos de comprobación de antecedentes diferentes, siempre preservando las políticas de NOVOSIT, siendo responsables por la actuación de las personas que autoricen en sus operaciones.

5.3.2. Procedimientos de investigación de historial

NOVOSIT antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

NOVOSIT obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

5.3.3. Requisitos de formación

Debe otorgarse al personal una formación respecto de los puestos fiables y de la gestión de estos, hasta que se obtenga la cualificación necesaria, manteniendo el archivo de la formación impartida.

Los programas de formación son revisados periódicamente, y son actualizados para su mejor y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4. Requisitos y frecuencia de actualización formativa

Se actualiza la formación del personal atendiendo a sus necesidades y con la frecuencia temporal suficiente para que los mismos puedan cumplir sus funciones y obligaciones de forma competente y satisfactoria, principalmente cuando se realicen modificaciones sustanciales de las tareas establecidas de certificación.

5.3.5. Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6. Sanciones para acciones no autorizadas

NOVOSIT dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7. Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por NOVOSIT. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la Declaración de Prácticas de Certificación, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la Entidad de Certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a NOVOSIT.

5.3.8. Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

Se produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.

- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Autoridad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Además de lo anterior, se realiza una revisión de los logs cuando existe una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

Se mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3. Período de conservación de registros de auditoría

NOVOSIT almacena la información de los logs durante un periodo de entre 1 y 20 años, en función del tipo de información registrada.

5.4.4. Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante su almacenamiento en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5. Procedimientos de copia de respaldo

Se dispone de un procedimiento adecuado de copia de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de seguridad de los logs.

Sumado a lo anterior, tiene implementado un procedimiento de copia de seguridad seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6. Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8. Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de NOVOSIT.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5. Archivos de informaciones

NOVOSIT garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1. Tipos de registros archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por NOVOSIT (o por las Unidades de Registro):

- Todos los datos de auditoría de sistema.
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

NOVOSIT y/o las Unidades de Registro según corresponda, serán responsables del correcto archivo de todo este material.

5.5.2. Período de conservación de registros

NOVOSIT archiva los registros especificados anteriormente durante al menos 20 años, o el período que establezca la legislación vigente.

En particular, los registros de certificados revocados estarán accesibles para su libre consulta durante al menos 20 años o el periodo que establezca la legislación vigente desde su cambio de estado.

5.5.3. Protección del archivo

Se protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable, asegurando la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.5.4. Procedimientos de copia de respaldo

Se dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

Respecto de los documentos electrónicos, se realizan copias de respaldo incrementales diarias de todos los documentos y copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, NOVOSIT (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Autoridad de Certificación.

5.5.5. Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP.

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

Se dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Se dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. Además, proporciona la información y medios de verificación al auditor.

5.6. Renovación de claves

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN. El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

Alternativamente, en el caso de Autoridades de Certificación subordinadas, se podrá optar por la renovación del certificado con o sin cambio de claves, no resultando aplicable el procedimiento antes descrito.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Procedimientos de gestión de incidencias y compromisos

NOVOSIT ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones, asegurando los servicios críticos de revocación y publicación del estado de los certificados.

5.7.2. Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de NOVOSIT.

5.7.3. Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de NOVOSIT se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.7.4. Continuidad del negocio después de un desastre

Deberán restablecerse los servicios críticos (suspensión y revocación, y publicación de información de estado de certificados) de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

Se dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.8. Terminación del servicio

NOVOSIT asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación. En este sentido, NOVOSIT garantiza un mantenimiento continuo de los registros definidos en el apartado 5.5.1, por el tiempo establecido en el apartado 5.5.2 de esta Declaración de Prácticas de Certificación.

No obstante lo anterior, si procede NOVOSIT ejecutará todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta Declaración de Prácticas de Certificación o la previsión legal que corresponda.

Antes de terminar sus servicios, se ha realizado el desarrollo de un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la EC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Comunicará al Organismo Supervisor Nacional que tenga atribuidas las competencias correspondientes, con una antelación mínima de 90 días, el

cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.

- Comunicará, también al Organismo Supervisor Nacional que tenga atribuidas las competencias correspondientes, la apertura de cualquier proceso concursal que se siga contra NOVOSIT, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6. Controles de seguridad técnica

Se emplean sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

El par de claves de la Autoridad de certificación intermedia “NOVOSIT CA1”, es creado por la entidad de certificación raíz “UANATACA ROOT 2016” de acuerdo con los procedimientos de ceremonia de UANATACA, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por NOVOSIT.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140-2 level 3 y Common Criteria EAL4+.

UANATACA ROOT 2016	4.096 bits	25 años
NOVOSIT CA1	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	Hasta 2 años

Los documentos Texto de Divulgación (PKI Disclosure Statement-PDS) de todos los perfiles de certificados digitales indicados en el presente documento, se encuentran accesibles bajo el enlace: <https://www.novofirma.com/public/pds/>.

