


 <b>Indecopi</b> <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	<b>Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ</b>	Rev: 2018
		Aprobado:

**ANEXO XIV: AUDITORIA**  
**LISTA DE VERIFICACIÓN DE AUDITORIA**

 <b>Indecopi</b> <small>INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL</small>	<b>Infraestructura Oficial de Firma Electrónica (IOFE) - PERÚ</b>	Rev: 2018
		Aprobado:

## ENTIDAD DE CERTIFICACIÓN DIGITAL

A continuación, se presentan los requerimientos que el evaluador revisará como parte del proceso de acreditación, respecto de las Entidades de Certificación Digital. En cada caso el auditado deberá indicar si el requerimiento es aplicable al servicio o sistema a evaluar sustentando debidamente cada caso de no aplicabilidad.

El evaluador deberá adjuntar una referencia a la evidencia obtenida respecto del cumplimiento de cada requerimiento y sus complementos conforme se describe en la Guía de Acreditación y sus anexos. En el caso de procedimientos y documentos confidenciales, los nombres y códigos de estos documentos deben ser registrados. En caso de herramientas de software para uso de clientes de la EC, se deben adjuntar como evidencias las imágenes de las pantallas capturadas evidenciando el cumplimiento de los requerimientos solicitados.

En el caso que sea utilizado un certificado digital para efectuar una prueba, el evaluador deberá registrar el certificado, adjuntando a la evidencia la imagen de los detalles del perfil del certificado utilizado en la prueba.

### **Datos que deben ser registrar en el informe de auditoría respecto del alcance de la acreditación:**

- Nombre de la Entidad de Certificación:
- Nombre de la Entidad de Registro vinculada (puede estar en proceso de acreditación o haber logrado ya la acreditación):
- Nombre e identificador de los certificados raíz auditados:
- Nombre e identificador de los certificados de EC subordinada auditados:
- Nombre y ubicación de los centros de datos y centros de operación auditados:
- Incluye servicios CRL:
- Incluye servicios OCSP:
- Certificaciones internacionales:

No	Requerimiento	¿Aplica?	Evidencia	Observaciones
<b>1.2.1 Introducción y alcance del servicio</b>				
1	Introducción			
2	Visión general			
3	Nombre e identificación del documento			
4	Control de versiones			
5	Participantes			
6	Administración de la política			
7	Definiciones y Acrónimos			
8	Publicación y Responsabilidades del Repositorio			
9	Responsabilidades del suscriptor			
10	Responsabilidades de los terceros que confían			
11	Responsabilidades de otros participantes			
12	Entidades de Registro			
<b>1.2.2 Requisitos operacionales del ciclo de vida de los certificados</b>				
13	Certificados digitales			
14	Uso del certificado			
15	Titulares de certificados digitales			
16	Denominación			
17	Validación inicial de identidad			
18	Identificación y Autenticación para solicitudes de re-emisión de claves			

19	Identificación y Autenticación para solicitudes de revocación			
20	Solicitud del certificado			
21	Procesamiento de la solicitud del certificado			
22	Contrato del suscriptor			
23	Emisión del certificado			
24	Método para probar la posesión de la clave privada			
25	Aceptación del certificado			
26	Uso del par de claves y del certificado			
27	Re-emisión del certificado			
28	Suspensión del certificado			
29	Revocación del certificado			
30	Servicios de estado del certificado			
31	Finalización de la suscripción			
32	Almacenamiento y recuperación de la clave			
<b>1.2.3 Seguridad en la Gestión del ciclo de vida de las claves de los Certificados de la Entidad de Certificación</b>				
33	Generación de las claves de la EC			
34	Almacenamiento, respaldo y recuperación de la clave privada de la			

	EC			
35	Distribución de la clave pública			
36	Uso de la clave de la EC			
37	Archivo y destrucción de las claves.			
38	Compromiso de la Clave de la EC y cambio de clave			
<b>1.2.4 Ciclo de vida del módulo criptográfico de la EC</b>				
39	Gestión del ciclo de vida del módulo criptográfico			
<b>1.2.5 Repositorio de claves privadas (si fuera aplicable)</b>				
40	Almacenamiento de claves privadas de la EC			
<b>1.2.6 Seguridad en la Gestión del ciclo de vida de las claves de los Certificados del suscriptor</b>				
41	Servicios de generación y distribución de claves privadas (si se brinda el servicio)			
42	Periodos operacionales del certificado y periodo de uso de las claves			
<b>1.2.7 Requerimientos para la gestión de claves por parte del suscriptor</b>				
43	Requerimientos al suscriptor			
<b>1.2.8 Gestión de certificados del suscriptor</b>				
44	Solicitudes de certificados			
45	Re-emisión del certificado			
46	Emisión del certificado			
47	Distribución del			

