

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
	Área Responsable	Cargo Responsable	Fecha de Creación
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

POLÍTICA DE CERTIFICADOS

CLASE 2

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
	Área Responsable	Cargo Responsable	Fecha de Creación
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

OBJETIVO DE POLITICAS

Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.

ALCANCE

Certificados Digitales Clase 2 para Personas Físicas con Vínculo Institucional.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

IDENTIFICACIÓN DE POLÍTICAS

La forma de identificar distintos tipos de Certificados Digitales es a través de identificadores de objeto (*OID*). Un *OID* permite a las aplicaciones distinguir claramente la Política de Certificados que aplica a un determinado Certificado Digital y/o un atributo que se presenta dentro del Certificado Digital.

El identificador de políticas está compuesto por una serie de números, separados entre sí por puntos, y con un significado definido de cada uno de ellos.

La siguiente estructura muestra la nomenclatura de los *OID* de la Cámara de Comercio y Producción de Santo Domingo.

- (1) - iso
- (3) - org
- (6) - dod
- (1) - internet
- (4) - private
- (1) - enterprise
- (26236) - Identifica a la Entidad de Certificación, es decir, a la Cámara de Comercio y Producción de Santo Domingo.
- (r) - Identifica la Autoridad de Certificación (Offline CA) con la que se emite el Certificado Raíz de la Entidad de Certificación.
- (s) - Identifica la Autoridad de Certificación Subrogada (Online Sub-CA) con la que se hizo la emisión del Certificado Digital.
- (c) - Identifica la Clase a la que corresponde el Certificado Digital (1, 2, 3, 4).
- (t) - Identifica el tipo de suscriptor (Personal, Empresarial, Gubernamental, EIF o SSL).

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

El siguiente cuadro muestra las diferentes variables respecto a los Certificados Digitales emitidos por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo.

Nombre Abreviado	Nomenclatura <i>OID</i>				Descripción
	(r) CA	(s) Sub-CA	(c) Clase	(t) Tipo	
ccpsd_ca	1				Certificado Raíz de la Entidad de Certificación Cámara de Comercio y Producción de Santo Domingo.
ccpsd_subca_id	1	1			Certificado Raíz de la Entidad de Certificación Subrogada de la Cámara de Comercio y Producción de Santo Domingo. El mismo está destinado a la emisión de Certificados Digitales para suscriptores individuales, empresariales, gubernamentales y Entidades de Intermediación Financiera.
ccpsd_subca_id_class1	1	1	1		Identifica la Política de Certificados para Certificados Digitales de Clase 1.
ccpsd_subca_id_class2	1	1	2		Identifica la Política de Certificados para Certificados Digitales de Clase 2.
ccpsd_subca_id_class3	1	1	3		Identifica la Política de Certificados para Certificados Digitales de Clase 3.
ccpsd_subca_id_class1_sgl	1	1	1	1	Identifica los Certificados Digitales de Clase 1 emitidos a personas físicas.
ccpsd_subca_id_class2_bis	1	1	2	2	Identifica los Certificados Digitales de Clase 2 emitidos a suscriptores empresariales y o gubernamentales.
ccpsd_subca_id_class3_bis	1	1	3	2	Identifica los Certificados Digitales de Clase 3 emitidos a suscriptores empresariales y o gubernamentales.
ccpsd_subca_id_class3_eif	1	1	3	3	Identifica los Certificados Digitales de Clase E emitidos a Entidades Privadas y Públicas.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

TABLA DE CONTENIDOS

1. INTRODUCCIÓN.....	13
1.1. VISIÓN GENERAL.....	13
1.2. IDENTIFICACIÓN	14
1.3. SUJETOS, APLICABILIDAD Y USOS	15
1.3.1. Sujetos	15
1.3.2. Ámbito de Aplicación y Usos.....	16
1.3.3. Usos Prohibidos y No Autorizados	17
1.4. DATOS DE CONTACTO.....	19
2. PREVISIONES GENERALES	20
2.1. RESPONSABILIDADES	20
2.1.1. Responsabilidades Asumidas por la Entidad de Certificación al Emitir el Certificado Digital.....	21
2.1.2. Responsabilidades de las Unidades de Registro.....	21
2.1.3. Responsabilidad del Suscriptor	22
2.1.4. Exoneración de Responsabilidad.....	23
2.1.5. Exoneración de Responsabilidad en Caso de Incumplimiento del Suscriptor.....	24
2.1.6. Exoneración de Responsabilidad en Caso de Incumplimiento del Tercero que Confía	25
2.1.7. LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES	25
2.1.8. RESPONSABILIDAD FINANCIERA	26
2.2. OBLIGACIONES.....	27
2.2.1. Entidad de Certificación (EC).....	27
2.2.2. Unidad de Registro (UR)	28
2.2.3. Obligaciones del Solicitante	30
2.2.4. Obligaciones del Suscriptor	30

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2.2.5.	Obligaciones del Tercero que Confía.....	31
2.2.6.	Obligación de Repositorio	31
3.	INTERPRETACIÓN Y EJECUCIÓN.....	32
3.1.	LEGISLACIÓN	32
3.2.	INDEPENDENCIA	32
3.3.	NOTIFICACIÓN.....	32
3.4.	PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS	32
4.	TARIFAS DE SERVICIOS	33
4.1.	TARIFAS DE EMISIÓN DE CERTIFICADOS DIGITALES Y RENOVACIÓN PARA CERTIFICADOS DIGITALES	33
4.2.	TARIFAS DE ACCESO A LOS CERTIFICADOS DIGITALES	33
4.3.	TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS DIGITALES	33
4.4.	POLÍTICA DE REMBOLSO	33
4.5.	TARIFAS SOBRE PETICIONES DE SELLADO DE TIEMPO Y GENERACIÓN DE SELLOS DE TIEMPO	34
5.	PUBLICACIONES Y REPOSITORIOS.....	35
5.1.	POLÍTICA DE CERTIFICADOS Y MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN.....	35
5.2.	TÉRMINOS Y CONDICIONES	35
5.3.	DIFUSIÓN DE LOS CERTIFICADOS DIGITALES	36
5.4.	FRECUENCIA DE PUBLICACIÓN	37
5.5.	CONTROLES DE ACCESO	37
6.	AUDITORÍAS.....	37
6.1.	AUDITORÍA DE LA ENTIDAD DE CERTIFICACIÓN	37
6.2.	PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	39
7.	CONFIDENCIALIDAD	40
7.1.	TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL	40

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

7.2.	TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL	40
7.3.	DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN/SUSPENSIÓN DE CERTIFICADOS DIGITALES	41
8.	IDENTIFICACIÓN Y AUTENTICACIÓN	42
8.1.	REGISTRO INICIAL	42
8.1.1.	Tipos de Nombres.....	42
8.1.2.	Pseudónimos	42
8.1.3.	Reglas Utilizadas para Interpretar Varios Formatos de Nombres.....	42
8.1.4.	Unicidad de los Nombres	42
8.1.5.	Procedimiento de Resolución de Disputas de Nombres.....	42
8.1.6.	Reconocimiento, Autenticación y Función de las Marcas Registradas	43
8.1.7.	Métodos de Prueba de la Posesión de la Clave Privada	43
8.1.8.	Autenticación de la Identidad de una Organización	43
8.1.9.	Requerimiento de Autenticación Mediante Presencia Física de la Identidad de un Individuo	43
8.1.10.	Requerimiento de Autenticación Remota de la Identidad de un Individuo.....	44
8.1.11.	Procedimiento Simplificado de Emisión de Certificados Digitales.....	45
8.2.	REGISTRO.....	45
8.2.1.	REGISTRO CENTRALIZADO.....	46
8.2.2.	REGISTRO DESCENTRALIZADO	47
8.3.	SOLICITUD DE REVOCACIÓN.....	47
8.4.	SOLICITUD DE RENOVACIÓN POSTERIOR A LA REVOCACIÓN (SIN COMPROMISO DE CLAVE PRIVADA)	49
8.5.	RENOVACIÓN DE LA CLAVE Y DEL CERTIFICADO DIGITAL.....	49
8.6.	PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES	50
9.	REQUERIMIENTOS OPERACIONALES	51
9.1.	SOLICITUD DE CERTIFICADOS DIGITALES	51

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.2.	EMISIÓN DE CERTIFICADOS DIGITALES	51
9.3.	ACEPTACIÓN DEL CERTIFICADO DIGITAL	52
9.4.	SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS DIGITALES	53
9.4.1.	Suspensión	53
9.4.2.	Revocación	55
9.4.3.	Lista de Certificados Revocados (LCR).....	58
9.4.4.	Disponibilidad de consulta de estado de Certificados Digitales	58
9.5.	DISTRIBUCIÓN DE CERTIFICADOS DIGITALES	59
9.6.	CONTROLES DE SEGURIDAD	60
9.6.1.	Aspectos Generales	60
9.6.2.	Generación del Certificado Digital.....	61
9.6.3.	Entrega del dispositivo al suscriptor.....	61
9.6.4.	Gestión de la revocación	61
9.6.5.	Tipos de eventos registrados.....	61
9.6.6.	Frecuencia de procesamiento de registro de eventos (bitácoras)	62
9.6.7.	Períodos de retención para auditoría de eventos	62
9.6.8.	Protección de las bitácoras para auditoría	63
9.6.9.	Procedimientos de respaldo de las bitácoras de auditoría.....	63
9.6.10.	Sistema de recogida de información de auditoría.....	63
9.7.	ARCHIVOS.....	63
9.8.	Archivado de la Entidad de Certificación	63
9.9.	Archivado de las Unidades de Registro.....	64
9.9.1.	Protección del archivo	64
9.9.2.	Procedimientos de respaldo de archivo	64
9.10.	SITUACIONES DE EMERGENCIA	65
9.10.1.	PLAN DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRES	65

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.10.2.	Plan de protección de claves.....	65
9.10.3.	Instalación de seguridad después de un desastre natural u otro tipo de desastre	66
9.11.	CESE DE LA ENTIDAD CERTIFICACIÓN	66
10.	CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL	67
10.1.	CONTROLES DE SEGURIDAD FÍSICA	68
10.2.	Ubicación y construcción.....	68
10.3.	Hardware Criptográfico.....	69
10.4.	Acceso físico.....	70
10.5.	Alimentación eléctrica y Aire Acondicionado	70
10.6.	Exposición al agua	71
10.7.	Protección y prevención de incendios	71
10.8.	Sistema de Almacenamiento.....	71
10.9.	Eliminación de Residuos.....	71
10.10.	Respaldo.	72
10.11.	CONTROLES PROCEDIMENTALES	72
10.12.	CONTROLES DE SEGURIDAD DE PERSONAL	73
10.12.1.	Procedimientos de Calificación para Roles de Confianza	73
10.12.2.	Requerimientos de Formación	74
10.12.3.	Requerimientos y Frecuencia de la Actualización de la Formación.....	75
10.12.4.	Sanciones por Acciones No Autorizadas	75
10.12.5.	Requerimientos de Contratación de Personal	75
10.12.6.	Documentación Proporcionada al Personal.....	75
11.	CONTROLES DE SEGURIDAD TÉCNICA.....	76
11.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	76
11.1.1.	Generación del Par de Claves de la Entidad Certificación	76
11.1.2.	Generación del Par de Claves de Firmante/Suscriptor	76

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.1.3.	Entrega de la Clave Privada al Firmante/Suscriptor	77
11.1.4.	Entrega de la Clave Pública del Firmante/Suscriptor al Emisor del Certificado Digital.....	77
11.1.5.	Entrega de la Clave Pública de la Entidad de Certificación a los Terceros que Confían.....	77
11.1.6.	Tamaño y Período de Validez de las Claves del Emisor	77
11.1.7.	Tamaño y Período de Validez de las Claves del Suscriptor.....	78
11.1.8.	Parámetros de Generación de la Clave Pública.....	78
11.1.9.	Comprobación de la Calidad de los Parámetros.....	78
11.1.10.	Dispositivo de Generación de Claves	78
11.1.11.	Fines del Uso de la Clave.....	79
11.2.	PROTECCIÓN DE LA CLAVE PRIVADA	79
11.2.1.	De la Entidad de Certificación	79
11.2.2.	13.3.2 Del Firmante/Suscriptor	80
11.3.	ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS	80
11.3.1.	Control Multi-Persona (n de entre m) de la Clave Privada	80
11.3.2.	Depósito de la Clave Privada (Key Escrow).....	80
11.3.3.	Copia de Seguridad de la Clave Privada	81
11.3.4.	Archivo de la Clave Privada	81
11.3.5.	Método de Activación de la Clave Privada	81
11.3.6.	Método de Desactivación de la Clave Privada	81
11.3.7.	Método de Destrucción de la Clave Privada.....	81
11.4.	OTROS ASPECTOS DE ADMINISTRACIÓN DEL PAR DE CLAVES	82
11.4.1.	Archivo de la Clave Pública.....	82
11.4.2.	Período de Uso para las Claves Públicas y Privadas.....	82
11.5.	CICLO DE VIDA DEL DISPOSITIVO CRIPTOGRÁFICO.....	82
11.6.	CONTROLES DE SEGURIDAD TECNOLÓGICOS	82

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.7.	CONTROLES DE SEGURIDAD DEL CICLO DE VIDA	83
11.7.1.	Controles de Desarrollo del Sistema	83
11.7.2.	Controles de Gestión de la Seguridad	83
11.7.3.	Gestión de Seguridad	84
11.7.4.	Clasificación y Gestión de Información y Bienes.....	84
11.7.5.	Gestión de Operaciones	85
11.7.6.	Tratamiento de los Soportes y Seguridad.....	85
11.7.7.	Planificación del Sistema	85
11.7.8.	Reportes de Incidencias y Respuesta.....	85
11.7.9.	Procedimientos Operacionales y Responsabilidades.....	86
11.7.10.	Gestión del Sistema de Acceso	86
11.8.	GESTIONES DE CERTIFICADOS DIGITALES	86
11.8.1.	Gestión del Ciclo de Vida del Dispositivo Criptográfico.....	87
11.9.	CONTROLES DE SEGURIDAD DE LA RED	87
11.10.	CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS	87
11.11.	Preparación del Dispositivo Criptográfico de Creación de Claves y Firmas Digitales	87
12.	PERFILES DE CERTIFICADOS DIGITALES Y LISTA DE CERTIFICADOS REVOCADOS	89
12.1.	PERFIL DEL CERTIFICADO DIGITAL	89
12.1.1.	Número de Versión.....	90
12.1.2.	Extensiones del Certificado Digital.....	90
12.1.3.	Identificadores de Objeto (OID) de los Algoritmos	92
12.1.4.	Restricciones de los Nombres.....	92
12.2.	PERFIL DE LAS LISTAS DE CERTIFICADOS REVOCADOS	92
12.3.	PERFIL DEL PROTOCOLO DE CERTIFICADOS EN LÍNEA (OCSP)	92
13.	ESTAMPADO CRONOLÓGICO DE TIEMPO	93
13.1.	Requerimientos para el estampado cronológico de tiempo	93

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

14.	ESPECIFICACIÓN DE LA ADMINISTRACIÓN	94
14.1.	AUTORIDAD DE LAS POLÍTICAS.....	94
14.2.	PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS	94
14.3.	PUBLICACIÓN Y NOTIFICACIÓN	94
14.4.	PROCEDIMIENTOS DE APROBACIÓN DE LA PC	94
15.	DERECHOS DE PROPIEDAD INTELECTUAL	96
16.	ANEXO I. ACRÓNIMOS.	97
17.	ANEXO II. OTRAS DEFINICIONES.	99
18.	CONTROL DE CAMBIO.....	100

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

1. INTRODUCCIÓN

1.1. VISIÓN GENERAL

El presente documento especifica la Política de Certificados Clase 2 de la Cámara de Comercio y Producción de Santo Domingo. La misma está basada en las especificaciones de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales; el Reglamento de Aplicación aprobado mediante el Decreto No. 335-03 y las Norma Complementarias sobre Políticas y Procedimientos de Certificación. Estas normas comprenden las obligaciones y responsabilidades que deben seguir la Entidad de Certificación y las Unidades de Registro que emitan Certificados Digitales bajo esta Política.

Estos certificados son utilizados para trámites con el Estado en las transacciones económicas de bajo monto y para el intercambio de documentos, de riesgo bajo o medio con connotaciones financieras. Los Certificados Digitales emitidos bajo esta política requieren de la verificación de la identidad y autenticación de los suscriptores por las Unidades de Registro correspondientes, en cumplimiento a los procedimientos del presente documento.

En lo que se refiere al contenido de esta Política de Certificados, se considera que el lector conoce los conceptos básicos de Infraestructura de Clave Pública (*PKI*, siglas en inglés de *Public Key Infrastructure*), Certificados Digitales y Firma Digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto o visite la página de Internet <http://www.camarasantodomingo.do>.