6.1.1.1. Generación del par de claves del firmante

Las claves del firmante pueden ser generadas por él mismo mediante dispositivos hardware y/o software autorizados por NOVOSIT. Las claves no generadas en un QSCD, serán generadas por el firmante. NOVOSIT nunca genera claves fuera de un QSCD para ser enviadas al firmante.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2. Envío de la clave privada al firmante

En certificados en dispositivo cualificado de creación de firma la clave privada se genera y se almacena debidamente protegida en el interior de dicho dispositivo cualificado.

En certificados en archivo p12 la clave privada del firmante se genera y se almacena en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que en este caso no existe envío de clave privada, garantizando el control exclusivo de la clave por parte del usuario

En certificados en QSCD Centralizado la clave privada del firmante se genera en un área privada del firmante en un HSM remoto. Las credenciales de acceso a la clave privada son introducidas por el propio firmante, no siendo almacenadas ni susceptibles de capacidad de deducción o interceptación por el sistema de generación y custodia remota. La clave privada no se envía al firmante, es decir, nunca abandona el entorno de seguridad que garantiza el control exclusivo de la clave privada por parte del firmante.

6.1.3. Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios electrónicos de confianza es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado.

6.1.4. Distribución de la clave pública del prestador de servicios de certificación

Las claves son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las Autoridades de Certificación Raíz y Subordinadas estarán a disposición de los usuarios en la página web de NOVOSIT.

6.1.5. Tamaños de claves

- La longitud de las claves de la Autoridad de Certificación raíz es de 4096 bits.
- La longitud de las claves de las Autoridad de Certificación subordinada es de 4096 bits.
- La longitud de las claves de los Certificados de Entidad final es de 2048 bits.

6.1.6. Generación de parámetros de clave pública

La clave pública de la Autoridades de Certificación raíz, subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

6.1.7. Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9. Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final son exclusivamente para la firma digital, el no repudio y cifrado de datos.

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de NOVOSIT y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2. Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta Declaración de Prácticas de Certificación, en concreto existe una política de **3 de 6** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3. Depósito de la clave privada

No se realiza el almacenamiento de copias utilizables por medios propios de las claves privadas de los firmantes.

6.2.4. Copia de respaldo de la clave privada

Se realiza copia de seguridad o respaldo de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. Tanto la

generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Claves generadas en dispositivo software: NOVOSIT no puede realizar backups de las claves, ya que no dispone de acceso a las mismas. El firmante sí que puede realizar una copia de seguridad.

Claves generadas en QSCD: no se puede realizar backups de las claves, ya que no es posible su exportación del QSCD.

Claves generadas en QSCD Centralizado: Sólo es posible realizar backups de un blob cifrado con la clave Security World del HSM utilizado, siendo imposible su descifrado sin el uso de las credenciales que sólo el titular del certificado conoce.

6.2.5. Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

Solo en caso de certificados de cifrado, el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso también se guardará copia de la clave privada asociada al certificado de cifrado.

NOVOSIT no genera ni archiva claves de certificados, emitidas en software.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción.

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción.

6.2.7. Método de activación de la clave privada

La clave privada se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n (3 de 6).

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.8. Método de desactivación de la clave privada

Para la desactivación de la clave privada se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

6.2.9. Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de NOVOSIT. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en software se podrán destruir mediante el borrado de estas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware y podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de NOVOSIT.

6.2.10. Clasificación de módulos criptográficos

Ver la sección 6.2.1

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

Las claves públicas son archivadas de forma rutinaria, atendiendo a lo establecido en la sección 5.5 del presente documento.

6.3.2. Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción y en caso de existir, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, se generan de forma segura los datos de activación.

6.4.2. Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, están protegidos por los poseedores de

las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una o varias contraseñas lo más completas y complejas posible. El firmante debe recordar dicha(s) contraseña(s).

6.5. Controles de seguridad informática

Se emplean sistemas fiables para ofrecer sus servicios de certificación. Para atender a este fin, se han realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, NOVOSIT aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de tráfico de red.

6.5.1. Requisitos técnicos específicos de seguridad informática

Cada servidor de incluye las siguientes funcionalidades:

- Control de acceso a los servicios de las Autoridades de Certificación subordinadas y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.

- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor, de las Autoridades de Certificación subordinadas y datos de auditoría.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de las Autoridades de Certificación subordinadas.
- Mecanismos de recuperación de claves y del sistema de las Autoridades de Certificación subordinadas.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de Entidad de Certificación y de registro empleadas por NOVOSIT son fiables.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por NOVOSIT de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2. Controles de gestión de seguridad

NOVOSIT desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

NOVOSIT exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de confianza.