**Indecopi**

INSTITUTO NACIONAL  
DE DEFENSA DE LA  
COMPETENCIA Y DE LA  
PROTECCIÓN DE LA  
PROPIEDAD INTELECTUAL

**Infraestructura Oficial de Firma  
Electrónica (IOFE) - PERÚ**

Rev: 2018

Aprobado:

	certificado			
48	Revocación del certificado			
49	Suspensión del certificado (si es brindado el servicio)			
50	Validación del certificado			
<b>1.2.9 Gestión de certificados de EC Subordinadas y certificaciones cruzadas</b>				
51	Protección del ciclo de vida de EC subordinadas			
52	Certificación cruzada			
<b>1.2.10 Controles de seguridad</b>				
53	Organización de la seguridad de la información			
54	Política de seguridad de la información			
55	Planificación			
56	Gestión de riesgos			
57	Documentación			
58	Seguridad en el trato con terceros			
59	Clasificación y gestión de activos			
60	Seguridad del personal			
61	Seguridad física y del entorno			
62	Gestión de operaciones			
63	Manejo de medios y seguridad			
64	Planificación del sistema			
65	Reporte y respuesta a incidentes			

66	Seguridad en redes			
67	Monitoreo			
68	Intercambio de datos y software			
69	Gestión de accesos a los sistemas			
70	Sistemas operativos			
71	Desarrollo y mantenimiento de sistemas confiables			
72	Control de cambios			
73	Gestión de Continuidad del Negocio			
<b>1.2.11 Compromiso de los servicios de la EC (Raíz e intermedias)</b>				
74	Recuperación ante compromiso de las claves			
75	Notificación			
76	Interrupción de operaciones			
77	Mecanismos de verificación para terceros que confían			
<b>1.2.12 Fin de operaciones de la organización que administra la EC</b>				
78	Preparación antes del término			
79	Capacidad financiera			
80	Revocación del certificado de la EC			
81	Notificación			
<b>1.2.13 Registros de información concerniente a la operación de los servicios de certificación digital</b>				
82	Eventos registrados			
83	Protección de los registros			

84	Archivo de registros			
85	Eventos significativos			
86	Notificación de eventos			
87	Evidencias legales			
88	Archivo luego de expiración de la EC			
89	Privacidad			
90	Gestión de la clave de la EC			
<b>1.2.14 Auditoría</b>				
91	Conformidad legal			
92	Conformidad de la Política de seguridad			
93	Auditoría de registros			
94	Auditoría del archivo			
95	Auditoría de los procedimientos y controles			
96	Auditor			
<b>1.2.15 Aspectos legales de la operación de la EC</b>				
97	Tarifas			
98	Políticas de reembolso			
99	Responsabilidad financiera			
100	Información confidencial			
101	Información privada			
102	Información no privada			
103	Derechos de Propiedad intelectual			
104	Representaciones y garantías			
105	Excepciones de responsabilidad de garantías			
106	Notificaciones y			



**Indecopi**INSTITUTO NACIONAL  
DE DEFENSA DE LA  
COMPETENCIA Y DE LA  
PROTECCIÓN DE LA  
PROPIEDAD INTELECTUAL**Infraestructura Oficial de Firma  
Electrónica (IOFE) - PERÚ**

Rev: 2018

Aprobado:

	comunicaciones entre participantes			
107	Correcciones o enmiendas			
108	Procedimiento de resolución de disputas			
109	Conformidad con la Ley aplicable			
110	Cumplimiento de la Ley aplicable			
111	Limitaciones de responsabilidad			
112	Indemnizaciones			
113	Vigencia y conclusión			
114	Provisiones misceláneas			
115	Otras provisiones			
<b>1.2.16 Registro de tiempo</b>				
116	Fuente de tiempo confiable			
<b>1.2.17 Identificador único de certificados</b>				
117	Generación del OID			
<b>1.2.18 Perfiles de los certificados, CRL y OCSP</b>				
118	Perfil del certificado			
119	Perfil CRL			
120	Perfil OCSP			