- **Política de Certificados** (en adelante, PC) es el conjunto de reglas que definen los usos y/o aplicación de un Certificado Digital en una comunidad y/o en algún programa o aplicativo, con requisitos de seguridad y utilización comunes.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Esta política define la normativa, obligaciones y responsabilidades que siguen la Entidad de Certificación Cámara de Comercio y Producción de Santo Domingo, como emisora del tipo de Certificado Digital definido en el presente documento y las Unidades de Registro, responsable de autorizar la emisión de los Certificados Digitales. Ambas crean obligaciones de interés para los Firmantes/Suscriptores contemplados como usuarios del Certificado Digital al que se rige este documento.

Las llaves de los Firmantes/Suscriptores tienen un período de validez determinado por esta política y en ningún caso podrán realizarse copias de respaldo, ni almacenarse por la Entidad de Certificación.

La información personal recabada del Firmante/Suscriptor se recogerá con el debido consentimiento del interesado y únicamente para los fines propios del servicio de certificación, el cual podrá ejercitar en todo caso sus oportunos derechos de información, rectificación y cancelación. La Entidad Certificación deberá respetar así mismo la normativa aplicable en materia de protección de datos.

Esta política define la normativa, obligaciones y responsabilidades que siguen la Entidad de Certificación Cámara de Comercio y Producción de Santo Domingo, como emisora del tipo de Certificado Digital definido en el presente documento, y las Unidades de Registro responsables de autorizar la emisión de los Certificados Digitales. Ambas crean obligaciones de interés para los Suscriptores contemplados como usuarios del Certificado Digital al que se rige este documento.

1.2.IDENTIFICACIÓN

El presente documento de Política de Certificados está identificado con el *OID*: 1.3.6.1.4.1.26236.1.1.2.2

- *iso* (1)
- *org* (3)
- *dod* (6)
- *internet* (1)
- *private* (4)
- *enterprise* (1)
- Cámara de Comercio y Producción de Santo Domingo (26236)
- Certificado Raíz de la Entidad de Certificación Cámara de Comercio y Producción de Santo Domingo. (1)

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- Certificado Raíz de la Entidad de Certificación Subrogada de la Cámara de Comercio y Producción de Santo Domingo (1)
- Identifica la Política de Certificados para Certificados Digitales de Clase 2 (2)
- Identifica los Certificados Digitales de Clase 2 emitidos a suscriptores empresariales y/o gubernamentales. Personas Físicas con Vínculo Institucional. (2)

1.3. SUJETOS, APLICABILIDAD Y USOS

1.3.1. Sujetos

La Política descrita en este documento aplica a los siguientes integrantes:

La Entidad de Certificación (EC):

La Cámara de Comercio y Producción de Santo Domingo es responsable de la emisión de los Certificados Digitales. Actúa como parte de confianza, entre el Suscriptor y el Tercero que confía, en las relaciones electrónicas, vinculando una determinada clave pública con una persona u organización (Suscriptor) a través de la emisión de este Certificado Digital.

Unidad de Registro (UR):

Ente que actúa mediante acuerdo suscrito con la Entidad de Certificación para realizar las funciones que se dispongan en el MPC para la gestión de las solicitudes, identificación y registro de los solicitantes de Certificados Digitales.

La Entidad de Certificación ha delegado las funciones de validación de los datos y la identidad de los suscriptores de Certificados Digitales en sus Unidades de Registro.

Firmante o Suscriptor:

Persona física poseedor de un dispositivo de creación de firma digital con un Certificado Digital emitido bajo esta política.

Tercero que Confía:

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Persona física que voluntariamente confía en el Certificado Digital emitido a favor del Suscriptor y responsable de la verificación y el estado del Certificado Digital y uso del mismo de acuerdo a lo establecido en el presente documento, por lo que no se requerirá acuerdo posterior alguno.

Solicitante:

Toda persona física vinculada a una entidad que solicita un Certificado Digital.

1.3.2. Ámbito de Aplicación y Usos

El Certificado Digital emitido bajo la presente Política, permite identificar a una persona física frente a una empresa, institución, organización o entidad gubernamental en el ámbito de su actividad.

Los Certificados Digitales emitidos bajo esta PC son válidos para:

- 1) Asumir responsabilidades, compromisos y/o derechos previamente establecidos por el empleador del firmante/suscriptor.
- 2) Validar la identidad de los suscriptores en la Internet, en las transacciones en línea que pueden o no corresponder a operaciones económicas y en las redes privadas virtuales,
- 3) Cifrar las llaves de sesión.
- 4) Firmar transacciones económicas y financieras.
- 5) Firmar los documentos digitales y mensajes de datos relacionados a sus funciones y responsabilidades dentro de la entidad, institución o empresa en la cual laboran para garantizar la integridad de sus contenidos.

Dentro de los propósitos que cumplen estos Certificados Digitales podemos citar:

Identificación del Firmante/Suscriptor: El Firmante/Suscriptor puede autenticar frente a otra parte y su identidad, demostrando la asociación de su llave privada con la respectiva llave pública, contenida en el Certificado Digital. El mismo podrá identificarse válidamente ante cualquier persona mediante la firma de cualquier otro tipo de mensaje de datos.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Integridad del Documento Firmado: La utilización de este Certificado Digital garantiza que el documento firmado es íntegro, es decir que el documento no fue alterado o modificado después de firmado por el Firmante/Suscriptor. Se garantiza que el mensaje recibido por el Tercero que confía es el mismo que fue emitido por el Firmante/Suscriptor.

No Repudio de Origen: Con el uso de este Certificado Digital, el Firmante/Suscriptor que ha firmado un mensaje de datos no puede repudiarlo, es decir no puede negar su autoría.

A pesar de que un Certificado Digital puede ser utilizado para el cifrado de datos, la EC no se responsabiliza por este uso, ni por la recuperación de los datos cifrados en caso de pérdida de las llaves por parte del Firmante/Suscriptor o el Tercero que confía. Por lo que implica que las partes lo harán bajo su propia responsabilidad.

La Entidad de Certificación establece que los Certificados Digitales emitidos bajo esta política pueden almacenarse en sistemas, aplicaciones o programas al igual que en dispositivos criptográficos. En el caso de los dispositivos, estos deben estar respaldados por procedimientos y requisitos técnicos apropiados, de manera tal de asegurar que el par de llaves que permiten la generación de firmas digitales:

- 1) No se repitan y se encuentren adecuadamente protegidos.
- 2) No puedan ser calculadas, derivadas y/o replicadas, y que se evite su falsificación mediante el empleo de las tecnologías disponibles.
- 3) Puedan ser razonablemente protegidos por su titular del acceso indebido de terceros.

1.3.3. Usos Prohibidos y No Autorizados

Este Certificado Digital sólo podrá ser empleado con los límites y para los usos a los cuales haya sido emitido, el Firmante/Suscriptor no puede actuar en nombre de una empresa o entidad ni algunas de sus dependencias, a excepción de que así haya sido establecido en sus estatutos sociales de la misma.

De igual forma, el Firmante/Suscriptor no deberá hacer uso del Certificado Digital emitido bajo esta PC más que a lo que ha sido permitido en virtud de las políticas internas a la entidad jurídica a la cual está vinculado.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

La Entidad de Certificación, en función de la legislación vigente, se exime de cualquier responsabilidad por el uso indebido y/o no autorizado de los Certificados Digitales, que realice el Firmante/Suscriptor o cualquier tercero mediante el incumplimiento de los lineamientos establecidos en la PC, el MPC y los Contratos firmados con las Unidades de Registro.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

En función de los servicios prestados por la Entidad de Certificación mediante la emisión de sus Certificados Digitales, no le es posible el acceso o conocimiento del contenido del mensaje de datos al que haya sido adjuntado o con el que se relacione el uso de un Certificado Digital. Por lo tanto, no es posible por parte de la EC emitir alguna valoración sobre dicho contenido, asumiendo el signatario cualquier responsabilidad dimanante, aparejada al uso de un Certificado Digital. La obligación de custodia es de exclusiva responsabilidad del suscriptor.

1.4.DATOS DE CONTACTO

La presente Política de Certificados, está administrada y gestionada por la Consultoría Jurídica y la Gerencia de Soluciones Digitales, de la Cámara de Comercio y Producción de Santo Domingo pudiendo ser contactados por los siguientes medios:

Medio	Información
Correo Electrónico:	digifirma@camarasantodomingo.do
Teléfono:	+1 (809) 682-2688
Dirección:	Avenida 27 de Febrero No. 228, Torre Friusa, Sector La Esperilla, Santo Domingo, Distrito Nacional.
Sitio Web:	http://www.camarasantodomingo.do

Ente regulador: Instituto Dominicano de las Telecomunicaciones (INDOTEL)

Medio	Información
Correo Electrónico:	cmoline@indotel.gob.do
Teléfono:	+1 (829) 732-5555
Dirección:	Avenida Abraham Lincoln No. 962, Santo Domingo, Distrito Nacional.
Sitio Web:	http://www.indotel.gob.do

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2. PREVISIONES GENERALES

2.1. RESPONSABILIDADES

La Entidad de Certificación dispondrá en todo momento de un seguro de responsabilidad civil y actuará en la cobertura de sus responsabilidades por sí o a través de la entidad aseguradora, satisfaciendo los requerimientos de los solicitantes de los Certificados Digitales, de los signatarios y de los terceros que confíen en los Certificados Digitales.

Las responsabilidades de la Entidad de Certificación incluyen las establecidas por la presente Política de Certificados, así como las que resulten de aplicación como consecuencia de la Ley No. 126-02, su Reglamento de Aplicación y las normas complementarias dictadas por el INDOTEL. Además será responsable del daño causado ante Suscriptor o cualquier persona que de buena fe confíe en el Certificado Digital, siempre que exista dolo o culpa grave, respecto de:

- 1) La exactitud de toda la información contenida en el Certificado Digital en la fecha de su emisión.
- 2) La garantía de que, en el momento de la entrega del Certificado Digital, obra en poder del Suscriptor, la clave privada correspondiente a la clave pública dada o identificada en el Certificado Digital.
- 3) La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- 4) La correspondencia entre el Certificado Digital solicitado y el Certificado Digital entregado.
- 5) El proceso de identificación y autenticación del suscriptor, en el ejercicio de sus funciones delegadas a la Unidad de Registro.
- 6) La emisión de Certificados Digitales.
- 7) La administración de Certificados Digitales, incluyendo el proceso de revocación.
- 8) La publicación de las Listas de Certificados Revocados y de toda la documentación establecida en las normas aplicables dictadas por INDOTEL.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2.1.1. Responsabilidades Asumidas por la Entidad de Certificación al Emitir el Certificado Digital

Al emitir el Certificado Digital, la Entidad de Certificación garantiza:

- 1) Que el Certificado Digital ha sido emitido siguiendo las pautas establecidas en esta política y los procedimientos para la validación de los datos en él incluidos.
- 2) Que el Certificado Digital satisface todos los requisitos exigidos por la Ley No. 126-02, su Reglamento de Aplicación y las Normas Complementarias dictadas por el INDOTEL.
- 3) Que los algoritmos y longitudes de claves utilizados cumplen con la última versión de los Estándares Tecnológicos aprobada por Resolución del INDOTEL.
- 4) Que el Certificado Digital y su eventual revocación, serán publicados según lo dispuesto por la Ley No. 126-02, su Reglamento de Aplicación, sus Normas Complementarias y esta Política de Certificados.
- 5) Que el Certificado Digital cumple con todas las disposiciones aplicables vigentes.
- 6) Que la información general del solicitante así como el certificado de Firma Digital otorgado, sean conservados en los archive de la Entidad de Certificación, por el periodo establecido en el reglamento, sus normas complementarias y en esta política de certificación. (detallar como se reguarda la información en los archivos digitales).

2.1.2. Responsabilidades de las Unidades de Registro

Las Unidades de Registro, serán responsables por el cumplimiento de las funciones de validación de la identidad y autenticación de los datos de los Solicitantes de Certificados Digitales por su intermedio, y por el archivo y conservación de toda la documentación que respalde dicho proceso por un plazo no inferior a diez (10) años desde la revocación o expiración de los Certificados Digitales, en los términos establecidos por la Entidad de Certificación en esta política.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Las responsabilidades de las Unidades de Registro vinculadas a la Entidad de Certificación, son las siguientes:

- 1) Recibir las solicitudes de emisión, de suspensión y de revocación de Certificados Digitales.
- 2) Verificar la identidad del solicitante y validar el contenido de la solicitud, de acuerdo a lo establecido en la PC y en el MPC.
- 3) Remitir las solicitudes de emisión, suspensión y revocación aprobadas y autorizadas, a la Entidad de Certificación.
- 4) Informar a los titulares de Certificados Digitales sobre el estado del proceso de emisión, suspensión y revocación de Certificados Digitales.
- 5) Registrar y documentar las acciones realizadas y conservarlas, de acuerdo a lo establecido en el Reglamento, las normas complementarias y esta política de certificado.
- 6) Gestionar el registro de usuarios y sus solicitudes de certificados digitales, así como las respuestas a dichas solicitudes. Mantener contacto directo con los usuarios y gestionar el ciclo de vida de un certificado (solicitud de Certificación, renovación, suspensión o revocación).

A fin de recopilar las informaciones correspondientes a los datos de identidad de los suscriptores, los mismos deberán completar los formularios suministrados por la Entidad de Certificación. Estos documentos conjuntamente con los demás informaciones serán debidamente archivados y resguardados por la EC.

2.1.3. Responsabilidad del Suscriptor

El suscriptor tendrá las siguientes responsabilidades:

- 1) Remitir a la Entidad de Certificación a través de las Unidades de Registro la información precisa y completa, de acuerdo a los lineamientos de esta política, en particular con relación al proceso de validación de su identidad.
- 2) Garantizar la protección de sus claves privadas, sus claves de activación y sus dispositivos criptográficos, si los tuviera.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 3) Utilizar su par de claves respetando todas las limitaciones que le fueron notificadas por la Entidad de Certificación, las Unidades de Registro y/o a la empresa, organización o entidad gubernamental a la cual está vinculado, en cuanto al uso de los Certificados Digitales.
- 4) Tomar precauciones razonables para evitar el uso indebido y/o no autorizado de su clave privada.
- 5) En caso de que el suscriptor o la entidad a la que esté vinculado genere su propio par de claves debe:
 - a. Generar sus claves utilizando un algoritmo establecido por la Entidad de Certificación Cámara de Comercio y Producción de Santo Domingo, aceptados por los Estándares Tecnológicos dictados por el INDOTEL.
 - b. Utilizar claves de longitud igual a 2048 bits, según se especifica en los estándares antes mencionados.
- 6) Notificar en forma inmediata a la Entidad de Certificación o su Unidad de Registro, la ocurrencia de cualquiera de las circunstancias enunciadas a continuación, durante el período de vigencia del Certificado Digital:
 - a. La pérdida, robo o la sospecha de vulneración o mal uso de su clave privada.
 - b. La pérdida del control del suscriptor sobre su clave privada debido a la vulneración de los datos de activación de su clave privada de firma u otras razones.
 - c. Los cambios o errores en los datos contenidos en el Certificado Digital.
- 7) Informar a la Entidad de Certificación ante cualquier sospecha de vulnerabilidad o mal uso de su clave privada y solicitar la revocación de su certificado digital.

El Suscriptor de un Certificado Digital de acuerdo a los lineamientos de esta Política asume la absoluta responsabilidad por la utilización de dicho Certificado Digital, incluyendo la custodia exclusiva y permanente de su clave privada. En particular, el Suscriptor es responsable de solicitar la revocación de su Certificado Digital, en caso de pérdida del dispositivo criptográfico de creación de firmas digitales.

2.1.4. Exoneración de Responsabilidad

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

La Entidad de Certificación y las Unidades de Registro no serán responsables en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- 1) Por causa de fuerza Mayor (Estado de Guerra, desastres naturales, etc.).
- 2) Por el daño causado durante el proceso de suspensión y/o revocación.
- 3) Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- 4) Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.
- 5) Por el uso indebido o fraudulento de los Certificados Digitales o LCR emitidos por la Entidad de Certificación.
- 6) Por el uso de la información contenida en el Certificado Digital o en la LCR.
- 7) Por la inexactitud de los datos que consten en el Certificado Digital, si éstos le han sido acreditados mediante documento público.
- 8) Por el incumplimiento de las obligaciones establecidas para el Suscriptor en la normativa vigente de la República Dominicana, la presente PC o el MPC correspondiente.
- 9) Por el uso de los Certificados Digitales siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente PC.

2.1.5. Exoneración de Responsabilidad en Caso de Incumplimiento del Suscriptor

La Entidad de Certificación y las Unidades de Registro no serán responsables en ningún caso si el Suscriptor incurre en alguno de los siguientes supuestos:

- 1) No haber proporcionado la información veraz, completa y exacta sobre los datos que deban constar en el Certificado Digital o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia.
- 2) La falta de comunicación sin demora de cualquier modificación de las circunstancias reflejadas en el Certificado Digital.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 3) La negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- 4) No solicitar la suspensión o revocación del Certificado Digital en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- 5) Utilizar los datos de creación de firma cuando haya expirado el período de validez del Certificado Digital o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

2.1.6. Exoneración de Responsabilidad en Caso de Incumplimiento del Tercero que Confía

La Entidad de Certificación y las Unidades de Registro no serán responsables en ningún caso si el Tercero que confía actúa de forma negligente. Se entenderá por negligencia los siguientes casos:

- 1) Cuando no tenga en cuenta el estado de suspensión o revocación del Certificado Digital publicada en el servicio de consulta.
- 2) Cuando no verifique la validez del Certificado Digital.
- 3) Cuando no verifique el propósito de uso para el cual fue emitido el Certificado Digital.

2.1.7. LÍMITE DE RESPONSABILIDAD EN CASO DE PÉRDIDAS POR TRANSACCIONES

Los Certificados Digitales emitidos bajo esta Política son válidos para transacciones con valor monetario o para operaciones financieras, las cuales serán definidas por las entidades a la cual estén vinculadas.

La Entidad de Certificación y las Unidades de Registro no son responsables en ningún caso de las consecuencias causadas por realizar transacciones con valor monetario o para operaciones financieras utilizando los Certificados Digitales emitidos por la presente Política.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2.1.8. RESPONSABILIDAD FINANCIERA

La Entidad Certificación no asume ningún tipo de responsabilidad financiera. Deberán establecerse garantías particulares a través de seguros específicos que se negociarán individualmente.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2.2.OBLIGACIONES

2.2.1. Entidad de Certificación (EC)

La Entidad de Certificación que actúan bajo esta Política de Certificados estará obligada a cumplir con lo dispuesto por la normativa vigente y además a:

- 1) Proteger sus claves privadas de forma segura.
- 2) Emitir Certificados Digitales conforme a esta Política y a los estándares de aplicación.
- 3) Emitir Certificados Digitales según la información que obra en su poder y libres de errores de entrada de datos.
- 4) Emitir Certificados Digitales cuyo contenido mínimo sea el definido por la legislación vigente para los Certificados Digitales.
- 5) Suspender y revocar los Certificados Digitales según lo dispuesto en esta Política y publicar las mencionadas revocaciones en la Lista de Certificados Revocados (LCR).
- 6) Informar a los Suscriptores de la revocación o suspensión de sus Certificados Digitales, en tiempo y forma de acuerdo con la legislación vigente.
- 7) Publicar esta Política y el MPC correspondiente en su página *Web*.
- 8) Informar sobre las modificaciones de esta Política a los Suscriptores y a la Unidad de Registro que esté vinculada a ella.
- 9) No almacenar ni copiar el par de claves para la generación de Firmas Digitales del Suscriptor.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 10) Establecer los mecanismos de generación de las claves.
- 11) Conservar la información sobre el Certificado Digital emitido por el período mínimo exigido por la normativa vigente, estableciendo los mecanismos necesarios para la protección ante la pérdida o destrucción ante la misma.
- 12) Informar al Suscriptor de su Certificado Digital, en un lenguaje claro y accesible a través de una Política de Certificados.
- 13) Notificar la emisión del Certificado Digital al suscriptor titular del mismo, a quien éste señale y a terceros indicados en la presente política de certificación.
- 14) Notificar la revocación o suspensión del Certificado Digital al suscriptor titular del mismo, a quien éste señale, y a terceros indicados en la presente política de certificación.
- 15) Informar al solicitante respecto de las características del certificado solicitado, las limitaciones a la responsabilidad, y demás condiciones concernientes a la prestación del servicio.
- 16) Velar por que las Unidades de Registro cumplan con sus obligaciones y responsabilidades establecidas en las PC, MPC, al igual que en la legislación y normativa vigente, ya que son responsables por los actos de las Unidades de Registro con las que se encuentre operativamente vinculada.
- 17) Cumplir con las obligaciones establecidas por la Ley No. 126-02, su Reglamento de Aplicación y las normas complementarias que a tal efecto dicte el INDOTEL.

2.2.2. Unidad de Registro (UR)

Las Unidades de Registro que actúan bajo esta Política de Certificados serán responsables por el cumplimiento de las funciones de validación de la identidad y autenticación de los datos de los solicitantes de Certificados Digitales por su intermedio, y por el archivo y conservación de toda la documentación que respalde dicho proceso y está obligada a cumplir con lo dispuesto por la normativa vigente, además de:

- 1) Respetar lo dispuesto en esta Política.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 2) Comprobar la identidad de los solicitantes de Certificados Digitales.
- 3) Verificar la exactitud y autenticidad de la información suministrada por el Solicitante.
- 4) Archivar, por período dispuesto en la legislación vigente, los documentos suministrados por el Suscriptor.
- 5) Respetar lo dispuesto en los contratos firmados con la Entidad de Certificación y con el Suscriptor.
- 6) Informar a la Entidad de Certificación las causas de revocación, inmediatamente tomen conocimiento.
- 7) Informar al Suscriptor de su Certificado Digital, en un lenguaje claro y accesible a través de una Política de Certificados.
- 8) Validar los datos de la solicitud de Certificado Digital del suscriptor en los términos establecidos en la presente política.
- 9) Notificar sobre la emisión del Certificado Digital al suscriptor titular del mismo.
- 10) Notificar la revocación o suspensión del Certificado Digital al suscriptor titular del mismo.
- 11) Cumplir con las obligaciones establecidas por la Ley No. 126-02, su Reglamento de Aplicación y las normas complementarias que a tal efecto dicte el INDOTEL.
- 12) Remitir las solicitudes de emisión, suspensión y revocación aprobadas y autorizadas, a la Entidad de Certificación.
- 13) Gestionar el registro de usuarios y sus solicitudes de certificados digitales, así como las respuestas a dichas solicitudes. Mantener contacto directo con los usuarios y gestionar el ciclo de vida de un certificado (solicitud de Certificación, renovación, suspensión o revocación).

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2.2.3. Obligaciones del Solicitante

El solicitante de un Certificado Digital estará obligado a cumplir con lo dispuesto por la normativa aplicable y además a:

- 1) Suministrar a la UR la información necesaria para realizar una correcta identificación.
- 2) Confirmar la exactitud y veracidad de la información suministrada.
- 3) Notificar cualquier cambio en los datos aportados para la creación del Certificado Digital durante su período de validez.

2.2.4. Obligaciones del Suscriptor

El Suscriptor de un Certificado Digital estará obligado a cumplir con lo dispuesto por la normativa vigente y en adición:

- 1) Custodiar su clave privada de manera diligente y bajo su absoluto y exclusivo control.
- 2) Usar el Certificado Digital según lo establecido en la presente Política.
- 3) Respetar lo dispuesto en el contrato firmado con la Entidad de Certificación a través de la Unidad de Registro.
- 4) Informar de la existencia de alguna causa de suspensión o revocación.
- 5) Notificar cualquier cambio en los datos aportados para la creación del Certificado Digital durante su período de validez.
- 6) Brindar a la Unidad de Registro, si existiere, datos válidos, susceptibles de verificación.
- 7) Notificar a la Entidad de Certificación o en su caso, a la Unidad de Registro, toda sospecha de vulneración de su clave privada.
- 8) Cumplir con las obligaciones establecidas por la Ley No. 126-02, su Reglamento de Aplicación y las normas complementarias que a tal efecto dicte el INDOTEL.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

2.2.5. Obligaciones del Tercero que Confía

Será obligación de los Terceros que confían cumplir con lo dispuesto por la normativa vigente y además:

- 1) Verificar la validez de los Certificados Digitales en el momento de realizar cualquier operación basada en los mismos.
- 2) Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los Certificados Digitales en los que confía.
- 3) Aceptar Certificados Digitales que permitan la verificación de Firmas Digitales correspondientes a transacciones sujetas al alcance de este documento.
- 4) Verificar las Firmas Digitales recibidas y la validez de los Certificados Digitales.
- 5) Verificar el estado del Certificado Digital en la Lista de Certificados Revocados y Suspendidos.

2.2.6. Obligación de Repositorio

La información relativa a la publicación y revocación/suspensión de los Certificados Digitales se mantendrá accesible al público en los términos establecidos en la normativa vigente, la Ley No. 126-02, su Reglamento de Aplicación y las Normas Complementarias.

La Entidad de Certificación mantendrá un sistema seguro que garantice la publicación de los Certificados Digitales e información sobre la revocación de los mismos.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

3. INTERPRETACIÓN Y EJECUCIÓN

3.1.LEGISLACIÓN

La ejecución, interpretación, modificación o validez de las presentes Política de Certificados se regirá por lo dispuesto en la Ley No. 126-02 de Comercio Electrónico, Documentos y Firmas Digitales; del reglamento de aplicación mediante el Decreto No. 335-03; la Norma Complementaria aprobada por la Resolución No. 169-07 y la Normas Complementarias sobre Políticas y Procedimientos de Certificación, así como, otras normas complementarias aplicables dictadas por el INDOTEL.

En caso de que se presenten situaciones en las cuales las Políticas de Certificados entre en conflicto con otras normas, acuerdos, contratos o documentos que se pudieran adoptar, procederemos a realizar una evaluación sobre la situación y remitir la misma con nuestras inquietudes, observaciones y sugerencias por ante el ente regulador.

3.2.INDEPENDENCIA

La invalidez de una de las cláusulas contenidas en estas Política de Certificados no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

3.3.NOTIFICACIÓN

Cualquier notificación referente a la presente Política de Certificados se realizará por correo electrónico, mediante comunicación escrita dirigido a cualquiera de las direcciones referidas en el apartado de datos de contacto o a través de la publicación de la misma en la página *Web* de la Entidad de Certificación.

3.4.PROCEDIMIENTO DE RESOLUCIÓN DE DISPUTAS

Toda controversia, conflicto, diferendos y/o litigios que puedan surgir que se derive del presente documento, se resolverá por ante el Instituto Dominicano de las Telecomunicaciones (INDOTEL) como

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

órgano de control de las actividades de las EC. Este es el único órgano con facultad para resolver las controversias que devenguen entre la EC y los suscriptores.

4. TARIFAS DE SERVICIOS

4.1. TARIFAS DE EMISIÓN DE CERTIFICADOS DIGITALES Y RENOVACIÓN PARA CERTIFICADOS DIGITALES

Los precios de los servicios de certificación o cualesquiera otros servicios relacionados estarán disponibles en la página *Web* de la Cámara de Comercio y Producción de Santo Domingo (<http://www.camarasantodomingo.do>).

4.2. TARIFAS DE ACCESO A LOS CERTIFICADOS DIGITALES

El acceso a las consultas de los Certificados Digitales emitidos es gratuito.

4.3. TARIFAS DE ACCESO A LA INFORMACIÓN RELATIVA AL ESTADO DE LOS CERTIFICADOS DIGITALES

La Entidad de Certificación proveerá de un acceso a la información relativa al estado de los Certificados Digitales Revocados en forma gratuita, a través de la CRL, publicado en su sitio *Web* <http://www.camarasantodomingo.do>.

4.4. POLÍTICA DE REMBOLSO

Para fines de esta Política la Entidad de Certificación no dispone de una Política de Rembolso para los suscriptores de Certificados Digitales.

	GERENCIA SOLUCIONES DIGITALES		Código
	POLÍTICA DE CERTIFICADOS CLASE 2		DAF-SD-013
			Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	Fecha de Actualización
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

4.5. TARIFAS SOBRE PETICIONES DE SELLADO DE TIEMPO Y GENERACIÓN DE SELLOS DE TIEMPO

Los precios de los servicios sobre peticiones de sellado de tiempo y generación de sellos de tiempo estarán disponibles en la página *Web* de la Cámara de Comercio y Producción de Santo Domingo (<http://www.camarasantodomingo.do>) una vez dicho servicio haya sido habilitado.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

5. PUBLICACIONES Y REPOSITORIOS

5.1.POLÍTICA DE CERTIFICADOS Y MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN

La Entidad de Certificación Cámara de Comercio y Producción de Santo Domingo y las Unidades de Registro están obligadas a publicar la información relativa a la Política de Certificados.

La presente Política de Certificados es pública y se encuentra disponible en la siguiente dirección de Internet.

La Entidad de Certificación y las Unidades de Registro permitirán el acceso las veinticuatro (24) horas, los siete (7) días a la semana, sujeto a un programa razonable y previsible de mantenimiento, de la siguiente información:

- 1) La Política de Certificados y toda documentación técnica pertinente a los Certificados Digitales es emitidos por la Entidad de Certificación.
- 2) Servicio de acceso en línea al estado de los Certificados Digitales emitidos que hagan referencia a esta Política.

5.2.TÉRMINOS Y CONDICIONES

Las Unidades de Registro pondrán a disposición de los Suscriptores y Terceros que confían los términos y condiciones del servicio antes de proceder a la emisión del Certificado Digital o de entregar las claves que permitan el acceso a la clave privada.

Lo dicho es aplicable con relación a:

- 1) La política de certificación para firmas digitales seguras, bajo cuyas condiciones se emiten los certificados, especificando si se requiere el empleo de dispositivos seguros de creación de firma,
- 2) Toda limitación en el uso de los certificados emitidos,
- 3) Las obligaciones del suscriptor,

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 4) Toda información sobre la validación de los certificados, incluyendo los requerimientos de verificación del estado del certificado (si fuera aplicable), a fin de que los usuarios puedan confiar de manera razonable en los mismos,
- 5) Las limitaciones en cuanto a la responsabilidad de la Entidad de Certificación,
- 6) El período por el cual se retiene la información y documentación utilizada en el proceso de validación, el cual no podrá ser inferior a DIEZ (10) años,
- 7) El lapso durante el cual la Entidad de Certificación retendrá el registro de eventos (logs),
- 8) Los procedimientos a seguir en caso de quejas, denuncias y resolución de conflictos,
- 9) Las normas legales aplicables,

5.3.DIFUSIÓN DE LOS CERTIFICADOS DIGITALES

La Entidad de Certificación deberá confirmar que los Certificados Digitales son accesibles para los Suscriptores y Terceros que confían.

En concreto:

- 1) El Certificado Raíz de la Entidad de Certificación es público y se encontrará disponible en la página *Web* de la misma (<http://www.camarasantodomingo.do>).
- 2) La Lista de Certificado Digital Revocados (LCR) y los demás Certificados Digitales estarán disponibles al público en la página *Web* de la Cámara de Comercio y Producción de Santo Domingo sólo en los casos en que el Suscriptor haya otorgado su consentimiento, salvo que su publicación sea obligatoria en consonancia a los requerimientos regulatorios.
- 3) La información a la que se refieren los puntos 1) y 2) estarán disponible las veinticuatro (24) horas al día, los siete (7) días a la semana. En caso de fallo del sistema u otros factores que no se encuentran bajo el control de la Entidad de Certificación, la Entidad de Certificación hará todos los esfuerzos para conseguir que este servicio informativo no esté inaccesible durante un período máximo de 24 horas.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

5.4.FRECUENCIA DE PUBLICACIÓN

La Política de Certificados y el Manual de Procedimientos de Certificación se publicarán una vez hayan sido creadas o en el momento en que se apruebe una modificación de las mismas por el Instituto Dominicano de las Telecomunicaciones (INDOTEL).

La Entidad de Certificación publicará las emisiones o renovaciones, suspensiones y revocaciones de Certificados Digitales tan pronto se hayan cumplido los procedimientos de validación de identidad de los solicitantes por parte de las Unidades de Registro para cada caso en particular en el momento en que reciba una petición autenticada y existan indicios de su necesidad.

5.5.CONTROLES DE ACCESO

La Entidad de Certificación podrá establecer sistemas de seguridad para controlar el acceso a la información contenida en el *Web*, *LDAP* o *LCR* con el fin de evitar usos indebidos que afecten a la protección de datos personales.

6. AUDITORÍAS

6.1.AUDITORÍA DE LA ENTIDAD DE CERTIFICACIÓN

Se realizará una auditoria con una periodicidad anual, la misma deberá ser realizada por el Instituto Dominicano de las Telecomunicaciones (INDOTEL) o por un auditor independiente y neutral, la cual deberá verificar en todo caso:

- 1) Que la Entidad de Certificación tiene un sistema que garantice la calidad del servicio prestado.
- 2) Que la Entidad de Certificación cumple con los requerimientos de esta Política de Certificados.
- 3) Que el Manual de Procedimientos de Certificación se ajustan a lo establecido en este documento, con lo acordado por el INDOTEL y con lo establecido en la Ley No. 126-02 de Comercio Electrónico, Documentos y Firmas Digitales; el Reglamento de Aplicación aprobado mediante el Decreto No.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

335-03; la Resolución No. 169-07 y las Normas Complementarias sobre Política de Certificados y Procedimientos de Certificación aprobadas por el Consejo Directivo del INDOTEL.

- 4) La fecha y el resultado de la última auditoría.
- 5) Las medidas adoptadas en caso de haberse recibido recomendaciones.
- 6) Los temas cubiertos por la auditoría.
- 7) La entidad que realizó la auditoría.
- 8) Cumplimiento de los procedimientos establecidos para la verificación y validación de los datos de los Solicitantes.
- 9) Cumplimiento de los procedimientos de generación de las claves de los suscriptores.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

6.2.PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD

Todos los hechos significativos que afecten la seguridad del sistema de la Entidad de Certificación serán almacenados en archivos de transacciones de auditoría, los cuales serán conservados en las instalaciones de la Entidad de Certificación por un período no inferior a un (1) año y posteriormente, archivados en un lugar físico protegido hasta completar un periodo mínimo a diez (10) años

La Entidad de Certificación pone dichos archivos a disposición del INDOTEL, en un plazo que no podrá exceder los cinco (5) días hábiles. La misma documentará los eventos y datos que serán conservados en los registros y se compromete a resguardar en un medio que no pueda ser fácilmente destruido o modificado.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

7. CONFIDENCIALIDAD

7.1. TIPO DE INFORMACIÓN A MANTENER CONFIDENCIAL

Toda información referida a Solicitantes que sea recibida por la Entidad de Certificación y las Unidades de Registro en las solicitudes de emisión de Certificados Digitales es considerada confidencial y no puede hacerse pública, sin el consentimiento previo de los solicitantes o suscriptores, salvo aquellos datos que deben ser publicados en cumplimiento a las normas que rigen las EC y las Unidades de Registro o aquellos casos en que la información sea requerida judicialmente.

La Entidad de Certificación determinará otro tipo de información que deba ser considerada confidencial, debiendo cumplir en todo caso con la normativa vigente en materia de protección de datos personales.

Las Unidades de Registro garantizan la confidencialidad frente a terceros, durante el proceso de generación de las claves privadas de Firma Digital que estas proporcionan. Asimismo, una vez generadas y entregadas las claves privadas, ésta y la Entidad de Certificación se abstendrán de almacenar, copiar o conservar cualquier tipo de información que sea suficiente para reconstruir dichas claves.

7.2. TIPO DE INFORMACIÓN CONSIDERADA NO CONFIDENCIAL

Se considerará como información no confidencial:

- 1) La contenida en la presente Política y en el Manual de Procedimientos de Certificación.
- 2) La información contenida en los Certificados Digitales siempre que el Suscriptor haya otorgado su consentimiento.
- 3) Cualquier información cuya publicidad sea impuesta normativamente.
- 4) Las que así se determinen por el Manual de Procedimientos de Certificación siempre que no contravengan la normativa vigente, lo dispuesto en esta Política de Certificados o los lineamientos de seguridad establecidos por la Entidad de Certificación.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

7.3.DIVULGACIÓN DE INFORMACIÓN DE REVOCACIÓN/SUSPENSIÓN DE CERTIFICADOS DIGITALES

La forma de difundir la información relativa a la suspensión o revocación de un Certificado Digital se realizará mediante la publicación de las correspondientes Lista de Certificados Revocados (LCR).

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

8. IDENTIFICACIÓN Y AUTENTICACIÓN

8.1. REGISTRO INICIAL

8.1.1. Tipos de Nombres

Todos los Suscriptores requieren un nombre distintivo (*DN*, del inglés *Distinguished Name*) conforme al estándar *X.500*.

8.1.2. Pseudónimos

Los pseudónimos no son admitidos.

8.1.3. Reglas Utilizadas para Interpretar Varios Formatos de Nombres

Se atenderá en todo caso a lo marcado por el estándar *X.500* de referencia en la *ISO/IEC 9594*.

8.1.4. Unicidad de los Nombres

La Entidad de Certificación realizará los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los Certificados Digitales emitidos. Los atributos del número de serial (*SN*, del inglés *SerialNumber*) y el Nombre Común (*CN*, del inglés *CommonName*), se usarán para distinguir entre dos DN's similares, y que en todo caso el *SerialNumber* debe ser suficiente para resolver las posibles colisiones entre nombres.

8.1.5. Procedimiento de Resolución de Disputas de Nombres

La indicación de que los nombres deben ser únicos para cada suscriptor de certificado, en el ámbito de la Entidad de Certificación responsable de la emisión.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

8.1.6. Reconocimiento, Autenticación y Función de las Marcas Registradas

No aplica.

8.1.7. Métodos de Prueba de la Posesión de la Clave Privada

Si el par de claves es generado por el Suscriptor, las Unidades de Registro deberán tomar las medidas necesarias que aseguren que el Suscriptor está en posesión de la clave privada asociada a la clave pública del Certificado Digital generado.

8.1.8. Autenticación de la Identidad de una Organización

Los Certificados Digitales emitidos bajo la presente Política identifican a una persona física con vinculaciones a una empresa u organización determinada.

8.1.9. Requerimiento de Autenticación Mediante Presencia Física de la Identidad de un Individuo

Para realizar una correcta verificación de la identidad del solicitante, se deberá atender a lo dispuesto por la legislación vigente de la República Dominicana, mediante la presencia física del mismo.

Los solicitantes de Certificados Digitales remitirán la documentación necesaria ante las Unidades de Registro, una vez efectuada la validación de la información, se procederá a la aprobación de la solicitud sobre cuya base la Entidad de Certificación emitirá el Certificado Digital correspondiente.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

El solicitante debe de validar su identidad ante la Unidad de Registro. Los documentos admitidos son los siguientes:

- 1) Documento de identidad (Cédula de Identidad y Electoral, Licencia de Conducir, Pasaporte u otro documento similar de validez nacional que haya sido previamente autorizado por el INDOTEL), en original y fotocopia.
- 2) Formulario de Solicitud completado.
- 3) Toda otra documentación que le sea requerida como evidencia de los atributos contenidos en el Certificado Digital a emitir bajo el ámbito de esta Política.

8.1.10. Requerimiento de Autenticación Remota de la Identidad de un Individuo

Para realizar una correcta verificación de la identidad del solicitante, se deberá atender a lo dispuesto por la legislación vigente de la República Dominicana, vía remota.

Los solicitantes de Certificados Digitales remitirán la documentación necesaria ante las Unidades de Registro, una vez efectuada la validación de la información, se procederá a la aprobación de la solicitud sobre cuya base la Entidad de Certificación emitirá el Certificado Digital correspondiente.

El solicitante debe de validar su identidad ante la Unidad de Registro, enviando la siguiente documentación al correo electrónico **digifirma@camarasantodomingo.do**:

- Formulario de Solicitud Completado
- Formulario de Autorización Completado
- Copia digital de documento de identidad del usuario de ambos lados debidamente legible y a color
 - Nacionales Dominicanos: Cédula de Identidad y Electoral Dominicana
 - Extranjeros: Pasaporte o Licencia de Conducir
 - Cualquier documento similar de validez nacional que haya sido previamente autorizado por el INDOTEL
- Prueba de vida: El usuario debe grabar un video de máximo 30 segundos donde podamos validar su identidad, en dicho video debe decir la siguiente expresión: "Mi nombre es XXXXXX y esta es mi solicitud para mi certificado de firma digital."

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- Toda otra documentación que le sea requerida como evidencia de los atributos contenidos en el Certificado Digital a emitir bajo el ámbito de esta Política.

8.1.11. Procedimiento Simplificado de Emisión de Certificados Digitales

No aplica.

8.2. REGISTRO

Antes de comenzar una relación contractual, las Unidades de Registro deberán informar al Solicitante de los términos y condiciones relativos al uso del Certificado Digital. Esta información se comunicará a través de un medio perdurable, susceptible de ser transmitido electrónicamente y en un lenguaje comprensible.

Las Unidades de Registro deben comprobar, de acuerdo con la legislación vigente y los lineamientos establecidos en la PC y MPC de la Entidad de Certificación, la identidad y los atributos específicos del Solicitante. La comprobación de la identidad se realizará mediante la autenticación remota o la comparecencia física del Solicitante y la presentación por éste de la Cédula de Identidad y Electoral, Licencia de Conducir o Pasaporte, en caso de ser extranjero para solicitar Certificados Digitales emitidos bajo esta Política.

Se registrará en todo caso:

- 1) Nombre completo del Solicitante.
- 2) Fecha y lugar de nacimiento.
- 3) Número de la Cédula de Identidad y Electoral, Licencia de Conducir o Pasaporte.
- 4) Empresa para la que labora y posición que ocupa en ella;
- 5) Número de Registro Nacional de Contribuyente.

El Solicitante deberá facilitar su dirección física y electrónica u otros datos que permitan contactarse con él.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Las Unidades de Registro deben registrar y conservar toda la información usada para comprobar la identidad de los Solicitante, incluyendo cualquier número de referencia en la documentación empleada para la verificación y los límites de su validez. De igual forma deben guardar el contrato firmado con el Firmante/Suscriptor, el cual incluirá:

- 1) Acuerdo de las obligaciones del Solicitante/Suscriptor.
- 2) Compromiso del Firmante/Suscriptor a usar, en caso de utilizar un dispositivo de creación de firma digital, ofrecido por las Unidades de Registro de forma diligente.
- 3) Consentimiento para que las Unidades de Registro guarden la información usada para el registro, entrega del dispositivo del Firmante/Suscriptor, para una futura revocación, así como para el traspaso de información a una tercera parte en el caso de que la Entidad Certificación cese su actividad.
- 4) Que la información contenida en el Certificado Digital es correcta.

Los registros identificados deberán conservarse durante el período de tiempo estipulado en la legislación Dominicana vigente.

8.2.1. REGISTRO CENTRALIZADO

El suscriptor interesado en adquirir un Certificado Digital, solo debe comunicarse a la Entidad de Certificación, ya sea trasladándose a las oficinas de o comunicación por teléfono o correo electrónico.

El suscriptor debe iniciar el pedido de emisión del certificado al ingresar al sitio Web de la Entidad de Certificación, y completar el formulario de solicitud con los datos requeridos.

Debe trasladarse a la Entidad de Certificación y presentar la siguiente información:

- Documento de identidad
- Código de identificación que le sea requería como evidencia de los árbitros contenido en el certificado a emitir bajo el ámbito de esta política.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

8.2.2. REGISTRO DESCENTRALIZADO

Esta Entidad de Certificación admite la constitución de una o varias Unidades de Registro externas al ámbito donde desarrolla sus actividades. En particular, se admitirán aquellas unidades que se encuentren en condiciones de efectuar un adecuado control de identidad de los suscriptores de certificados que les presentaran una solicitud de emisión, dado el tipo de información que manejan y su cercanía al usuario final.

El funcionamiento de las Unidades de Registro será sometido a la aprobación del INDOTEL. Esta Unidad de Registro asume, como mínimo, las siguientes obligaciones:

- Designar un responsable del proceso de validación de identidad de los suscriptores (Responsable de la Unidad de Registro) y su correspondiente sustituto,
- Cumplir con las obligaciones establecidas en la Política de Certificación y en el Manual de Procedimientos de Certificación de la Entidad de Certificación que ha delegado en dicha unidad las funciones relativas al proceso de validación de identidad de los suscriptores,
- Cumplir con las disposiciones establecidas en la Política de Certificación y en el Manual de Procedimientos de Certificación de la Entidad de Certificación, respecto a la conservación de archivos y documentación respaldatoria referida al proceso de validación de identidad de los suscriptores, y con todas las disposiciones aplicables vigentes,
- Permitir la realización de las auditorias periódicas e inspecciones, por parte de la Entidad de Certificación y del INDOTEL, a fin de garantizar la seguridad del sistema, y el seguimiento de los procedimientos adecuados, e) Toda otra obligación específica que se establezca en el Reglamento de Aplicación de la Ley No. 126-02, sus normas complementarias, esta Política de Certificación y el Manual de Procedimientos de Certificación de la Entidad de Certificación.

Las Unidades de Registro deben adherirse a los términos de la Política de Certificación, del Manual de Procedimientos de Certificación y del resto de la documentación técnica emanada del INDOTEL.

8.3. SOLICITUD DE REVOCACIÓN

Todas las solicitudes de revocación deberán ser autenticadas.

Las solicitudes y los procedimientos empleados para gestionar una revocación serán debidamente documentados.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

La revocación tendrá validez cuando la Unidad de Registro haya efectuado las confirmaciones correspondientes y la comunique de manera formal al suscriptor del Certificado Digital por cualquiera de los siguientes medios:

- 1) Documentos digitales o mensajes de datos firmados digitalmente, transmitidos por protocolos de comunicación electrónica tales como correo electrónico, transferencia de archivos, entre otros.
- 2) Facsímil, con la condición de que el remitente pueda dejar constancia de la recepción.
- 3) Correspondencia con acuse de recibo.
- 4) Otros medios físicos o electrónicos mediante los cuales las Unidades de Registro puedan dejar constancia de la certitud de su recepción.

Las circunstancias por las cuales la Entidad de Certificación procederá a la revocación de los Certificados Digitales emitidos bajo esta política son los siguientes casos:

- 1) A solicitud del suscriptor del Certificado Digital.
- 2) Por iniciativa de las Unidades de Registro.
 - a. Si se determina que un Certificado Digital fue emitido sobre la base de una información errónea que en el momento de la emisión hubiera sido objeto de verificación.
 - b. Si la Entidad de Certificación o las Unidades de Registro determinan que los procedimientos de verificación han dejado de ser seguros.
 - c. Por determinación de que la información contenida en el Certificado Digital ha dejado de ser válida.
- 3) Por Resolución Judicial, debidamente motivada.
- 4) Por declaración judicial de ausencia con presunción de fallecimiento del suscriptor.
- 5) Por declaración mediante sentencia con la autoridad de la cosa irrevocablemente juzgada de incapacidad jurídica del suscriptor.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 6) En caso de que el INDOTEL haya desautorizado a la Entidad de Certificación, siempre y cuando no se haya cedido el Certificado Digital a otra Entidad de Certificación.
- 7) Por la cesación de actividades de la Entidad de Certificación y siempre que no se haya decidido la transferencia del Certificado Digital a otra Entidad de Certificación.

8.4.SOLICITUD DE RENOVACIÓN POSTERIOR A LA REVOCACIÓN (SIN COMPROMISO DE CLAVE PRIVADA)

Los procedimientos de identificación y autenticación a seguir para la renovación de Certificados Digitales una vez que el Certificado Digital está vencido coinciden con los detallados en el punto 10.1 sobre Registro Inicial.

8.5.RENOVACIÓN DE LA CLAVE Y DEL CERTIFICADO DIGITAL

La Entidad de Certificación y las Unidades de Registro deben informar al Firmante/Suscriptor antes de renovar, sobre los términos y condiciones que hayan cambiado respecto de la anterior emisión y en ningún caso emitirá un nuevo Certificado Digital usando la anterior llave pública del Firmante/Suscriptor.

Un Certificado Digital podrá ser renovado un máximo de tres (3) veces y por un período cuya sumatoria de renovaciones no excedan tres (3) años, debiendo proceder a una nueva solicitud una vez transcurrido este plazo siguiendo el procedimiento empleado para una primera solicitud.

La presentación física del solicitante puede no ser necesaria cuando la solicitud de renovación se realice de forma electrónica y utilizando el Certificado Digital aún vigente que se pretende renovar. No obstante lo anterior, se exigirá presencia física siempre que hayan transcurrido más de tres (3) años de la última verificación de la identidad realizada mediante la presencia física del solicitante antes de requerir la generación de un nuevo par de llaves.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

8.6. PERÍODO DE VALIDEZ DE LOS CERTIFICADOS DIGITALES

Los Certificados Digitales emitidos por Entidades de Certificación para la generación de Firmas Digitales tienen un período máximo de validez de tres (3) años a partir de la fecha y hora de emisión.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9. REQUERIMIENTOS OPERACIONALES

9.1. SOLICITUD DE CERTIFICADOS DIGITALES

Las Unidades de Registro asegurarán que los Solicitantes están correctamente identificados y que la petición del Certificado Digital está completa.

El Solicitante deberá presentar el Formulario de Solicitud de Certificado y copia de su Cedula de Identidad y Electoral, además de presentarse ante la UR con la finalidad de comprobar los datos y la identidad del suscriptor/solicitante.

El suscriptor deberá aceptar en forma expresa los Términos y Condiciones bajo las cuales fue emitido el certificado, mediante este mecanismo el suscriptor declara que está consciente de la que la emisión del certificado a su favor implica su autorización de utilizar el mismo con los alcances definidos por las normativas aplicables

.

9.2. EMISIÓN DE CERTIFICADOS DIGITALES

La Entidad Certificación debe poner todos los medios a su alcance para asegurar que la emisión y renovación de Certificados Digitales se realiza de una forma segura. En particular:

- 1) La Entidad de Certificación debe confirmar la unicidad de los *DN* asignados a los Firmantes/Suscriptores.
- 2) La confidencialidad y la integridad de los datos registrados serán especialmente protegidos cuando estos datos sean intercambiados con el Firmante/Suscriptor o entre distintos componentes del sistema de certificación.
- 3) Las Unidades de Registro notificarán al Suscriptor de la emisión de su Certificado Digital.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.3.ACEPTACIÓN DEL CERTIFICADO DIGITAL

Se entenderá como aceptado el Certificado Digital, una vez el Solicitante/Suscriptor haya:

- 1) Firmado el Acuerdo de Términos y Condiciones en el Formulario de solicitud en línea.
- 2) Verifique y constate de forma expresa, por escrito y ante las Unidades de Registro en los casos que se use dispositivo criptográfico, que le es entregado contiene el Certificado Digital solicitado. El solicitante emitirá esta aceptación en su propio nombre.

No obstante, a partir de la entrega del Certificado Digital, el Firmante/Suscriptor dispondrá de un período de siete (7) días naturales para revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a las Unidades de Registro y a la Entidad de Certificación y el contenido del Certificado Digital, dicha discrepancia deberá ser comunicado de inmediato a las Unidades de Registro, de forma que proceda a su revocación y a gestionar la emisión de un nuevo Certificado Digital.

La Entidad de Certificación emitirá el nuevo Certificado Digital sin costo para el Firmante/Suscriptor en el caso de que la diferencia entre los datos sea causada por un error no imputable al mismo. Transcurrido el período de revisión, anteriormente mencionado, sin que haya existido comunicación, se entenderá que el Firmante/Suscriptor ha confirmado y aceptado el Certificado Digital y su contenido.

Aceptando el Certificado Digital, el Firmante/Suscriptor confirma y asume la exactitud del contenido del mismo, con las consiguientes obligaciones que se deriven frente a las Unidades de Registro, la Entidad Certificación o cualquier tercero que de buena fe confíe en el contenido del Certificado Digital. El Certificado emitido se publicará en el portal de la Cámara de Comercio y Producción de Santo Domingo (CCPSD).

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.4.SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS DIGITALES

9.4.1. Suspensión

La suspensión supone la interrupción temporal de la validez de un Certificado Digital, hasta que se decida sobre la oportunidad o no de realizar una revocación.

9.4.1.1. Procedimiento de Solicitud de Suspensión

La Entidad de Certificación y las Unidades de Registro utilizará mecanismos para verificar la identidad del suscriptor o de quien solicita la suspensión, y su capacidad para requerir de tal procedimiento. La misma debe incluir el domicilio, la dirección electrónica, el número telefónico y de facsímil entre otros.

Dicho procedimiento puede ser realizado a través de una llamada telefónica a las Unidades de Registro o por medio de un servicio en línea o electrónico.

Los medios que se admitirán para la comunicación de las solicitudes de suspensión son los siguientes:

- 1) Presentándose personalmente ante la Unidad de Registro.
- 2) Documentos digitales o mensajes de datos firmados digitalmente, transmitidos por protocolos de comunicación electrónica tales como correo electrónico, transferencia de archivos, entre otros.
- 3) Facsímil, con la condición de que el remitente pueda dejar constancia de la recepción.
- 4) Correspondencia física con acuse de recibo.
- 5) Otros medios físicos o electrónicos mediante los cuales la Entidad de Certificación y las Unidades de Registro puedan dejar constancia de la certitud de su recepción.

La información relativa al estado de suspensión estará disponible las veinticuatro (24) del día, los siete (7) días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la Entidad de Certificación, la misma deberá confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el período máximo dispuesto en esta política.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
	Área Responsable	Cargo Responsable	Fecha de Creación
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

La Entidad de Certificación solo aceptara las solicitudes de suspensión que se reciban bajo estas medidas. Quien proceda a realizar la solicitud deberá demostrar, de modo indudable, su identidad y capacidad para solicitar este procedimiento.

Toda solicitud deberá dirigirla a:

Teléfono: 809.682.2688 ext. 2334

Dirección: Av. 27 de Febrero esq. Alma Mater No. 225, La Esperilla

Correo: digifirma@camarasantodomingo.do

9.4.1.2. Causas de Suspensión de Certificados Digitales

Las causas de suspensión de un Certificado Digital pueden ser por:

- 1) Requerimiento de la entidad a la cual el Certificado Digital o Suscriptor están vinculados.
- 2) La iniciación del trámite de ausencia con presunción de fallecimiento del suscriptor del Certificado Digital;
- 3) Solicitud de las Unidades de Registro por razones, técnicas y/o administrativas.
- 4) La decisión de la Entidad de Certificación en virtud de razones técnicas, circunstancia que será comunicada en forma inmediata en un plazo máximo de veinticuatro (24) horas al suscriptor del Certificado Digital y al INDOTEL, por los medios establecidos en el Artículo No. 51 del Reglamento de Aplicación de la Ley No. 126-02.
- 5) Sentencia de un tribunal con la autoridad de la cosa irrevocablemente juzgada debidamente fundada.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.4.1.3. Límites del Período de Suspensión

Tanto la Entidad de Certificación, como las Unidades de Registro deben ejercer los esfuerzos necesarios para confirmar que un Certificado Digital no permanezca suspendido por más tiempo que los indicados a continuación:

Casos	Duración
Extravío o pérdida temporal del dispositivo de almacenamiento del Certificado Digital	Suspensión por un período mayor de una (1) semana

9.4.2. Revocación

Se entenderá por revocación aquel cambio en el estado de un Certificado Digital motivado por la pérdida de validez de un Certificado Digital en función de alguna circunstancia distinta a la caducidad del mismo. Al hablar de revocación nos referiremos a la pérdida de validez definitiva.

9.4.2.1. Procedimiento de Solicitud de Revocación

La Entidad de Certificación y las Unidades de Registro utilizarán mecanismos para verificar la identidad del suscriptor o de quien solicita la revocación, y su capacidad para requerir de tal procedimiento. La misma debe incluir el domicilio, la dirección electrónica, el número telefónico y de Facsímil entre otros.

La revocación de un Certificado Digital podrá solicitarse por el Suscriptor, las Unidades de Registro o un representante de la entidad a la cual está vinculado el Suscriptor, en caso de que aplique. Todas las solicitudes deberán ser en todo caso autenticadas.

Dicho procedimiento puede ser realizado a través de una llamada telefónica a la Unidad de Registro correspondiente o por medio de un servicio en línea o electrónico.

Los medios que se admitirán para la comunicación de las solicitudes de suspensión son los siguientes:

- 1) Presentándose personalmente ante la Unidad de Registro.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 2) Documentos digitales o mensajes de datos firmados digitalmente, transmitidos por protocolos de comunicación electrónica tales como correo electrónico, transferencia de archivos, entre otros.
- 3) Facsímil, con la condición de que el remitente pueda dejar constancia de la recepción.
- 4) Correspondencia física con acuse de recibo.
- 5) Otros medios físicos o electrónicos mediante los cuales la Entidad de Certificación y las Unidades de Registro puedan dejar constancia de la certitud de su recepción.

La Entidad de Certificación requiere de la autorización y aprobación por la Unidad de Registro a la que pertenece el Certificado Digital de las peticiones de revocación para ejecutar dicha solicitud.

El plazo entre la recepción de una petición de revocación y su paso al estado de suspendido, no será mayor a tres (3) horas. Toda información relativa a este procedimiento estará disponible para los interesados en las páginas de Internet correspondientes. En lo que respecta al Suscriptor cuyo Certificado Digital haya sido revocado, deberá ser informado del cambio de estado de su Certificado Digital.

El servicio de gestión de las revocaciones estará disponible las veinticuatro (24) horas del día, los siete (7) días de la semana. En caso de fallo del sistema, servicio o cualquier otro factor que no esté bajo el control de la Entidad Certificación, la misma deberá confirmar que este servicio no se encuentre indisponible durante más tiempo que el período máximo dispuesto en esta Política.

Se deberá confirmar la autenticidad y la confidencialidad de la información relativa al estado de los Certificados Digitales.

La información relativa al estado de los Certificados Digitales estará disponible públicamente a través de los LCR o un servicio en línea.

9.4.2.2. Causas de Revocación

Los Certificados Digitales pueden ser revocados cuando concurra alguna de las circunstancias siguientes:

- 1) Solicitud voluntaria del Firmante/Suscriptor.
- 2) Pérdida o inutilización por daños del soporte del dispositivo criptográfico.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 3) Fallecimiento del Firmante/Suscriptor o incapacidad sobrevenida, total o parcial.
- 4) Cese en la actividad del prestador de servicios de certificación salvo que los Certificados Digitales expedidos por aquel sean transferidos a otro prestador de servicios.
- 5) Inexactitudes graves en los datos aportados por el Suscriptor para la obtención del Certificado Digital, así como la concurrencia de circunstancias que provoquen que dichos datos, originalmente incluidos en el Certificado Digital, no se adecuen a la realidad.
- 6) Que se detecte que las claves privadas del Suscriptor o de la Entidad de Certificación han sido comprometidas, bien porque concurren las causas de pérdida, robo, hurto, modificación, divulgación o revelación de las claves privadas, bien por cualquiera otra circunstancia, incluidas las fortuitas, que indiquen el uso de las claves privadas por persona distinta al titular.
- 7) Por incumplimiento por parte de la Unidad de Registro, la Entidad de Certificación o el Suscriptor de las obligaciones establecidas en esta Política, el Manual de Procedimientos de Certificación, la Ley No. 126-02, su Reglamento de Aplicación y las normas complementarias del INDOTEL, o por otro acuerdo o regulación aplicable al Certificado Digital.
- 8) Por la resolución del contrato con el Suscriptor.
- 9) Por cualquier causa que razonablemente induzca a creer que el servicio de certificación haya sido comprometido hasta el punto que se ponga en duda la fiabilidad del Certificado Digital.
- 10) Por resolución judicial o administrativa que lo ordene.
- 11) Si la Entidad de Certificación determina que el Certificado Digital no fue emitido de acuerdo a los Estándares Tecnológicos dictados por el INDOTEL.
- 12) Por ausencia o desaparición definitivamente declarada por autoridad competente, de acuerdo a lo prescrito por el derecho común;
- 13) Por liquidación del suscriptor en el caso de las personas jurídicas;
- 14) Por la confirmación de que alguna información o hecho contenido en el certificado es falso;
- 15) La revocación tendrá lugar:
 - A petición del suscriptor o un tercero en su nombre y representación legal;

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- Por solicitud de la Entidad de Certificación,
- Por solicitud de la Unidad de Registro,
- Por requerimiento de una instancia judicial,
- Por decisión del INDOTEL, con causa fundada en la cesación de la actividad de la Entidad de Certificación y siempre que no medie la transferencia del certificado a otra Entidad de Certificación.

9.4.2.3. Requisitos Especiales en Caso de Compromiso de la Clave Privada

En caso de que se presentase una situación en la cual la Clave Privada del Certificado Digital, el suscriptor tendría que dirigirse a la Entidad de Certificación de manera inmediata, tanto vía telefónica como de manera física.

9.4.2.4. Período de Revocación

La decisión de revocar o no un Certificado Digital, no podrá retrasarse por un período máximo de 2 semanas, salvo aquellos períodos establecido para la suspensión de un Certificado Digital.

9.4.3. Lista de Certificados Revocados (LCR)

La LCR será generada y firmada únicamente por la Entidad de Certificación. La frecuencia de actualización de dicha lista será como mínimo cada veinticuatro (24) horas.

Los terceros que confían deben comprobar el estado de los Certificados Digitales en los cuales van a confiar, verificando el estado del Certificado Digital en el momento de recepción de cualquier comunicación o de cualquier dato electrónico.

9.4.4. Disponibilidad de consulta de estado de Certificados Digitales

Se proporcionará un servicio en línea de consulta de estados de Certificados Digitales, el cual estará disponible las veinticuatro (24) horas del día los siete (7) días de la semana. En caso de fallo del sistema, del servicio o de cualquier otro factor que no esté bajo el control de la Entidad Certificación, la misma deberá

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

realizar los esfuerzos que estén a su alcance para confirmar que este servicio de información no se encuentre indisponible durante más tiempo que el período máximo dispuesto en esta política.

Las Unidades de Registro dispondrán de un sistema de consulta que impida la obtención masiva de datos relativos a los Suscriptores, por lo que para la obtención del estado de un Certificado Digital deberán conocerse algunos parámetros del mismo como el correo electrónico.

No obstante lo anterior, el acceso a este sistema de consulta de Certificados Digitales será libre y gratuito.

9.5.DISTRIBUCIÓN DE CERTIFICADOS DIGITALES

Para los fines de este documento las Unidades de Registro pondrá a disposición de los Firmantes/Suscriptores los Certificados Digitales de la siguiente manera:

- 1) Una vez generado el Certificado Digital, el mismo se entregará mediante correo electrónico o en un dispositivo criptográfico a disposición del suscriptor a nombre de quien fue emitido, el cual contendrá datos precisos y completos.
- 2) Podrán identificarse mediante el número de *OID* correspondiente a esta Política, los términos y condiciones aplicables a cada Certificado Digital.

Que una vez generado, el certificado se ponga a disposición del suscriptor a nombre de quien fue emitido, el cual contendrá datos precisos y completos;

Que los certificados se encuentren disponibles para los usuarios en los términos y condiciones pautadas para el uso de los mismos;

Que puedan identificarse fácilmente los términos y condiciones aplicables a cada certificado;

Que la información mencionada en b) y c) se encuentre disponible 24 horas, 7 días a la semana. Ante fallas en el sistema o servicio u otras circunstancias que excedan su control, la Entidad de Certificación indicará los mecanismos que empleará para asegurar que el período de restablecimiento del servicio no exceda el máximo fijado para esta Política y por su Manual de Procedimientos de Certificación; y

Que la información mencionada en los puntos b) y c) se encuentre disponible al público en general, tanto del ámbito nacional como internacional.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.6.CONTROLES DE SEGURIDAD

La Entidad de Certificación y las Unidades de Registro deberán realizar los esfuerzos que estén a su alcance para asegurar que toda la información relevante y concerniente a un Certificado Digital sea conservada durante el período de tiempo que pueda ser necesario a efectos probatorios en los procedimientos legales.

9.6.1. Aspectos Generales

Los siguientes puntos son partes integras de la Infraestructura de la Entidad de Certificación y de la Unidad de Registro:

- 1) Asegurar la confidencialidad y la integridad de los registros relativos a los Certificados Digitales, tanto de los actuales como de aquellos que hayan sido previamente almacenados.
- 2) Los registros relativos a los Certificados Digitales deberán ser almacenados completa y confidencialmente de acuerdo con las mejores prácticas para sistemas de Infraestructura de Clave Pública.
- 3) Los registros relativos a los Certificados Digitales deberán estar disponibles, si estos son requeridos, a efectos probatorios en los procedimientos legales.
- 4) El momento exacto en que se produjeron los eventos relativos a la gestión de las claves y la gestión de los Certificados Digitales deberá ser almacenado.
- 5) Los registros relativos a los Certificados Digitales serán mantenidos durante el período de tiempo establecido en la legislación vigente.
- 6) Los eventos se registrarán de manera que no puedan ser fácilmente borrados o destruidos durante un período no menor de un (1) año.
- 7) Los eventos específicos y la fecha de registro serán documentados por la Entidad de Certificación y las Unidades de Registro.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.6.2. Generación del Certificado Digital

La Entidad de Certificación registrará todos los eventos relativos al ciclo de vida de las claves de la Entidad Certificación y de los Certificados Digitales.

9.6.3. Entrega del dispositivo al suscriptor

Es responsabilidad de las Unidades de Registro de registrar y documentar la entrega de los dispositivos criptográficos con el Certificado Digital correspondiente al Firmante/ Suscriptor.

9.6.4. Gestión de la revocación

La Entidad de Certificación y las Unidades de Registro deberán realizar los esfuerzos que estén a su alcance para confirmar que las peticiones e informes relativos a una revocación, así como su resultado, sean debidamente registrados.

9.6.5. Tipos de eventos registrados

La Entidad de Certificación y las Unidades de Registro registrarán y guardarán todos los eventos de seguridad relativos al sistema de Certificación, los cuales incluirán:

- 1) Encendido y apagado del sistema.
- 2) Encendido y apagado del sistema de Certificación.
- 3) Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- 4) Cambios en los detalles de la Entidad de Certificación y/o sus claves.
- 5) Cambios en la creación de Política de Certificados.
- 6) Intentos de inicio y fin de sesión.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
	Área Responsable	Cargo Responsable	Fecha de Creación
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 7) Intentos de accesos no autorizados al sistema de Certificación a través de la red.
- 8) Intentos de accesos no autorizados al sistema de archivos.
- 9) Generación de claves propias.
- 10) Creación y revocación de Certificados Digitales.
- 11) Intentos de dar de alta, eliminar, habilitar y deshabilitar Suscriptores y actualizar su información.
- 12) Acceso físico a los registros de eventos.
- 13) Cambios en la configuración y mantenimiento del sistema.
- 14) Cambios del personal.
- 15) Registros de la destrucción de los medios que contienen las claves y datos de activación.

9.6.6. Frecuencia de procesamiento de registro de eventos (bitácoras)

La Entidad de Certificación y las Unidades de Registro deberán revisar sus bitácoras cada veinticuatro (24) horas y en todo caso cuando se produzca una alerta del sistema por algún incidente, debe asegurarse de que los eventos no han sido manipulados y deberán documentar las acciones tomadas ante esta revisión.

9.6.7. Períodos de retención para auditoría de eventos

La información relacionada a las operaciones con los Certificados Digitales y susceptibles de auditoría, deberán ser conservadas por lo menos durante cuarenta (40) años.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

9.6.8. Protección de las bitácoras para auditoría

El respaldo de la bitácora o almacenamiento de los eventos debe ser hecho sobre un medio físico tomando en consideración proveerle de las condiciones óptimas para evitar amenazas de temperatura, humedad, fuego y magnetización.

Solamente personal autorizado puede visualizar los registros. Se han implementado niveles de protección de los registros de auditoría a fin de evitar modificaciones no autorizadas en los mismos. Al igual que posible borrado de registros.

9.6.9. Procedimientos de respaldo de las bitácoras de auditoría

Existe un procedimiento adecuado de respaldo, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un período corto de tiempo las correspondientes copias de respaldo de los eventos.

9.6.10. Sistema de recogida de información de auditoria

No estipulado.

9.7.ARCHIVOS

9.8.Archivado de la Entidad de Certificación

Los datos y la documentación de apoyo que debe conservar y archivar la Entidad de Certificación son:

- 1) Solicitudes de emisión, renovación, suspensión y revocación de Certificados Digitales.
- 2) Certificados Digitales emitidos y revocados.
- 3) Lista de Certificados Revocados.
- 4) Comunicación entre los aplicativos del sistema de certificación y las Unidades de Registro.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 5) Toda Comunicación relevante entre la Entidad de Certificación y el INDOTEL.
- 6) Los elementos listados en los puntos 1), 2) y 3), serán conservados por el período establecido por la legislación vigente.

9.9. Archivado de las Unidades de Registro

En el caso de la Unidad de Registro, esta debe conservar y archivar los siguientes datos y documentación de apoyo:

- 1) Todas las solicitudes de emisión, renovación, suspensión y revocación de Certificados Digitales y toda información y documentación que avale el proceso de identificación.
- 2) Las Reclamaciones y/o quejas presentadas por los suscriptores y usuarios.
- 3) Los archivos de auditoría correspondientes a dichas unidades.
- 4) Toda comunicación relevante entre la Entidad de Certificación, las Unidades de Registro y los suscriptores.
- 5) La información y documentación mencionada debe conservarse por un plazo mínimo de diez (10) años.

Los elementos listados 1), 2) y 3), serán conservados por el periodo establecido por la legislación vigente.

9.9.1. Protección del archivo

El respaldo de los archivos debe ser hecho sobre un medio físico tomando en consideración proveerle de las condiciones óptimas para evitar amenazas de temperatura, humedad, fuego y magnetización.

9.9.2. Procedimientos de respaldo de archivo

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Existe un procedimiento adecuado de respaldo, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un período corto de tiempo las correspondientes copias de respaldo de los eventos.

9.10. SITUACIONES DE EMERGENCIA

9.10.1. PLAN DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRES

La Entidad de Certificación ha desarrollado e implementado un Plan de Contingencias apropiado para sus instalaciones, que garantice la continuidad de las operaciones críticas. Dicho plan garantiza el mantenimiento mínimo de la operación, contemplando la recepción de solicitudes de revocación y el acceso a la Lista de Certificados Revocados.

De igual forma este plan contempla la puesta en operaciones de las aplicaciones críticas dentro de las primeras veinticuatro (24) horas de haberse detectado el origen de la emergencia.

La Entidad de Certificación vela por que las Unidades de Registro cumplan con un Plan de Contingencia y con tiempo de respuestas acorde a lo que en este documento se ha establecido. El plan contempla una simulación de por lo menos una vez al año.

Ver Plan de Contingencia y Continuidad de Negocios.

9.10.2. Plan de protección de claves

La Entidad de Certificación ha implementado procedimientos a cumplir cuando su clave privada se vea vulnerada y/o comprometida. Incluye las medidas a tomar en cuenta para revocar los Certificados Digitales emitidos y notificar en forma inmediata a la Unidad de Registro, sus suscriptores y terceros que confían. La misma deberá realizar los esfuerzos que estén a su alcance para garantizar que la clave privada de la Entidad de Certificación será restablecida tan pronto como sea posible.

En todo caso que la Entidad de Certificación considere que su clave privada ha sido comprometida, la misma procederá a:

- 1) Informar al INDOTEL, la Unidad de Registro, a los Suscriptores, a las entidades que están vinculados los suscriptores terceros que confían y otras EC's con los cuales tenga acuerdos u otro tipo de relación del compromiso.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 2) Proceder con la revocación del Certificado Raíz de la Entidad de Certificación.
- 3) Se eliminan el par de claves de la Entidad de Certificación.
- 4) Se generan un nuevo par de claves para la Entidad de Certificación.
- 5) Emitir un Certificado Raíz nuevo.
- 6) Notificar al INDOTEL, a todos los suscriptores y a la Unidad de Registro, que los Certificados Digitales emitidos con la clave privada comprometida han sido revocados. Indicar que los Certificados Digitales emitidos con dicha clave han sido revocados.

9.10.3. Instalación de seguridad después de un desastre natural u otro tipo de desastre

La Entidad de Certificación debe tener un plan apropiado de contingencias para la recuperación en caso de desastres y debe restablecer los servicios de acuerdo con esta política dentro de las veinticuatro (24) horas posteriores a un desastre o emergencia imprevista. Tal plan incluirá una prueba completa y periódica de la preparación para tal restablecimiento.

9.11. CESE DE LA ENTIDAD CERTIFICACIÓN

La Entidad de Certificación deberá emplear los posibles esfuerzos para minimizar los perjuicios que se puedan crear a los Suscriptores o terceros que confían como consecuencia del cese de su actividad y en particular del mantenimiento de los registros necesarios a efectos probatorios en los procedimientos legales.

Antes del cese de su actividad deberá realizar, como mínimo, las siguientes actuaciones:

- 1) Informar a la Unidad del Registro y todos los Suscriptores, terceros que confían y otras EC's con los cuales tenga acuerdos u otro tipo de relación del cese.
- 2) La Entidad de Certificación revocará toda autorización a las Unidades de Registro.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 3) La Entidad de Certificación realizará las acciones necesarias para transferir sus obligaciones relativas al mantenimiento de la información del registro y de las bitácoras durante el período de tiempo indicado a los Suscriptores y terceros que confían.
- 4) Las claves privadas de la Entidad de Certificación serán destruidas.
- 5) La Entidad de Certificación tendrá contratado un seguro de responsabilidad civil en cumplimiento a la legislación vigente.
- 6) Debe ejecutar todas las acciones necesarias para transferir el mantenimiento de los registros que sustenten sus procesos de emisión de Certificados Digitales, por un período establecido por la legislación vigente.

Se establecerán en el MPC las previsiones hechas para el caso de cese de actividad, estas incluirán:

- 1) Informar a las organizaciones afectadas.
- 2) Transferencia de las obligaciones de la Entidad de Certificación a otras partes previo acuerdo con las Unidades de Registro afectada.
- 3) Procedimiento sobre cómo debe ser tratada la revocación de los Certificados Digitales emitidos cuyo período de validez aún no ha expirado.

En particular, la Entidad Certificación deberá:

- 1) Informar puntualmente a las Unidades de Registro, a todos los Suscriptores, a las entidades a la que están vinculados los Suscriptores y los Certificados Digitales, empleados, terceros que confían con una anticipación mínima de seis (6) meses antes del cese.
- 2) Transferir todas las bases de datos importantes, archivos, registros y documentos a las Unidades de Registro o entidad designada durante las veinticuatro (24) horas siguientes a su terminación.

10. CONTROLES DE SEGURIDAD FÍSICA, PROCEDIMENTAL Y DE PERSONAL

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
	Área Responsable	Cargo Responsable	Fecha de Creación
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

En consonancia con la normativa y los lineamientos técnico y regulatorios, nacionales e internacionales, aprobados por el INDOTEL, la Entidad de Certificación debe cumplir con un serie de controles físicos, de procedimientos y de personal que le permitan realizar las funciones de autenticación, emisión, renovación, suspensión y revocación de Certificados Digitales, auditoria y archivo bajo mecanismos seguros.

De igual forma, es necesario tomar en cuenta los controles de seguridad no técnicos que permitan garantizar que las operaciones de la Entidad de Certificación, las Unidades de Registro y Suscriptores se realicen bajo el menor riesgo posible.

10.1. CONTROLES DE SEGURIDAD FÍSICA

La Entidad de Certificación deberá velar por que el acceso físico a los servicios críticos y que los riesgos físicos de estos elementos sean minimizados, permitiendo:

- 1) Evitar la intervención en los procesos de gestión de Certificados Digitales.
- 2) Controlar los accesos no autorizados al Sistema de Certificación.
- 3) Impedir la pérdida, daño o compromiso de los activos de la empresa y la interrupción de la actividad.
- 4) Evitar el compromiso o robo de información.
- 5) Asegurar la protección física del área donde se gestionan las operaciones de los Certificados Digitales.
- 6) Garantizar la implementación de los controles de seguridad física y medioambiental para proteger las instalaciones que albergan los recursos del sistema al igual que la entrega del dispositivo del Suscriptor.

10.2. Ubicación y construcción

La Entidad de Certificación ha contratado los servicios de hospedaje de la compañía Norteamericana *Quality Technology Services (QTS)* ubicados en el estado de la Florida de los Estados Unidos de

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Norteamérica. La contratación de los servicios de QTS le permiten a la Entidad de Certificación con el estándar ANSI/TIA-942, sobre Diseño y Construcción de Centro de Datos cumpliendo con el nivel de Tolerancia de Falla *Tier 4*.

10.3. Hardware Criptográfico

Los dispositivos de almacenamiento serán opcional para el cliente con un costo adicional al servicio de emisión de Certificado Digital.

Tarjetas Criptográficas,
Código PIN de Seguridad
Soporte de Certificados Digital para Estándar de PKI X.509 v3.
Sistema de algoritmo integrado DES, 3DES, MD5, SHA-1, SHA-256, RSA 1024, RSA 2048
Interfaces PKCS#11 y MS-CAPI para infraestructuras de seguridad.
Espacio de datos 64KB.

Lectora:

Interfaz USB

Avalado en cumplimiento de los estándares:

ISO 7816-1/2/3

RoHS

PC/SC

CCID

IEC/ EN 60950

Nivel 1 de Especificaciones EMV 2000

Soporte para Windows 2000SP2/XP/Server2003/Vista/Server2008/7, Windows CE y Linux 2.6+

USB Criptográfico:

Dispositivo Aprobado por Estándares FIPS para algoritmos RSA DES 3-DES SHA-1 y MD5

Soporte de generación de llaves RSA de 1024-bit/2048-bit

Soporte de algoritmos RC4 y SHA-2

Memoria segura con capacidad de hasta 64K

Soporte para almacenar múltiples llaves

Estándar de Certificados de formato X.509 v3

Soporte de Sistemas Operativos: Windows 98SE/Me/2000/XP/Vista/Server 2003/Server2008, Linux y MacOS

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

10.4. Acceso físico

El acceso físico al Centro de Datos debe estar disponible veinticuatro (24) horas al día, los siete (7) de la semana, los trescientos sesenta y cinco (365) del año, y debe contar con al menos dos (2) de tres (3) niveles de verificación para acceder a los sistemas:

- 1) Registro de Usuario Autorizado.
- 2) Control de Acceso.
- 3) Sistema Biométrico.

10.5. Alimentación eléctrica y Aire Acondicionado

El sistema de alimentación eléctrica y aire acondicionado de la Entidad de Certificación debe cumplir como mínimo con el estándar de Tolerancia de Fallas *Tier 1*, en cumplimiento con las Normas Complementarias del INDOTEL y los estándares internacionales de Infraestructura de Clave Pública (ICP), para garantizar la disponibilidad del servicio.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

10.6. Exposición al agua

El Centro de Datos de la Entidad de Certificación y las Unidades de Registro deben cumplir como mínimo con el estándar de Tolerancia de Fallas *Tier 1*, en cumplimiento con las Normas Complementarias del INDOTEL y los estándares internacionales de Infraestructura de Clave Pública (ICP), sobre protección de exposición de agua.

10.7. Protección y prevención de incendios

La Entidad de Certificación y las Unidades de Registro deben cumplir al menos con los lineamientos del estándar de Tolerancia de Fallas *Tier 1*, en cumplimiento con las Normas Complementarias del INDOTEL y los estándares internacionales de Infraestructura de Clave Pública (ICP), sobre sistemas de prevención y protección contra incendios.

10.8. Sistema de Almacenamiento

La Entidad de Certificación y las Unidades de Registro deberán confirmar que el sistema de almacenamiento usado está protegido de riesgos medioambientales como la temperatura, la humedad y la magnetización, al igual que mantener un respaldo de toda la información almacenada.

10.9. Eliminación de Residuos

La Entidad de Certificación y las Unidades de Registro deberán confirmar que los medios usados para almacenar o transmitir la información de carácter sensible como las claves, datos de activación o archivos críticos serán destruidos, así como que la información que contengan será irrecuperable.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

10.10. Respaldo.

La Entidad de Certificación cuenta un respaldo de la información y datos relativos al sistema de certificación, como el sistema mismo, un nivel mínimo de Tolerancia de Fallas *Tier 1*, en cumplimiento con las Normas Complementarias del INDOTEL y los estándares internacionales de Infraestructura de Clave Pública (ICP), para garantizar la disponibilidad del servicio.

10.11. CONTROLES PROCEDIMENTALES

La seguridad operativa de la Entidad de Certificación está basada en un modelo de roles que permiten segregar las funciones y responsabilidades de las diferentes actividades que permiten el funcionamiento de dicha entidad.

Los siguientes controles deben establecer los lineamientos procedimentales que la Entidad de Certificación y la Unidades de Registro deben cumplir.

Los roles de confianza incluyen las siguientes responsabilidades:

- 1) Responsable de Seguridad: asume las obligaciones relativas a la implementación de las políticas de seguridad, así como gestión y revisión de eventos y/o bitácoras.
- 2) Auditor de Sistemas: Realiza las labores de supervisión y control de la implementación de las políticas de seguridad.
- 3) Administradores de Sistemas: Están autorizados para instalar, configurar y mantener de los sistemas y aplicaciones que soportan las operaciones del Sistema de Certificación.
- 4) Operador de Sistemas: Está autorizado para realizar funciones relacionadas con el Sistema de respaldo y de recuperación.
- 5) Administrador de EC: Responsable de la administración y controles de gestión del Sistema de Certificación.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 6) Operador del EC: Realizan funciones de apoyo en el control dual de las operaciones del Sistema de Certificación.
- 7) Administrador de la Unidad de Registro: Responsables de la aprobación y firma de las solicitudes de Certificado Digital.
- 8) Operadores de la Unidad de Registro: Responsables de la validación y verificación de los datos de la solicitud de Certificado Digital.

Adiciona a lo anterior las siguientes tareas específicas requieren de la participación de al menos dos (2) personas:

- 1) La generación e implementación de las claves de la Entidad Certificación.
- 2) La recuperación y respaldo de la clave privada de la Entidad de Certificación.
- 3) Cualquier actividad realizada sobre los recursos tecnológicos que dan soporte a la Entidad de Certificación.

10.12. CONTROLES DE SEGURIDAD DE PERSONAL

10.12.1. Procedimientos de Calificación para Roles de Confianza

La Entidad de Certificación y las Unidades de Registro deberán confirmar que el personal asignado a los roles de confianza cumple con los requisitos mínimos para el desempeño de sus funciones, tomando en consideración los siguientes elementos:

- 1) El personal debe de tener conocimiento, experiencia y calificaciones necesarias y apropiadas para el puesto que desempeñará.
- 2) Las responsabilidades de los roles de confianza indicadas en esta Políticas serán documentadas en la descripción de puesto.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 3) El rol debe definir los privilegios con los que cuentan, los niveles de acceso y una diferenciación entre las funciones generales y las funciones específicas de la Entidad de Certificación y/o las Unidades de Registro.
- 4) El personal llevará a cabo los procedimientos administrativos y de gestión de acuerdo con los procedimientos especificados para la gestión de la seguridad de la información.
- 5) Deberá ser empleado el personal de gestión con responsabilidades en la seguridad que posea experiencia en tecnologías de firma electrónica y esté familiarizado con procedimientos de seguridad.
- 6) Todo el personal implicado en roles de confianza deberá estar libre de intereses que pudieran perjudicar su imparcialidad en las operaciones de la EC y/o Unidades de Registro.
- 7) La Entidad de Certificación no asignará funciones de gestión a una persona cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones.

10.12.2. Requerimientos de Formación

La Entidad de Certificación y las Unidades de Registro deben procurar que el personal que realiza las tareas operativas reciba la formación relativa a:

- 1) los principales mecanismos de Seguridad de Sistemas de Información.
- 2) sistemas de Infraestructura de Clave Pública (ICP) utilizada.
- 3) funciones relativas a operaciones de Infraestructura de Clave Pública (ICP).
- 4) procedimientos de recuperación de desastres y planes de contingencia.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

10.12.3. Requerimientos y Frecuencia de la Actualización de la Formación

La Entidad de Certificación y las Unidades de Registro de la Cámara de Comercio y Producción de Santo Domingo, cumplirán con el programa de formación establecido por la Gerencia de Recursos Humanos a fin de garantizar que el personal está desarrollando sus funciones correctamente.

10.12.4. Sanciones por Acciones No Autorizadas

La Cámara de Comercio y Producción ha establecido sanciones mediante las Normas de Conducta y Acción Disciplinaria, en la cual establece las sanciones dirigido al personal de la Entidad de Certificación y las Unidades de Registro por acciones no autorizadas.

10.12.5. Requerimientos de Contratación de Personal

La Entidad de Certificación debe seguir Política de Contratación e Ingreso de Personal, la cual provee seguridad razonable que garantiza la confiabilidad y competencia del personal en el adecuado cumplimiento de sus funciones. Este documento establece los requisitos que debe cumplir el personal de la Entidad de Certificación, en cuanto a probidad, ética, moral y capacidad profesional.

10.12.6. Documentación Proporcionada al Personal

Todo el personal de la Entidad de Certificación y las Unidades de Registro deben recibir los Manuales de Usuario en los que se detallen al menos los procedimientos para el gestionar las operaciones relativas a las solicitudes de emisión, renovación, suspensión y revocación de Certificados Digitales y la funcionalidad del Sistema empleado.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11. CONTROLES DE SEGURIDAD TÉCNICA

11.1. GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES

11.1.1. Generación del Par de Claves de la Entidad Certificación

La Entidad de Certificación deberá confirmar que las claves de la Entidad de Certificación sean generadas de acuerdo a los estándares aprobados por el INDOTEL, es decir:

- 1) La generación de la clave de la Entidad Certificación se realizará en un entorno asegurado físicamente por el personal adecuado según los roles de confianza y, al menos con un control dual.
- 2) El personal autorizado para desempeñar estas funciones estará limitado a aquellos requerimientos desarrollados en el MPC.
- 3) La generación de la clave de la Entidad Certificación se realizará cumpliendo con los requerimientos que se detallan en el *FIPS 140-2*.

11.1.2. Generación del Par de Claves de Firmante/Suscriptor

Para fines de la presente Política, las claves del Suscriptor son generadas utilizando sistemas operativos, aplicaciones, programas o dispositivos criptográficos que pertenezcan al Suscriptor, y con la asistencia de los Operadores de las Unidades de Registro o Soporte Técnico de la entidad a la cual están vinculados y se deberán tomar en consideración los siguientes puntos:

- 1) Las claves serán generadas usando los algoritmos autorizados por el INDOTEL.
- 2) Las claves tendrán una longitud fija de 2048 bits.
- 3) Las claves no deberán ser exportadas o extraídas del dispositivo o módulo criptográfico.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.1.3. Entrega de la Clave Privada al Firmante/Suscriptor

El par de claves generadas para Certificados Digitales de esta Políticas son generadas en sistemas operativos, aplicaciones, programas o dispositivos criptográficos del Suscriptor, por lo que la entrega de las claves en dispositivo se hace de forma segura y tomando en consideración el apartado 11.7.3.

Adicionalmente, para hacer la entrega al dispositivo criptográfico, se debe entregar un Manual de Instrucciones para el remplazo de la clave de acceso del dispositivo.

11.1.4. Entrega de la Clave Pública del Firmante/Suscriptor al Emisor del Certificado Digital

Cuando el Suscriptor genera sus propias claves, la clave pública del mismo debe transferirse desde la Unidad de Registro correspondiente al dispositivo de forma segura garantizando que no ha sido cambiado durante el traslado; que el remitente está en posesión de la clave privada que se corresponde con la clave pública transferida; y, que el proveedor de la clave pública es el legítimo usuario que aparece en el Certificado Digital.

El requerimiento de un certificado debe emitirse en formato PKCS#10, según lo establecido en los Estándares Tecnológicos de Firma Digital aprobados por el INDOTEL, o bien en los que se establezcan posteriormente, de acuerdo a los avances tecnológicos.

11.1.5. Entrega de la Clave Pública de la Entidad de Certificación a los Terceros que Confían

La Entidad de Certificación entrega a través de su página de Web <http://www.camarasantodomingo.do> el acceso a su Certificado Raíz y clave pública.

11.1.6. Tamaño y Período de Validez de las Claves del Emisor

El emisor utilizará llaves basadas en algoritmo *RSA* con una longitud mínima de *2048 bits* para firmar Certificados Digitales.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Los períodos de validez de las claves privadas de la Entidad de Certificación estarán determinadas por el período de validez de los Certificados Raíz utilizados por la misma. Los mismos están publicados en la página Web (<http://www.camarasantodomingo.do>) de la Entidad de Certificación.

11.1.7. Tamaño y Período de Validez de las Claves del Suscriptor

El Suscriptor deberá usar claves basadas en el algoritmo *RSA* con una longitud fija de 2048 bits.

El período de uso de la clave pública y privada del Firmante/Suscriptor no deberá ser superior a tres (3) años y no excederá del período durante el cual los algoritmos de criptografía aplicada y sus parámetros correspondientes dejan de ser criptográficamente fiables.

11.1.8. Parámetros de Generación de la Clave Pública

El Firmante/Suscriptor deberá usar claves basadas en el algoritmo *RSA* con una longitud fija de 2048 bits.

11.1.9. Comprobación de la Calidad de los Parámetros

De acuerdo a la Ley No. 126-02, su Reglamento de Aplicación y a sus normas complementarias, el par de claves puede ser generado por el suscriptor del certificado.

Al momento de generar el par de claves del suscriptor de un certificado para la emisión del Certificado Digital debe ser generado de manera tal que su clave privada se encuentre bajo su exclusivo y permanente control. El suscriptor es considerado titular del par de claves; como tal, debe generarlo en un sistema confiable, no debe revelar su clave privada a terceros bajo ninguna circunstancia y debe almacenarla en un medio que garantice su confidencialidad, según lo definido por el INDOTEL.

La Entidad de Certificación no genera el par de claves, desde dispositivos internos. La generación queda en manos exclusiva del suscriptor.

11.1.10. Dispositivo de Generación de Claves

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Las claves de la Entidad Certificación deberán ser generadas en un módulo criptográfico validado por *FIPS 140-2*.

El par de claves de los Suscriptores serán generadas utilizando sistemas operativos, aplicaciones, programas o dispositivos criptográficos que pertenezcan al Suscriptor.

11.1.11. Fines del Uso de la Clave

La Entidad de Certificación utilizara sus claves privadas únicamente para los propósitos de generación de Certificados Digitales y para la firma de LCR's.

La clave privada del Suscriptor deberá ser usada únicamente para la generación de firmas digitales de acuerdo con el apartado 1.3.

11.2. PROTECCIÓN DE LA CLAVE PRIVADA

11.2.1. De la Entidad de Certificación

La Entidad Certificación deberá ratificar que sus claves privadas continúan siendo confidenciales y mantienen su integridad. Para dichos fines se tomaran en consideración los siguientes puntos:

- 1) La clave privada de firma de la Entidad de Certificación cumple con los requerimientos que se detallan en el *FIPS 140-2*.
- 2) En caso de que se requiera la transportación o transferencia de las claves privadas de la EC ser harán mediante mecanismos cifrados o dispositivo criptográficas cifrados.
- 3) Se deberá hacer un respaldo de la clave privada de firma de la Entidad de Certificación, con al menos un control dual de personal autorizado.
- 4) Las copias de respaldo de la clave privada de firma de la Entidad de Certificación se registrarán por el mismo o más alto nivel de controles de seguridad que las claves que se usen en ese momento.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.2.2. 13.3.2 Del Firmante/Suscriptor

Las Unidades de Registro deberán confirmar que la clave privada del Firmante/Suscriptor, cuando esté almacenada en un dispositivo criptográfico, está protegida de forma que:

- 1) La clave privada este bajo el exclusivo control del Firmante/Suscriptor.
- 2) Su secreto está razonablemente asegurado.
- 3) La clave privada puede ser efectivamente protegida por el Firmante/Suscriptor contra un uso ajeno.

11.3. ESTÁNDARES PARA LOS MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas deben ser desarrolladas en un módulo validado por *FIPS 140-2*.

11.3.1. Control Multi-Persona (n de entre m) de la Clave Privada

Se requerirá un control multi-persona para la activación de la clave privada de la Entidad de Certificación. Este control deberá ser definido adecuadamente por el MPC en la medida en que no se trate de información confidencial o pueda comprometer de algún modo la seguridad del sistema.

11.3.2. Depósito de la Clave Privada (Key Escrow)

La clave privada de la Entidad de Certificación debe ser almacenada en un medio seguro protegido criptográficamente y al menos bajo un control dual.

En ningún caso la Entidad de Certificación podrá almacenar la clave privada de firma del Firmante/Suscriptor.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.3.3. Copia de Seguridad de la Clave Privada

La Entidad de Certificación deberá realizar una copia de respaldo de su propia clave privada que haga posible su recuperación en caso de desastre o de pérdida o deterioro de la misma de acuerdo con el apartado 13.3.2.

11.3.4. Archivo de la Clave Privada

La clave privada de la Entidad de Certificación no podrá ser archivada una vez finalizado su ciclo de vida, por lo que su destrucción es obligatoria.

Las claves privadas de Suscriptor no pueden ser archivadas por la Entidad de Certificación o la Unidad de Registro.

11.3.5. Método de Activación de la Clave Privada

Se deberá proteger el acceso a la llave privada del Firmante/Suscriptor por medio de una clave u otros métodos de acceso equivalentes. Estos datos de acceso deben ser entregados al Firmante/Suscriptor junto a un Manual de Instrucciones para cambiar dicha clave.

Estos datos de acceso deberán tener una longitud de al menos cuatro (4) dígitos en el caso de custodia en un dispositivo, siendo solo conocidos por el Firmante/Suscriptor y no deben ser compartidos.

11.3.6. Método de Desactivación de la Clave Privada

La Entidad de Certificación desarrollará un proceso por el cual su llave privada quede desactivada. Este proceso está pendiente de ser definido.

11.3.7. Método de Destrucción de la Clave Privada.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

La Entidad de Certificación deberá confirmar que su clave privada no será usada una vez finalizada su ciclo de vida, por lo que la destrucción de la misma y sus copias de respaldo, es obligatoria. Dicho proceso debe ser documentado.

Las claves privadas de los Suscriptores deberán ser destruidas o hacerlas inservibles después del fin de su ciclo de vida por el propio Firmante/Suscriptor.

11.4. OTROS ASPECTOS DE ADMINISTRACIÓN DEL PAR DE CLAVES

11.4.1. Archivo de la Clave Pública

La Entidad de Certificación deberá conservar todas las claves públicas.

11.4.2. Período de Uso para las Claves Públicas y Privadas

Ver apartado 13.1.7.

11.5. CICLO DE VIDA DEL DISPOSITIVO CRIPTOGRÁFICO

Las Unidades de Registro deberán realizar los mayores para asegurar que los Dispositivos Criptográficos:

- 1) Sean preparados de forma segura.
- 2) Ejecute de forma segura su almacenamiento y distribución.
- 3) No hayan sido utilizados por otro usuario o Suscriptor.
- 4) Queden inhabilitado su uso, en caso de ser devuelto por el Suscriptor.

11.6. CONTROLES DE SEGURIDAD TECNOLÓGICOS

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

La Entidad de Certificación y las Unidades de Registro emplearán sistemas fiables y productos que estén protegidos contra modificaciones, tomando en consideración el cumplimiento de las siguientes funciones:

- 1) Identificación de todos los usuarios.
- 2) Controles de acceso basados en privilegios.
- 3) Control dual para ciertas operaciones relativas a la seguridad.
- 4) Generación de eventos y/o bitácoras, revisión de auditoría y archivo de todos los eventos relacionados con la seguridad.
- 5) Respaldo y recuperación de sistemas y aplicaciones.
- 6) Control de acceso a los servicios de Certificación y gestión de privilegios.
- 7) Auditoría de eventos relativos a la seguridad.
- 8) Auto-diagnóstico de seguridad relacionado con los servicios de Certificación.

Las funcionalidades de arriba pueden ser provistas por el sistema operativo o mediante una combinación de sistemas operativos, sistema de Infraestructura de Clave Pública (ICP) y protección física.

11.7. CONTROLES DE SEGURIDAD DEL CICLO DE VIDA

11.7.1. Controles de Desarrollo del Sistema

La Entidad Certificación y las Unidades de Registro emplearán sistemas fiables y productos que estén protegidos contra modificaciones.

11.7.2. Controles de Gestión de la Seguridad

No estipulado.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.7.3. Gestión de Seguridad

La Entidad de Certificación y las Unidades de Registro deberán velar por que los procedimientos administrativos y de gestión son aplicados, son adecuados y se corresponden con los estándares reconocidos, Tomando en consideración:

- 1) La Entidad de Certificación será responsable por todos los aspectos relativos a la prestación de servicios de certificación.
- 2) Las responsabilidades de las terceras partes serán claramente definidas por la Entidad de Certificación en los acuerdos suscritos con dichas partes para asegurar que éstas están obligadas a implementar cualquier control requerido.
- 3) La Entidad Certificación y las Unidades de Registro deberán desarrollar las actividades necesarias para la formación y concienciación de los empleados en material de seguridad.
- 4) La información necesaria para gestionar la seguridad deberá mantenerse en todo momento. Cualquier cambio que pueda afectar al nivel de seguridad establecido deberá ser aprobado por el Comité de Tecnología.
- 5) Los controles de seguridad y procedimientos operativos para las instalaciones de la Entidad de Certificación y de la Unidad de Registro, sistemas e información necesarios para los servicios de certificación serán documentados, implementados y mantenidos.
- 6) La Entidad de Certificación deberá velar por que se mantengan los niveles de seguridad sobre las funciones delegadas a las Unidades de Registro.

11.7.4. Clasificación y Gestión de Información y Bienes

La Entidad Certificación y las Unidades de Registro deberán proteger de acuerdo a lo establecido en esta Política sus activos e informaciones, manteniendo un inventario de toda la información, clasificación de las mismas y sus requisitos de protección en relación al análisis de sus riesgos.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.7.5. Gestión de Operaciones

La Entidad de Certificación deberá confirmar que los sistemas de Certificación son seguros, son tratados correctamente, y con el mínimo riesgo de fallo, considerando:

- 1) Se protegerá la integridad de los sistemas de certificación y de su información contra virus y aplicaciones malignas o de uso no autorizado.
- 2) Los daños derivados de incidentes de seguridad y los errores de funcionamiento deberán ser minimizados por medio del uso de reportes de incidencias y procedimientos de respuesta.
- 3) Los soportes serán custodiados de manera segura para protegerlos de daños, robo y accesos no autorizados.
- 4) Se establecerán e implementarán los procedimientos para todos los roles administrativos y de confianza que afecten a la prestación de servicios de certificación.

11.7.6. Tratamiento de los Soportes y Seguridad

Todos los soportes serán provistos de forma segura de acuerdo cumpliendo con los requisitos del plan de clasificación de la información y previendo el acceso a datos sensibles.

11.7.7. Planificación del Sistema

Se deberá controlar la capacidad de atención a la demanda y la previsión de futuros requisitos de capacidad para asegurar la disponibilidad de recursos y de almacenamiento.

11.7.8. Reportes de Incidencias y Respuesta

La Entidad de Certificación y las Unidades de Registro responderán de manera inmediata y coordinada a los incidentes con el fin de reducir el impacto de los fallos de seguridad. Todos los incidentes serán reportados con posterioridad al mismo tan pronto como sea posible.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.7.9. Procedimientos Operacionales y Responsabilidades

Las operaciones de la Entidad de Certificación y las Unidades de Registro serán separadas de todo otro tipo de operaciones.

11.7.10. Gestión del Sistema de Acceso

La Entidad Certificación y las Unidades de Registro deberán garantizar que el sistema de acceso está limitado a las personas autorizadas, es decir:

- 1) Se implementarán controles para proteger la red interna de redes externas.
- 2) Los datos sensibles serán protegidos cuando estos sean transmitidos por redes no protegidas.
- 3) Garantizar una efectiva administración de acceso (incluyendo operadores, administradores y cualquier usuario que tenga un acceso directo al sistema) para mantener la seguridad.
- 4) El acceso a la información y a las funciones de los sistemas de certificación están restringido de acuerdo con la política de control de accesos, disponiendo de los controles de seguridad suficientes para la separación de los roles de confianza identificados en el MPC, incluyendo la separación de las funciones de seguridad y operaciones.
- 5) Procurar que se realice la identificación y autenticación de los usuarios sobre las aplicaciones críticas relativas a la gestión de Certificados Digitales.

11.8. GESTIONES DE CERTIFICADOS DIGITALES

La Entidad de Certificación y las Unidades de Registro deberán confirmar que los componentes de la red local están ubicados en un medio físico seguro y sus configuraciones son periódicamente auditadas.

Las instalaciones estarán provistas de sistemas de monitoreo continuo y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y/o irregulares.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

11.8.1. Gestión del Ciclo de Vida del Dispositivo Criptográfico

Las Unidades de Registro deberán confirmar la seguridad del dispositivo criptográfico a lo largo de su ciclo de vida, contemplando:

- 1) Que el dispositivo criptográfico no se manipula durante su transporte.
- 2) Que el dispositivo criptográfico este almacenado de forma segura.
- 3) Que el uso del dispositivo criptográfico requiere el uso de al menos dos empleados de confianza.
- 4) Que el dispositivo criptográfico funciona correctamente.
- 5) Que la clave privada almacenada en el dispositivo criptográfico se eliminará una vez se ha retirado el dispositivo.

11.9. CONTROLES DE SEGURIDAD DE LA RED

Ver apartado 13.7.10.

11.10. CONTROLES DE INGENIERÍA DE LOS MÓDULOS CRIPTOGRÁFICOS

Todas las operaciones criptográficas de la Entidad de Certificación y las Unidades de Registro deben ser desarrolladas en un módulo validado por *FIPS 140-2*.

11.11. Preparación del Dispositivo Criptográfico de Creación de Claves y Firmas Digitales

Cuando se utilice un dispositivo criptográfico, las Unidades de Registro emplearán un dispositivo criptográfico seguro de generación de claves y creación de firmas digitales, garantizando, como mínimo:

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
	Área Responsable	Cargo Responsable	Fecha de Creación
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

- 1) Que debe preverse que el proveedor de los dispositivos lo prepare en forma segura.
- 2) Que se asegure su adecuado almacenamiento y distribución.
- 3) Que su activación y desactivación sean correctamente controlados.
- 4) Que cuando existan datos de activación (claves), que los mismos se preparen de forma segura y se distribuyan en forma separada de los dispositivos.

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

12. PERFILES DE CERTIFICADOS DIGITALES Y LISTA DE CERTIFICADOS REVOCADOS

12.1. PERFIL DEL CERTIFICADO DIGITAL

Todos los Certificados Digitales emitidos bajo esta política serán conformes al estándar *X.509* versión 3 y al *RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile"*. Según se establece en la norma sobre Estándares Tecnológicos dictados por el INDOTEL.

Los datos que figuran en el Certificado Digital emitido bajo esta Política de Certificación, son:

- 1) Número de versión *X.509* del Certificado Digital.
- 2) Número de serie del Certificado Digital.
- 3) Dirección *URL* del dominio.
- 4) Nombre, dirección electrónica y lugar donde realiza actividades la Entidad de Certificación, y los antecedentes de la autorización obtenida.
- 5) Clave pública del suscriptor.
- 6) Algoritmos de firma de la clave pública.
- 7) Fecha y hora de la Emisión y Expiración del Certificado Digital.
- 8) Nombre de la Entidad de Certificación emisora del Certificado Digital.
- 9) Dirección de consulta de la Lista de Certificados Revocados (LCR).
- 10) Identificación de la Política de Certificación bajo la cual fue emitido el Certificado Digital.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

12.1.1. Número de Versión.

Deberá indicarse en el campo versión que se trata de la v.3.

12.1.2. Extensiones del Certificado Digital.

Atributos	Contenido
Tipo y Versión del Certificado Digital	X.509 v3
Numero Serial (OID 2.5.4.5)	Este valor es auto generado por el aplicativo de la CA
Algoritmo	sha256WithRSAEncryption
Algoritmo de Firma	sha256
Longitud de Llave	2048 bits
Válido desde	Indica la fecha y hora en la que se emitió el Certificado Digital
Válido hasta	Indica la fecha y hora de vencimiento del Certificado Digital
Emisor	-----
CN [Nombre Común] (OID 2.5.4.3)	Cámara de Santo Domingo ID CA
OU [Unidad Organizacional] (OID 2.5.4.11)	Digifirma
O [Organización] (OID 2.5.4.10)	CAMARA DE COMERCIO Y PRODUCCION DE SANTO DOMINGO
C [País] (OID 2.5.4.6)	DO
Sujeto	-----
CN [Nombre Común] (OID 2.5.4.3)	Nombre Completo del Sujeto o Suscriptor a quien se le está emitiendo el Certificado Digital, en el siguiente formato: CN=<Primer Nombre> <Segundo Nombre> <Primer Apellidos> <Segundo Apellido>
Llave Pública	RSA (2048)
Restricciones Básicas	Tipo de Sujeto=Entidad Final Restricciones de Longitud de Ruta=Ninguna
Política de Certificados	[1]Política de Certificados: Identificador de Política =1.3.6.1.4.1.26236.1.1.2.2 [1,1]Informacion de Calificador de Política: Identificador de Calificador de Política =CPS Calificador: http://cps.camarasantodomingo.do/ [1,2]Informacion de Calificador de Política: Identificador de Calificador de Política=Noticia de Usuario Calificador: Referencia de Noticia: Organizacion=Camara de Comercio y Produccion de Santo Domingo (RNC-401023687) Numero de Noticia=1

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

	Texto de Noticia= Certificados Digitales Clase 2 (Empresarial/Gubernamental) [1,3]Informacion de Calificador de Política: Identificador de Calificador de Política=Noticia de Usuario Calificador: Referencia de Noticia: Organizacion=Camara de Comercio y Produccion de Santo Domingo (RNC-401023687) Numero de Noticia=2 Texto de Noticia=Avenida 27 de Febrero No. 228, Torre Friusa, Sector La Esperilla, Codigo Postal 10106, Santo Domingo, Distrito Nacional, Republica Dominicana [1,4]Informacion de Calificador de Política: Identificador de Calificador de Política=Noticia de Usuario Calificador: Referencia de Noticia: Organizacion=Instituto Dominicano de las Telecomunicaciones (INDOTEL) Numero de Noticia=3 Texto de Noticia=Resolucion No.169-07 del Consejo Directivo
Uso de Llave	Firma Digital, No Repudio, Cifrado de Llaves (e0)
Uso Extendido de Llave	Autenticación de Cliente (1.3.6.1.5.5.7.3.2) Seguridad de Correo Electrónico (1.3.6.1.5.5.7.3.4) Conexión con Tarjeta Inteligente (1.3.6.1.4.1.311.20.2.2)
Identificador de Llave de la Autoridad	<Indicado en el Certificado Raíz>
Nombre Alterno del Sujeto	<Correo Electrónico del Sujeto>
Nombre Alterno del Sujeto	Este atributo extendido es utilizado para especificar el número y tipo de documento de identidad utilizado para validar y verificar los datos del Sujeto o Suscriptor del Certificado Digital. Todos los documentos son referenciados por una letra seguida de un guion. • Para el documento "Cédula de Identidad y Electoral" se utilizará "00000000000 - Cedula". • Para el documento "Licencia de Conducir" se utilizará "00000000000 - Licencia". • Para el documento "Pasaporte" se utilizará "00000000000 - Pasaporte".
Punto de Distribución de CRL	http://list.camarasantodomingo.do:8080/ca/ee/ca/getCRL?op=getCRL&crllssuingPoint=MasterCRL
Acceso de Información de la Autoridad	http://www.camarasantodomingo.do/
Algoritmo de Impresión de Huella	SHA1
Impresión de Huella	

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Nota:

* Las informaciones indicadas en letra color **negro** y tipo **bold**, indican informaciones no variables para este perfil de la presente Política de Certificados.

** Las informaciones indicadas en letra color *gris* de tipo *itálica* y **bold**, indican valores que varían de acuerdo a las informaciones suministradas por el Sujeto o Suscriptor en el proceso de gestión del Certificado Digital.

12.1.3. Identificadores de Objeto (OID) de los Algoritmos

El identificador de objeto del algoritmo de la llave pública será 1.2.840.113549.1.1.11 - *sha256WithRSAEncryption*.

12.1.4. Restricciones de los Nombres.

No estipulado.

12.2. PERFIL DE LAS LISTAS DE CERTIFICADOS REVOCADOS

Las Listas de Certificados Revocados se emiten en formato ITU-T X509 versión 2 según se establece en los mencionados Estándares.

12.3. PERFIL DEL PROTOCOLO DE CERTIFICADOS EN LÍNEA (OCSP)

[1]Authority Info Access

Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

Alternative Name:

URL=<http://list.camarasantodomingo.do:8080/ca/ocsp>

	GERENCIA SOLUCIONES DIGITALES		Código DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento 5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

13. ESTAMPADO CRONOLÓGICO DE TIEMPO

La Entidad de Certificación proveerá el servicio de estampado cronológico de tiempo de acuerdo a los lineamientos establecidos por el INDOTEL.

Las tarifas de este servicio estarán publicadas en el portal *Web* de la Cámara de Comercio y Producción de Santo Domingo.

13.1. Requerimientos para el estampado cronológico de tiempo

Está estipulado siguiendo la normativa dictada por el INDOTEL. Dicho servicio cumplirá los siguientes requisitos:

- 1) Se utilizara la zona horaria y servicio de hora autorizado por el INDOTEL.
- 2) Deberá ser accesible para el destinatario del documento digital y/o mensaje de datos.
- 3) No comprometerá en modo alguno la integridad del documento o mensaje de datos, ni la viabilidad de verificar la Firma Digital que pueda incorporar dicho documento o mensaje de datos, en su caso.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

14. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

14.1. AUTORIDAD DE LAS POLÍTICAS

La Política de Certificados está administradas por la Dirección Administrativa, la Gerencia de Soluciones Digitales y la Consultoría, quienes se encargan de la confección y modificación de dichos documentos. Los mismos son aprobados por la Comisión de Tecnología, la cual está conformada por miembros de la Junta Directiva de la Cámara de Comercio y Producción de Santo Domingo.

14.2. PROCEDIMIENTOS DE ESPECIFICACIÓN DE CAMBIOS

Cualquier elemento de esta política es susceptible de ser modificado. Todos los cambios realizados sobre este documento serán inmediatamente publicados en la *Web* de la Cámara de Comercio y Producción de Santo Domingo, conservando un histórico con las versiones anteriores.

Los interesados pueden presentar sus comentarios a la Cámara de Comercio y Producción de Santo Domingo dentro de los 15 días siguientes a la publicación. Cualquier acción tomada como resultado de estos comentarios queda a la discreción de la Autoridad de Políticas.

Si un cambio en la política afecta de manera relevante a un número significativo de terceros que confían, la Entidad de Certificación puede discrecionalmente asignar un nuevo *OID* a la política modificada.

14.3. PUBLICACIÓN Y NOTIFICACIÓN

El acceso a esta política estará disponible en formato electrónico en la dirección *Web* (<http://www.camarasantodomingo.do>).

14.4. PROCEDIMIENTOS DE APROBACIÓN DE LA PC

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

Esta Política de Certificados ha sido sometida a la aprobación de la Comisión de Tecnología y la Junta Directiva, y autorizada por el INDOTEL; cada vez que se le incorpore modificaciones para aprobación y autorización se deberán respetar los procedimientos especificados por los procedimientos de la Cámara de Comercio y Producción de Santo Domingo y la regulación del ente regulador.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

15. DERECHOS DE PROPIEDAD INTELECTUAL

La Entidad de Certificación es titular en exclusiva de todos los derechos de propiedad intelectual que puedan derivarse del sistema de certificación que regula esta Política de Certificados. Se prohíbe por tanto, cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son de titularidad exclusiva de la Entidad de Certificación, sin la autorización expresa por su parte.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	5.0
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

16. ANEXO I. ACRÓNIMOS.

Acrónimos Significado

EC	Entidad de Certificación
UR	Unidad de Registro
MPC	Manual de Procedimientos de Certificación
LCR	Lista de Certificados revocados
CSR	<i>Certificate Signing Request</i> . Petición de firma de Certificado
DES	<i>Data Encryption Standard</i> . Estándar de cifrado de datos
DN	<i>Distinguished Name</i> . Nombre distintivo dentro del Certificado Digital
DSA	<i>Digital Signature Algorithm</i> . Estándar de algoritmo de firma
DSCF	Dispositivo criptográfico de creación de firma
DSADCF	Dispositivo criptográfico de almacén de datos de creación de firma
FIPS	<i>Federal Information Processing Standard Publication</i>
IETF	<i>Internet Engineering Task Force</i>
ISO	<i>International Organization for Standardization</i> . Organismo Internacional de Estandarización
ITU	<i>International Telecommunications Union</i> . Unión Internacional de Telecomunicaciones
LDAP	<i>Lightweight Directory Access Protocol</i> . Protocolo de acceso a directorios
OCSP	<i>On-line Certificate Status Protocol</i> . Protocolo de acceso al estado de los Certificados
OID	<i>Object Identifier</i> . Identificador de objeto
PA	<i>Policy Authority</i> . Autoridad de Políticas
PC	Política de Certificados
PIN	<i>Personal Identification Number</i> . Número de identificación personal
IPC	Infraestructura de clave pública
RSA	<i>Rivest-Shimar-Adleman</i> . Tipo de algoritmo de cifrado
SHA-1	<i>Secure Hash Algorithm</i> . Algoritmo seguro de Hash
SSL	<i>Secure Sockets Layer</i> . Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	<i>Transmission Control</i> . Protocol/Internet Protocol. Sistema de protocolos, definidos en el marco de la IETF. El protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino. El protocolo IP se encarga de direccionar adecuadamente la información hacia su destinatario.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

URL *Uniform Resource Locator*. Localizador de Recursos Unificados, también conocido como dirección de Internet.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

17. ANEXO II. OTRAS DEFINICIONES.

Acrónimos	Significado
Autoridad de Políticas	Persona o conjunto de personas responsable de todas las decisiones relativas a la creación, administración, mantenimiento y supresión de las Política de Certificados y CPS.
Certificación Cruzada	El establecimiento de una relación de confianza entre dos EC's, mediante el intercambio de Certificados entre las dos en virtud de niveles de seguridad semejantes.
Certificado Digital	Archivo que asocia la clave pública con algunos datos identificativos del Firmante/Suscriptor y es firmada por la Entidad de Certificación
Clave Pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos. También llamada datos de verificación de firma.
Clave Privada	Valor matemático conocido únicamente por el Firmante/Suscriptor y usado para la creación de una firma digital o el descifrado de datos. También llamada datos de creación de firma. La clave privada de la Entidad Certificación será usada para firma de Certificados Digitales y firma de LCR's
LCR	Archivo que contiene una lista de los Certificados Digitales que han sido revocados en un periodo de tiempo determinado y que es firmada por la Entidad de Certificación
Datos de Activación	Datos privados, como claves o contraseñas empleados para la activación de la clave privada.
DSADCF	Dispositivo criptográfico de almacén de los datos de creación de firma. Elemento software o dispositivo empleado para custodiar la clave privada del Firmante/Suscriptor de forma que solo él tenga el control sobre la misma.

	GERENCIA SOLUCIONES DIGITALES		Código
			DAF-SD-013
	POLÍTICA DE CERTIFICADOS CLASE 2		Versión Documento
			5.0
Área Responsable	Cargo Responsable	Fecha de Creación	Fecha de Actualización
Soluciones Digitales	Subgerente Fortalecimiento Empresarial & Soluciones Digitales	02/10/2006	18/03/2021
OBJETIVO DE LAS POLITICAS:	Definir los criterios básicos a seguir por la Entidad de Certificación de la Cámara de Comercio y Producción de Santo Domingo que emite Certificados Digitales de Clase 2, por las Unidades de Registro y por los Suscriptores y terceros que confían en este tipo de certificado.		

18. CONTROL DE CAMBIO.

TABLA DE CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
04	06/05/2020	Actualización de Documento
05	03/18/2021	Agregado Proceso de Autenticación Remota

TABLA DE CONTROL DE APROBACIONES			
DOCUMENTO QUE SE APRUEBA O ACTUALIZA:		DAF-SD-013-POLITICA DE CERTIFICADOS CLASE 2	
CÓDIGO DOCUMENTO QUE SE ACTUALIZA:	DAF-SD-013	NÚMERO DE LA VERSIÓN:	05
FUNCIÓN	PERSONA	CARGO	FECHA
ACTUALIZADO	Carlos Guerrero	Subgerente de Fortalecimiento Empresarial & Soluciones Digitales	03/23/2021
REVISADO	Alexander Mañan / Anaika Placencia	Analista Jr. de Procesos	03/23/2021
APROBADO	Yojanny Reyes	Gerente Operaciones y Servicios	03/24/2021
APROBADO	Antonio Ramos	Vicepresidente Ejecutivo	03/24/2021