6.6.2.1. Clasificación y gestión de información y bienes

NOVOSIT mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO y CONFIDENCIAL.

6.6.2.2. Operaciones de gestión

Se dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad se desarrolla en detalle el proceso de gestión de incidencias.

NOVOSIT tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.3. Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.6.2.3.1 Planificación del sistema

El departamento de Sistemas mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.6.2.3.2 Reportes de incidencias y respuesta

Se dispone de un procedimiento para realizar el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.3.3 Procedimientos operacionales y responsabilidades

Se definen las actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4. Gestión del sistema de acceso

Deben realizarse todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

6.6.2.4.1 AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- NOVOSIT dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- NOVOSIT dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.

- El personal es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.6.2.4.2 Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada.

6.6.2.4.3 Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador.

6.6.2.4.4 Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5. Gestión del ciclo de vida del hardware criptográfico

NOVOSIT se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

Se registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

Además de ello, se realizan test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema, así como sus modificaciones y actualizaciones son documentadas y controladas.

Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7. Controles de seguridad de red

NOVOSIT protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8. Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas son realizadas en módulos con las certificaciones FIPS 140-2 nivel 3.

6.9. Fuentes de Tiempo

Se dispone de un procedimiento de sincronización de sincronización de tiempo coordinado vía NTP, que realiza el acceso a dos servicios independientes entre sí:

La primera sincronización es con un servicio basado en antenas y receptores GPS que permite un nivel de confianza de STRATUM 1 (con dos sistemas en alta disponibilidad).

La segunda dispone de una sincronización complementaria, vía NTP, con el Real Instituto y Observatorio de la Armada (ROA).

6.10. Cambio de estado de un Dispositivo Seguro de Creación de Firma (QSCD)

En el caso de modificación del estado de la certificación de los dispositivos cualificados de creación de firma (QSCD), se procederá de la siguiente manera:

1. Se dispone de una lista de varios QSCD certificados, así como una estrecha relación con proveedores de dichos dispositivos, con el fin de garantizar alternativas a posibles pérdidas de estado de certificación de dispositivos QSCD. En el supuesto de finalización del periodo de validez o pérdida de la certificación, no se utilizarán dichos QSCD para la emisión de nuevos certificados digitales, bien sea en nuevas emisiones.
2. En el supuesto de finalización del periodo de validez o pérdida de la certificación, no se utilizarán dichos QSCD para la emisión de nuevos certificados digitales, bien sea en nuevas emisiones como eventualmente en posibles renovaciones.
3. Procederá de inmediato a cambiar a de dispositivos QSCD con certificación válida.
4. En el supuesto caso que un dispositivo QSCD haya demostrado no haberlo sido nunca, por falsificación o cualquier otro tipo de fraude, se procederá de inmediato a comunicárselo a sus clientes y al ente regulador, revocar los certificados digitales emitidos en estos dispositivos y reemplazarlos emitiéndolos en QSCD válidos.

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen con el estándar X.509 versión 3 y el RFC 3739 y los diferentes perfiles descritos en la norma EN 319 412.

La documentación relativa a los perfiles de la norma EN 319 412 puede solicitarse a NOVOSIT.

7.1.1. Número de versión

NOVOSIT emite certificados X.509 Versión 3.

7.1.2. Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que están a disposición de los usuarios bajo petición a través de los medios de contactos indicados en la página web de NOVOSIT: <https://novofirma.com/>

De esta forma se permite mantener unas versiones más estables de la Declaración de Prácticas de Certificación y desligarlos de los frecuentes ajustes en los perfiles.

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5. Restricción 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 los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1

7.2. Perfil de la lista de revocación de certificados

7.2.1. Número de versión

Las CRL emitidas por NOVOSIT son de la versión 2.

7.2.2. Perfil de OCSP

Según el estándar IETF RFC 6960.

8. Auditoría de conformidad

NOVOSIT ha comunicado el inicio de su actividad como prestador de servicios de certificación al Organismo Supervisor Nacional y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1. Frecuencia de la auditoría de conformidad

NOVOSIT lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2. Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3. Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con NOVOSIT.

8.4. Listado de elementos objeto de auditoría

La auditoría verifica respecto a NOVOSIT:

- a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.

- b) Que la entidad cumple con los requerimientos de la Declaración de Prácticas de Certificación y otra documentación vinculada con la emisión de los distintos certificados digitales.
- c) Que la Declaración de Prácticas de Certificación y demás documentación jurídica vinculada, se ajusta a lo acordado por NOVOSIT y con lo establecido en la normativa vigente.
- d) Que la entidad gestiona de forma adecuada sus sistemas de información.

En particular, los elementos objeto de auditoría serán los siguientes:

- a) Procesos de las Autoridades de Certificación, Unidades de Registro y elementos relacionados.
- b) Sistemas de información.
- c) Protección del centro de proceso de datos.
- d) Documentos.

8.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solventen dichas deficiencias.

Si NOVOSIT es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad de NOVOSIT que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Entidad de Certificación y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Certificación.
- Otras acciones complementarias que resulten necesarias.

8.6. Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de NOVOSIT en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

NOVOSIT puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2. Tarifa de acceso a certificados

NOVOSIT no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3. Tarifa de acceso a información de estado de certificado

NOVOSIT no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4. Tarifas de otros servicios

Sin estipulación.

9.1.5. Política de reintegro

Sin estipulación.

9.2. Capacidad financiera

NOVOSIT dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401, en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1. Cobertura de seguro

NOVOSIT dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo con la normativa vigente aplicable.

9.2.2. Otros activos

Sin estipulación.

9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados

La Entidad de Certificación contará con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los requisitos establecidos por INDOTEL.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por NOVOSIT:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Autoridad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2. Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Autoridad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como 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 del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

NOVOSIT divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

NOVOSIT indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5. Divulgación de información por petición de su titular

NOVOSIT incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de datos personales

NOVOSIT garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales, reflejada en la normativa nacional que resulte de aplicación.

En cumplimiento de esta, NOVOSIT ha documentado en su política de protección de datos personales, los procedimientos de seguridad y organizativos con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

Únicamente NOVOSIT goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por NOVOSIT contienen un aviso legal relativo a la propiedad de estos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2. Propiedad de la Declaración de Prácticas de Certificación

Únicamente NOVOSIT goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido (DN) del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.4. Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. Obligaciones de NOVOSIT

NOVOSIT garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la Declaración de Prácticas de Certificación, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

NOVOSIT presta los servicios electrónicos de confianza conforme con esta Declaración de Prácticas de Certificación.

NOVOSIT informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor que incorpora por referencia los textos de divulgación (PDS) de cada uno de los certificados adquiridos.

El documento de texto de divulgación, también denominado PDS¹, cumple el contenido del anexo A de la ETSI EN 319 411-1, documento el cual puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

NOVOSIT vincula a suscriptores, poseedores de claves y terceros que confían en certificados, mediante dicho texto de divulgación o PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

1 “PKI Disclosure Statement”, o declaración de divulgación de PKI aplicable.

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.3, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Autoridad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

NOVOSIT, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

NOVOSIT, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación de este.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

NOVOSIT, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, NOVOSIT garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan.

9.6.3. Rechazo de otras garantías

NOVOSIT rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Limitación de responsabilidades

NOVOSIT limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Entidad de Certificación.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

NOVOSIT incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

NOVOSIT incluye en el texto de divulgación o PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6. Caso fortuito y fuerza mayor

NOVOSIT incluye en el texto de divulgación o PDS, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7. Ley aplicable

NOVOSIT establece, en el contrato de suscriptor y en el texto de divulgación o PDS, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley dominicana.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

NOVOSIT establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes

tras la terminación del servicio y de las condiciones generales de emisión/uso.

- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9. Cláusula de jurisdicción competente

NOVOSIT establece, en el contrato de suscriptor y en el texto de divulgación o PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

NOVOSIT establece, en el contrato de suscriptor, y en el texto de divulgación o PDS, los procedimientos de mediación y resolución de conflictos aplicables.

10. Anexo I - Acrónimos

AC	Autoridad de Certificación
CA	Certification Authority. Autoridad de Certificación
RA	Autoridad de Registro
CP	Certificate Policy
CPS	Certification Practice Statement. Declaración de Prácticas de Certificación
CRL	Certificate Revocation List. Lista de certificados revocados
CSR	Certificate Signing Request. Petición de firma de certificado
DES	Data Encryption Standard. Estándar de cifrado de datos
DN	Distinguished Name. Nombre distintivo dentro del certificado digital
DSA	Digital Signature Algorithm. Estándar de algoritmo de firma
DCCF	Dispositivo Cualificado de Creación de Firma
QSCD	Qualified Signature Creation Device. Dispositivo Cualificado de Creación de Firma
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardization. Organismo Internacional de Estandarización
LDAP	Lightweight Directory Access Protocol. Protocolo de acceso a directorios
OCSP	On-line Certificate Status Protocol. Protocolo de acceso al estado de los certificados
OID	Object Identifier. Identificador de objeto
PA	Policy Authority. Autoridad de Políticas
PC	Política de Certificación
PIN	Personal Identification Number. Número de identificación personal
PKI	Public Key Infrastructure. Infraestructura de clave pública
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	Secure Hash Algorithm. Algoritmo seguro de Hash
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol