GACETA OFICIAL
DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

AÑO CXLV - MES VI | Caracas, miércoles 21 de marzo de 2018 | Número 41.365

SUMARIO

PRESIDENCIA DE LA REPÚBLICA

Decreto Nº 3.325 19 de marzo de 2018

NICOLÁS MADURO MOROS
Presidente de la República

Con el supremo compromiso y voluntad de lograr la mayor eficacia política y calidad revolucionaria en la construcción del Socialismo, la refundación de la patria venezolana, basado en principios humanistas, sustentado en condiciones morales y éticas que persiguen el progreso del país y del colectivo, por mandato del pueblo, de conformidad con lo establecido en el artículo 226 de la Constitución de la República Bolivariana de Venezuela; en ejercicio de las atribuciones que me confieren los numerales 2 y 11 del artículo 236 *ejusdem,* concatenado con el numeral 4 del artículo 2° del Decreto N° 3.239 de fecha 09 de enero de 2018, mediante el cual se declara el Estado de Excepción y de Emergencia Económica en todo el Territorio Nacional, prorrogado mediante Decreto N° 3.308 de fecha 09 de marzo de 2018, en concordancia con los artículos 20 y 21 de la Ley Orgánica sobre Estados de Excepción, en Consejo de Ministros,

CONSIDERANDO

Que en el marco del Decreto mediante el cual se declara el Estado de Excepción y de Emergencia Económica y su prórroga, se requiere hacer erogaciones no previstas en el Presupuesto Anual, con cargo al Tesoro Nacional, que permitan enfrentar la situación excepcional hasta alcanzar el restablecimiento del orden financiero de la Nación,

CONSIDERANDO

Que es obligación y firme compromiso del Gobierno Revolucionario impedir que se generen daños a la economía del país, a fin de garantizar al pueblo venezolano el direccionamiento preferente de los recursos económicos disponibles, para los proyectos sociales y la generación de la infraestructura necesaria que permitan el mejoramiento de su calidad de vida, aún en condiciones de estado de emergencia económica, formalmente declarado y vigente,

CONSIDERANDO

Que el Estado debe asegurar a las venezolanas y venezolanos el disfrute de sus derechos e igualmente, reducir los efectos de la inflación inducida y de la especulación y contrarrestar los problemas que afectan gravemente el equilibrio económico financiero del país,

CONSIDERANDO

Que a los fines de materializar la ejecución de los proyectos enmarcados en el Plan de la Patria, Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, se requiere transferir al Poder Electoral, los recursos necesarios que permitan garantizar los procesos electorales en un clima de estabilidad y que se reconozca de forma pacífica, la voluntad soberana de las venezolanas y los venezolanos.

DICTO

El siguiente,

DECRETO N° 18 EN EL MARCO DEL ESTADO DE EXCEPCIÓN Y DE EMERGENCIA ECONÓMICA, MEDIANTE EL CUAL SE AUTORIZA LA DISTRIBUCIÓN DE RECURSOS ADICIONALES CON CARGO AL PRESUPUESTO DE EGRESOS DEL CONSEJO NACIONAL ELECTORAL.

Artículo 1°. Se autoriza la distribución de recursos adicionales con cargo al presupuesto de egresos del **CONSEJO NACIONAL ELECTORAL**, por la cantidad de **CUATRO BILLONES DOSCIENTOS NUEVE MIL SEISCIENTOS SEIS MILLONES CUATROCIENTOS DIECIOCHO MIL SETECIENTOS SESENTA Y OCHO BOLÍVARES (Bs. 4.209.606.418.768)**; destinados a la ejecución de los proyectos Elecciones y Consultas 2018 y gestión administrativa del organismo.

Artículo 2°. Los recursos para financiar los gastos a que se refiere este Decreto, provienen de Otros Ingresos Extraordinarios, debidamente certificados por la Tesorería Nacional.

Artículo 3°. La distribución de los recursos a los que se refiere el artículo 1° de este Decreto, se realizará según la siguiente imputación presupuestaria:

CONSEJO NACIONAL ELECTORAL			**Bs.**	**4.209.606.418.768,00**
Acción Centralizada:	**0030002000**	**"Gestión administrativa"**	"	**226.642.463.169,00**
Acción Específica:	**0030002001**	**"Apoyo institucional a las acciones específicas de los proyectos del organismo"**	"	**226.642.463.169,00**
Partida:	**4.02**	**"Materiales, suministros y mercancías"** -Otras Fuentes	"	**14.561.269.557,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	01.01.00	"Alimentos y bebidas para personas"	"	868.340.000,00
	03.02.00	"Prendas de vestir"	"	415.750.000,00
	04.03.00	"Cauchos y tripas para vehículos"	"	2.146.500.000,00
	05.03.00	"Productos de papel y cartón para oficina"	"	1.183.264.000,00
	06.04.00	"Productos farmacéuticos y medicamentos"	"	4.270.000,00
	06.08.00	"Productos plásticos"	"	1.091.250.000,00
	08.03.00	"Herramientas menores, cuchillería y artículos generales de ferretería"	"	61.320.327,00
	08.09.00	"Repuestos y accesorios para equipos de transporte"	"	677.250.000,00
	10.05.00	"Útiles de escritorio, oficina y materiales de instrucción"	"	3.355.611.300,00
	10.06.00	"Condecoraciones, ofrendas y similares"	"	3.000.000,00
	10.07.00	"Productos de seguridad en el trabajo"	"	29.900.000,00
	10.08.00	"Materiales para equipos de computación"	"	4.722.643.930,00
	99.01.00	"Otros materiales y suministros"	"	2.170.000,00
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**211.825.133.757,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	01.01.00	"Alquileres de edificios y locales"	"	3.347.253.982,00
	02.02.00	"Alquileres de equipos de transporte, tracción y elevación"	"	94.770.000.000,00
	04.01.00	"Electricidad"	"	169.854.456,00
	04.03.00	"Agua"	"	35.555.760,00
	04.05.00	"Servicio de comunicaciones"	"	10.500.000,00
	04.06.00	"Servicio de aseo urbano y domiciliario"	"	293.521.200,00
	04.07.00	"Servicio de condominio"	"	39.210.976,00
	06.05.00	"Servicios de protección en traslado de fondos y de mensajería"	"	200.000.000,00
	07.02.00	"Imprenta y reproducción"	"	1.996.800.000,00
	07.04.00	"Avisos"	"	288.000.000,00
	09.01.00	"Viáticos y pasajes dentro del país"	"	164.637.000,00
	09.02.00	"Viáticos y pasajes fuera del país"	"	5.000.000.000,00
	10.09.00	"Servicios de lavandería y tintorería"	"	3.690.000,00
	10.11.00	"Servicios para la elaboración y suministro de comida "	"	46.485.321.509,00

	11.02.00	"Conservación y reparaciones menores de equipos de transporte, tracción y elevación"	"	7.047.000.000,00
	12.01.00	"Conservación y reparaciones menores de obras en bienes del dominio privado"	"	5.405.000.000,00
	18.01.00	"Impuesto al valor agregado"	"	17.673.788.874,00
	99.01.00	"Otros servicios no personales"	"	28.895.000.000,00
Partida:	**4.11**	**"Disminución de pasivos "**	"	**256.059.855,00**
		-Otras Fuentes	"	256.059.855,00
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	11.04.00	"Compromisos pendientes de ejercicios anteriores"	"	256.059.855,00
Proyecto:	**0030115000**	**"Inscripción de las ciudadanas y ciudadanos para su inclusión en el Registro Electoral y Actualización de datos para el año 2018."**	"	**16.088.647.278,00**
Acción Específica:	**0030115001**	**"Realizar el seguimiento a los procesos de Inscripción, Actualización y Depuración del Registro Electoral año 2018"**	"	**16.088.647.278,00**
Partida:	**4.01**	**"Gastos de personal"**	"	**674.423.100,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	01.18.01	"Remuneraciones al personal contratado a tiempo determinado"	"	96.769.440,00
	04.26.00	"Bono compensatorio de alimentación al personal contratado"	"	497.653.200,00
	04.28.00	"Complemento al personal contratado por días feriados"	"	52.783.524,00
	08.03.00	"Prestaciones sociales e indemnizaciones al personal contratado"	"	27.216.936,00
Partida:	**4.02**	**"Materiales, suministros y mercancías"**	"	**13.369.675.000,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	05.03.00	"Productos de papel y cartón para oficina"	"	2.299.825.000,00
	10.05.00	"Útiles de escritorio, oficina y materiales de instrucción"	"	4.711.437.500,00
	10.08.00	"Materiales para equipos de computación"	"	6.358.412.500,00
Partida:	**4.03**	**"Servicios no personales"**	"	**2.044.549.178,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	08.02.00	"Comisiones y gastos bancarios"	"	16.860.578,00
	09.01.00	"Viáticos y pasajes dentro del país"	"	499.816.100,00
	10.11.00	"Servicios para la elaboración y suministro de comida "	"	962.500.000,00
	18.01.00	"Impuesto al valor agregado"	"	565.372.500,00
Proyecto:	**0030118000**	**"Campañas informativas y de posicionamiento institucional del Poder Electoral"**	"	**210.901.912.188,00**
Acción Específica:	**0030118001**	**"Emitir mensajes publicitarios e institucionales en televisión"**	"	**38.570.808.810,00**
Partida:	**4.03**	**"Servicios no personales"**	"	**38.570.808.810,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.01.00	"Publicidad y propaganda"	"	34.438.222.152,00
	18.01.00	"Impuesto al valor agregado"	"	4.132.586.658,00
Acción Específica:	**0030118002**	**"Emitir mensajes publicitarios e institucionales en radio"**	"	**42.394.632.430,00**
Partida:	**4.03**	**"Servicios no personales"**	"	**42.394.632.430,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.01.00	"Publicidad y propaganda"	"	37.852.350.384,00
	18.01.00	"Impuesto al valor agregado"	"	4.542.282.046,00
Acción Específica:	**0030118003**	**"Publicar mensajes publicitarios y avisos oficiales en prensa"**	"	**21.790.434.248,00**
Partida:	**4.03**	**"Servicios no personales"**	"	**21.790.434.248,00**
		-Otras Fuentes	"	21.790.434.248,00
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.01.00	"Publicidad y propaganda"	"	19.455.744.864,00
	18.01.00	"Impuesto al valor agregado"	"	2.334.689.384,00
Acción Específica:	**0030118004**	**"Difusión de mensajes en medios publicitarios no convencionales"**	"	**6.851.456.909,00**
Partida:	**4.03**	**"Servicios no personales"**	"	**6.851.456.909,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.01.00	"Publicidad y propaganda"	"	6.117.372.240,00
	18.01.00	"Impuesto al valor agregado"	"	734.084.669,00
Acción Específica:	**0030118005**	**"Producción general publicitaria"**	"	**31.097.910.760,00**
Partida:	**4.03**	**"Servicios no personales"**	"	**31.097.910.760,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.01.00	"Publicidad y propaganda"	"	27.765.991.750,00
	18.01.00	"Impuesto al valor agregado"	"	3.331.919.010,00
Acción Específica:	**0030118007**	**"Gestionar la Instalación y operatividad del Centro Internacional de Prensa"**	"	**70.196.669.031,00**
Partida:	**4.01**	**"Gastos de personal"**	"	**39.618.324,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	01.18.02	"Remuneraciones por honorarios profesionales"	"	39.618.324,00
Partida:	**4.02**	**"Materiales, suministros y mercancías"**	"	**801.750.000,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	03.01.00	"Textiles"	"	270.000.000,00
	10.05.00	"Útiles de escritorio, oficina y materiales de instrucción"	"	114.750.000,00
	10.08.00	"Materiales para equipos de computación"	"	417.000.000,00
Partida:	**4.03**	**"Servicios no personales"**	"	**69.355.300.707,00**
		-Otras Fuentes		
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	02.02.00	"Alquileres de equipos de transporte, tracción y elevación"	"	326.562.500,00
	02.99.00	"Alquileres de otras maquinaria y equipos"	"	65.000.000.000,00
	10.11.00	"Servicios para la elaboración y suministro de comida "	"	3.476.197.060,00
	18.01.00	"Impuesto al valor agregado"	"	552.541.147,00
Proyecto:	**0030119000**	**"Elecciones y Consultas 2018"**	"	**3.755.973.396.133,00**
Acción Específica:	**0030119003**	**"Elaborar los instrumentos electorales (material electoral que forma parte del Cotillón Electoral, Paquete de Contingencia y Material Divulgativo e Informativo)."**	"	**508.206.111.390,00**

Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**508.206.111.390,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.02.00	"Imprenta y reproducción"	"	508.206.111.390,00
Acción Específica:	**0030119004**	**"Activar la Plataforma de Telecomunicaciones y Soporte Electoral (Simulacro, Prueba de Ingeneria y Evento Electoral)"**	"	**250.000.000.000,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**250.000.000.000,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	04.05.00	"Servicio de comunicaciones"	"	250.000.000.000,00
Acción Específica:	**0030119005**	**"Coordinar las actividades de logística operacional del proceso electoral."**	"	**411.104.985.868,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**411.104.985.868,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	10.11.00	"Servicios para la elaboración y suministro de comida "	"	161.104.985.868,00
	99.01.00	"Otros servicios no personales"	"	250.000.000.000,00
Acción Específica:	**0030119006**	**"Alistar equipos tecnológicos de la Plataforma Automatizada del Voto"**	"	**69.582.959.604,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**68.544.959.604,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	18.01.00	"Impuesto al valor agregado"	"	124.560.000,00
	99.01.00	"Otros servicios no personales"	"	68.420.399.604,00
Partida:	**4.04**	**"Activos reales"** -Otras Fuentes	"	**1.038.000.000,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	09.01.00	"Mobiliario y equipos de oficina"	"	1.032.000.000,00
	09.02.00	"Equipos de computación"	"	6.000.000,00
Acción Específica:	**0030119007**	**"Procesar (embalaje, despliegue y repliegue) el material electoral (cotillón) a utilizar en las mesas de votación"**	"	**734.754.947.984,00**
Partida:	**4.02**	**"Materiales, suministros y mercancías"** -Otras Fuentes	"	**700.674.060.700,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	05.02.00	"Envases y cajas de papel y cartón"	"	240.034.072.800,00
	05.03.00	"Productos de papel y cartón para oficina"	"	18.802.337.400,00
	06.08.00	"Productos plásticos"	"	74.304.080.000,00
	10.05.00	"Útiles de escritorio, oficina y materiales de instrucción"	"	367.533.570.500,00
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**34.080.887.284,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	18.01.00	"Impuesto al valor agregado"	"	34.080.887.284,00
Acción Específica:	**0030119009**	**"Ejecutar el plan de Acompañamiento Internacional en el Proceso Electoral."**	"	**500.000.000.000,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**500.000.000.000,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	09.02.00	"Viáticos y pasajes fuera del país"	"	500.000.000.000,00
Acción Específica:	**0030119012**	**"Ejecutar los planes de producción y distribución de Boletas Electorales Válidas y no Válidas."**	"	**606.855.000.000,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**606.855.000.000,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	10.99.00	"Otros servicios profesionales y técnicos"	"	606.855.000.000,00
Acción Específica:	**0030119013**	**"Capacitar al personal técnico y operativo del Sistema Automatizado de Votación para el simulacro y evento electoral"**	"	**597.536.105.234,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**597.536.105.234,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	10.99.00	"Otros servicios profesionales y técnicos"	"	597.536.105.234,00
Acción Específica:	**0030119014**	**"Producir los Instrumentos Electorales Codificados"**	"	**62.647.964.803,00**
Partida:	**4.02**	**"Materiales, suministros y mercancías"** -Otras Fuentes	"	**62.647.964.803,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	05.02.00	"Envases y cajas de papel y cartón"	"	9.677.250.000,00
	05.03.00	"Productos de papel y cartón para oficina"	"	17.668.320.940,00
	06.08.00	"Productos plásticos"	"	1.471.714.980,00
	08.03.00	"Herramientas menores, cuchillería y artículos generales de ferretería"	"	99.700.000,00
	10.02.00	"Materiales y útiles de limpieza y aseo"	"	1.844.723.893,00
	10.05.00	"Útiles de escritorio, oficina y materiales de instrucción"	"	86.309.990,00
	10.07.00	"Productos de seguridad en el trabajo"	"	212.600.000,00
	10.08.00	"Materiales para equipos de computación"	"	31.587.345.000,00
Acción Específica:	**0030119015**	**"Ejecutar Auditorias al Proceso Electoral"**	"	**270.000.000,00**
Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**270.000.000,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	10.99.00	"Otros servicios profesionales y técnicos"	"	270.000.000,00
Acción Específica:	**0030119018**	**"Ejecutar plan de Seguridad a las Altas Autoridades del Poder Electoral, a los Acompañantes Internacionales, Instalaciones Físicas y Operatividad General del Evento Electoral"**	"	**15.015.321.250,00**
Partida:	**4.02**	**"Materiales, suministros y mercancías"** -Otras Fuentes	"	**10.015.321.250,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	03.01.00	"Textiles"	"	2.420.000.000,00
	05.03.00	"Productos de papel y cartón para oficina"	"	3.575.000.000,00
	10.05.00	"Útiles de escritorio, oficina y materiales de instrucción"	"	4.020.321.250,00

Partida:	**4.03**	**"Servicios no personales"** -Otras Fuentes	"	**5.000.000.000,00**
Sub-Partidas Genéricas, Específicas y Sub-Específicas:	07.02.00	"Imprenta y reproducción"	"	5.000.000.000,00

Artículo 4°. El Ministro del Poder Popular de Economía y Finanzas y la Presidenta del Consejo Nacional Electoral, quedan encargados de la ejecución de este Decreto.

Artículo 5°. Este Decreto entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Dado en Caracas, a los diecinueve días del mes de marzo de dos mil dieciocho. Años 207° de la Independencia, 159° de la Federación y 19° de la Revolución Bolivariana.

Ejecútese,
(L.S.)

NICOLÁS MADURO MOROS

Refrendado
El Vicepresidente Ejecutivo
de la República y Primer Vicepresidente
del Consejo de Ministros
(L.S.)

TARECK EL AISSAMI

Refrendado
El Ministro del Poder Popular del
Despacho de la Presidencia y Seguimiento
de la Gestión de Gobierno
(L.S.)

JORGE ELIESER MÁRQUEZ MONSALVE

Refrendado
El Ministro del Poder Popular
para Relaciones Exteriores
(L.S.)

JORGE ALBERTO ARREAZA MONTSERRAT

Refrendado
El Ministro del Poder Popular
para Relaciones Interiores, Justicia y Paz
(L.S.)

NÉSTOR LUIS REVEROL TORRES

Refrendado
El Ministro del Poder Popular
para la Defensa y Vicepresidente Sectorial
de Soberanía Política, Seguridad y Paz
(L.S.)

VLADIMIR PADRINO LÓPEZ

Refrendado
El Ministro del Poder Popular para
la Comunicación e Información y Vicepresidente
Sectorial de Comunicación y Cultura
(L.S.)

JORGE JESÚS RODRÍGUEZ GÓMEZ

Refrendado
El Ministro del Poder Popular de Economía y
Finanzas
(L.S.)

SIMÓN ALEJANDRO ZERPA DELGADO

Refrendado
El Ministro del Poder Popular para
Industrias Básicas, Estratégicas y Socialistas
(L.S.)

JUAN BAUTISTA ARIAS PALACIO

Refrendado
El Ministro del Poder Popular para
el Comercio Exterior e Inversión Internacional
(L.S.)

JOSÉ GREGORIO VIELMA MORA

Refrendado
El Ministro del Poder Popular
para la Agricultura Productiva y Tierras,
y Vicepresidente Sectorial de Economía
(L.S.)

WILMAR ALFREDO CASTRO SOTELDO

Refrendado
El Ministro del Poder Popular de
Agricultura Urbana
(L.S.)

FREDDY ALIRIO BERNAL ROSALES

Refrendado
El Ministro del Poder Popular
de Pesca y Acuicultura
(L.S.)

ORLANDO MIGUEL MANEIRO GASPAR

Refrendado
El Ministro del Poder Popular para
la Alimentación
(L.S.)

LUIS ALBERTO MEDINA RAMÍREZ

Refrendado
La Ministra del Poder Popular para
el Turismo
(L.S.)

MARLENY JOSEFINA CONTRERAS HERNÁNDEZ

Refrendado
El Ministro del Poder Popular
de Petróleo
(L.S.)

MANUEL SALVADOR QUEVEDO FERNÁNDEZ

Refrendado
El Ministro del Poder Popular de
Desarrollo Minero Ecológico
(L.S.)

VÍCTOR HUGO CANO PACHECO

Refrendado
El Ministro del Poder Popular
de Planificación y Vicepresidente
Sectorial de Planificación
(L.S.)

RICARDO JOSÉ MENÉNDEZ PRIETO

Refrendado
El Ministro del Poder Popular para
la Salud
(L.S.)

LUIS SALERFI LÓPEZ CHEJADE

Refrendado
La Ministra del Poder Popular
para los Pueblos Indígenas
(L.S.)

ALOHA JOSELYN NÚÑEZ GUTIÉRREZ

Refrendado
La Ministra del Poder Popular
para la Mujer y la Igualdad de Género
(L.S.)

BLANCA ROSA EEKHOUT GÓMEZ

Refrendado
El Ministro del Poder Popular para
la Juventud y el Deporte
(L.S.)

PEDRO JOSÉ INFANTE APARICIO

Refrendado
La Ministra del Poder Popular
para el Servicio Penitenciario
(L.S.)

MARÍA IRIS VARELA RANGEL

Refrendado
El Ministro del Poder Popular para
el Proceso Social de Trabajo
(L.S.)

NÉSTOR VALENTÍN OVALLES

Refrendado
El Ministro del Poder Popular para
la Cultura
(L.S.)

ERNESTO EMILIO VILLEGAS POLJAK

Refrendado
El Ministro del Poder Popular para
la Educación y Vicepresidente Sectorial para el
Desarrollo Social y la Revolución
de las Misiones
(L.S.)

ELÍAS JOSÉ JAUA MILANO

Refrendado
El Ministro del Poder Popular para la
Educación Universitaria, Ciencia y Tecnología
(L.S.)

HUGBEL RAFAEL ROA CARUCI

Refrendado
El Ministro del Poder Popular
para el Ecosocialismo y Aguas
(L.S.)

RAMÓN CELESTINO VELÁSQUEZ ARAGUAYAN

Refrendado
El Ministro del Poder Popular para Hábitat y
Vivienda
(L.S.)

ILDEMARO MOISES VILLARROEL ARISMENDI

Refrendado
El Ministro del Poder Popular para las
Comunas y los Movimientos Sociales y Vicepresidente
Sectorial de Desarrollo del Socialismo Territorial
(L.S.)

ARISTÓBULO IZTÚRIZ ALMEIDA

Refrendado
El Ministro del Poder Popular para el
Transporte
(L.S.)

CARLOS ALBERTO OSORIO ZAMBRANO

Refrendado
El Ministro del Poder Popular de
Obras Públicas
(L.S.)

CÉSAR ALBERTO SALAZAR COLL

Refrendado
El Ministro del Poder Popular
para la Energía Eléctrica y Vicepresidente
Sectorial de Obras Públicas y Servicios
(L.S.)

LUIS ALFREDO MOTTA DOMÍNGUEZ

Refrendado
El Ministro de Estado para la
Nueva Frontera de Paz
(L.S.)

GERARDO JOSÉ IZQUIERDO TORRES

MINISTERIO DEL PODER POPULAR DE ECONOMÍA Y FINANZAS

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR DE ECONOMÍA Y FINANZAS
SERVICIO NACIONAL INTEGRADO DE ADMINISTRACIÓN ADUANERA Y TRIBUTARIA (SENIAT)

SNAT/2018/0018

Caracas, 01 de marzo de 2018

207º, 159º Y 19º

El Superintendente del Servicio Nacional Integrado de Administración Aduanera y Tributaria, en uso de las potestades y competencias otorgadas en el artículo 7º y el artículo 4º numeral 28 del Decreto con Rango, Valor y Fuerza de Ley del Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT), publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.211 Extraordinario, de fecha 30 de diciembre de 2015; y el Artículo 9 numeral 5 de la Resolución Nº 32 sobre la Organización, Atribuciones y Funciones del Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT), publicada en la Gaceta Oficial de la República de Venezuela Nº 4.881 Extraordinario, de fecha 29 de marzo de 1995.

CONSIDERANDO

Que se ha constatado en el Inventario de Especies Fiscales depositados en la Gerencia Regional de Tributos Internos Región Zuliana la existencia de formularios que se encuentran en obsolescencia, dañados y en desuso.

Dicta la siguiente:

PROVIDENCIA ADMINISTRATIVA MEDIANTE LA CUAL SE DESINCORPORA DEL INVENTARIO DE ESPECIES FISCALES DE LA GERENCIA REGIONAL DE TRIBUTOS INTERNOS DE LA REGIÓN ZULIANA, LOS FORMULARIOS QUE EN ELLA SE SEÑALAN.

Artículo 1º: Desincorpórense del inventario de Especies Fiscales de la Gerencia Regional de Tributos Internos de la Región Zuliana; por razones de obsolescencia, dañados y en desuso los formularios, que a continuación se especifican, los cuales no pueden ser utilizados en el servicio de la Renta:

INVENTARIO DE FORMULARIOS
GERENCIA REGIONAL DE TRIBUTOS INTERNOS
DE LA REGION ZULIANA

FORMULARIO	NUMERACION		VALOR FACIAL	FECHA DE EMISIÓN	TOTAL UNIDADES	Total Bs.
	DESDE	HASTA				
[illegible]						
	16.501	17.250	S/V	F-2011	750	0,00
SUB-TOTAL					**750**	**0,00**
FORMA 02						
	306.519	306.532	0,50	F-2003	14	7,00
	306.548	306.564	0,50	F-2003	17	8,50
	306.596	306.603	0,50	F-2003	8	4,00
	306.645	306.679	0,50	F-2003	35	17,50
	306.684	306.687	0,50	F-2003	4	2,00
	306.747	306.747	0,50	F-2003	1	0,50
	306.750	306.870	0,50	F-2003	121	60,50
	306.876	306.884	0,50	F-2003	9	4,50
	306.951	306.999	0,50	F-2003	49	24,50
	307.840	307.856	0,50	F-2003	17	8,50
	307.000	307.147	0,50	F-2003	148	74,00
	307.168	307.199	0,50	F-2003	32	16,00
	307.200	307.226	0,50	F-2003	27	13,50
	307.228	307.231	0,50	F-2003	4	2,00
	307.233	307.247	0,50	F-2003	15	7,50
	307.249	307.250	0,50	F-2003	2	1,00
	307.751	307.777	0,50	F-2003	27	13,50
	307.797	307.813	0,50	F-2003	17	8,50
	307.820	307.839	0,50	F-2003	20	10,00
	307.859	307.928	0,50	F-2003	70	35,00
	307.938	308.000	0,50	F-2003	63	31,50
	52.586	53.000	0,50	F-2004	415	207,50
	429.601	430.800	0,50	F-2004	1.200	600,00
	430.801	432.000	0,50	F-2004	1.200	600,00
	25.517	25.607	0,50	F-2004	91	45,50
	25.638	25.750	0,50	F-2004	113	56,50
	25.792	25.796	0,50	F-2004	5	2,50
	25.798	25.806	0,50	F-2004	9	4,50
	25.840	25.847	0,50	F-2004	8	4,00
	25.857	25.886	0,50	F-2004	30	15,00
	26.075	26.250	0,50	F-2004	176	88,00
	26.394	26.560	0,50	F-2004	167	83,50
	26.569	26.587	0,50	F-2004	19	9,50
	26.589	26.630	0,50	F-2004	42	21,00
	26.632	26.640	0,50	F-2004	9	4,50
	26.751	27.000	0,50	F-2004	250	125,00
	27.004	27.200	0,50	F-2004	197	98,50
	27.206	27.289	0,50	F-2004	84	42,00
	27.302	27.958	0,50	F-2004	657	328,50
	27.990	28.500	0,50	F-2004	511	255,50
SUB-TOTAL					**5.883**	**2.941,50**
FORMA 11 PNR						
	129.398	129.400	0,25	H-2001	3	0,75
	129.451	129.500	0,25	H-2001	50	12,50
	112.249	112.251	0,80	F-2003	3	2,40
	112.290	112.293	0,80	F-2003	4	3,20
	112.297	112.297	0,80	F-2003	1	0,80
	112.299	112.309	0,80	F-2003	11	8,80
	112.310	112.318	0,80	F-2003	9	7,20
	112.372	112.393	0,80	F-2003	22	17,60
	112.399	112.415	0,80	F-2003	17	13,60
	112.438	112.465	0,80	F-2003	28	22,40
	112.473	112.487	0,80	F-2003	15	12,00
	112.488	112.496	0,80	F-2003	9	7,20
	112.548	112.548	0,80	F-2003	1	0,80
	112.552	112.552	0,80	F-2003	1	0,80
	112.564	112.564	0,80	F-2003	1	0,80
	112.567	112.590	0,80	F-2003	24	19,20
	296.716	296.800	1,50	F-2008	85	127,50
	296.801	297.600	1,50	F-2008	800	1.200,00
	209.754	209.800	1,50	F-2008	47	70,50
	209.901	210.400	1,50	F-2008	500	750,00
SUB-TOTAL					**1.631**	**2.278,05**
FORMA 12 PNR						
	86.906	87.000	0,25	H-2007	95	23,75
	15.751	16.500	1,50	H-2007	750	1.125,00
SUB-TOTAL					**845**	**1.148,75**
FORMA 18 PJD						
	1.053.447	1.053.496	1,50	F-2008	50	75,00
	1.053.707	1.053.707	1,50	F-2008	1	1,50
	1.053.714	1.053.750	1,50	F-2008	37	55,50

	600.751	601.500	2,50	F-2008	750	1.875,00
	633.859	634.500	2,50	F-2009	642	1.605,00
	634.501	635.250	2,50	F-2009	750	1.875,00
SUB-TOTAL					**2.230**	**5.487,00**
FORMA 14 2 IND						
	15.275	15.500	1,50	F-2005	226	339,00
	17.001	17.500	1,50	F-2005	500	750,00
SUB-TOTAL					**726**	**1.089,00**
FORMA 22						
	18.695	18.850	S/V	H-1998	156	0,00
	25.351	26.000	S/V	H-1998	650	0,00
	29.901	30.550	S/V	H-1998	650	0,00
	30.551	31.200	S/V	H-1998	650	0,00
	31.201	31.850	S/V	H-1998	650	0,00
	31.851	32.500	S/V	H-1998	650	0,00
	32.501	33.150	S/V	H-1998	650	0,00
SUB-TOTAL					**4.056**	**0,00**
FORMA 25 DPN						
	639.890	639.900	0,70	F-2003	11	7,70
	333.012	333.213	0,70	F-2003	202	141,40
	333.232	333.431	0,70	F-2003	200	140,00
	333.432	333.750	0,70	F-2003	319	223,30
	334.117	334.122	0,70	F-2003	6	4,20
	334.155	334.155	0,70	F-2003	1	0,70
	334.244	334.251	0,70	F-2003	8	5,60
	334.274	334.279	0,70	F-2003	6	4,20
	334.333	334.359	0,70	F-2003	27	18,90
	334.455	334.457	0,70	F-2003	3	2,10
	334.498	334.500	0,70	F-2003	3	2,10
	475.501	476.250	2,00	F-2007	750	1.500,00
	471.051	471.300	0,30	F-2007	250	75,00
	472.001	472.473	0,30	F-2007	473	141,90
	473.501	474.000	0,30	F-2007	500	150,00
SUB-TOTAL					**2.759**	**2.417,10**
FORMA 26 DPJ						
	130.389	130.500	0,70	F-2003	112	78,40
	429.101	429.139	0,70	F-2003	39	27,30
	429.144	429.153	0,70	F-2003	10	7,00
	429.166	429.235	0,70	F-2003	70	49,00
	429.243	429.333	0,70	F-2003	91	63,70
	429.394	429.395	0,70	F-2003	2	1,40
	429.399	429.404	0,70	F-2003	6	4,20
	429.415	429.435	0,70	F-2003	21	14,70
	429.442	429.467	0,70	F-2003	26	18,20
	429.498	429.580	0,70	F-2003	83	58,10
	429.587	429.622	0,70	F-2003	36	25,20
	429.623	429.636	0,70	F-2003	14	9,80
	429.638	429.659	0,70	F-2003	22	15,40
	429.662	429.750	0,70	F-2003	89	62,30
	21.942	21.952	0,70	F-2003	11	7,70
	21.978	21.979	0,70	F-2003	2	1,40
	21.988	21.991	0,70	F-2003	4	2,80
	22.020	22.028	0,70	F-2003	9	6,30
	22.266	22.267	0,70	F-2003	2	1,40
	22.324	22.327	0,70	F-2003	4	2,80
	721.501	722.250	2,00	F-2006	750	1.500,00
	722.251	723.000	2,00	F-2006	750	1.500,00
	723.001	723.750	2,00	F-2006	750	1.500,00
	723.751	724.500	2,00	F-2006	750	1.500,00
SUB-TOTAL					**3.653**	**6.457,10**
FORMA 28 EPN						
	11.442	11.442	0,25	F-2002	1	0,25
	11.500	11.500	0,25	F-2002	1	0,25
	11.502	11.502	0,25	F-2002	1	0,25
	11.505	11.551	0,25	F-2002	47	11,75
	11.562	11.576	0,25	F-2002	15	3,75
	11.605	11.605	0,25	F-2002	1	0,25
	11.617	11.622	0,25	F-2002	6	1,50
	11.624	11.624	0,25	F-2002	1	0,25
	11.627	11.630	0,25	F-2002	4	1,00
	11.633	11.660	0,25	F-2002	28	7,00
	11.662	11.672	0,25	F-2002	11	2,75
	11.684	11.692	0,25	F-2002	9	2,25
	11.698	11.698	0,25	F-2002	1	0,25
	11.824	11.833	0,25	F-2002	10	2,50
	11.836	11.870	0,25	F-2002	35	8,75
	11.872	11.883	0,25	F-2002	12	3,00
	11.891	11.893	0,25	F-2002	3	0,75
	11.895	11.895	0,25	F-2002	1	0,25
	11.994	11.999	0,25	F-2002	6	1,50
	11.976	11.988	0,25	F-2002	13	3,25
	11.900	11.930	0,25	F-2002	31	7,75
	11.955	11.956	0,25	F-2002	2	0,50
	3.653	4.000	3,00	F-2009	348	1.044,00
	4.001	4.500	3,00	F-2009	500	1.500,00
	10.501	11.000	3,00	F-2009	500	1.500,00
	11.001	11.500	3,00	F-2009	500	1.500,00
	11.501	12.000	3,00	F-2009	500	1.500,00
	12.001	12.500	3,00	F-2009	500	1.500,00
	12.501	13.000	3,00	F-2009	500	1.500,00
SUB-TOTAL					**3.587**	**10.103,75**
FORMA 28 EPN						
	89.604	90.000	0,25	H-1996	397	99,25
	93.001	93.600	0,25	H-1996	600	150,00
	93.601	94.200	0,25	H-1996	600	150,00
	88.812	88.819	0,25	H-1996	8	2,00
	88.824	88.900	0,25	H-1996	77	19,25
	88.901	89.400	0,25	H-1996	500	125,00
SUB-TOTAL					**2.182**	**545,50**
FORMA 30 IVA						
	130.796	131.242	3,00	F-2003	447	1.341,00
	148.501	149.250	3,00	F-2009	750	2.250,00
	149.251	150.000	3,00	F-2009	750	2.250,00
SUB-TOTAL					**1.947**	**5.841,00**
FORMA 31						
	5.310	5.449	1,00	F-2004	140	140,00
	5.501	5.525	1,00	F-2004	25	25,00
	5.531	5.541	1,00	F-2004	11	11,00
	5.565	5.620	1,00	F-2004	56	56,00
	5.626	5.667	1,00	F-2004	42	42,00
	5.676	5.706	1,00	F-2004	31	31,00
	5.707	5.782	1,00	F-2004	76	76,00
	5.787	5.799	1,00	F-2004	13	13,00
	5.800	5.839	1,00	F-2004	40	40,00
	5.841	5.853	1,00	F-2004	13	13,00
	5.857	5.901	1,00	F-2004	45	45,00
	5.902	6.000	1,00	F-2004	99	99,00
	29.787	30.000	1,00	F-2003	214	214,00
	6.791	7.500	1,00	F-2004	710	710,00
	7.501	8.250	1,00	F-2004	750	750,00
	8.251	9.000	1,00	F-2004	750	750,00
SUB-TOTAL					**3.015**	**3.015,00**
FORMA 56						
	131.960	132.300	S/V	H-2001	341	0,00
SUB-TOTAL					**341**	**0,00**
FORMA 60						
	6.301	6.650	S/V	H-1997	350	0,00
	6.651	7.000	S/V	H-1997	350	0,00
	7.001	7.350	S/V	H-1997	350	0,00
	7.351	7.700	S/V	H-1997	350	0,00
	7.701	8.050	S/V	H-1997	350	0,00
	8.051	8.400	S/V	H-1997	350	0,00
	8.401	8.750	S/V	H-1997	350	0,00
	8.751	9.100	S/V	H-1997	350	0,00
	60.551	60.900	S/V	H-1997	350	0,00
	60.901	61.250	S/V	H-1997	350	0,00
	61.251	61.600	S/V	H-1997	350	0,00
	61.601	61.950	S/V	H-1997	350	0,00
	61.951	62.300	S/V	H-1997	350	0,00
	62.301	62.650	S/V	H-1997	350	0,00
	62.651	63.000	S/V	H-1997	350	0,00
	63.001	63.350	S/V	H-1997	350	0,00
	63.351	63.700	S/V	H-1997	350	0,00
	63.701	64.050	S/V	H-1997	350	0,00
SUB-TOTAL					**6.300**	**0,00**
				TOTAL GENERAL	**39.905**	**41.323,75**

Artículo 2°.- La desincorporación y destrucción deberá realizarse en presencia de un funcionario adscrito a la División de Especies Fiscales de la Gerencia Financiera Administrativa y de un funcionario adscrito a la Oficina de Auditoría Interna.

Artículo 3°.- La Gerencia Regional de Tributos Internos de la Región Zuliana deberá realizar el ajuste a la Cuenta Contable de Especies Fiscales a que diere lugar la desincorporación a que se refiere esta Providencia Administrativa.

Artículo 4°.- La presente Providencia Administrativa entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y publíquese,

JOSÉ DAVID CABELLO RONDÓN
Superintendente del Servicio Nacional Integrado de Administración Aduanera y Tributaria
Decreto N° 5.851, de fecha 01 de Febrero de 2008
Gaceta Oficial de la República Bolivariana de Venezuela N° 38.863, de fecha 01 de Febrero de 2008.

MINISTERIO DEL PODER POPULAR DE PLANIFICACIÓN

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR DE PLANIFICACIÓN
CORPORACIÓN DE DESARROLLO DE LA
REGIÓN DE LOS LLANOS (CORPOLLANOS)
PROVIDENCIA ADMINISTRATIVA Nº 450-18
CALABOZO, 15 DE MARZO DE 2018
207°, 158° Y 18°

Quien suscribe **TANIA ALTUVE MORENO**, titular de la Cédula de Identidad N° **V-9.885.479**, en su condición de Presidenta Encargada de la Corporación de Desarrollo de la Región de los Llanos (CORPOLLANOS), designada mediante Decreto Nº 2.824 de fecha 26 de abril de 2017, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.138 de la misma fecha; en uso de las facultades previstas en el artículo 11, literal "b", "d" y "f" de la Ley de Corporación de Desarrollo de la Región de los Llanos (CORPOLLANOS), publicada en la Gaceta Oficial de la República de Venezuela N° 2.832 Extraordinario de fecha 30 de julio de 1981; en concordancia con lo establecido en el artículo 17 y 72 de la Ley Orgánica de Procedimientos Administrativos y numeral 5, artículo 5 de la Ley del Estatuto de la Función Pública, dicta la siguiente:

PROVIDENCIA ADMINISTRATIVA

Artículo 1. Designar a la ciudadana **HEIDY CAROLINA PEÑA FAJARDO**, titular de la Cédula de Identidad N° **V- 18.405.511**, como **AUDITORA INTERNO (E)**.

Artículo 2. Los actos y documentos que se suscriban en ejercicio de la presente designación, deberán indicar inmediatamente, bajo la firma de la funcionaria la fecha y número de ésta providencia, así como el número y fecha de la Gaceta Oficial de la República Bolivariana de Venezuela donde hubiere sido publicada.

Artículo 3. La presente providencia entrará en vigencia a partir del 15 de Marzo de 2018.

Comuníquese y Publíquese,

Msc. TANIA ALTUVE MORENO
PRESIDENTA (E) DE LA CORPORACIÓN DE
DESARROLLO DE LA REGIÓN DE LOS LLANOS (CORPOLLANOS)
DECRETO N.º 2.824 DEL 26/04/2017
GACETA OFICIAL N.º 41.138 DEL 26/04/2017

MINISTERIO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS

REPÚBLICA BOLIVARIANA DE VENEZUELA. MINISTERIO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS. DESPACHO DEL MINISTRO. RESOLUCIÓN DM/Nº 005/2017. CARACAS, 19 DE ENERO DE 2017.

AÑOS 207°, 158° y 18°

El Ministro del Poder Popular para la Agricultura Productiva y Tierras, **WILMAR ALFREDO CASTRO SOTELDO**, designado mediante Decreto N° 2.181 de fecha 06 de enero de 2016, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.822 de la misma fecha, reimpreso por fallas en los originales en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.826 de fecha 12 de enero de 2016, de conformidad con lo establecido en el artículo 16 de la Ley Orgánica de Procedimientos Administrativos; en ejercicio de las atribuciones conferidas en los numerales 1, 3, 19 y 27 del artículo 78 del Decreto N° 1.424 de fecha 17 de noviembre de 2014 con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de la misma fecha, y el numeral 2 del artículo 5 de la Ley del Estatuto de la Función Pública, dicta la siguiente;

RESOLUCIÓN

Artículo 1. Se designa a la ciudadana **GLENDY YANETZY FERNÁNDEZ**, titular de la cédula de identidad N° **V-16.184.932**, como **DIRECTORA GENERAL DE LA DIRECCIÓN GENERAL DE ESPECIES MAYORES**, en calidad de **Encargada**, adscrita al Despacho del Viceministro de Desarrollo Pecuario Integral del **MINISTERIO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS**, con las competencias inherentes al referido cargo, de conformidad con el ordenamiento jurídico vigente.

Artículo 2. La presente Resolución entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela .

Comuníquese y Publíquese.
Por el Ejecutivo Nacional,

WILMAR ALFREDO CASTRO SOTELDO
Ministro del Poder Popular para la
Agricultura Productiva y Tierras

REPÚBLICA BOLIVARIANA DE VENEZUELA. MINISTERIO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS. DESPACHO DEL MINISTRO. RESOLUCIÓN DM/Nº 006/2017. CARACAS, 19 DE ENERO DE 2017.

AÑOS 207°, 158° y 18°

El Ministro del Poder Popular para la Agricultura Productiva y Tierras, **WILMAR ALFREDO CASTRO SOTELDO**, designado mediante Decreto N° 2.181 de fecha 06 de enero de 2016, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.822 de la misma fecha, reimpreso por fallas en los originales en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.826 de fecha 12 de enero de 2016, de conformidad con lo establecido en el artículo 16 de la Ley Orgánica de Procedimientos Administrativos; en ejercicio de las atribuciones conferidas en los numerales 1, 3, 19 y 27 del artículo 78 del Decreto N° 1.424 de fecha 17 de noviembre de 2014 con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de la misma fecha, y el numeral 2 del artículo 5 de la Ley del Estatuto de la Función Pública, dicta la siguiente;

RESOLUCIÓN

Artículo 1. Se designa a la ciudadana **MARYORI DEL CARMEN RAMONES BRITO**, titular de la cédula de identidad N° **V-13.189.261**, como **DIRECTORA GENERAL DE LA DIRECCIÓN GENERAL DE INVESTIGACIÓN Y DESARROLLO PRODUCTIVO PECUARIO**, en calidad de **Encargada**, adscrita al Despacho del Viceministro de Desarrollo Pecuario Integral del **MINISTERIO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS**, con las competencias inherentes al referido cargo, de conformidad con el ordenamiento jurídico vigente.

Artículo 2. La presente Resolución entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela .

Comuníquese y Publíquese.
Por el Ejecutivo Nacional,

WILMAR ALFREDO CASTRO SOTELDO
Ministro del Poder Popular para la
Agricultura Productiva y Tierras

REPÚBLICA BOLIVARIANA DE VENEZUELA. MINISTRO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS. DESPACHO DEL MINISTRO. RESOLUCIÓN DM/N°012/2018. CARACAS, 22 DE FEBRERO DE 2018.

AÑOS 207°, 158° y 19°

El Ministro del Poder Popular para la Agricultura Productiva y Tierras, **WILMAR ALFREDO CASTRO SOTELDO**, designado mediante Decreto Nº 2.181 de fecha 06 de enero de 2016, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.822 de la misma fecha, reimpreso por fallas en los originales en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.826 de fecha 12 de enero de 2016, de conformidad con el artículo 8 numeral 2 del referido Decreto; de conformidad con el artículo 16 de la Ley Orgánica de Procedimientos Administrativos; y en ejercicio de las atribuciones conferidas en los numerales 2 y 27 del artículo 78 del Decreto Nº 1.424 con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública; en concordancia el numeral 2 del artículo 5 de la Ley del Estatuto de la Función Pública y lo establecido en los artículos 47, 48 y 51 del Reglamento Nº 1 de la Ley Orgánica de la Administración Financiera del Sector Público, sobre el Sistema Presupuestario, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 5.781 Extraordinario del 12 de agosto de 2005, así como lo dispuesto en el artículo 1 del Reglamento de Delegación de firma de los Ministros del Ejecutivo Nacional, dictado a través del Decreto Nº 140 de fecha 17 de septiembre de 1969, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 29.025 del 18 de septiembre de 1969,

RESUELVE

Artículo 1. Designan al ciudadano **MARCOS RAFAEL CALLES CRUZ**, titular de la cédula de identidad **Nº V-20.948.439**, como **DIRECTOR DE**

LA UNIDAD TERRITORIAL DEL MINISTERIO DEL PODER POPULAR PARA LA AGRICULTURA PRODUCTIVA Y TIERRAS DEL ESTADO GUÁRICO, y como cuentadante y responsable de los fondos de avance o anticipos que les sean girados a esa Unidad Administradora (Sede Calabozo, Código: 03020).

Artículo 2. Se delega en el ciudadano mencionado en el artículo 1 de la presente Resolución, la competencia y firma de los actos y documentos que se especifican a continuación:

1) Aprobar, ordenar y tramitar los gastos y pagos que afecten los créditos presupuestarios que le sean asignados con fondos de anticipo girados a la Unidad Territorial del Ministerio del Poder Popular para la Agricultura Productiva y Tierras del estado Guárico, mediante cheques, órdenes de compra y/o de servicios, conforme a lo previsto en la Ley de Presupuesto y sus modificaciones, en virtud de ello deberá registrar su firma autógrafa en la Oficina Nacional del Tesoro. De igual forma participará a la Contraloría General de la República y a la Oficina de Auditoría Interna de este Ministerio su designación como Cuentadante.

2) Certificación de los documentos que reposan en los archivos de la Unidad Territorial del Ministerio del Poder Popular para la Agricultura Productiva y Tierras del estado Guárico.

3) Aprobación de viáticos y pasajes nacionales, de conformidad con lo previsto en la normativa aplicable.

4) Informar al ciudadano Ministro trimestralmente la ejecución presupuestaria y financiera, así como los compromisos pendientes de pago, en función de la presente delegación.

Artículo 3. Los actos y documentos firmados en virtud de la delegación prevista en el artículo 2 de la presente Resolución deberán indicar de forma inmediata, bajo la firma del funcionario delegado, la fecha y el número de Resolución y de la Gaceta Oficial de la República Bolivariana de Venezuela donde haya sido publicada la misma.

Artículo 4. Queda derogada la Resolución DM/N° 024/2017 de fecha 8 de mayo de 2017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.153 de fecha 18 de mayo de 2017.

Artículo 5. La presente Resolución entrará en vigencia a partir de su fecha de publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional,

WILMAR ALFREDO CASTRO SOTELDO
Ministro del Poder Popular para Agricultura Productiva y Tierras

MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA
EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: 19/02/2018 **Nº 010**

207º, 158º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 04 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 04 de enero de 2017; actuando de conformidad con lo previsto en los artículos 65 y 78 numerales 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la *República Bolivariana de Venezuela* Nº 6.147 Extraordinario de fecha 17 de noviembre de 2014, y de conformidad con lo dispuesto en las Cláusulas Séptima y Octava del Acta Constitutiva Estatutaria de la Fundación Centro Nacional de Tecnología Química "CNTQ", publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 38.408 de fecha 29 de marzo de 2006, este Despacho,

RESUELVE

Artículo 1.- Se designan los miembros del Consejo Directivo de la Fundación Centro Nacional de Tecnologías de Química "CNTQ", ente adscrito a este Ministerio, que se mencionan a continuación:

Por el Sector Académico, Investigación y Desarrollo:

NOMBRE Y APELLIDO	MIEMBRO	SUSTITUCIÓN DE
José Gregorio Biomorgi Muzattiz C.I. V-11.684.094	Principal	Yris Gonzalez Triana
Miguel Ángel Murillo Araque C.I. V- 3.624.848	Suplente	Olgioly Dominguez Quintero
German Siegert Carrasquel C.I. V- 2.998.847	Suplente	Lusliany Josefina Rondón Verenzuela
Santiago Abraham Marrero Clemente C.I. V- 5.423.244	Suplente	Nathalie Ochoa

Por el Sector Industrial:

NOMBRE Y APELLIDO	MIEMBRO	SUSTITUCIÓN DE
César Alejandro Basanta C.I. V- 12.912.007	Principal	Xiomara Graciela Gutiérrez Santana
Álvaro Simón Pérez Guánchez C.I. V- 2.099.502	Suplente	Ricardo Barreto Muskus
Gloria María Basanta C.I. V-5.963.943	Suplente	Oscar Eduardo Vemáez Hernández
Juan Carlos Hernández Carrasquero C.I. V-7.129.263	Suplente	Jesus Enrique Ceballos Jiménez

Artículo 2.- Los ciudadanos designados mediante esta Resolución, enmarcará sus actuaciones, dentro de lo establecido en la Constitución de la República Bolivariana de Venezuela, y demás Leyes; y rendirá cuenta de sus actuaciones al Ministro o Ministra del Poder Popular para Educación Universitaria, Ciencia y Tecnología en los términos y condiciones que determine la Ley.

Artículo 3.- Esta Resolución entrará en vigencia a partir de la fecha de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional.

HUGBEL RAFAEL ROA CARUCI
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: 26/02/2018 **N°013**

207º, 159º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 4 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 4 de enero de 2017; lo establecido en los artículos 65 y 78 numeral 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública; y lo dispuesto en los artículos 21, 23, 37 y 46 del Reglamento de Organización y Funcionamiento de la Universidad Politécnica Territorial del Estado Portuguesa "Juan de Jesús Montilla" establecido mediante Resolución N° 056 de fecha 2 de mayo de 2017, publicado en Gaceta Oficial de la República de Venezuela N°6.321 Extraordinario de fecha 4 de agosto de 2017; este Despacho,

RESUELVE

ARTÍCULO 1: Se designan como autoridades de la **Universidad Politécnica Territorial del Estado Portuguesa "Juan de Jesús Montilla"**, a los siguientes ciudadanos:

Autoridades de la Universidad Politécnica Territorial del Estado Portuguesa "Juan de Jesús Montilla"

Rector	**FREDDY ANTONIO SILVA MARCHAN**	CÉDULA DE IDENTIDAD **N° V.- 5.945.142**
Vicerrectora Académica	**ZULAY MARBIT SILVA DE VERACIERTO**	CÉDULA DE IDENTIDAD **N° V.- 9.561.863**
Vicerrector Territorial	**LEONARDO ANTONIO MORALES GOYO**	CÉDULA DE IDENTIDAD **N° V.- 14.888.003**
Secretaría	**YASMILA DEL CARMEN FLORES CASTILLO**	CÉDULA DE IDENTIDAD **N° V.- 14.346.576**

ARTÍCULO 2: Las ciudadanas y los ciudadanos designados mediante esta Resolución, enmarcarán sus actuaciones dentro de lo establecido en la Constitución de la República Bolivariana de Venezuela, y demás leyes; y rendirán cuenta de sus actuaciones al Ministro o Ministra del

Poder Popular para Educación Universitaria, Ciencia y Tecnología en los términos y condiciones que determine la ley.

ARTÍCULO 3: Se dejan sin efecto la Resolución Nº 3.159 de fechas 27 de abril de 2012, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.911.

Así como también, se deja sin efecto la Resolución N° 179 de fecha 07 de julio de 2016, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N°40.938.

ARTÍCULO 4: Esta Resolución entrará en vigencia a partir de la fecha de su publicación en Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional

HUGBEL RAFAEL ROA CARUCI
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: **05/03/2018** **Nº 015**

207º, 159º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 04 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 04 de enero de 2017; con lo previsto en los artículos 65 y 78 numerales 19 y 27 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.147 Extraordinario de fecha 17 de noviembre de 2014, en concordancia con lo dispuesto en los artículos 5 numeral 2; 19 en su último aparte y 20 de la Ley del Estatuto de la Función Pública, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.522 de fecha 06 de septiembre de 2002, este Despacho;

RESUELVE

Artículo 1.- Designar al ciudadano **JORGE ALEXANDER ANTEQUERA SAN**, titular de la Cédula de Identidad Nº **V-15.335.346**, como Director General Encargado de la Dirección de Universalización de la Educación, adscrito al Despacho del Viceministro o de la Viceministra para la Educación y Gestión Universitaria del Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología.

Artículo 2.- El ciudadano designado mediante esta Resolución, enmarcará sus actuaciones, dentro de lo establecido en la Constitución de la República Bolivariana de Venezuela, y demás Leyes; y rendirá cuenta de sus actuaciones al Ministro o Ministra del Poder Popular para Educación Universitaria, Ciencia y Tecnología en los términos y condiciones que determine la Ley.

Artículo 3.- Esta Resolución entrará en vigencia a partir del 05 de marzo de 2018.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional.

HUGBEL RAFAEL ROA CARUCI
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: **14/03/2018** **N° 017**

AÑOS 207º, 159º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 4 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 4 de enero de 2017; lo establecido en los artículos 65 y 78 numeral 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública; en concordancia con los artículos 3 y 10 de la Resolución Nº 4021 de fecha 18 de marzo de 2013, publicada en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.130 de fecha 18 de marzo de 2013, mediante la cual se Regulan los Programas Nacionales de Formación Avanzada en el Subsistema de Educación Universitaria; este Despacho,

POR CUANTO

El Plan de la Patria formula como uno de sus objetivos estratégicos la construcción de una sociedad igualitaria y justa, a través de la formación de los distintos profesionales que se desempeñan en el área de la salud, procurando así la consolidación del Sistema Público Nacional de Salud y la profundización de la atención médica de la población venezolana en forma universal y desde la perspectiva de la promoción de la calidad de vida y el buen vivir, la prevención, diagnóstico, tratamiento, rehabilitación, oportuna y de calidad,

POR CUANTO

Los Ministerios del Poder Popular para la Salud y para Educación Universitaria Ciencia y Tecnología, como entes rectores de las políticas en materia salud y de educación universitaria, respectivamente, deben generar propuestas de formación avanzada para elevar el nivel académico y el desempeño profesional del personal de salud, con principios éticos, morales y una excelente preparación científica-técnica, con calidad y pertinencia para la transformación permanente de los determinantes del proceso salud - enfermedad a partir de la atención integral de la población, la investigación e innovación y la gestión de las redes de servicios asistenciales,

POR CUANTO

Los estudios de Formación Avanzada constituyen un proceso formativo integral de la más alta relevancia por su relación con el desarrollo científico, tecnológico, humanístico, económico y social del país que trasciende la disciplina desde la contextualización del conocimiento y de la praxis transformadora,

POR CUANTO

El Programa Nacional de Formación Avanzada en Anestesiología fue diseñado a partir del estudio de las necesidades de formación de médicos y médicas en el país, orientado hacia el desarrollo social inclusivo y humano establecido en la Constitución de la República Bolivariana de Venezuela, el Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, el Plan de Salud y los lineamientos de los Ministerios del Poder Popular para la Salud y para Educación Universitaria, Ciencia y Tecnología,

POR CUANTO

La formación de médicos y médicas especialistas en Anestesiología con pertinencia social, conocimientos, habilidades, destrezas, capacidad para resolución de problemas y portador de valores humanos, alta sensibilidad social y sentido de compromiso ético y moral para el desarrollo de acciones de diagnóstico, promoción de la salud y prevención de la enfermedad de la población en el área, en la que se enfatice y dignifique la relación médico-paciente, ocupa un lugar primordial dentro de las políticas públicas del Estado venezolano,

RESUELVE

Artículo 1. Crear el Programa Nacional de Formación Avanzada en Anestesiología, para la continuidad del proceso formativo de médicos y médicas del país, centrado en el desarrollo de un conjunto de actividades académicas, de investigación, innovación y transformación para contribuir con la atención integral en salud de la población venezolana.

Artículo 2. El Programa Nacional de Formación Avanzada en Anestesiología tiene como propósito formar médicos anestesiólogos y médicas anestesiólogas con principios éticos y morales, elevados conocimientos científicos-técnicos, docentes-asistenciales, de investigación e innovación, con una visión liberadora, humanística, con sensibilidad y compromiso social que les permita comprender las determinaciones de los problemas de salud que enfrenta y transforma en su ámbito de acción profesional, aplicando con eficiencia los conocimientos adquiridos para la realización de las diferentes técnicas anestésicas, del manejo perioperatorio y del dolor agudo y/o crónico, preservando los más altos valores de la bioética, desde una visión integradora que contribuya con el perfeccionamiento de la atención médica, el desarrollo e investigaciones y la generación de nuevos conocimientos en esta área del saber y fortalezca el Sistema Público Nacional de Salud, para optimizar el modo de atención de la población para el buen vivir.

Artículo 3. El grado académico que se otorga es Especialista en Anestesiología, una vez cumplido con la aprobación de la totalidad de las unidades curriculares exigidas por el programa que comprende 72 Unidades de Crédito, la presentación y aprobación del Trabajo Especial de Grado y los demás requisitos que apliquen.

Artículo 4. El Despacho de la Viceministra o Viceministro para Educación y Gestión Universitaria queda encargada o encargado de la ejecución de esta Resolución.

Artículo 5. Las dudas y lo no previsto en esta Resolución serán resueltas por la Ministra o Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología.

Artículo 6. Esta Resolución entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional

HUGBEL RAFAEL ROA CARUCI
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: 14/03/2018 **N° 018**

AÑOS 207º, 159º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 4 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 4 de enero de 2017; lo establecido en los artículos 65 y 78 numeral 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública; en concordancia con los artículos 3 y 10 de la Resolución Nº 4021 de fecha 18 de marzo de 2013, publicada en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.130 de fecha 18 de marzo de 2013, mediante la cual se Regulan los Programas Nacionales de Formación Avanzada en el Subsistema de Educación Universitaria; este Despacho,

POR CUANTO

El Plan de la Patria formula como uno de sus objetivos estratégicos la construcción de una sociedad igualitaria y justa, a través de la formación de los distintos profesionales que se desempeñan en el área de la salud, procurando así la consolidación del Sistema Público Nacional de Salud y la profundización de la atención médica de la población venezolana en forma universal y desde la perspectiva de la promoción de la calidad de vida y el buen vivir, la prevención, diagnóstico, tratamiento y rehabilitación oportuna y de calidad,

POR CUANTO

Los Ministerios del Poder Popular para la Salud y para Educación Universitaria Ciencia y Tecnología, como entes rectores de las políticas en materia salud y de educación universitaria, respectivamente, deben generar propuestas de formación avanzada para elevar el nivel académico y el desempeño profesional del personal de salud, con principios éticos, morales y una excelente preparación científica-técnica, con calidad y pertinencia para la transformación permanente de los determinantes del proceso salud - enfermedad a partir de la atención integral de la población, la investigación e innovación y la gestión de las redes de servicios asistenciales,

POR CUANTO

Los estudios de Formación Avanzada constituyen un proceso formativo integral de la más alta relevancia por su relación con el desarrollo científico, tecnológico, humanístico, económico y social del país que trasciende la disciplina desde la contextualización del conocimiento y de la praxis transformadora,

POR CUANTO

El Programa Nacional de Formación Avanzada en Medicina Interna fue diseñado a partir del estudio de las necesidades de formación de médicos y médicas en el país para la atención integral de la población adulta desde un enfoque inclusivo y humano establecido en la Constitución de la República Bolivariana de Venezuela, el Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, el Plan de Salud y los lineamientos de los Ministerios del Poder Popular para la Salud y para Educación Universitaria, Ciencia y Tecnología,

POR CUANTO

La formación de médicos y médicas especialistas en Medicina Interna con pertinencia social, conocimientos, habilidades, destrezas, capacidad para resolución de problemas y portador de valores humanos, alta sensibilidad social y sentido de compromiso ético y moral para el desarrollo de acciones de diagnóstico, promoción de la salud y prevención de las enfermedades no quirúrgicas en personas adultas en la que se enfatice, dignifique y humanice la relación médico-paciente, ocupa un lugar primordial dentro de las políticas públicas del Estado venezolano,

RESUELVE

Artículo 1. Crear el Programa Nacional de Formación Avanzada en Medicina Interna, para la continuidad del proceso formativo de médicos y médicas del país, centrado en el desarrollo de un conjunto de actividades académicas, de investigación, innovación y transformación para contribuir con el mejoramiento de la atención a la salud de la población adulta.

Artículo 2. El Programa Nacional de Formación Avanzada en Medicina Interna tiene como propósito formar médicos y médicas especialistas con principios éticos y morales, elevados conocimientos y prácticas que le permitan desarrollar capacidades para identificar e incidir sobre los determinantes sociales del proceso salud-enfermedad y la realización de acciones de diagnóstico, promoción de la salud y prevención de la enfermedades no quirúrgicas en personas adultas en los establecimientos de la Red Integrada del Sistema Público Nacional de Salud que se ha venido estructurando en el país, desde la perspectiva de transformación social que ha propiciado la revolución bolivariana, con una racionalidad enraizada en los valores de solidaridad, inclusión, respeto al otro y a la diversidad, comprometidos con las necesidades sociales, políticas, económicas en el contexto nacional, latinoamericano y mundial, apropiándose de su papel transformador e impulsor de cambios que la atención a la salud requiere para el buen vivir.

Artículo 3. El grado académico que se otorga es Especialista en Medicina Interna, una vez cumplido con la aprobación de la totalidad de las unidades curriculares exigidas por el programa que comprende 72 Unidades de Crédito, la presentación y aprobación del Trabajo Especial de Grado y los demás requisitos que apliquen.

Artículo 4. El Despacho de la Viceministra o Viceministro para Educación y Gestión Universitaria queda encargada o encargado de la ejecución de esta Resolución.

Artículo 5. Las dudas y lo no previsto en esta Resolución serán resueltas por la Ministra o Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología.

Artículo 6. Esta Resolución entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional.

HUGBEL RAFAEL ROA CARRERO
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: 14/03/2018 **N° 019**

AÑOS 207º, 159º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 4 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 4 de enero de 2017; lo establecido en los artículos 65 y 78 numeral 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública; en concordancia con los artículos 3 y 10 de la Resolución Nº 4021 de fecha 18 de marzo de 2013, publicada en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.130 de fecha 18 de marzo de 2013, mediante la cual se Regulan los Programas Nacionales de Formación Avanzada en el Subsistema de Educación Universitaria; este Despacho,

POR CUANTO

El Plan de la Patria formula como uno de sus objetivos estratégicos la construcción de una sociedad igualitaria y justa, a través de la formación de los distintos profesionales que se desempeñan en el área de la salud, procurando así la consolidación del Sistema Público Nacional de Salud y la profundización de la atención médica de la población venezolana en forma universal y desde la perspectiva de la promoción de la calidad de vida y el buen vivir, la prevención, diagnóstico, tratamiento y rehabilitación oportuna y de calidad,

POR CUANTO

Los Ministerios del Poder Popular para la Salud y para Educación Universitaria Ciencia y Tecnología, como entes rectores de las políticas en materia salud y de educación universitaria, respectivamente, deben generar propuestas de formación avanzada para elevar el nivel académico y el desempeño profesional del personal de salud, con principios éticos, morales y una excelente preparación científica-técnica, con calidad y pertinencia para la transformación permanente de los determinantes del proceso salud - enfermedad a partir de la atención integral de la población, la investigación e innovación y la gestión de las redes de servicios asistenciales,

POR CUANTO

Los estudios de Formación Avanzada constituyen un proceso formativo integral de la más alta relevancia por su relación con el desarrollo científico, tecnológico, humanístico, económico y social del país que trasciende la disciplina desde la contextualización del conocimiento y de la praxis transformadora,

POR CUANTO

Que el Programa Nacional de Formación Avanzada en Pediatría y Puericultura fue diseñado a partir del estudio de las necesidades de formación de médicos y médicas en el país, para la atención integral en salud de los niños y niñas y adolescentes desde un enfoque inclusivo y humano establecido en la Constitución de la República Bolivariana de Venezuela, el Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, el Plan de Salud y los lineamientos de los Ministerios del Poder Popular para la Salud y para Educación Universitaria, Ciencia y Tecnología,

POR CUANTO

La formación de médicos y médicas especialistas en Pediatría y Puericultura con pertinencia social, conocimientos, habilidades, destrezas, capacidad para resolución de problemas y portador de valores humanos, alta sensibilidad social y sentido de compromiso

ético y moral para el desarrollo de acciones de diagnóstico, promoción de la salud y prevención de la enfermedad de los niños, niñas y adolescentes que dignifique y humanice la parte humana en la relación médico-paciente, ocupa un lugar primordial dentro de las políticas públicas del Estado venezolano,

RESUELVE

Artículo 1. Crear el Programa Nacional de Formación Avanzada en Pediatría y Puericultura para la continuidad del proceso formativo de médicos y médicas del país, centrado en el desarrollo de un conjunto de actividades académicas, de investigación, innovación y transformación para contribuir con la atención integral en salud de niños, niñas y adolescentes.

Artículo 2. El Programa Nacional de Formación Avanzada tiene como propósito formar médicos y médicas especialistas en Pediatría y Puericultura con principios éticos y morales, conocimientos y prácticas que les permitan desarrollar capacidades para identificar e incidir sobre los determinantes sociales del proceso salud-enfermedad y brindar atención integral de salud a niños, niñas y adolescentes en los establecimientos de la Red Integrada del Sistema Público Nacional de Salud que se ha venido estructurando en el país desde la perspectiva de transformación social, que ha propiciado la revolución bolivariana.

Artículo 3. El grado académico que se otorga es Especialista en Pediatría y Puericultura una vez cumplido con la aprobación de la totalidad de las unidades curriculares exigidas por el programa que comprende 72 Unidades de Crédito, la presentación y aprobación del Trabajo Especial de Grado y los demás requisitos que apliquen.

Artículo 4. El Despacho de la Viceministra o Viceministro para Educación y Gestión Universitaria queda encargada o encargado de la ejecución de esta Resolución.

Artículo 5. Las dudas y lo no previsto en esta Resolución serán resueltas por la Ministra o Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología.

Artículo 6. Esta Resolución entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional.

HUGBEL RAFAEL ROA CARUCI
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
DESPACHO DEL MINISTRO

FECHA: 14/03/2018 **N° 020**

AÑOS 207º, 159º y 19º

RESOLUCIÓN

De conformidad con el artículo 3 del Decreto Presidencial Nº 2.652 de fecha 4 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.067 de fecha 4 de enero de 2017; lo establecido en los artículos 65 y 78 numeral 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública; en concordancia con los artículos 3 y 10 de la Resolución Nº 4021 de fecha 18 de marzo de 2013, publicada en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.130 de fecha 18 de marzo de 2013, mediante la cual se Regulan los Programas Nacionales de Formación Avanzada en el Subsistema de Educación Universitaria; este Despacho,

POR CUANTO

El Plan de la Patria formula como uno de sus objetivos estratégicos la construcción de una sociedad igualitaria y justa, a través de la formación de los distintos profesionales que se desempeñan en el área de la salud, procurando así la consolidación del Sistema Público Nacional de Salud y la profundización de la atención médica de la población venezolana en forma universal y desde la perspectiva de la promoción de la calidad de vida y el buen vivir, la prevención, diagnóstico, tratamiento y rehabilitación oportuna y de calidad,

POR CUANTO

Que los Ministerios del Poder Popular para la Salud y para Educación Universitaria, Ciencia y Tecnología, como entes rectores de las políticas en materia salud y de educación universitaria, respectivamente, deben generar propuestas de formación avanzada para elevar el nivel académico y el desempeño profesional del personal de salud, con principios éticos, morales y una excelente preparación científica-técnica, con calidad y pertinencia para la transformación permanente de los determinantes del proceso salud-enfermedad a partir de la atención integral de la población, la investigación e innovación y la gestión de las redes de servicios asistenciales,

POR CUANTO

Que los estudios de Formación Avanzada constituyen un proceso formativo integral de la más alta relevancia por su relación con el desarrollo científico, tecnológico, humanístico, económico y social del país que trasciende la disciplina desde la contextualización del conocimiento y de la praxis transformadora,

POR CUANTO

El Programa Nacional de Formación Avanzada en Cirugía Ortopédica y Traumatológica fue diseñado a partir del estudio de las necesidades de formación de médicos y médicas en el país, orientado hacia el desarrollo social inclusivo y humano establecido en la Constitución de la República Bolivariana de Venezuela, el Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, el Plan de Salud y los lineamientos del Ministerio del Poder Popular para la Salud y los lineamientos de los Ministerios del Poder Popular para la Salud y para Educación Universitaria, Ciencia y Tecnología,

POR CUANTO

Que la formación de médicos y médicas especialistas en Cirugía Ortopédica y Traumatológica con pertinencia social, conocimientos, habilidades, destrezas, capacidad para resolución de problemas y portador de valores humanos, alta sensibilidad social y sentido de compromiso ético y moral para el desarrollo de acciones de diagnóstico, promoción de la salud y prevención de la enfermedad en el área osteomusculoarticular médica y quirúrgicas de la población en general, en la que se dignifique la relación médico-paciente, ocupa un lugar primordial dentro de las políticas públicas del Estado venezolano,

RESUELVE

Artículo 1. Crear el Programa Nacional de Formación Avanzada en Cirugía Ortopédica y Traumatológica, para la continuidad del proceso formativo de médicos y médicas especialistas del país, centrado en el desarrollo de un conjunto de actividades académicas, de investigación, innovación y transformación para contribuir con la atención integral en el área osteomusculoarticular médicas y quirúrgicas de la población en general.

Artículo 2. El Programa Nacional de Formación Avanzada en Cirugía Ortopédica y Traumatológica tiene como propósito formar médicos y médicas especialistas con principios éticos y morales y conocimiento de las determinaciones sociales de la enfermedad y su enfoque preventivo, desde la mirada de la familia y la comunidad como parte integral del ser humano, con enfoque transdisciplinario, interdisciplinario, humanístico y científico, investigativo para la generación de nuevos conocimientos desde la práctica profesional, con capacidades de introducir aportes de la ciencia y la técnica desde la actividad laboral diaria en la solución de los diversos problemas de salud del área osteomusculoarticular médicas y quirúrgicas de la población en general para el buen vivir.

Artículo 3. El grado académico que se otorga es Especialista en Cirugía Ortopédica y Traumatológica, una vez cumplido con la aprobación de la totalidad de las unidades curriculares exigidas por el programa que comprende 92 Unidades de Crédito, la presentación y aprobación del Trabajo Especial de Grado y los demás requisitos que apliquen.

Artículo 4. El Despacho de la Viceministra o Viceministro para Educación y Gestión Universitaria queda encargada o encargado de la ejecución de esta Resolución.

Artículo 5. Las dudas y lo no previsto en esta Resolución serán resueltas por la Ministra o Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología.

Artículo 6. Esta Resolución entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese,
Por el Ejecutivo Nacional.

HUGBEL RAFAEL ROA CARUCI
Ministro del Poder Popular para Educación Universitaria, Ciencia y Tecnología
Decreto N° 2.652 de fecha 04 de enero de 2017
Gaceta Oficial N° 41.067 de fecha 04 de enero de 2017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
CONSEJO NACIONAL DE UNIVERSIDADES
SECRETARIADO PERMANENTE
Caracas, 20 de febrero de 2018
ACUERDO N° 001

Años 207°,159° y 19°

De conformidad con lo establecido en el Decreto N° **2.652** de fecha 04 de enero de 2017, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela . N° **41.067** de fecha 04 de enero de 2017, en relación con lo preceptuado en el artículo **23** de la Ley de Universidades y el artículo **2 y 3** del Reglamento Interno del Consejo Nacional de Universidades, y de conformidad con lo dispuesto por el Consejo Nacional de Universidades en su Sesión Ordinaria N° **533** de fecha 07 de febrero de 2018,

ACUERDA

Artículo 1-. Aprobar el calendario anual de las sesiones ordinarias del Consejo Nacional de Universidades, a realizarse durante el año 2018.

Calendario Anual de reuniones Ordinarias – Año 2018

Enero	**Febrero 27**	**Marzo 20**	**Abril 24**
Mayo 29	**Junio 26**	**Julio 31**	**Agosto Vacaciones**
Septiembre 25	**Octubre 30**	**Noviembre 27**	**Diciembre 11**

Artículo 2-. El presente Acuerdo entrará en vigencia a partir del veinte (20) del mes de febrero del año 2018.

COMUNÍQUESE y PUBLÍQUESE,

HUGBEL RAFAEL ROA CARUCI
Presidente del
Consejo Nacional de Universidades

ASALIA R. VENEGAS S.
Secretaria Permanente

CONSULTORÍA JURÍDICA MPPEUCT VISTO

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA
EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

Caracas, 26 de febrero de 2018

207º, 158º y 19°

Quien suscribe, **LUIS FERNANDO PRADA FUENTES**, titular de la cédula de identidad N° **V-17.059.842**, designado como Superintendente de Servicios de Certificación Electrónica, según nombramiento contenido en la Resolución N° 095, de fecha 19 de junio de 2017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.177, de fecha 21 de junio de 2017; en ejercicio de las atribuciones conferidas en el artículo 22, numeral 1 y 2 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148, de fecha 28 de febrero de 2001; de conformidad con lo previsto en los artículos 4, 10, 12 y 26 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Extraordinario N° 6.147, de fecha 17 de noviembre de 2014; y con el artículo 72 de la Ley Orgánica de Procedimientos Administrativos, publicada en la Gaceta Oficial de la República de Venezuela N° 2.818 Extraordinario, de fecha 01 de julio de 1981, en observancia con los estándares Internacionales que rigen la materia; dicta la siguiente:

PROVIDENCIA ADMINISTRATIVA Nº 001 -2018

Artículo 1. La presente Providencia Administrativa, tiene por objeto describir la Infraestructura Nacional de Certificación Electrónica, su estructura, certificados y listas de certificados revocados; conforme a los lineamientos establecidos por la Superintendencia de Servicios de Certificación Electrónica **(SUSCERTE)**. Así mismo, contempla la estructura mínima necesaria que deben tener los certificados y los valores que deben estar presentes en sus campos con el propósito de mantener la coherencia en los perfiles generados por los PSC acreditados ante la Superintendencia.

De conformidad con lo dispuesto en el artículo 22, numerales 1° y 5° y el artículo 27 del Decreto con Fuerza de Ley sobre Mensaje de Datos y Firmas Electrónicas; en concordancia con el artículo 36 del Reglamento Parcial Del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.

Artículo 2. La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), define en la presente providencia los aspectos técnicos de la Infraestructura Nacional de Certificación Electrónica, los certificados creados y emitidos bajo la misma; detalla su clasificación, valores, estructura y organización interna; especifica los requerimientos de las listas de certificados revocados y su estructura interna, según el procedimiento identificado como **NORMA SUSCERTE 032-06/17** edición 3.2 de fecha 30 de Junio de 2017; cuyo tenor es el siguiente:

"INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA: ESTRUCTURA, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS"

NORMA SUSCERTE Nº 032-06/2017, EDICIÓN Nº: 3.2, FECHA: 06/2017

1. PRELIMINARES

1.1. Objeto y Campo de Aplicación

La presente norma describe la Infraestructura Nacional de Certificación Electrónica, su estructura, certificados y listas de certificados revocados; conforme a los lineamientos presentados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

Así mismo, se presenta la estructura mínima necesaria que deben tener los certificados y los valores que deben estar presentes en sus campos con el propósito de mantener la coherencia en los perfiles generados por los PSC acreditados ante la Superintendencia.

1.2. Referencias Normativas

.- Constitución de la República Bolivariana de Venezuela.

.- Decreto con Fuerza de Ley 1.204 Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE) (Febrero 2001).

.- Reglamento Parcial de la Ley Sobre Mensajes de Datos y Firmas Electrónicas (Diciembre 2004).

.- Providencia Administrativa Nº 016 de SUSCERTE (Febrero 2007).

.- ITU-T Rec. X.509 V.3 Tecnología de la Información. Interconexión de Sistemas abiertos - El Directorio: Marcos para certificados de claves públicas y atributos (2008).

.- RFC 5280 PKIX Certificate and CRL Profile (2008).

.- RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2013).

.- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile (2004).

.- RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (2002).

.- 3erd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification 3GPP TS 23.003.

1.3. Definiciones y Terminologías

A los efectos de esta norma se establecen las siguientes definiciones y terminologías:

CERTIFICADO ELECTRÓNICO	Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación (PSC) que le atribuye certeza y validez a la firma electrónica
IDENTIFICADOR DE OBJETO	Valor universal único asociado a un objeto para identificarlo inequívocamente.
FUNCIÓN HASH	Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas de caracteres, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
LISTA DE CERTIFICADOS REVOCADOS	Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por ella.
SIGNATARIO	Entidad identificada en un certificado electrónico, quien usa la clave privada para firmar electrónicamente, y que se encuentra asociada con la clave pública del certificado.
SUSCRIPTOR	Persona que contrata la generación de un certificado electrónico con un proveedor de servicios de certificación.

1.4. Símbolos y Abreviaturas

A los efectos de esta norma se establecen los siguientes símbolos y abreviaturas:

AC	Autoridad de Certificación.
AR	Autoridad de Registro.
ASN.1	Abstract Syntax Notation One – Notación de Sintaxis Abstracta Uno.
DPC	Declaración de Prácticas de Certificación.
GSM	Sistema global para las comunicaciones móviles, es un sistema estándar ampliamente utilizado en redes de telefonía celular de segunda, tercera y cuarta generación.
HSM	Hardware Security Module. (Módulo de Seguridad de Hardware)
IMEI	Identidad internacional de equipo móvil, es un código USSD pregrabado en los teléfonos móviles GSM. Código que identifica univocamente al dispositivo móvil y es transmitido por éste una vez que se ha conectado a la red a la cual pertenezca.
ITU-T	International Telecommunications Union-Telecommunications. (Unión Internacional de Telecomunicaciones.)
LCR	Lista de Certificados Revocados.
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
OID	Identificador de Objeto.
OCSP	Online Certificate Status Protocol (Protocolo de estado de certificados en línea).
PC	Política de Certificados.
PSC	Proveedor de Servicios de Certificación.
RBV	República Bolivariana de Venezuela.
RPLSMDFE	Reglamento Parcial de Ley Sobre Mensajes de Datos y Firmas Electrónicas.
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.
URI	Uniform Resource Identifier (Identificador de recurso uniforme)
USSD	Servicio suplementario de datos no estructurados, es un servicio para el envío de datos a través de dispositivos móviles GSM.
MAC	*Media Access Control*, es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a un dispositivo de red. Se conoce también como dirección física. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el *Organizationally Unique Identifier*.

2. DESARROLLO

2.1. Consideraciones Generales

2.1.1 La presente norma tiene como principio describir los aspectos técnicos asociados a la Infraestructura Nacional de Certificación Electrónica, los certificados creados y emitidos bajo la misma; detallar su clasificación, valores, estructura y organización interna; especificar los requerimientos de las listas de certificados revocados y su estructura interna.

2.1.2 Para la selección del modelo de la Infraestructura Nacional de Certificación Electrónica, se realizó un estudio de las diferentes topologías de Infraestructura de Claves Públicas, seleccionándose el modelo jerárquico con una Autoridad de Certificación Raíz única nacional de la cual dependen los Proveedores de Servicios de Certificación Acreditados y los Casos especiales.

2.1.3 Este modelo de arquitectura jerárquica, debe ser adoptado por todo Proveedor de Servicios de Certificación (PSC) que desee solicitar su acreditación ante SUSCERTE.

2.1.4 En la Figura Nº 1 se establecen las relaciones de confianza basadas en la arquitectura jerárquica con una única raíz de la Infraestructura Nacional de Certificación Electrónica.

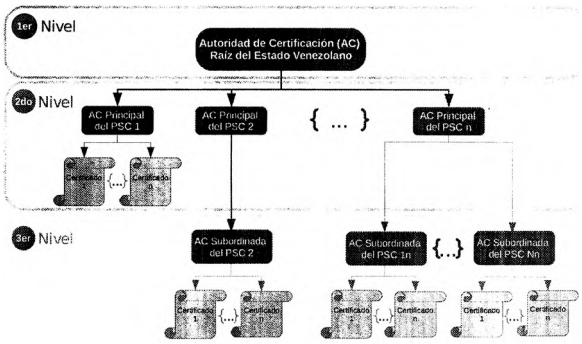


Figura Nº 1. *Modelo de Jerarquía.*

2.1.5 SUSCERTE es el ente rector y responsable de la Infraestructura Nacional de Certificación Electrónica, a través de la Autoridad de Certificación Raíz del Estado Venezolano.

2.1.6 La relación de confianza sólo se especifica en una dirección. La Autoridad de Certificación Raíz es quien emite los certificados a los PSC y estos a su vez pueden generar y emitir certificados a usuarios finales o AC subordinadas, más no pueden emitir certificados a su AC superior.

2.1.7 En la arquitectura jerárquica de la Infraestructura Nacional de Certificación Electrónica, se permite que los PSC constituyan por debajo de ellos un solo nivel de AC subordinadas.

2.1.8 Con el fin de segmentar los riesgos, un PSC que constituya al menos una AC subordinada no podrá emitir certificados a usuarios finales con su AC principal, de manera que si una de estas se ve comprometida no afectará a las otras.

2.1.9 No existe otra AC que pueda firmar el certificado de la AC Raíz. Este es el único caso en el que la AC raíz crea un certificado autofirmado.

2.1.10 La AC Raíz firma los certificados electrónicos de las AC principales de los PSC, AC de casos especiales, su Lista de Certificados Revocados (LCR) y certificado del servicio OCSP de la AC raíz.

2.1.11 La AC Raíz genera y firma los certificados de la AC principal de los PSC éstos PSC, a su vez, generan y firman los certificados de usuarios finales o de sus AC subordinadas y estas sólo generan y firman los certificados de sus usuarios finales.

2.1.12 La AC Raíz establece las condiciones para los tipos de certificados que pueden emitir las AC de los PSC.

2.2. Consideraciones Específicas

2.2.1 Cada PSC debe contar con una AC principal y una o varias AR encargadas de atender a su comunidad de usuarios.

2.2.2 Los PSC son responsables de la gestión (generación, suspensión y revocación) de los certificados electrónicos de sus signatarios y no de los usos posteriores que estos le den a los certificados. Sin embargo, los PSC deben velar por el buen uso de los certificados en función de las obligaciones que el signatario asume como usuario del servicio de certificación de acuerdo al Decreto con Fuerza Ley Sobre Mensaje de Datos y Firmas Electrónicas.

2.2.3 Los PSC pueden gestionar varios tipos de certificados de acuerdo al tipo de signatario:

a) Certificados de AC: son los únicos que se pueden utilizar para firmar otras AC o certificados de usuario final, se deben tener condiciones especiales de generación y resguardo de los mismos.

b) Certificado para Personas: cuando el signatario sea una persona, quien en nombre propio o representación de tercero, y previa validación de la identidad y del suscriptor ante la autoridad que expide el certificado, solicita la generación del mismo, con lo cual tendrá a su disposición el certificado electrónico mediante el uso de dispositivos criptográficos para tal fin (tarjeta inteligente, token USB, entre otros) o de software.

c) Certificado para Sistemas: serán usados por componentes, equipos y/o dispositivos que requieran o no de la intervención directa de la persona. El certificado reside en un almacén basado en software o hardware.

d) Certificados para Operaciones de ICP: destinados a las operaciones y servicios requeridas para el funcionamiento óptimo de la AC y/o AR del AC raíz, AC Principales y AC Subordinadas.

Todos los certificados deben ser evaluados y aprobados por parte de SUSCERTE utilizando esta norma como directriz.

2.2.4 Los tipos de certificados electrónicos a ser emitidos por los PSC deben cumplir con lo establecido en la presente Norma y en los estándares en la materia, someterse a la consideración, evaluación y aprobación por parte de SUSCERTE, a efectos de asegurar su interoperabilidad en la Infraestructura Nacional de Certificación Electrónica.

2.2.5 Los tipos de certificados, los dispositivos para la generación y almacenamiento del par de claves, la vigencia y el tamaño mínimo del par de claves se muestran en la Tabla Nº 1.

Tabla Nº 1. *Tipos de Certificados, dispositivo, almacenamiento, vigencia y tamaño del par de claves*

PARA AUTORIDADES DE CERTIFICACIÓN			
Tipo de Certificado	**Dispositivo para Generación y Almacenamiento del par de claves**	**Vigencia Máxima en años**	**Tamaño Mínimo del par de claves (bits)**
AC Raíz	Hardware (HSM)	20	4096
AC Principal PSC		10	4096
AC Subordinada PSC		5	4096
AC Caso Especial		1	4096

PARA USUARIO FINAL			
Tipo de Certificado	**Dispositivo para Generación y Almacenamiento del par de claves**	**Vigencia Máxima en meses**	**Tamaño Mínimo del par de claves (bits)**
Para persona	Software	12	2048
	Hardware (token criptográfico, tarjeta inteligente)	24	2048
Para software o aplicaciones	Software	12	2048
	Hardware (HSM)	24	2048

2.2.6 Es obligatorio el uso de HSM para la generación y el almacenamiento del par de claves para los certificados de la AC Raíz, AC Principal del PSC, AC Subordinadas del PSC y AC Caso Especial.

2.2.7 Los procedimientos para las solicitudes y emisiones de los pares de claves, se especificarán en la Declaración de Prácticas de Certificación (DPC) del PSC y en las PC.

2.2.8 Los procedimientos en caso de pérdida, reemplazo o renovación de algún certificado, se establecerán en la DPC y/o PC del PSC.

2.2.9 El signatario y suscriptor deben conocer las políticas de uso de los certificados electrónicos establecidas por el PSC para dar curso a las buenas prácticas y al uso permitido de los mismos. Para ello, el PSC deberá promover que los signatarios y suscriptores conozcan dichas políticas. En caso de menores de edad se someterá a la evaluación del carácter legal del certificado por parte de SUSCERTE y el PSC, para los casos que se presenten. En el caso de extranjeros serán identificados en el certificado electrónico con su número de pasaporte.

2.3. Procedimiento General

2.3.1 Los certificados generados y firmados bajo la Infraestructura Nacional de Certificación Electrónica son los definidos para X.509v3, así como lo establecido en el RFC 3739 (Internet X.509 Public Key Infrastructure. Qualified Certificates Profile). Dicho estándar define la siguiente estructura general: Datos del certificado, Datos del emisor, Periodo de validez, Datos del titular, Información de clave pública y Extensiones.

2.3.2 En la sección de Datos del Certificado se debe incluir la versión, serial y algoritmo de firma.

2.3.2.1 La versión contemplada para los certificados emitidos en la Infraestructura Nacional de Certificación Electrónica es la Versión 3 (Indicado por el entero 2).

2.3.2.2 El serial, contemplado en los Datos del Certificado, es el valor entero único asignado por la AC al emitir el certificado. Puede ser expresado en formato hexadecimal de 20 octetos. Este valor no puede ser negativo.

2.3.2.3 El algoritmo de firma es el algoritmo SHA256 para los Certificados Electrónicos de Entidad Final con longitud de cifrado de 2048bits y para los Certificados Electrónicos de AC la longitud de cifrado es de 4096bits.

2.3.3 El Emisor (issuer) del certificado contiene información que identifica unívocamente al PSC emisor del certificado electrónico. Dicha información es de tipo *Distinguished Name*.

2.3.3.1 La nomenclatura que debe utilizarse para los campos de tipo nombre distinguido (Distinguished Name - DN). Los atributos utilizados para identificar al emisor y titular del certificado son definidos por el RFC 3739 (Ver Anexo C).

2.3.3.2 El DN Serial Number (serialNumber) debe identificar al PSC a través del R.I.F. (Ver Anexo A).

2.3.4 La validez del certificado contiene la fecha exacta de emisión (noBefore) y de expiración del certificado (noAfter). Debe ser expresada en formato UTC (GMT 0) y coincidir con los límites establecidos por esta norma (Ver Vigencia en la Tabla N° 1).

2.3.5 El Titular (subject) del certificado contiene información que identifica unívocamente al mismo del certificado electrónico. Dicha información es de tipo Distinguished Name. El formato de dicho campo al igual que en Distinguished Name y se debe garantizar que dichos atributos lo distingan unívocamente.

2.3.6 La Información de Clave Pública del Titular deberá especificar el algoritmo y otras características del cifrado de la misma.

2.3.7 Las extensiones de los certificados constituyen métodos para asociar información del certificado, emisor y titular. Dichas extensiones pueden ser carácter crítico o no crítico, que le permite ser ignorada o no por un sistema.

2.3.7.1 Como mínimo, los certificados, deben poseer las siguientes extensiones: Restricciones Básicas, Clave de Uso, Identificador de clave de Titular, Identificador de clave de Autoridad Certificadora, Clave de Usos Extendidos, Nombre Alternativo del Titular, Nombre Alternativo del Emisor, Puntos de Distribución de las LCR, Acceso a la Información de Autoridad (AIA) y Política de Certificación (PC).

2.3.7.2 La extensión Restricciones Básicas (basicConstrain) es de carácter crítico, determina si el certificado será utilizado como AC y especifica si puede firmar otra AC.

2.3.7.3 La extensión Clave de Uso (Key Usage) es de carácter crítico y puede tener los siguientes valores habilitados: Firma digital, Compromiso con el Contenido, Cifrado de claves, Cifrado de datos, Acuerdo de claves, Firma de certificado, Firma de LCR, Solo cifrado y Solo descifrado (Ver Anexo D).

Las Claves de Uso: Firma de Certificado y Firma de LCR están reservadas exclusivamente a los certificados de AC raíz, AC principal y AC subordinada.

La Clave de Uso "No Repudio" fue renombrada "Compromiso o Vinculación con el Contenido".

Para la elaboración de Políticas de Certificación se debe utilizar "Compromiso con el Contenido".

2.3.7.4 El Identificador de Clave de Titular contiene el resultado de la Función Hash sobre la Clave Pública del Titular.

2.3.7.5 El Identificador de clave de Autoridad Certificadora contiene el resultado de la Función Hash sobre la Clave Pública de la Autoridad de Certificación, Nombre y Serial de la misma.

2.3.7.6 La Clave de Uso Extendido puede ser de carácter crítico o no crítico y complementan la funcionalidad de un certificado. El PSC podrá incorporar tantos Usos de Clave Extendidos como sean necesarios de acuerdo a la Política de Certificación. Ver Anexo E.

2.3.7.7 Nombre Alternativo del Titular, es una extensión de carácter no crítico. Debe contener uno o más nombres alternativos en formato de Nombres Generales (General Name – GN). Ver la Anexo B.

2.3.7.8 Nombre Alternativo del Emisor, es una extensión de carácter no crítico. Debe contener uno o más nombres alternativos en formato de Nombres Generales (General Name – GN). Ver la Anexo B.

2.3.7.9 En Puntos de Distribución de las LCR se deben colocar al menos un punto para poder validar el estatus del certificado.

2.3.7.10 El Acceso a la Información de la Autoridad (Authority Info Access) está destinada a contener el método y URL donde se puede consultar el estatus del certificado. Estos pueden ser servicios como LDAP, OCSP y otras soportadas por el estándar X.509.

2.3.7.11 Las Políticas de Certificación deben contener información que identifique las políticas bajo las cuales fue emitido el certificado y donde se puede obtener dicha documentación.

Si el PSC contiene más de una política u otra documentación en la ubicación a la que hace referencia en esta extensión, debe proveer información que permita reconocer exactamente a cuál PC está asociada el certificado.

2.3.7.1 Las limitaciones de uso de cada tipo de certificado deben estar establecidas en su correspondiente política de certificados.

2.3.8 La Lista de Certificados Revocados es un instrumento de validación del estatus de un certificado electrónico definido en el RFC 5280. Esta contiene los números seriales, fecha y motivo de suspensión y/o revocación de los certificados electrónicos. Estos deben estar ordenados por tiempo de ingreso a la lista y deben permanecer en ella a pesar de expirar por motivos de seguridad.

2.3.9 Todo campo que no este clasificado en la estructura del certificado (Anexo J) como opcional, es obligatorio.

2.3.10 En caso de que el PSC o Caso Especial estimen, en sus políticas de certificados campos adicionales a los obligatorios por esta Norma, para la estructura de los certificados electrónicos y de la LCR, deben ceñirse a lo estipulado como campos opcionales tanto en su denominación como uso.

2.3.11 En caso de que el PSC o Caso Especial estimen, en sus políticas de certificados campos adicionales a los obligatorios por esta Norma, para la estructura de los certificados electrónicos y de la LCR, y ninguno de los campos opcionales estipulados cumplan en su denominación y uso, quedará a juicio de SUSCERTE aprobar su empleo o no en función de los estándares internacionales.

3. PARTE FINAL

3.1. Disposiciones transitorias

PRIMERA: A partir de la fecha de publicación en gaceta de esta Norma, se deberá iniciar un proceso de actualización de sus políticas de certificación y las plantillas de los certificados electrónicos que no cumplan con lo aquí previsto, por parte de los Proveedores de Servicio de Certificación (PSC) acreditados, a tales efectos se estima un período de 12 meses contados a partir de su publicación. Durante ese lapso el PSC debe consignar ante SUSCERTE informes trimestrales donde se evidencie el alcance y avance de esta actualización. De igual forma, SUSCERTE como parte de este proceso de actualización por parte de los PSC, debe realizar la asignación de los OID requeridos para permitir dichas actualizaciones.

SEGUNDA: Para que los certificados de la Cadena de Confianza Nacional cumplan con lo establecido en esta Norma, los certificados electrónicos de las autoridades de certificación (AC Raíz, AC Principal de los PSC, AC Subordinada del PSC y AC de los Casos Especiales), que estén en producción, pasaran por un proceso de migración iniciándo por la AC Raíz, a través del cual se generarán nuevos certificados electrónicos a las autoridades de certificación.

3.2. Disposiciones finales

Si los estándares y recomendaciones internacionales utilizados para la elaboración de esta norma son actualizados o reemplazados, SUSCERTE puede solicitar a los PSC aplicar dichos cambios a fin de garantizar el funcionamiento óptimo de la Infraestructura Nacional de Certificación Electrónica.

Para los casos en que no se hace una mención explícita sobre un aspecto en particular, se debe utilizar como recomendación, lo establecido en las referencias normativas de este documento.

4. ANEXOS

Los anexos constituyen parte integral de la norma y deben ser de cumplimiento obligatorio por los PSC.

4.1 Anexo A: Uso del *DN Serial Number*

Se debe utilizar para identificar unívocamente al emisor, titular y/o propietario del certificado electrónico. Es responsabilidad de la Autoridad de Registro verificar que se aplique el correspondiente según esta norma y la PC bajo la cual se emitió el certificado.

Para identificar personas se debe utilizar la Cédula de Identidad (C.I.), Registro Único de Información Fiscal (R.I.F) o Número de Pasaporte.

Para identificar organizaciones y empresas públicas o privadas se debe utilizar el Registro Único de Información Fiscal (R.I.F).

Para identificar dispositivos, sistemas o componentes de sistema se deben utilizar la Dirección MAC, DNS, IMEI según sea el caso.

Como última opción SUSCERTE podrá asignar y autorizar la utilización de Identificador de Objeto Único (OID) para distinguir al sujeto.

La cédula de identidad deberá incluir en un literal la nacionalidad del titular (V o E) y los dígitos que lo identifican en el siguiente formato: V-00000000 o E-00000000 según sea el caso.

El Registro Único de Información Fiscal deberá seguir el formato del ente emisor, ejemplo: V-00000000, G-000000000, J-000000000

El Pasaporte deberá incluir todos los dígitos de dicho documento.

DNS o Sistema de Dominio de Nombres identifica de manera jerárquica a sistemas conectados a internet.

La dirección MAC es definida por 48 bits que identifican de manera única al dispositivo de red. Se compone de 6 bloques en formato hexadecimal de la siguiente manera xx-xx-xx-xx-xx-xx o xx:xx:xx:xx:xx:xx.

El código IMEI debe tener de 15 a 16 dígitos basado en el estándar internacional 3GPP TS 23.003.

4.2 Anexo B: Nombres Generales

Nombre	X.509	Tipo de Dato
Otro Nombre	otherName	OtherName
Nombre RFC822	rfc822Name	IA5String
Nombre DNS	dNSName	IA5String
Dirección X400	x400Address	ORAddress
Nombre de Directorio	directoryName	Name
Nombre de Identificación de Datos Electrónicos	ediPartyName	EDIPartyName
Identificador Uniforme de Recursos	uniformResourceIdentifier	IA5String
Dirección IP	iPAddress	OCTET STRING
ID registrada	registeredID	OBJECT IDENTIFIER

4.3 Anexo C: Nombres Distinguidos

Nombre	X.509	O.I.D.
Nombre Común	commonName	2.5.4.3
Organización	organization	2.5.4.10
Departamento	organizationalUnity	2.5.4.11
País	country	2.5.4.6
Correo Electrónico	emailAddress	1.2.840.113549.1.9.1
Localidad	locality	2.5.4.7
Estado	state	2.5.4.8
Título	title	2.5.4.12
Teléfono	telephoneNumber	2.5.4.20
Categoría de Negocio	businessCategory	2.5.4.15
Nombre	givenName	2.5.4.42
Apellido	surName	2.5.4.4
Identificador de documento	documentIdentifier	0.9.2342.19200300.100.1.11
Serial	serialNumber	2.5.4.5
Iniciales	initials	2.5.4.43
Descripción	description	2.5.4.13
Propietario	owner	2.5.4.32
Título de Documento	documentTitle	0.9.2342.19200300.100.1.12
Hospedaje	host	0.9.2342.19200300.100.1.9
Calle(Dirección)	streetAddress	2.5.4.9
Código Postal	postalCode	2.5.4.17
Dirección Postal	postalAddress	2.5.4.16

4.4 Anexo D: Claves de Uso

Nombre de Uso	X.509 (bit)	Observación
Firma Digital	digitalSignature(0)	Permite realizar la operación de firma electrónica
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	nonRepudiation(1) – fue renombrado este bit a contentCommitment [RFC3280]. Función que se usa para dar a conocer que el firmante ha comprendido lo que firma y manifiesta la intención de firmar el compromiso del contenido.
Cifrado de claves	keyEncipherment(2)	Su función consiste en la gestión y transporte de claves para establecer sesiones seguras
Cifrado de datos	dataEncipherment(3)	Se usa para cifrar datos del usuario que no sean claves criptográficas
Acuerdo de claves	keyAgreement(4)	Cifra el mensaje entre el transmisor y el receptor, usada con cifrado Diffie-Hellman.
Firma de certificado	keyCertSign(5)	Permite a las ACs, firmar certificados electrónicos. Utilizada cuando la clave pública es usada para verificar una firma en un certificado.
Firma de LCR	cRLSign(6)	Se activa el bit cRLSign cuando la clave pública se usa para verificar una firma en la lista de certificados revocados. (Ejemplo: CRL, delta CRL o ARL).
Solo cifrado	encipherOnly(7)	Habilita la clave pública solo para cifrar datos mientras se ejecuta el acuerdo de claves.
Solo descifrado	decipherOnly(8)	Habilita la clave pública solo para descifrar datos mientras se ejecuta el acuerdo de claves.

4.5 Anexo E: Claves de Usos Extendidos

A continuación se presentan diferentes Claves de Usos Extendidos que pueden añadir funcionalidades a los certificados electrónicos.

Nombre	X.509 (Bit)	OID
Autenticación de Servidor	serverAuth	1.3.6.1.5.5.7.3.1
Autenticación de Cliente	clientAuth	1.3.6.1.5.5.7.3.2
Firma de Código	codeSigning	1.3.6.1.5.5.7.3.3
Protección Correo Electrónico	emailProtection	1.3.6.1.5.5.7.3.4
Estampado de Tiempo	timeStamping	1.3.6.1.5.5.7.3.8
Firma de OCSP	ocspSigning	1.3.6.1.5.5.7.3.9
EAP over PPP	eapOverPPP	1.3.6.1.5.5.7.3.13
EAP over LAM	eapOverLAN	1.3.6.1.5.5.7.3.14
Server based certification validation protocol responder	scvpServer	1.3.6.1.5.5.7.3.15
Server based certification validation protocol responder	scvpClient	1.3.6.1.5.5.7.3.16
Internet Key Exchange	ipSecIke	1.3.6.1.5.5.7.3.17
Secure Shell Authentication Client	sshClient	1.3.6.1.5.5.7.3.21
Secure Shell Authentication Server	sshServer	1.3.6.1.5.5.7.3.22
Microsoft Smart Card Logon	smartCardLogon	1.3.6.1.4.1.311.20.2.2
Microsoft Document Signing	documentSigning	1.3.6.1.4.1.311.10.3.12
Microsoft Individual Code Signing	individualCodeSigning	1.3.6.1.4.1.311.2.1.21
Microsoft Comercial Code Signing	comercialCodeSingning	1.3.6.1.4.1.311.2.1.22
Microsoft Encrypted File System	encryptedFileSystem	1.3.6.1.4.1.311.10.3.4
Microsoft Encrypted File System Recovery	encryptedFileSystemRecovery	1.3.6.1.4.1.311.10.3.4.1
Adobe PDF Signing	adobePdfSigning	1.2.840.113583.1.1.5

4.6 Anexo F: Perfil de Lista de Certificados Revocados (LCR)

Perfil de Lista de Certificados Revocados		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de LCR		
Versión (version)	Entero Hexadecimal [V2] < 0x1 >(Representa la versión 2 del X.509)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos de Emisor (Issuer)		
Nombre Común (commonName)	<Identificación de la AC Principal del Proveedor de Servicios de Certificación>	
Correo Electrónico (emailAddress)	<Correo electrónico de la AC >	
Teléfono (telephoneNumber)	<Número de teléfono local del emisor>(Opcional)	
Departamento (organizationalUnity)	<Nombre o razón social tal cual aparezca en el documento constitutivo del emisor>	
Organización (organization)	[Sistema Nacional de Certificación Electrónica]	
Localidad (locality)	<Dirección física del emisor>	
Estado	<Estado en el cual se ubica el emisor >	
País	[VE]	

Datos de Validez		
Última Fecha de Actualización (thisUpdate o lastUpdate)	Fecha (UTC)	
Siguiente Fecha de Actualización (nextUpdate)	Fecha (UTC)	
Extensiones de LCR		
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad (keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralName <Contiene la información de la AC Raíz con el formato DN >	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Certificados Revocados		
Certificados revocados (Revoked Certificates)		
Serial del Certificado (Serial Number)	Entero Hexadecimal <Serial de certificado a revocar >	
Fecha de revocación (Revocation Date)	Fecha <fecha y hora en formato UTC>	
Razón de Revocación (CRL Reason Code)	Razón de Revocación < Ver Anexo G >	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado	
Firma(signature)	<Contenido de la Firma>	

4.7 Anexo G: Razón de Revocación

Se utilizan para indicar la razón de revocación de un certificado en la LCR.

Nombre	X.509
Sin Especificar	unspecified
Compromiso de Clave	keyCompromise
Compromiso de AC	cACompromise
Cambio de Afiliación	affiliationChanged
Sustitución	superseded
Cese de operaciones	cessationOfOperation
Retención de Certificado	certificateHold
Borrado de LCR	removeFromCRL
Retiro de privilegios	privilegeWithdrawn
Compromiso de AA	aACompromise

4.8 Anexo H: Directorio de Nombres del Titular (Subject Directory Name)

Es una extensión del certificado que contiene atributos que describen al titular del mismo.

Nombre	X.509	Observación
Fecha de Nacimiento	dateOfBirth	Indica la fecha de nacimiento del Titular
Lugar de Nacimiento	placeOfBirth	Indica el lugar de nacimiento del Titular
Género	gender	El tamaño del campo es de 1, puede contener solo "M", "m", "F" o "f".
País de Ciudadanía	countryOfCitizenship	El tamaño del campo es de 2 y debe contener el código de país en ISO 3166. Ejemplo "VE"
País de Residencia	countryOfResidence	El tamaño del campo es de 2 y debe contener el código de país en ISO 3166. Ejemplo "VE"

4.9 Anexo I: Información de Datos Biométricos (Biometric Data Info)

Es una extensión del certificado que contiene información que permite relacionar al titular con sus datos biométricos.

Nombre	X.509	Observación
Tipo de datos biométrico	typeOfBiometricData	Describe el tipo de información biométrica que hace referencia esta extensión. Por defecto es una imagen de la firma autógrafa del titular (handwritten-signature).
Algoritmo de Hash	hashAlgorithm	Es la función hash utilizada para la digerir información.
Hash de datos Biométricos	biometricDataHash	Es el resultado de la función hash de la información biométrica.
URI de la Fuente	sourceDataUri	Contiene la ubicación de dónde se almacena la información biométrica a la cual se hace referencia en esta extensión. Esta URI no implica que sea la única ubicación de dicha información.

4.10 Anexo J: Estructuras de Certificados

4.10.1 Estructura Certificado AC Raíz o Certificado Electrónico Autofirmado

Es el único certificado de la Infraestructura Nacional de Certificación Electrónica que es autofirmado y se utiliza para firmar certificados necesarios para su operación y los certificados de AC Principal de los PSC Acreditados.

Certificado de la AC Raíz		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos del Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos como mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 [Autoridad de Certificación Raíz del Estado Venezolano]	
Correo Electrónico (emailAddress)	UTF8 [acraiz@suscerte.gob.ve]	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto> (Opcional)	
Departamento (organizationUnity)	UTF8 [Superintendencia de Servicios de Certificación Electrónica]	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad (locality)	UTF8 <Dirección física de SUSCERTE>	
Estado (state)	UTF8 <Estado en el cual se ubica SUSCERTE>	
País (country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 [Autoridad de Certificación Raíz del Estado Venezolano]	
Correo Electrónico(emailAddress)	UTF8 [acraiz@suscerte.gob.ve]	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto>(Opcional)	
Departamento (organizationUnity)	UTF8 [Superintendencia de Servicios de Certificación Electrónica]	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física de SUSCERTE>	
Estado(state)	UTF8 <Estado en el cual se ubica SUSCERTE>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular (subjectPublicKey)		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa, id-ecPublicKey)	
Módulo(modulus) *	Cadena de Octetos [4096 bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para el caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano [true]	
Claves de Usos(keyUsage)		X
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Identificador de clave de Titular (Subject Key Identifier)	**Valor hexadecimal <Hash> (Resultado de Función Hash)**	
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	[RIF G-20004036-0]	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	[suscerte.gob.ve]	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el AC RAIZ> [URI:http://www.suscerte.gob.ve/lcr]	
Punto de distribución LCR (distributionPoint)	[URI:http://acraiz.suscerte.gob.ve/lcr/]	
Punto de distribución LCR (distributionPoint)	[ldap://acraiz.suscerte.gob.ve]	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio del OCSP del AC RAIZ> [URI:http://acraiz.suscerte.gob.ve/ocsp/]	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.2 [CAI]	
Dirección de Acceso (accessLocation)	<Dirección del CERTIFICADO DE LA AUTORIDAD *.CRT>	
Políticas de Certificación (PolicyInformation) (Opcional: No aplica de acuerdo a las guías Webtrust)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice	(No se usa)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.2 Estructura Certificado AC Principal

Certificados emitidos y firmados por el AC Raíz, se utilizan para firmar certificados de AC Subordinadas o Certificados de Entidad o Usuario Final. También puede generar y firmar certificados y listas de certificados necesarias para su operación.

Certificado de AC Principal		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal <Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos como mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 [Autoridad de Certificación Raíz del Estado Venezolano]	
Correo Electrónico(emailAddress)	UTF8 [acraiz@suscerte.gob.ve]	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto> (Opcional)	
Departamento (organizationUnity)	UTF8 [Superintendencia de Servicios de Certificación Electrónica]	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física de SUSCERTE>	
Estado(state)	UTF8 <Estado en el cual se ubica SUSCERTE>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Subordinada del Proveedor de Servicios de Certificación>	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico del ente que gestiona la AC Subordinada>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Titular>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o razón social tal cual aparezca en el documento constitutivo del ente que gestiona la AC Subordinada>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física del PSC>	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa, id-ecPublicKey)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [4096 bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano [true]	
Longitud de Certificación(pathLen)	Entero Hexadecimal [1] (Delimita a un nivel AC que pueden estar por debajo de ella)	
Claves de Usos(keyUsage)		X
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Nombre Alternativo del Emisor (IssuerAltName)		
Otro Nombre (otherName)	[RIF G-20004036-0]	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	<DNS del PSC registrado en nic.ve>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Otro Nombre (otherName)	<RIF del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección del servicio OCSP del AC RAIZ> [URI:http://acraiz.suscerte.gob.ve/ocsp/]	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el AC RAIZ> [URI:http://www.suscerte.gob.ve/lcr]	
Punto de distribución LCR (distributionPoint)	[URI:http://acraiz.suscerte.gob.ve/lcr/]	
Punto de distribución LCR (distributionPoint)	[ldap://acraiz.suscerte.gob.ve]	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice	(No se usa)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.3 Estructura Certificado AC Subordinada del PSC

Certificados emitidos y firmados por el AC Principal, se utilizan para firmar Certificados de Entidad o Usuario Final. También puede generar y firmar certificados y listas de certificados necesarias para su operación.

Certificado de AC Subordinada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado (OID de los algoritmos permitidos como mínimo SHA384withRSAEncryption o SHA512withRSAEncryption o Superior)	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Identificación de la AC Principal del Proveedor de Servicios de Certificación>	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de la AC del PSC >	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o razón social tal cual aparezca en el documento constitutivo del PSC >	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Dirección física del PSC>	
Estado(state)	UTF8 <Estado en el cual se ubica el PSC>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, Id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [4096 bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano [true]	
Longitud de Certificación(pathLen)	Entero Hexadecimal [0] (No permite la creación de AC en niveles inferiores a ella)	
Claves de Usos(keyUsage)		X
Firma de certificado	keyCertSign(5)	
Firma de LCR	cRLSign (6)	
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	<DNS del Ente poseedor de la AC Subordinada >	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Otro Nombre (otherName)	<RIF del Ente poseedor de la AC Subordinada>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<Dirección de descarga de la LCR por el PSC>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<Dirección de consulta de certificados revocados>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice	(No se usa)	
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.4 Estructura Certificado Persona Natural

Certificado cuyo suscriptor y titular es una persona natural, destinado para firmar electrónicamente mensajes de datos para expresar la voluntad del signatario como persona natural. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Persona Natural		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	

Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF o Pasaporte>(Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1>(Opcional)	
Apellido (surName)	UTF8 <Apellido 1>(Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular>(Opcional)	
Código Postal (postalCode)	UTF8 <Código postal al que pertenece su dirección>(Opcional)	
Calle (streetAddress)	UTF8 <Calle de residencia del Titular >(Opcional)	
Localidad(locality)	UTF8<Ciudad de residencia del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave(extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Individual Code Signing	individualCodeSigning 1.3.6.1.4.1.311.2.1.21	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de Identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Nombre Alternativo del Titular (subjectAltName)		
Nombre RFC822 (rfc822Name)	<Correo electrónico del Titular>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.5 Estructura Certificado Persona Jurídica

Certificado cuyo suscriptor es una empresa u organización y el titular es una persona natural que representa legalmente a dicho ente destinado para firmar electrónicamente documentos, mensajes de datos para expresar la voluntad del signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Persona Jurídica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF o Pasaporte>(Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1>(Opcional)	
Apellido (surName)	UTF8 <Apellido 1>(Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular>(Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica o suscriptor tal cual aparece en el documento constitutivo de la organización>	
Código Postal (postalCode)	UTF8 <Código postal al que pertenece su dirección>(Opcional)	
Calle (streetAddress)	UTF8 <Calle de residencia del titular >(Opcional)	
Localidad(locality)	UTF8<Ciudad de residencia del titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Comercial Code Signing	comercialCodeSingning 1.3.6.1.4.1.311.2.1.22	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre RFC822 (rfc822Name)	<Correo electrónico del Titular>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.6 Estructura Certificado Profesional Titulado

Certificado cuyo suscriptor y el titular es una persona natural perteneciente a un Gremio o Colegiatura de Profesionales, se destina para firmar electrónicamente mensajes de datos para expresar la voluntad del

signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Profesional Titular		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte>(Ver Anexo A)	
Nombre Común	UTF8 <Cadena compuesta por el nombre del Profesional y el número de	
(commonName)	Colegiado>	
Nombre (givenName)	UTF8 <Nombre 1 Nombre 2> (Opcional)	
Apellido (surName)	UTF8 <Apellido 1 Apellido 2> (Opcional)	
Título (title)	UTF8 <Nombre del Título registrado ante la Colegiatura> (Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Organización (organization)	UTF8<Nombre del Colegio al que pertenece la Colegiatura> (Opcional)	
Localidad(locality)	UTF8<Ciudad de ubicación del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Individual Code Signing	individualCodeSigning 1.3.6.1.4.1.311.2.1.21	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre RFC822 (rfc822Name)	<Correo electrónico del Titular>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.7 Estructura Certificado Empleado de Institución Pública

Certificado cuyo suscriptor es una organización o ente del Estado y el titular o signatario es una persona natural que desempeña actividades bajo relación laboral para una institución pública. Dicho certificado se destina para firmar electrónicamente mensajes de datos para expresar la voluntad del signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Empleado de Institución Pública		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte>(Ver Anexo A)	
Título (title)	UTF8 <Título y/o cargo o funciones del titular del certificado>	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1> (Opcional)	
Apellido (surName)	UTF8 <Apellido 1> (Opcional)	
Identificador de documento o Nombramiento (documentIdentifier)	UTF8 <Especificar documento que lo acredita como empleado>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la organización>	
Localidad(locality)	UTF8<Ciudad donde se ubica organización propietaria del certificado>	
Estado(state)	UTF8 <Estado donde se ubica organización propietaria del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos(keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Comercial Code Signing	comercialCodeSingning 1.3.6.1.4.1.311.2.1.22	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF del Ente Suscriptor>	
Nombre RFC822 (rfc822Name)	<Correo electrónico del Ente Suscriptor>	

AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.8 Estructura Certificado de Empleado de Empresa

Certificado cuyo suscriptor es una empresa u organización y el titular o signatario es una persona natural que está bajo relación laboral con dicho ente. Este certificado se destina para firmar electrónicamente documentos, mensajes de datos para expresar la voluntad del signatario. Se pueden obtener diversas aplicaciones utilizando combinación de Claves de Usos y Claves de Usos Extendidos.

Certificado de Empleado de Empresa Privada		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Serial (serialNumber)	UTF8 <Cédula, RIF, Pasaporte del signatario>(Ver Anexo A)	
Título (title)	UTF8 <Título y/o Cargo del empleado>	
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Nombre (givenName)	UTF8 <Nombre 1> (Opcional)	
Apellido (surName)	UTF8 <Apellido 1> (Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa>	
Localidad(locality)	UTF8<Ciudad donde se ubica organización propietaria del certificado>	
Estado(state)	UTF8 <Estado donde se ubica organización suscriptora del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo (modulus) *	Cadena de Octetos [2048bit]	
Exponente (exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
** Se deben evaluar la aplicación de cada uno de estas Clave de Uso		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Comercial Code Signing	comercialCodeSingning 1.3.6.1.4.1.311.2.1.22	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuer AltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF de la Empresa Suscriptora>	
Nombre RFC822 (rfc822Name)	<Correo electrónico de la Empresa Suscriptora>	
Nombre DNS (dNSName)	<Sitio Web de la Empresa>(Opcional)	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.9 Propuesta de Estructura de Certificado para la Cédula Electrónica

Certificado cuyo suscriptor y el titular o signatario es una persona natural, destinado a identificarlo y representarlo para permitir firmar y autenticar operaciones legales ante los trámites electrónicos con el Estado y sólo podrá ser emitido por las autoridades de certificación del ente gubernamental con competencia en identificación (SAIME). Posee atributos especiales para describir detalles de titular, por ejemplo fecha y lugar de nacimiento, nacionalidad e información biométrica.

Certificado de Cédula Electrónica		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos del Titular		
Serial (serialNumber)	UTF8 <Cédula> (Ver Anexo A)	
Nombre Común (commonName)	UTF8 <Apellido1 Apellido2, Nombre1 Nombre2>	
Nombres (givenName)	UTF8 <Nombre 1 Nombre 2> (Opcional)	
Apellidos (surName)	UTF8 <Apellido 1 Apellido 2> (Opcional)	
Correo Electrónico(emailAddress) [1]	UTF8 <Correo electrónico de la persona natural portadora del certificado> (Opcional)	
Teléfono (telephoneNumber) [1]	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Calle (streetAddress) [1]	UTF8 <Calle de residencia del Titular>(Opcional)	
Localidad(locality)	UTF8<Ciudad de residencia del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
1 .- Condicionado a la capacidad del dispositivo y al marco legal de protección de datos personales.		
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) [2]	Cadena de Octetos [2048bit]	
Exponente(exponent) [2]	Entero Hexadecimal [65537] <0x10001>	
2.- Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Solo cifrado	encipherOnly(7)	
Solo descifrado	decipherOnly(8)	
*Se debe evaluar la aplicación de cada uno de estos Usos		
Usos Extendidos de las Claves (extKeyUsage)		
Firma de Código	codeSigning 1.3.6.1.5.5.7.3.3	
Protección Correo Electrónico	emailProtection 1.3.6.1.5.5.7.3.4	
Microsoft Smart Card Logon	smartCardLogon 1.3.6.1.4.1.311.20.2.2	
Microsoft Document Signing	documentSigning 1.3.6.1.4.1.311.10.3.12	
Microsoft Individual Code Signing	individualCodeSigning 1.3.6.1.4.1.311.2.1.21	
Adobe PDF Signing	adobePdfSigning 1.2.840.113583.1.1.5	

** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de Identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Atributos Adicionales del Titular (subjectDirectoryAttributes)		
Atributos o Características del titular (Attributes) Crítico		X
Fecha de Nacimiento (dateOfBirth)	<Fecha de Nacimiento del Titular> (Datos visibles en la tarjeta criptográfica)	
Lugar de Nacimiento (placeOfBirth)	<Lugar de Nacimiento del Titular> (Ver Anexo H, Datos visibles en la tarjeta criptográfica)	
Género (gender)	<Género del Titular> (Ver Anexo H)	
País de Ciudadanía (countryOfCitizenship)	<País de Ciudadanía del Titular> (Formato UTF8 ISO 3166-1-alpha-2, Datos visibles en la tarjeta criptográfica)	
País de Residencia (countryOfResidence)	<País de Residencia del Titular> (Formato UTF8 ISO 3166-1-alpha-2, Datos visibles en la tarjeta criptográfica)	
Información Biométrica (biometricInfo)		
Tipo de datos biométrico (typeOfBiometricData)	<Tipo de información biométrica que hace referencia esta extensión>	
Algoritmo de Hash (hashAlgorithm)	<Es la función hash utilizada>	
Hash de datos Biométricos (biometricDataHash)	Es el resultado de la función hash de la información biométrica.	
URI de la Fuente (sourceDataUri)	<Contiene la ubicación de dónde se almacena la información biométrica>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.10 Estructura Certificado de Servidor

Certificado cuyo suscriptor es una persona natural o jurídica y cuyo principal objetivo es identificar a un servicio web y proporcionarle seguridad a la comunicación. Entre las aplicaciones que se le puede dar a este tipo certificado está la de Servidor SSL/TLS, Servidor SSL/TLS con Validación Extendida, Servidor de Conexiones VPN, Servidor de Correo Electrónico, entre otras aplicaciones, se pueden hacer implementaciones más específicas agregando Claves de Usos y Claves Usos Extendidos.

Certificado de Servidor (General)		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos del Titular		
Nombre Común (commonName)	UTF8 <Identificación del servidor, dominio o la aplicación>	
Serial (serialNumber)	UTF8 <RIF de la organización o empresa suscriptora del certificado>	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de la Organización suscriptora>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico del departamento que se encarga de la administración y/o seguridad del servidor> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	
Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora>	
Categoría de Negocio (businessCategory)*	UTF8<"Private Organization" || " Government Entity" || " Business Entity" || "Non-Commercial Entity">(Sólo una de las siguientes opciones)	
País de Jurisdicción (jurisdictionCountryName)*	UTF8 [VE] (ISO 3166-1-alpha-2, Aplica para Certificados de Validación Extendida)	
Código Postal (postalCode)	UTF8 <Código Postal donde se ubica la organización propietaria del certificado>(Opcional)	
Calle (streetAddress)	UTF8 <Dirección donde se ubica organización propietaria del certificado>(Opcional)	
Localidad(locality)	UTF8<Ciudad donde se ubica organización propietaria del certificado>	
Estado(state)	UTF8 <Estado donde se ubica organización suscriptora del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
* Necesarios para la Certificación EV		
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se deben evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Usos Extendidos de la Clave (extKeyUsage)		
Autenticación de Servidor	serverAuth 1.3.6.1.5.5.7.3.1	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario y deben ser sometidos a un análisis técnico de acuerdo a las necesidades (Para más información Ver Anexo E)		
Nombre Alternativo del Emisor (issuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de Identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF de la Empresa Suscriptora>	
Nombre RFC822 (rfc822Name)	<Correo electrónico de la Empresa Suscriptora>	
Nombre DNS (dNSName)	<Sitio Web de la Empresa> (Mínimo debe colocarse un DNS, se pueden agregar todos los que posea la empresa de acuerdo a la política del certificado)	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.2	
Dirección de Acceso (accessLocation)	<URL del certificado de la autoridad>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.11 Estructura Certificado de Servidor de OCSP

Emitido para Firmar respuestas generadas del servicio OCSP de una AC.

Certificado de Servidor de OCSP Responder		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor> (Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos del Titular		
Nombre Común (commonName)	UTF8 <Identificación del servidor OCSP Responder>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto de la Unidad Responsable>	

Organización (organization)	UTF8 <Nombre o Razón social como aparece en documento constitutivo de la AC>	
Localidad(locality)	UTF8 <Ciudad de ubicación del Titular>	
Estado(state)	UTF8 <Estado de ubicación del Titular>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false>(Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se deben evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Usos Extendidos de la Clave (extKeyUsage)		
Firma de OCSP	ocspSigning 1.3.6.1.5.5.7.3.9	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario y deben ser sometidos a un análisis técnico de acuerdo a las necesidades (Para más información Ver Anexo E)		
Nombre Alternativo del Emisor (IssuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Identificador de clave de Titular (Subject Key Identifier)	Valor hexadecimal <Hash> (Resultado de Función Hash)	
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Nombre DNS (dNSName)	<DNS del PSC>	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint)	<LCR del repositorio del PSC>	
AIA (authorityInfoAccess)		
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.2 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

4.10.12 Estructura Certificado de Dispositivos Móviles

Destinado a mejorar la privacidad en las comunicaciones y utilización de aplicaciones seguras en Dispositivos Móviles.

Certificado de Dispositivos Móviles		
Nombre(X.509)	**Tipo de dato [Constante] < Valor >**	**Crítica (para extensiones)**
Datos de Certificado		
Versión (version)	Entero Hexadecimal [V3] < 0x2 >(Representa la versión 3 del X.509)	
Serial (serialNumber)	Entero Hexadecimal<Asignado por la AC> (No negativo)	
Algoritmo de Firma (signature)	Algoritmo Autorizado	
Datos del Emisor (issuer)		
Nombre Común (commonName)	UTF8 <Identificación de la AC>	
Correo Electrónico(emailAddress)	UTF8 <Dirección de correo electrónico de contacto del Emisor>	
Teléfono (telephoneNumber)	UTF8 <Teléfono de contacto del Emisor>(Opcional)	
Departamento (organizationUnity)	UTF8 <Nombre o Razón social como aparece en documento constitutivo del PSC>	
Organización (organization)	UTF8 [Sistema Nacional de Certificación Electrónica]	
Localidad(locality)	UTF8 <Ciudad de ubicación del Emisor>	
Estado(state)	UTF8 <Estado de ubicación del Emisor>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Datos de Validez		
No Antes(notBefore)	Fecha (UTC)	
No Después(noAfter)	Fecha (UTC)	
Datos de Titular (subject)		
Nombre Común (commonName)	UTF8 <Nombre1 Nombre2 Apellido1 Apellido2>	
Serial (serialNumber)	UTF8 <IMEI del dispositivo móvil>	
Nombres (givenName)	UTF8 <Nombre 1 Nombre 2> (Opcional)	
Apellidos (surName)	UTF8 <Apellido 1 Apellido 2> (Opcional)	
Correo Electrónico(emailAddress)	UTF8 <Correo electrónico de contacto del Titular>	
Teléfono (telephoneNumber)	UTF8 <Número telefónico de contacto del Titular> (Opcional)	
Departamento (organizationUnity)	UTF8<Nombre del departamento, dirección o unidad de trabajo al cuál pertenece el titular> (Opcional)	

Organización (organization)	UTF8<Nombre completo de la persona jurídica tal cual aparece en el documento constitutivo de la empresa suscriptora> (Opcional)	
Calle (streetAddress)	UTF8 <Dirección donde se ubica el titular o suscriptor del certificado>(Opcional)	
Localidad(locality)	UTF8<Ciudad donde se ubica el titular o suscriptor del certificado>	
Estado(state)	UTF8 <Estado donde se ubica el titular o suscriptor del certificado>	
País(country)	UTF8 [VE] (ISO 3166-1-alpha-2)	
Información de Clave Pública del Titular		
Algoritmo de clave pública (algorithm)	<Algoritmo Asignado> (rsaEncryption, dhpublicnumber, id-dsa,)	
Clave Pública de Titular (subjectPublicKey)		
Módulo(modulus) *	Cadena de Octetos [2048bit]	
Exponente(exponent) *	Entero Hexadecimal [65537] <0x10001>	
* Para caso de RSA se exigen estos campos		
Extensiones		
Restricciones Básicas (basicConstraints)		X
Autoridad de Certificación(aC)	Booleano <false> (Determina no emitir o firmar certificados)	
Claves de Usos (keyUsage)		X
Firma Digital	digitalSignature(0)	
Compromiso con el Contenido (Anteriormente No Repudio)	contentCommitment(1)	
Cifrado de claves	keyEncipherment(2)	
Acuerdo de claves	keyAgreement(4)	
** Se deben evaluar la aplicación de cada uno o combinación de estas Clave de Uso.		
Usos Extendidos de la Clave (extKeyUsage)		
Autenticación de Servidor	serverAuth 1.3.6.1.5.5.7.3.1	
Autenticación de Cliente	clientAuth 1.3.6.1.5.5.7.3.2	
*** Los Usos Extendidos son opcionales y aplicables de acuerdo a las necesidades del Usuario y deben ser sometidos a un análisis técnico de acuerdo a las necesidades (Para más información Ver Anexo E)		
Identificador de clave de Titular (Subject Key Identifier)	**Valor hexadecimal <Hash> (Resultado de Función Hash)**	
Nombre Alternativo del Emisor (IssuerAltName)		
Otro Nombre (otherName)	<RIF del PSC>	
Otro Nombre (otherName)	<Código de identificación del PSC acreditado asignado por SUSCERTE>	
Nombre DNS (dNSName)	<DNS del PSC emisor del certificado>	
Identificador de clave de Autoridad Certificadora (Authority Key Identifier)		
Clave de Autoridad(keyIdentifier)	KeyIdentifier <Identificador de la clave pública de la AC Raíz>	
Nombre distintivo (authorityCertIssuer)	GeneralNames <Contiene la información de la AC Raíz con el formato DN>	
Serial (authorityCertSerialNumber)	CertificateSerialNumber <Contiene el número del certificado del emisor>	
Nombre Alternativo del Titular (subjectAltName)		
Otro Nombre (otherName)	<RIF de la Empresa Suscriptora>	
Nombre RFC822 (rfc822Name)	<Correo electrónico de la Empresa Suscriptora>	
Nombre DNS (dNSName)	<Sitio Web de la Empresa> (Mínimo debe colocarse un DNS, se pueden agregar todos los que posea la empresa de acuerdo a la política del certificado)	
Puntos de Distribución de las LCR (cRLDistributionPoints)		
Punto de distribución LCR (distributionPoint **AIA (authorityInfoAccess)**	<LCR del repositorio del PSC>	
Método de Acceso (accessMethod)	1.3.6.1.5.5.7.48.1 [OCSP]	
Dirección de Acceso (accessLocation)	<URL del servicio OSCP>	
Políticas de Certificación (PolicyInformation)		
PolicyInformation (PC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la PC>	
userNotice	(No se usa)	
PolicyInformation (DPC)		
policyIdentifier	<OID Autorizado por SUSCERTE>	
cPSuri	<Dirección dónde se puede descargar la DPC>	
userNotice		
Firma		
Algoritmo de Firma (signatureAlgorithm)	Algoritmo Autorizado (OID de los algoritmos permitidos mínimo SHA256withRSAEncryption o SHA384withRSAEncryption o Superior)	
Firma(signature)	<Contenido de la Firma>	

Artículo 3. Con la publicación en Gaceta Oficial de esta Providencia queda sin efecto la **NORMA SUSCERTE 032-01/11 edición 2 DE FECHA 30 de Enero 2011.**

Artículo 4. La Norma N° **032-06/17 " INFRAESTRUCTURA NACIONAL DE CERTIFICACIÓN ELECTRÓNICA: ESTRUCTURA, CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS",** se encuentra a disposición en la sede de La Superintendencia de Servicios de Certificación Electrónica como en la página Web www.suscerte.gob.ve.

Artículo 5. La presente Providencia Administrativa entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese.

LUIS FERNANDO PRADA FUENTES

Resolución Nº 095 del 19 de junio de 2.017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.177 de fecha 21 de junio de 2.017. Resolución N° 106 de fecha 13 de julio de 2.017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.195 en fecha 18 de julio de 2.017

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA
EDUCACIÓN UNIVERSITARIA, CIENCIA Y TECNOLOGÍA
SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA

Caracas, 26 de febrero de 2018

207º, 158º y 19°

Quien suscribe, **LUIS FERNANDO PRADA FUENTES**, titular de la cédula de identidad N° **V-17.059.842**, designado como Superintendente de Servicios de Certificación Electrónica, según nombramiento contenido en la Resolución N° 095, de fecha 19 de junio de 2017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.177, de fecha 21 de junio de 2017; en ejercicio de las atribuciones conferidas en el artículo 22, numeral 1 y 2 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148, de fecha 28 de febrero de 2001; de conformidad con lo previsto en los artículos 4, 10, 12 y 26 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Extraordinario N° 6.147, de fecha 17 de noviembre de 2014; y con el artículo 72 de la Ley Orgánica de Procedimientos Administrativos, publicada en la Gaceta Oficial de la República de Venezuela N° 2.818 Extraordinario, de fecha 01 de julio de 1981, en observancia con los estándares Internacionales que rigen la materia; dicta la siguiente:

PROVIDENCIA ADMINISTRATIVA Nº 002 -2018

Artículo 1. La presente Providencia Administrativa, tiene por objeto establecer los estándares desarrollados para el análisis de los requisitos tecnológicos, de seguridad y confianza que deben cumplir, para obtener la acreditación o su renovación, los Proveedores de Servicios de Certificación (PSC) o los Casos Especiales, de acuerdo a lo establecido en el Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento Parcial. Así mismo, se dictan los lineamientos técnicos con respecto a la emisión de Certificados de Validación Extendida; conforme a los lineamientos establecidos por la Superintendencia de Servicios de Certificación Electrónica **(SUSCERTE)**.

De conformidad con lo dispuesto en el artículo 22, numerales 1° y 5°, y en el artículo 27 del Decreto con Fuerza de Ley sobre Mensaje de Datos y Firmas Electrónicas; en concordancia con el artículo 36 del Reglamento Parcial Del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.

Artículo 2. La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), define en la presente providencia los aspectos necesarios a cumplir por parte del PSC solicitante, en la aplicación de los estándares desarrollados para el análisis de los requisitos tecnológicos, seguridad y confianza para lograr obtener la acreditación o renovación como Proveedor de Servicios de Certificación o Caso Especial, según el procedimiento identificado como **NORMA SUSCERTE 040-06/17** edición 4.1 de fecha 30 de Junio de 2017; cuyo tenor es el siguiente:

"GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN Y RENOVACIÓN COMO PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN Ó CASOS ESPECIALES"

NORMA SUSCERTE Nº 040–06/2017, EDICIÓN Nº: 4.1, FECHA: 06/2017

1. OBJETO Y CAMPO DE APLICACIÓN

El propósito de esta guía es orientar al solicitante acerca de la aplicación de los estándares desarrollados para el análisis de los requisitos tecnológicos, seguridad y confianza que debe cumplir para obtener la acreditación o renovación como Proveedor de Servicios de Certificación o Caso Especial.

Especifica los requerimientos técnicos en relación a los PSC o Casos Especiales que prestarán servicios de certificación electrónica, de acuerdo a lo establecido en LSMDFE y su Reglamento, en el entendido que la Firma Electrónica en este marco legal es firma electrónica que cuenta con la misma validez legal que la firma autógrafa, en otros contextos, firma electrónica reconocida o avanzada. Así mismo los lineamientos técnicos respecto de la emisión de Certificados de Validación Extendida.

2. REFERENCIAS NORMATIVAS

2.1 Decreto con Fuerza de Ley N° 1.204 de Fecha 10 de febrero de 2001, de Mensajes de Datos y Firmas Electrónicas (LSMDFE).

2.2 Reglamento Parcial del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas (RPLSMDFE).

2.3 Norma SUSCERTE Nro 027. Guía para la Acreditación o Renovación de Proveedores de Servicios de Certificación.

2.4 ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad – Sistema de Gestión de la Seguridad de la Información - Requisitos. (2013).

2.5 ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de Seguridad – Código de buenas prácticas para controles de seguridad de la información.

2.5 ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Versión 3 (2009)

2.6 FIPS PUB 140-2: Security Requirements for Cryptographic Modules, (Diciembre 2002).

2.7 ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates". V2.4.1 (2013-02) (ETSI)

2.8 ISO/IEC 9594-8:2005 Information Tecnology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks.

2.9 ITU-T Rec. X.509 Tecnología de la información. Interconexión de sistemas abiertos – El directorio – Marco de autenticación. (2008)

2.10 ITU-T Rec. X.690 (07/2002) / ISO/IEC 8825-1:2008. ASN.1 Basic Encoding Rules

2.11 RFC 2559 Boeyen, S. et al. "Internet X.509 Public Key Infrastructure. Abril 2002.

2.12 RFC 3647. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Noviembre 2003.

2.13 NIST SP800-18 Rev.1, Guide for Developing Security Plans for Information Technology Systems. Febrero 2006.

2.14 NIST SP800-53A Rev.4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Diciembre 2014.

2.15 CA/Browser Forum Baselines Requeriment Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v 1.2.5 (CA/BR B)

2.16 CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates v 1.5.2 (CA/BR G)

2.17 RFC 5280 PKIX Certificate and CRL Profile (2008) y su actualización: Updates to the Internet X.509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile (2013) (RFC 6818)

2.18 Providencia Administrativa N° 016 de fecha 05 de Febrero de 2007.

2.19 Norma SUSCERTE No. 032 "Infraestructura Nacional de Certificación Electrónica: Estructura, Certificados y Lista de Certificados Revocados".

2.20 RCF 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

3. DEFINICIONES Y TERMINOLOGÍAS

A los efectos de esta norma, se establecen las siguientes definiciones y terminologías:

ACREDITACIÓN	Título que otorga la Superintendencia de Servicios de Certificación Electrónica a los Proveedores de Servicios de Certificación para proporcionar certificados electrónicos, una vez cumplidos los requisitos y condiciones establecidos en el Decreto-Ley 1.204.
AUDITOR REGISTRADO	Profesional independiente que cuentan con la capacidad técnica para realizar el proceso de evaluación, las cuales son inscritas en un registro que lleva la Supenntendencia, una vez comprobada su capacidad.
AUDITORÍA TÉCNICA	Proceso sistemático que consiste en obtener y evaluar objetivamente evidencias concernientes al cumplimiento de las políticas, planes, procedimientos de seguridad y requisitos técnicos, orientados a garantizar la prestación continua de los servicios de certificación, para luego comunicar los resultados a las personas o entes interesados.
CASO ESPECIAL	Casos Especiales son entidades de Certificación excepcionales para Proyectos de Interés Nacional que son acreditados por SUSCERTE, siempre y cuando se de alguno de los extremos del artículo. 11 de la Providencia Administrativa N°016 de fecha 05 de febrero de 2007. Para los cuales aplica, a los efectos de la presente Norma las mismas obligaciones y derechos que los PSC, con las excepciones establecidas en las respectivas Providencias de Creación.
SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE)	Servicio Autónomo, integrado a la estructura orgánica del Ministerio del Poder Popular para la Educación Universitaria, Ciencia y Tecnología, según Gaceta Oficial de la República Bolivariana de Venezuela No 5.836 Extraordinario de fecha 08 de Enero de 2007.
SIGNATARIO	Entidad identificada en un certificado electrónico, quien usa la clave privada que se encuentra asociada con clave pública del certificado.
SUSCRIPTOR	Persona que contrata la generación de un certificado electrónico con un proveedor de servicios de certificación.
IDENTIFICADOR DE OBJETO	Valor universal único asociado a un objeto para identificarlo inequívocamente.
FUNCIÓN HASH	Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
LISTA DE CERTIFICADOS REVOCADOS	Documento mantenido y publicado por una Autoridad de Certificación (AC) que enumera los certificados revocados por ella.
CERTIFICADO DE VALIDACIÓN EXTENDIDA	Certificado que emitido y administrado en cumplimientos a las políticas de Validación Extendida de la CA/Brower Forum.
SOLICITANTE	Persona aspirante a PSC, PSC acreditado y/o que requiera incorporar Autoridades de Certificación Subordinadas y/o Autoridades de Registro Externas.

4. SÍMBOLOS Y ABREVIATURAS

A los efectos de esta norma, se establecen los siguientes símbolos y abreviaturas:

AC	Autoridad de Certificación
AR	Autoridad de Registro
DEF	Dirección de Estandarización y Fiscalización
DPC	Declaración de Prácticas de Certificación.
DCEC	Dirección de Certificación Electrónica y Criptografía
LCR	Lista de Certificados Revocados
LSMDFE	Ley Sobre Mensajes de Datos y Firmas Electrónicas.
OCSP	On - line Certificate Status Protocol (Protocolo de estado de certificados en línea)
PC	Política de Certificados.
PSC	Proveedor de Servicios de Certificación.
CE	Casos Especiales
SUSCERTE	Superintendencia de Servicios de Certificación Electrónica.
HSM	Hardware Security Module. (Módulo de Seguridad de Hardware)
OID	Identificador de Objeto (Object identifier)
RPLSMDFE	Reglamento Parcial de Ley Sobre Mensajes de Datos y Firmas Electrónicas.
CA/BR B	CA/Browser Forum Baselines Requeriment Baseline Requirements for the Issuance and

	Management of Publicly-Trusted Certificates v 1.2.5
CA/BR G	CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates v 1.5.2

5. PROCEDIMIENTO

5.1. Principio Básico

Con el uso de esta guía de evaluación se pueden recolectar y analizar, con detalle y rigurosidad que exige el Decreto-Ley 1.204, los aspectos que deben ser revisados en el área tecnológica, seguridad y confianza del solicitante, los cuales permitirán definir un criterio preciso sobre su capacidad para lograr y mantener en el tiempo la acreditación o renovación como Proveedor de Servicios de Certificación o Caso Especial.

Especificando los requerimientos técnicos en relación a los PSC o Casos Especiales que prestarán servicios de certificación electrónica, de acuerdo a lo establecido en LSMDFE y su Reglamento, en el entendido que la Firma Electrónica en este marco legal es firma electrónica que cuenta con la misma validez legal que la firma autógrafa, en otros contextos, firma electrónica reconocida o avanzada. Así mismo los lineamientos técnicos respecto de la emisión de Certificados de Validación Extendida.

5.2. Consideraciones Generales

5.2.1 El objetivo de la acreditación o renovación para los Proveedores de Servicio de Certificación (PSC) o Caso Especial (CE) es asegurar la existencia de un sistema de certificación de firma electrónica confiable, que garantice su continuidad en el tiempo y que sirva de base para el desarrollo tecnológico del país.

5.2.2 Como criterios generales de la acreditación o renovación, se tienen:

5.2.2.1 Los criterios de acreditación o renovación están definidos con base en el cumplimiento del conjunto de requisitos y obligaciones definidas por la Ley Sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE), el Reglamento Parcial del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas, así como por las Normas y Resoluciones emitidas por SUSCERTE.

5.2.2.2 El proceso de acreditación o renovación de los PSC coloca a disposición pública los requisitos que se deben cumplir para ser acreditados o renovados por el Gobierno de la República Bolivariana de Venezuela, a través de SUSCERTE, con el propósito de proveer confianza a los usuarios y generar las condiciones y los acuerdos necesarios para el desarrollo de la actividad.

5.2.2.3 Los requerimientos del proceso de acreditación o renovación deben garantizar la compatibilidad de la Infraestructura Nacional de Certificación Electrónica con los estándares internacionales, permitiendo así la interoperabilidad entre los sistemas.

5.2.2.4 Los niveles de exigencia del proceso de acreditación o renovación deben ajustarse a las mejores prácticas y los estándares internacionales.

5.2.2.5 Se considera fundamental promover el desarrollo tecnológico de los servicios de certificación electrónica, sin preferencia hacia una tecnología en particular. Además los PSC o CE podrán introducir cambios tecnológicos siempre que estos cumplan con la normativa establecida, se notifique a SUSCERTE y sean aprobados por ella.

5.2.2.6 La realización de un proceso de acreditación o renovación riguroso requiere de información estratégica o altamente sensible de parte de los PSC o CE. Por lo anterior, SUSCERTE se compromete a no usar ni divulgar la información entregada por el PSC o CE, clasificada como confidencial, más que para los fines propios del procedimiento de acreditación o renovación. Este compromiso es extensible a todo organismo y persona que intervenga en el proceso de acreditación o renovación.

5.2.2.7 El contenido de estos criterios puede cambiar en el tiempo, dependiendo de los avances de la tecnología y consideraciones de seguridad nacional. Si el cambio es considerado significativo, el proceso de revisión incorporará consultas con la industria y debe ser validado por SUSCERTE.

5.2.2.8 Cualquier PSC o CE acreditado debe ser notificado de los cambios de este documento. Si existiera alguna duda respecto a la actualización de estos criterios, deberá contactarse con la Superintendencia.

5.2.2.9 Los lineamentos establecidos en este documento corresponden al cumplimiento de los estándares internacionales, para ofrecer de forma segura y confiable servicios de certificación electrónica. Los estándares tecnológicos utilizados a lo largo del documento son los siguientes:

a) En cuanto a Prácticas de Certificación:

- ETSI TS 102 042: "Policy requirements for certification authorities issuing public key certificates". V2.4.1 (2013-02)
- RFC 3647. "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Noviembre 2003.
- CA/Browser Forum Baselines Requeriment Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v 1.2.5
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates v 1.5.2

b) Respecto a Seguridad:

- ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad – Sistema de Gestión de la Seguridad de la Información. (2013)
- ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de Seguridad – Código de buenas prácticas para controles de seguridad de la información
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Versión 3 (2009)
- FIPS PUB 140-2: (2009) Security Requirements for Cryptographic Modules, (Diciembre 2002)

c) Referentes a Estructura de Certificados:

- ITU-T Rec. X.509 Tecnología de la información. Interconexión de sistemas abiertos – El directorio – Marco de autenticación (2001)
- ITU-T Rec. X.690 (07/2002) / ISO/IEC 8825-1:1998. ASN.1 Basic Encoding Rules

d) Para Repositorio de Información:

- [RFC 2559] Boeyen, S. , "Internet X.509 Public Key Infrastructure. Abril 2002
- [RFC 4386] Boeyen, S. , "Internet X.509 Public Key Infrastructure repository locator services. Febrero 2006

e) En cuanto a criptografía

- RFC 6818 Updates to the Internet X.509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile (2013)

5.2.3 Con base en la LSMDFE y su Reglamento Parcial, es posible establecer un sistema de acreditación o renovación para PSC o CE que involucra los siguientes elementos:

5.2.3.1 SUSCERTE

El proceso de acreditación o renovación de PSC o CE es desarrollado por SUSCERTE quien se apoya en expertos (auditores), para realizar la evaluación de dichas entidades.

Además, debe velar porque los requisitos y obligaciones que se observaron al momento de otorgarse la acreditación se mantengan durante la vigencia de la misma. (LSMDFE Art. 22).

Para ello puede requerir información y ordenar Auditorías a las instalaciones del PSC o CE inspeccionado, sin previo aviso, ya sea con su personal o por medio de los auditores registrados.

5.2.3.2 Auditores Registrados

Corresponde a un profesional independiente que cuentan con la capacidad técnica para realizar el proceso de evaluación, las cuales son inscritas en un registro que lleva la Superintendencia, una vez comprobada su capacidad.

El proceso de evaluación y Auditoría es el procedimiento por el cual la Superintendencia verifica el cumplimiento de la LSMDFE y sus reglamentos, tanto para los PSC o CE acreditados como para los que solicitan acreditación o renovación, respectivamente.

5.2.3.3 Proveedores de Servicios de Certificación (PSC)

Corresponde a la entidad emisora de certificados de firma electrónica, la cual solicita ser acreditada.

5.2.3.4 Casos Especiales

Corresponde a la entidad de certificación extraordinaria que por motivos de proyectos de interés nacional son acreditados ante SUSCERTE, de acuerdo a la providencia administrativa de SUSCERTE 016.

5.2.3.5 Registro de PSC Acreditados

Registro público que mantiene la Superintendencia, en el cual están identificados los PSC acreditados (Artículo 22 LSMDFE).

5.2.3.5 Registro de Auditores

Registro público que mantiene la Superintendencia, en el cual están identificados los Auditores autorizados para realizar las auditorías a PSC o CE.

5.2.3.6 Estándares Técnicos

Conjunto de estándares internacionales vigentes que debe cumplir el PSC o CE para ser acreditado por la Superintendencia, además de los requisitos y obligaciones establecidas explícitamente en el Artículo 31 de la LSMDFE y los establecidos en el presente Documento.

5.2.3.7 Renovación

La vigencia de la acreditación de los PSC ante SUSCERTE, tendrá la duración de un (1) año. El PSC deberá solicitar la renovación de la acreditación dentro de los cuarenta y cinco (45) días continuos, previos al vencimiento de la acreditación. Al momento de la solicitud de renovación el PSC deberá presentar nuevamente todos los recaudos de conformidad con lo establecido en el artículo 3, 8 y 9 del RPDLSMDFE. (Artículos 8 y 9 del RPDLSMDFE).

5.2.3.8 Solicitante

Aspirante a PSC o PSC acreditado que solicita e inicia un trámite de acreditación o renovación ante SUSCERTE.

5.2.4 Los recaudos técnicos, estándares tecnológicos y lineamientos de seguridad a aplicar para la acreditación o renovación como PSC o CE, se resumen en el Anexo No 1 y se detallan a continuación en las consideraciones específicas, considerando las áreas técnicas en las cuales se agrupan, a saber:

5.3.1 Infraestructura de Clave Pública. Perfiles de certificado y servicios de publicación
5.3.2 Infraestructura de Clave Pública. Ciclo de vida de las claves
5.3.2 Administración, operación y seguridad de la infraestructura de clave pública
5.3.3 Declaración de prácticas de certificación y políticas de certificados
5.3.4 Organización
5.3.5 Reconocimiento de los certificados de la cadena de confianza

5.3. Consideraciones Específicas

5.3.1 Infraestructura de Clave Pública. Perfiles de Certificado y Servicios de Publicación

5.3.1.1 Estructura e Información del Certificado Electrónico

5.3.1.1.1 Objetivo

Comprobar los aspectos mínimos que dispone la LSMDFE con relación a la conformidad con el estándar ITU-T Rec. X.509, contenidos mínimos, incorporación de los requisitos mínimos obligatorios, límites y atributos del certificado de firma electrónica.

5.3.1.1.2 Descripción

1. La estructura de datos que conforma el certificado de firma electrónica emitido por el PSC o CE debe estar en conformidad al estándar ITU-T Rec. X.509.
2. El certificado de firma electrónica emitido por el PSC o CE debe contener al menos los siguientes datos:
   a) Un código de identificación único del certificado.
   b) Identificación del PSC o CE, con indicación de su nombre o razón social, RIF, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica.
   c) Los datos de la identidad del signatario, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y cédula de identidad.
   d) Plazo de vigencia (fecha de inicio y de vencimiento).
3. El PSC o CE debe incorporar en sus certificados el RIF propio y la identificación del signatario de acuerdo a la estructura e identificadores que se especifica por la Superintendencia de acuerdo al caso.
4. Los PSC o CE deben indicar en forma explícita, que el certificado emitido corresponde a una política de certificados con los límites de uso (ej. de firma electrónica). Esta indicación debe quedar inserta en el campo Certificate Policies de las extensiones del certificado del formato X.509 versión 3.
5. El PSC o CE interesado debe estructurar los certificados que emite, de forma que los atributos adicionales que introduce, así como la incorporación de límites al uso del certificado, no impidan la lectura del mismo ni su reconocimiento por terceros de la Infraestructura Nacional de Certificación Electrónica.
6. Los límites de uso que se incorporen en los certificados, deben ser reconocibles por terceros de la Infraestructura Nacional de Certificación Electrónica.
7. Los datos de creación de firma del PSC o CE acreditado para emitir certificados, no deben ser utilizados más allá de lo establecido en la DPC aprobada por SUSCERTE.

5.3.1.1.3 Estándares de Evaluación

- ITU-T Rec. X.509 / ISO/IEC 9594-8
- ITU-T X.690
- Norma SUSCERTE 032.

5.3.1.1.4 Documentación Solicitada

-Modelo de Certificado de firma electrónica, emitido por el PSC o CE en evaluación.
-Modelo de solicitud de firma del certificado (CSR), en caso de acreditación.
-Modelo de certificados electrónicos emitidos por el PSC o CE (DPC y PC).

5.3.1.1.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ITU-T Rec. X.509 Norma SUSCERTE No. 032.	Se verificará que la estructura básica del certificado esté en conformidad a la norma y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias para incluir el RIF o CI, puedan ser *leídos por cualquier aplicación que cumpla dicho estándar.*
Contenido básico del certificado de firma electrónica emitido por el PSC o CE (Norma SUSCERTE No. 032)	Se confirmará que el certificado contiene la siguiente información: a) Un código de identificación único del certificado b) Identificación del PSC o CE, con indicación de su nombre o razón social, RIF, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica c) Los datos de la identidad del signatario, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico, su RIF O CI, y d) El tiempo de vigencia.
Método de incorporación de identificación del signatario (Norma SUSCERTE No. 032)	Se verificará que el PSC o CE incorpore en sus certificados el identificador que venga al caso, como por ejemplo en caso de que el signatario sea persona jurídica se debe incluir el RIF.
***Lectura y reconocimiento* del contenido mínimo cuando existen atributos *adicionales en* el certificado**	*Se validará que el PSC o CE estructure sus certificados*, de forma que los atributos adicionales que introduzca, con el fin de incorporar límites al uso del certificado, si los hay, no impidan la lectura ni su reconocimiento por terceros.
Reconocimiento de límites de uso del certificado de firma electrónica por terceros	Se verificará que el PSC o CE estructure sus certificados de manera que *los límites de uso, si los hay, sean reconocibles por terceros.*
Uso de clave pública acreditada	Se verificará que los datos de creación de firma del PSC o CE acreditado para emitir certificados no sean utilizados más allá de lo establecido en la DPC aprobada por SUSCERTE.
Algoritmos de firma	Se validará que el PSC o CE utilice algoritmos de firma estándares de la industria (establecidos por el RFC 5280) que provean el adecuado nivel de seguridad aprobado por SUSCERTE tanto para su propia firma como para la firma del signatario.
Tamaño de las claves	Se comprobará que el PSC o CE utilice el tamaño de clave pública y privada, de mínimo 4096 para su propia firma y 2048 para la firma del signatario; o en su defecto se establecerá una longitud acorde a los estándares internacionales y conforme con las normativas emitidas formalmente por SUSCERTE.
Funciones Hash	Se verificará que el PSC o CE utilice funciones Hash de última generación para el proceso de firma, debidamente elegida a través de un estudio de factibilidad por la Superintendencia, que provean el nivel de seguridad, tanto para su propia firma como para la firma del signatario. El uso de funciones de hash debe actualizarse cada año, posterior a la creación de este documento, ya que al cumplirse el lapso, se debe haber superado cualquier problema de interoperabilidad de algoritmos de mayor complejidad.

5.3.1.2 Estructura de la Lista de Certificados Revocados (LCR) y Servicio OCSP – Online Certificate Status Protocol

5.3.1.2.1 Objetivo

Verificar que las listas de certificados revocados tengan el formato y contenido establecido en el estándar, y permita al signatario identificar plenamente al PSC o CE emisor de la LCR y se verificará la integridad y funcionalidad del servicio OCSP, el cual sirve para determinar el estado de revocación de un certificado electrónico, como método alternativo a la LCR. Este protocolo se describe en el RFC 2560.

5.3.1.2.2 Descripción

La lista de certificados revocados (LCR) debe contener la información y estructura que especifica el RFC 6818.

Este RFC especifica que la lista debe contener al menos la identificación del emisor, fecha de su emisión e identificación de los certificados revocados a dicha fecha. Ya que la lista podría ser almacenada y enviada en medios inseguros, debe estar debidamente firmada por el PSC o CE emisor.

Para el Servicio OCSP se verificará que el PSC o CE:

- Garantice la existencia de un servicio seguro de consulta de la validez de los certificados electrónicos a través del servicio OCSP
- Provea acceso al servicio a partes interesadas por medios electrónicos de manera continua y regular.
- Use sistemas y productos confiables que garanticen la seguridad de su sistema.
- Cuente con procedimientos para informar a los signatarios las características generales del servicio.

5.3.1.2.3 Estándares de Evaluación

- RFC 6818
- RFC 2560
- Norma SUSCERTE No 032

5.3.1.2.4 Documentación Solicitada

- DPC y PC del PSC o CE.
- LCR emitida por el PSC o CE en evaluación y el certificado de firma electrónica de la AC que la emite.
- Reportes de solicitudes y/o peticiones al servicio OCSP

5.3.1.2.5 Detalles de la Evaluación

Aspectos	Evaluación
Contenido Mínimo	Se verificará que la LCR contenga al menos la siguiente información: • Versión. Debe tener el valor 2 • Algoritmo de firma. Este campo debe contener la identificación del algoritmo de firma utilizado, siguiendo el RFC 6818. • Nombre del emisor. Este campo debe contener el nombre de la entidad que emitió y firmó la lista de certificados revocados. • Fecha actual. Este campo debe contener la fecha y hora en que fue emitida la lista de certificados revocados (LCR). • Próxima actualización. Se deberá incluir en este campo la fecha en que se emitirá la próxima lista de certificados revocados. • Certificados revocados. En este campo se deben incluir los números de serie de los certificados revocados por el emisor, indicando además la fecha y hora de revocación correspondiente.
Comprobación de firma	Se comprobará que la lista de certificados revocados esté debidamente firmada por el PSC o CE emisor.
Mecanismo de suspensión de certificados	Se verificará que la lista de certificados revocados incluya la información necesaria para indicar el estado de suspensión de un certificado.
Para el Servicio OCSP:	
Pruebas de las peticiones	El PSC o CE debe mantener un sitio de acceso electrónico, el servicio del OCSP el cual debe aceptar peticiones respecto a la vigencia o no de los certificados electrónicos por él emitidos. Se debe asegurar una disponibilidad del sitio no menor al 99%.
Comprobación del contenido de las consultas	Debe revisarse el contenido de las respuestas esperadas. Los estatus de las respuestas deben ser: VÁLIDO, REVOCADO Y DESCONOCIDO.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnología y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de ataques maliciosos tanto internos como externos en contra del sitio.

5.3.1.3 Registro de Acceso Público. (Servicios, contenido y accesibilidad electrónica del sistema público de información del PSC o CE)

5.3.1.3.1 Objetivo

Asegurar el acceso a información relevante descriptiva del sistema por parte de los signatarios y terceros, como mínimo se requiere acceso a la DPC y a las PC, así como a los servicios de publicación como el certificado de la AC y LCR.

5.3.1.3.2 Descripción

Se verificará que el PSC o CE:

- Garantice la existencia de un servicio seguro de consulta remota de un registro de certificados emitidos, en el que quede constancia de los certificados emitidos indicando si el mismo se encuentra vigente, revocado o suspendido, si le ha sido traspasado de otro PSC o CE acreditado o si es homologado.
- Provea acceso al registro público de certificados a los signatarios y partes interesadas por medios electrónicos de manera continua y regular.
- Use sistemas y productos confiables que garanticen la seguridad de su sistema de difusión de información.
- Cuente con procedimientos para informar a los signatarios las características generales de los procesos de creación y verificación de firma electrónica, así como de las reglas sobre prácticas de certificación que el PSC o CE se comprometa a utilizar en la prestación del servicio.
- Tenga procedimientos para dejar sin efecto temporal o definitivamente (suspender o revocar) los certificados.
- Cuente con procedimientos para publicar y actualizar en su(s) sitio(s) la información de acceso electrónico, las resoluciones de la Superintendencia que le afecten. Esto debe realizarse como mínimo en los sitios de dominio público registrados durante el proceso de acreditación o renovación. Además, debe incluirse la DPC y PC.

5.3.1.3.3 Estándares de Evaluación

Este apartado no aplica

5.3.1.3.4 Documento Solicitado

Documento descriptivo que contenga al menos la siguiente información:

- Detalle del sitio Web donde publicara la información.
- Descripción de la tecnología.
- Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento.
- Medidas de seguridad.
- Sitio Web de prueba con las funcionalidades requeridas.
- Publicación y vigencia de DPC y PC
- Publicación y vigencia de la LCR

5.3.1.3.5 Detalles de la Evaluación

Aspectos	Evaluación
Existencia y contenido mínimo del Sitio Web de información pública	El PSC o CE debe mantener un sitio de acceso electrónico, con información relevante para los signatarios y las partes que confían. Al menos debe contener los siguientes documentos: • Registro de certificados emitidos, indicando código de identificación único del certificado y su estado (vigente, suspendido o revocado). • Copia de la LCR actualizada cada 24 horas. • Indicar si el certificado ha sido traspasado de otro PSC o CE acreditado o ha sido homologado. • Acceso seguro a los signatarios para realizar revocación o suspensión de certificados vigentes. • DPC y PC(s).
Disponibilidad de la información y servicio	Se debe asegurar una disponibilidad del sitio no menor al 99%, anual. Para esto se verificará la existencia de mecanismos redundantes o alternativos de conexión y sitios de contingencia que permitan levantar la plataforma manual o automáticamente en caso de desastres.
Seguridad	Se debe proteger la integridad y disponibilidad de la información mediante el uso de tecnologías y medidas de seguridad tanto físicas como lógicas que reduzcan los riesgos y consecuencias de

	ataques maliciosos tanto internos como externos en contra del sitio.

5.3.2 Infraestructura de Clave Pública. Ciclo de Vida de las Claves

5.3.2.1 Plan de Administración de Claves Criptográficas. (Implementación y Mantenimiento)

5.3.2.1.1	**Objetivo** Comprobar que la organización implementa un plan de administración del ciclo de vida de sus claves criptográficas coherente con su política de seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio y que asegure que las claves de la AC son generadas bajo circunstancias controladas.
5.3.2.1.2	**Descripción** Las claves criptográficas son la base de una infraestructura de claves públicas (PKI), siendo el elemento principal a resguardar y administrar por el PSC o CE, y por lo tanto requiere de un plan específico para su administración. Para la generación y resguardo de las claves de la AC , se exige el cumplimiento de las directrices establecidas en la ETSI TS 102 042 secciones 7.2.1 – 7.2.2 – 7.2.3 – 7.2.4 - 7.2.5 – 7.2.6 – 7.2.7 – , considerando que de acuerdo a lo establecido en la LSMDFE y su Reglamento, la firma electrónica es reconocida o avanzada y el reconocimiento de certificados de validación extendida. El contenido mínimo de este plan consistirá en lo siguiente: • Documentación del ciclo de vida completo de las claves criptográficas de la AC, esto es: 1. Generación de las claves de la Autoridad de Certificación de firma electrónica del PSC o CE 2. Almacenamiento, respaldo y recuperación de la clave privada de la AC de firma electrónica. 3. Distribución de la clave pública de la AC de firma electrónica. 4. Uso de la clave privada por parte de la AC de firma electrónica. 5. Término del ciclo de vida de la AC de firma electrónica . 6. Revocación del Certificado del PSC o CE • Administración del ciclo de vida del hardware criptográfico utilizado por la AC. • Servicios de administración de las claves de los signatarios suministradas por la AC (generación de clave, renovación después de vencimiento y revocación de la clave) • Preparación de los dispositivos seguros de los signatarios. • A su vez el plan debe ser consistente con la DPC y PC.
5.3.2.1.3	**Estándares de Evaluación** - ETSI TS 102 042 - FIPS 140-1 - FIPS 140-2 - CA/BR B - CA/BR G
5.3.2.1.4	**Documentación Solicitada** *Documento descriptivo de la implementación del Plan de Administración de Claves Criptográficas de la Organización.*
5.3.2.1.5	**Detalles de la Evaluación**

Aspectos	Evaluación
Relación entre el Plan de Administración de Claves y los recursos asignados	Verificar que el PSC o CE dispone de los recursos y capacidades adecuados para implementar el plan de administración de claves.
Relación entre Plan de Administración de Claves y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de administración de claves implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Administración de Claves	Confirmar que los procedimientos implementados de acuerdo al Plan de Administración de Claves posibilitan que la seguridad de las claves se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Administración de Claves con las prácticas y Política de Certificados	Comprobar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través de la implementación del Plan de Administración de Claves.
Requerimientos ETSI TS 102 042, sección 7.2.1	**Generación de Claves de la AC:** El PSC o CE se asegurará de que las claves CA se generan en circunstancias controladas. En particular: a) La generación de claves de la AC se llevará a cabo en un ambiente protegido físicamente (Véase Plan de Seguridad de la Información – Acceso Físico) por personal autorizado (Véase Documento Evaluación del Personal) bajo, al menos, el control dual. El número de personal autorizado para llevar a cabo esta función deberán mantenerse al mínimo, considerando las contingencias y ser coherentes con la DPC. b) La generación de claves se llevará a cabo con una aplicación o dispositivo que asegure que las claves se generan de una manera confiable y no ponen en peligro la seguridad de la clave privada. La generación de claves de CA se llevará a cabo dentro de un dispositivo que: • Cumpla los requisitos identificados en FIPS PUB 140-2 el nivel 3 o superior; • Un sistema confiable como EAL 3[1] (Evaluation Assureance Level) o superior, de acuerdo con la norma ISO / IEC 15408 [4]; • O con otros estándares de seguridad equivalentes. c) La generación de claves se debe realizar utilizando un algoritmo reconocido por la industria como aptos para los usos de firma. d) La longitud de la clave seleccionada y algoritmo para la clave de firma de la AC será uno que es reconocido por la industria para fines de firma de la AC. e) Un tiempo adecuado antes de la expiración de la clave de firma, el PSC o CE deberá generar un nuevo par de claves de firma de certificado y se aplicaran todas las medidas necesarias para evitar la interrupción de las operaciones de una entidad que puede confiar en la clave de la AC. La nueva clave de la AC será también generada y distribuida de acuerdo con esta política. **NOTA 1:** Con el fin de cumplir con este requisito estas operaciones deben realizarse lo suficientemente oportunas para permitir que todas las partes que tienen relaciones con la AC estén conscientes del cambio de clave y de implementar los procesos necesarios para evitar inconvenientes y disfunciones. Esto no se aplica a una AC que cesará sus operaciones antes de su fecha de caducidad.
Requerimientos ETSI TS 102 042, sección 7.2.2	**Almacenamiento, Respaldo y Recuperación:** El PSC o CE se asegurará de que las claves privadas de la AC se mantienen confidenciales y mantendrán su integridad. En particular: a) La firma de la clave de la AC se realizará con aplicación o dispositivo que no permita comprometer la seguridad de la misma y que cumpla con los requisitos identificados en los estándares • FIPS PUB 140-2 , el nivel 3 o superior; o • Un sistema confiable como EAL 4 o superior, de acuerdo con la norma ISO / IEC 15408; • o con otros estándares de seguridad equivalentes Esto se hará bajo un perfil objetivo de seguridad o de protección que cumple con los requisitos del presente documento, basado en un análisis de riesgos, y teniendo en cuenta las medidas de seguridad de carácter no técnico. b) Se debe garantizar la confidencialidad de la clave privada luego del proceso de creación o firma dentro de la aplicación o dispositivo utilizado. **NOTA 2:** Esto se puede lograr con la aplicación de controles de seguridad físicos y lógicos o de cifrado. c) La clave privada de la AC deberá ser respaldada, almacenada y recuperada sólo por personal autorizado, al menos, con un control dual en un entorno protegido físicamente (Véase Plan de Seguridad de la Información – Acceso Físico). El número de personal autorizado para llevar a cabo esta función, deberán mantenerse al mínimo, de acuerdo a los planes de contingencia y ser coherentes con la DPC. d) Las copias de seguridad de las claves privadas de la AC estarán bajo las mismas o con mayores niveles de seguridad que las claves privadas que están actualmente en uso. e) Cuando las claves se almacenan en un módulo de hardware criptográfico o HSM, los controles de acceso a éste deberán asegurar que las llaves no son accesibles fuera del módulo de hardware.
Requerimientos ETSI TS 102 042, sección 7.2.3	**Distribución de la clave pública de la AC:** El PSC o CE deberá asegurar la integridad y autenticidad de la clave pública de la AC, y cualquier otro parámetro asociado al uso de la clave, durante su distribución a terceras personas. En particular: a) La verificación de la clave pública de la AC estará a disposición de terceras personas, de esta manera se asegurará la integridad de misma y la autenticación de su origen. b) La clave pública de la AC debe ser firmada por si misma para su distribución.
Requerimiento ETSI TS 102 042, sección 7.2.4	**Depósito de claves (Key escrow)** Si la clave del signatario es usada para firmar electrónicamente, el PSC o CE no puede mantener la clave del signatario, ya que esto podría proveer la capacidad de descifrarla desde el respaldo.
Requerimientos ETSI TS 102 042, sección 7.2.5	**Usos de la Clave de la AC:** El PSC O CE se asegurará de que la clave privada no se utilizará de forma inadecuada. En particular: a) La clave de la CA utilizada para la generación de certificados, tal como se define en la sección 7.3.3 de la ETSI 102 042, y/o la emisión de la información del estado de revocación, no será utilizada para ningún otro propósito. b) Las claves de firma de certificado sólo serán utilizados dentro de espacios físicamente seguros (Véase Plan de Seguridad de la Información – Acceso Físico).
Requerimientos ETSI TS 102 042, sección 7.2.6	**Final del Ciclo de Vida de la Calve** El PSC O CE se asegurará de que la clave privada no se utilizará posterior al final de su ciclo de vida. En particular: a) El uso de la clave privada de la AC correspondiente, se limitará a que es compatible con el algoritmo de hash, el algoritmo de firma y la longitud de clave usados en la generación del certificado, tal y como se define en la cláusula ETSI 7.2.1. b) Todas las copias de las claves privada de la AC serán destruidos posterior al final de su ciclo de vida.
Requerimientos ETSI TS 102 042, sección 7.2.7	**Ciclo de vida de la administración del hardware criptográfico usado para la firma de certificados:** El PSC o CE garantizará la seguridad del dispositivo criptográfico lo largo de su ciclo de vida. En particular, el PSC o CE se asegurará de que: a) Los certificados y el estatus de la información de revocación que maneja el hardware criptográfico no debe ser manipulada durante la generación.

1 Proporciona aseguramiento completo por objetivo. Ir al estándar ISO/IEC 15408

b) Los certificados y el estatus de la información de revocación que maneja el hardware criptográfico no debe ser manipulada mientras es almacenada.

c) La instalación, activación, copia de seguridad y recuperación de la clave de la AC en el hardware criptográfico deberá requerir el control simultáneo o conjunto de al menos dos (2) de los empleados autorizados.

d) Los certificados y el estatus de la información de revocación que maneja el hardware criptográfico deberá estar funcionando correctamente.

e) La clave privada de la AC que está almacenada en el hardware criptográfico debe destruirse en caso de finalizar las operaciones o funcionamiento del dispositivo. Esta destrucción no afecta a todas las copias de la clave privada. Sólo la instancia física de la clave almacenada en el hardware criptográfico en consideración será destruida.

Requerimientos ETSI TS 102 042, sección 7.4.9

Terminación de una AC:

El AC deberá garantizar que las posibles interrupciones a los suscriptores y partes de confianza se minimicen como resultado del cese de los servicios, y asegurar la continuidad de mantenimiento de registros debe proporcionar evidencia de certificación a los efectos de los procedimientos judiciales, que para el caso de Venezuela, la LSMDFE establece un mínimo de diez (10) años.

1.- Antes que la AC termine sus servicios debe asegurar como mínimo que:

a) el PSC o CE deberá informar la terminación de la AC a todos los suscriptores y entidades con las que tenga acuerdos u otras formas de relaciones que se establezcan entre las cuales las partes que confían en la AC. Adicionalmente, esta información deberá ponerla a disposición de otras partes de confianza;

b) la AC terminará todas las autorizaciones de los subcontratistas que habiliten sus operaciones como los que actúen en nombre de ella, en el desempeño de las funciones relacionadas con el proceso de emisión de certificados;

c) la AC llevará a cabo las acciones necesarias para la transferencia de las obligaciones de mantener el registro de información de sus operaciones, la información de estado de revocación y los archivos de registro de eventos, por un periodo de diez (10) años tal y como lo establece la LSMDFE.

d) la AC deberá destruir o retirar de su uso, sus claves privadas, como se define en la cláusula 7.2.6. del la ETSI.

2.- El PSC o CE llegará a un acuerdo para cubrir los costos de cumplir con estos requisitos mínimos en caso de que el Cese de la AC este vinculado con una situación de quiebra o por otras razones que eviten poder cubrir los costos por sí mismos, en la medida de lo posible dentro de las limitaciones de la legislación aplicable en materia de quiebra.

3.- La AC deberá indicar en sus prácticas las provisiones consideradas para la interrupción del servicio. Esto incluirá:

a) la notificación de las entidades afectadas;

b) la transferencia de sus obligaciones frente a terceros;

c) el manejo del estado de revocación de los certificados no vencidos que se han emitido.

Requerimientos CA/BR B, sección 4.9.1.2

Razones para revocar un certificado de una CA Subordinada (PSC o CE).

La AC Raíz revocará un certificado de AC subordinada dentro de los siete (07) días siguientes si se presenta uno o más de los siguientes supuestos:

1. La AC Subordinada solicita la revocación por escrito;
2. La AC Subordinada notifica a la AC Raíz que la solicitud de certificado original no fue autorizada y no concede retroactivamente la autorización;
3. La AC Raíz obtiene pruebas de que la clave privada de la AC subordinada correspondiente a la clave pública en el certificado, sufrió un Compromiso de clave;
4. La AC Raíz obtiene pruebas de que el certificado fue mal utilizado;
5. La entidad emisora conoce que el certificado no fue emitido de conformidad o que AC Subordinada no ha cumplido con los requisitos de base de la Declaración de Política de Certificados o Prácticas de Certificación aplicable;
6. La AC Raíz determina que alguna de la información que aparece en el certificado es inexacta o engañosa;
7. La entidad emisora o AC subordinada cesa operaciones por cualquier razón y no ha hecho arreglos para otra AC para proporcionar apoyo en la revocación del Certificado;
8. El derecho de emisión de AC o AC subordinada para emitir certificados bajo estos requisitos vence o es revocado o cancelado, a menos, que la entidad emisora ha hecho arreglos para continuar manteniendo el repositorio de la CRL / OCSP;
9. La Revocación es requerida por la Política de Certificados de la AC y/o Declaración de Prácticas de Certificación;
10. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para el software de aplicación de los Proveedores o las Partes que Confían (por ejemplo, el CA/Browser Forum podría determinar obsoleta los algoritmos criptográficos de firma o el tamaño de las claves presentan un riesgo inaceptable y que dichos certificados deberán ser revocados y sustituidos por la misma dentro de un período de tiempo dado)

Nivel de seguridad del dispositivo seguro de los signatarios

Verificar que el dispositivo seguro de los signatarios cumple como mínimo con los requerimientos del estándar FIPS 140-2 nivel 3 (o Common Criteria EAL 3 ISO/IEC 15408) en sus elementos de seguridad e implementación de los algoritmos criptográficos estándares.

5.3.2.2 Modelo y Manual de Operación de la Autoridad de Certificación (AC)

5.3.2.2.1 Objetivo

Comprobar a través de la documentación presentada, el cumplimiento de los aspectos operacionales mínimos que dispone la LSMDFE, el Reglamento parcial, la ETSI y CA/BR con relación a los requisitos de confiabilidad e interoperabilidad en la forma de operar y prestar los servicios de la AC principales y subordinadas de un PSC o CE.

5.3.2.2.2 Descripción

El propósito del modelo y manual es describir la administración diaria y las prácticas operacionales de la AC principal y/o las subordinadas, del PSC o CE, y garantizar que las directrices primarias de la DPC y PC estén implementadas operacionalmente; con el fin de facilitar al personal (de operaciones, consultores y/o auditores), la comprensión de esta información, se permite el uso de gráficos, diagramas de flujo, funcionales, líneas de tiempo, etc.

El Modelo y Manual de Operación de la AC principal y/o subordinadas del PSC deberá tener al menos las siguientes características:

- Ser consistente con la Política de Certificados.
- Se consistente con el estándar ETSI y CA/BR.
- Incluir la interacción entra la AC principal y subordinada, así como con las AR.
- Describir los controles de seguridad física, de red, de recursos humanos y de procedimientos.
- Incluir los procedimientos adoptados para el manejo de claves públicas y privadas .

5.3.2.2.3 Estándares de Evaluación

- ETSI TS 102 042
- CA/BR
- RFC 3647

5.3.2.2.4 Documentación Solicitada

Modelo y Manual de operación de la AC principal y/o subordinadas del PSC o CE
Manual del Hardware Criptográfico usados para la generación y protección de las claves privadas de la(s) autoridades de certificación

5.3.2.2.5 Detalles de la Evaluación

Aspectos	Evaluación
Asignación de funciones y responsabilidades	Identificación del personal encargado de la operación y administración de la AC principal y/o subordinadas del PSC o CE, en relación a lo establecido en la "Evaluación del Personal".
Referencias de los cargos en los planes de la PSC o CE	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencias.
Descripción de las Operaciones	Descripción detallada de los siguientes procedimientos: 1. Generación de pares de claves 2. Publicación de la LCR 3. Publicación de la información del certificado 4. Distribución de claves y certificados 5. Renovación de certificados 6. Renovación de certificados luego de una revocación 7. Suspensión de certificados 8. Medidas de control de acceso 9. Procedimientos de respaldo y recuperación
Actualización de DPC y PC	Procedimiento de actualización de la DPC y PC de firma electrónica.
Servicios de la AC	Descripción de los servicios de la AC principal y/o subordinadas
Interacción AC - AR	Descripción de modelo de interacción entre la AC principal y/o subordinadas, así como con la(s) AR(s)

Requerimientos ETSI TS 102 042, sección 7.2.8

Servicio de la AC de gestión de Certificados para signatarios

La AC se asegurará de que la generación de las claves de los signatarios, se lleve a cabo de forma segura y se conserve el secreto de la clave privada.

Generación Certificado

a) Las claves de los signatarios se deben generar con un algoritmo reconocido por la industria (RSA) y las políticas de certificados deben estar adaptadas a los usos identificados en el algoritmo durante el tiempo que dure el certificado.

b) la longitud de las claves de los signatarios generadas por la AC deben ser de un tamaño (mínimo 2048) y uso de acuerdo a un algoritmo de clave publica reconocido por la industria (RSA) de forma que se adapte a los propósitos establecidos en las Políticas de Certificado por el tiempo que dure o de su validez.

c) la clave privada del signatario deberá ser entregada al mismo asegurando su secreto y la integridad, a los efectos de que la misma no se vea comprometida.

d) una vez entregada la clave al signatario, solo se debe mantener bajo el control y uso exclusivo del signatario.

Requerimientos ETSI TS 102 042, sección 7.3.2

Renovación, cambio de claves y actualización de Certificados Electrónicos

La AC se asegurará de que las solicitudes de un signatario que ya ha sido previamente registrado en la misma AC sea completa, precisa y debidamente autorizada. Esto aplica para la renovación de certificados, cambio de claves seguidas a la revocación y antes de una expiración, o una actualización debido a cambio a los atributos del signatario.

a) La AC verificará la existencia y validez del certificado que se renueva y que la información que utiliza para verificar la identidad y los atributos del signatario siguen siendo válidos.

b) Si alguno de los términos y condiciones de la AC han cambiado, éstas serán comunicadas y acordadas de nuevo con el suscriptor.

c) Si los nombres o atributos del certificado han cambiado, o el certificado anterior ha sido revocado, el registro información debe ser verificado, grabado, acordado por el signatario de conformidad con la cláusula 7.3.1 de la ETSI apartados d) e l).

d) La AC deberá emitir un nuevo certificado utilizando la clave pública previamente certificadas del signatario, sólo si su seguridad criptográfica es todavía suficiente para el período de validez del nuevo certificado y no existen indicios de que la la clave privada del sujeto ha sido comprometida.

Requerimientos ETSI TS 102 042, sección 7.3.3

Generación de Certificados

El PSC o CE deberá garantizar las condiciones de seguridad necesarias para la emisión de los certificados a objeto de asegurar su autenticidad.

En particular:

a) Los certificados deben incluir, de acuerdo a los estándares X.509 y RFC 5280 :

1) identificación de la CA que emite el certificado y el país en el que está establecida;

2) el nombre del sujeto, o un seudónimo que lo identifique como tal;

3) la existencia de un atributo específico del signatario, se incluirá de ser necesario, según la función o finalidad para la que el certificado este destinado;

4) la clave pública que corresponde a la clave privada bajo el control del sujeto;

5) una indicación relativa a la fecha inicial y final del período de validez del certificado;

6) el número de serie del certificado;

7) la firma electrónica de la autoridad de certificación que lo emite;

8) el alcance del uso del certificado, si aplica; y

9) los límites del valor de las transacciones para las que puede utilizarse el certificado, si aplica;

b) El PSC o CE tomará medidas contra la falsificación de certificados y debe garantizar la confidencialidad durante el proceso de generación de dichos datos.

c) El procedimiento de emisión del certificado estará firmemente vinculado al registro asociado, de renovación o revocación, incluyendo el suministro de cualquier clave pública generada por el signatario.

d) Si el PSC o CE genera la clave del signatario:

1) el procedimiento de emisión del certificado estará firmemente ligado a la generación del par de claves del PSC o CE;

2) la clave privada se pasa de forma segura al signatario registrado;

3) el dispositivo seguro que contiene la clave privada del signatario debe almacenar con seguridad esa clave registrada por el signatario (FIPS PUB 140-2 nivel 3).

e) El PSC o CE se asegurará de que durante el tiempo de vida de la AC, el nombre distinguido que se ha utilizado en un certificado nunca se vuelve a asignar a otra entidad.

f) La confidencialidad y la integridad de los datos de registro deberán estar protegidos, especialmente cuando se intercambian entre el emisor y el signatario o entre los componentes del sistema de la AC.

g) El PSC o CE verificará que los datos de registro que intercambia con el servicios de registro (AR), serán autenticados o validados.

Requerimientos ETSI TS 102 042, sección 7.3.4

Difusión de los términos y condiciones

El PSC o CE se asegurará de que los términos y condiciones estén a disposición de los suscriptores y partes de confianza.

En particular:

a) El PSC o CE pondrá a disposición de los suscriptores y partes de confianza los términos y condiciones sobre el uso de los certificados:

a.1) la política aplicada al certificado, incluyendo una declaración clara en cuanto a si la política es para los certificados emitidos al público o si la política es requerida para el uso de algún producto, aplicación o dispositivo en particular, para efectos de la aplicación del par de claves asociados al certificado expedido;

a.2) cualquier limitación en el uso del certificado;

a.3) las obligaciones del suscriptor como se define en la cláusula 6.2 (ETSI), incluyendo si la política requiere el uso de cualquier producto, aplicación o dispositivo en particular, para los fines de la aplicación del par de claves asociados con la emisión del certificado;

a.4) información sobre cómo validar el certificado, incluyendo los requisitos para comprobar el estado de revocación del mismo, de manera que las partes que confía consideren "una confianza razonable" en el certificado

a.5) cualquier limitación de responsabilidad que el PSC o CE acepte o excluya, incluyendo los fines y usos;

a.6) el período de tiempo en el cual es retenida la información de registro

a.7) el período de tiempo en el cual se conservan los registros de eventos de la AC;

a.8) los procedimientos de reclamo y solución de controversias;

a.9) el ordenamiento jurídico aplicable; y

a.10) si el PSC ha sido evaluado conforme con la política de certificados identificada, y si es así a través de cual esquema.

b) La información que se indica en el apartado (a) debe estar disponible y ser pública, transmitida electrónicamente, y en un lenguaje fácilmente y comprensible.

Requerimientos ETSI TS 102 042, sección 7.3.5

Difusión de los certificados

El PSC o CE debe asegurarse que los certificados están a disposición de los suscriptores, signatarios y terceras partes que confían.

En particular:

Se difunde

a) Luego de la generación, el certificado completo y exacto, deberá estar disponible para el suscriptor o signatario para el cual se emite el certificado.

b) Los certificados están disponibles para su consulta pública.

c) El PSC o CE pondrá a disposición de las partes que confían los términos y condiciones con respecto al uso del certificado

d) Los términos y condiciones aplicables serán fácilmente identificables para un certificado determinado.

e) La información indicada en las letras b) y c) anteriores deberá estar disponible las 24 horas al día, 7 días a la semana. En caso de fallo del sistema, servicio u otros factores que no están bajo el control del PSC o CE, deberán aplicar medidas para garantizar que el servicio de información no está disponible para un periodo mayor al establecido en la declaración de prácticas de certificación lo cual debe ir de la mano con los lapsos fijados en la LSMDFE y su Reglamento.

f) Si la AC emite certificados al público la información indicada en los literales b y c anteriores debe estar publicada y disponible a nivel internacional.

Requerimientos ETSI TS 102 042, sección 7.3.6

Revocación y Suspensión de certificados

El PSC o CE se asegurará de que los certificados que se revoquen, una vez se verifique y valide la autorización, deben ser revocados de manera oportuna y a la brevedad posible

Gestión de Revocación

a) El PSC o CE deberá documentar como parte de su declaración de prácticas de certificación los procedimientos para revocación de certificados, incluyendo:

a.1) quienes pueden presentar reportes y solicitudes de revocación;

a.2) la forma en la que se pueden presentar;

a.3) los requisitos para la posterior confirmación de los reportes y solicitudes de revocación;

a.4) las razones para la suspensión de los certificados

a.5) el mecanismo utilizado para la distribución de la información de estado de revocación;

a.6) el retardo máximo entre la recepción de una solicitud de revocación o reporte y el cambio de estado al de revocación, debe estar a disposición de todas las partes que dependen de la información, que para todos los casos no puede exceder de 24 horas.

b) Las solicitudes y los reportes relativos a la revocación, se tramitarán en el recibo (por ejemplo, compromiso de la clave privada del signatario, la muerte del signatario, terminación inesperada de sus funciones de acuerdo o de negocios respecto al signatario o al suscriptor, la violación de obligaciones contractuales):

b.1) Se aplican, los requisitos de la CA/BR G, las secciones 9.3.2 (5) y 9.3.3 (5)

b.2) Se aplican, los requisitos de CA/BR B, sección 10.3.2 (5)

c) Se aplican los requisitos de CA/BR G, secciones 11.2.1 y 11.3.3.

d) Las solicitudes y los reportes relativos a la revocación deben ser autenticados, revisando que provengan de una fuente confiable y deben estar conforme a lo dispuesto en las prácticas de la AC.

e) El estado de revocación de un certificado puede ser "suspendido" mientras se está confirmando las causales y los reportes de revocación. El PSC se asegurará de que el certificado no se mantiene suspendido por más tiempo del necesario a los efectos de confirmar su estado.

f) El signatario, y en su caso el suscriptor, de un certificado revocado o suspendido, debe ser informado de el cambio de estado de su certificado.

g) Una vez que el certificado es revocado definitivamente (es decir, no suspendido) no podrá ser utilizado y deberá emitirse un nuevo certificado al signatario en caso de que éste lo solicite.

h) Cuando se utilizan listas de certificado revocado (LCR), incluyendo sus posibles variantes (por ejemplo, Delta CRL), éstas se publicarán por lo menos cada 24 horas, o cuando un certificado sea revocado;

i) Cuando se utilizan listas de certificados revocados (LCR) incluyendo sus posibles variantes (por ejemplo, Delta CRL) como el único de los medios de suministro de información para el estado de revocación:

i.1) cada LCR deberá indicar un tiempo para la próxima edición programada de la LCR (el cual no podrá exceder de 24 horas); y

i.2) una nueva LCR puede ser publicada antes de la hora indicada de la próxima edición de LCR;

i.3) la LCR será firmada por la AC.

i.4) La LCR debe ser emitida cumpliendo con Recomendación UIT-T X.509

Estado de revocación

j) La información del estado de revocación, deberá estar disponible las 24 horas al día, 7 días a la semana. Si se produce un fallo del sistema, servicio u otros factores que no están bajo el control del PSC o CE, el PSC o CE deberá hacer el mejor esfuerzo para asegurar que este servicio de información este disponible dentro de los lapsos establecidos en su declaración de prácticas de certificación y de acuerdo a lo definido en la LSMDFE y su Reglamento

o) Si la AC emite certificados al público, la información del estado de revocación debe ser pública y deberá estar disponible a nivel internacional.

p) La información de revocación debe incluir la información del estado de revocación hasta que el certificado expire.

q) Si se admite la firma de código, en caso de un certificado de firma de código de EV, la CA debe seguir el procedimiento de revocación que se indican en el artículo 13 de CA/BR B.

Requerimientos ETSI TS 102 042, sección 7.2.7

Ciclo de vida del hardware criptográfico utilizado para firmar certificados

La AC deberá garantizar la seguridad del dispositivo criptográfico lo largo de su ciclo de vida.

En particular, la AC se asegurará de que:

a) Que la firma del Certificado y su información del estado de revocación realizada por el hardware criptográfico no sea manipulada durante se envío.

b) Que la firma del Certificado y su información del estado de revocación realizada por el hardware criptográfico no sea manipulada durante se almacenamiento.

c) La instalación, activación, copia de seguridad y recuperación de claves de firma de la AC en el hardware criptográfico deberá requerir el control simultáneo de al menos tres (3) de los empleados de confianza.

d) Que la firma del Certificado y su información del estado de revocación realizada por el hardware criptográfico este funcionando correctamente.

e) La clave privada de la(s) AC almacenadas en el hardware criptográfico se destruyan al dejarse de usarse el dispositivo o al desincorporarse el dispositivo.

Requerimientos CA/BR B, sección 4.9.1.1

Razones para Revocación de un Certificado del Suscriptor

El PSC o CE revocará un certificado dentro de 24 horas si se presenta uno o más de las siguientes razones:

1.Una solicitud del suscriptor por escrito;

2.El suscriptor notifica que la solicitud original de certificado no fue autorizada y no concederá retroactivamente la autorización.

3. El PSC o CE obtiene pruebas de que el suscriptor de la clave privada correspondiente a la clave pública en el certificado sufrió un Compromiso de Clave.

4. El PSC o CE obtiene evidencia de que el certificado ha sido mal utilizado.

5. El PSC o CE descubre que un suscriptor ha violado una o más de sus obligaciones como suscriptor o los Términos de Uso;

6. El PSC o CE tiene conocimiento de circunstancias que indican que el uso de un nombre de dominio o la dirección IP en el certificado ya no está legalmente permitida (por ejemplo, un tribunal o árbitro ha revocado un derecho a utilizar el nombre de dominio, un acuerdo de licencia o servicios relevantes entre el Domain Name Registrant's y el solicitante ha terminado, o nombres de dominio que no han logrado renovar);

7. El PSC o CE conoce que un Certificado ha sido utilizado para autenticar a un subordinado de manera fraudulenta, engañosa;

8.El PSC o CE conoce de un cambio en la información contenida en el Certificado;
9.El PSC o CE conoce que el certificado no se hubiere expedido de acuerdo con estos requisitos o política de certificación de la entidad emisora o Declaración de Prácticas de Certificación;
10.El PSC o CE determina que alguna de la información que aparece en el certificado es inexacta o engañosa;
11.El PSC o CE cesa su actividad por cualquier razón y no ha hecho arreglos con otra CA para proporcionar apoyo en revocación del Certificado;
12.El derecho del PSC o CE para emitir certificados bajo estos requisitos expira o se revoca, a menos que el PSC o CE ha hecho arreglos para continuar manteniendo los repositorios de la CRL / OCSP;
13.El PSC o CE tiene conocimiento de un posible compromiso de la clave privada de la AC Subordinada utilizada para la emisión del Certificado;
14. La Revocación es requerida por la Política de Certificados de la CA y/o Declaración de Prácticas de Certificación; o
15.El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para el software de aplicación de los Proveedores o las Partes que Confían (por ejemplo, el CA/Browser Forum podría determinar obsoleta los algoritmos criptográficos de firma o el tamaño de las claves presentan un riesgo inaceptable y que dichos certificados deberán ser revocados y sustituidos por la misma dentro de un período de tiempo dado).

5.3.2.3 Modelo y Manual de Operación de la Autoridad de Registro (AR)

5.3.2.3.1 Objetivo

Comprobar a través de la documentación presentada los aspectos operacionales mínimos que dispone la LSMDFE y su reglamento parcial con relación a los requisitos de confiabilidad e interoperabilidad de la operación del PSC o CE para realizar las funciones de Autoridad de Registro.

El PSC o CE se asegurará de constatar de que los suscriptores y signatarios sean identificados con precisión, que sus datos, sus nombres y otros asociados, sean debidamente revisados como parte del servicio, o si aplica, concluir a través de la revisión y certificación a través de fuentes confiables; y que la solicitud del certificado sea exacta, autorizada y completa.

5.3.2.3.2 Descripción

El Modelo y Manual de Operación deberá describir como operará el servicio de registro del PSC o CE y su administración diaria. Entre otros aspectos debería tener las siguientes características:

- Ser consistente con la PC.
- Describir el plan de entrenamiento de los empleados.
- Incluir la forma en que se verifica la identidad de las personas.
- Incluir procedimientos de entrega y uso de la clave privada por los signatarios de los certificados. Según la norma ETSI TS 102 042, se entiende que el PSC o CE tiene la obligación de generar y entregar en forma segura la clave privada del signatario de un certificado de firma electrónica emitido por él, asegurar la fiabilidad del dispositivo seguro y los mecanismos que el signatario utiliza para firmar.
- Contener la metodología adoptada para manejar los temas de:
  - Análisis de riesgos
  - Plan de recuperación de desastres
  - Plan de seguridad
- Incluir la interacción entre las unidades internas que cumplen la función de AC y AR.
- Incluir la descripción de los mecanismos a través del cual se constatará la solicitud del certificado, su autorización, su completitud y su veracidad.
- Incluir la descripción de los mecanismos a través del cual se validará la identificación de los suscriptores y signatarios, así como sus datos.

5.3.2.3.3 Estándares de Evaluación

- ETSI 102 042
- CA/BR B
- CA/BR G
- RFC 3647

5.3.2.3.4 Documentación Solicitada

Modelo y Manual de Operación de la AR
Manual técnico de los dispositivos seguros de firma electrónica

5.3.2.3.5 Detalles de la Evaluación

Aspectos	Evaluación
Nómina y descripción de cargos	Nómina de los cargos de personal empleado, con la descripción de los procedimientos operacionales y la forma en que los empleados realizan sus funciones.
Proceso de registro	Se verifica el registro del signatario. La autenticación, confirmación de su identidad y forma de política para comprobar el nombre y datos asociados al signatario.
Entrega segura de los datos de creación de firma	El PSC o CE debe tener implementados procedimientos y prácticas que permitan entregar en forma personal y segura los datos de creación de firma al signatario del certificado.
Dispositivo seguro y mecanismos de firma del signatario	El PSC o CE debe tener implementados procedimientos y prácticas que aseguren que una vez entregados los datos de creación de firma sólo el signatario tenga control de ellos. El dispositivo seguro entregado al signatario debe firmar internamente el documento sin ser jamás accesible la clave privada del signatario. El mecanismo de control de acceso a la clave privada sólo debe ser conocido por el signatario al momento de la entrega del dispositivo y en lo posible modificable por el mismo signatario, antes de ser utilizado por primera vez. El dispositivo seguro debe contar con mecanismos que inhabiliten el dispositivo en caso de reiterados intentos fallidos de acceso. El PSC o CE debe entregar al signatario herramientas, aplicaciones e instrucciones para que el signatario pueda firmar en forma segura.
Capacitación y servicio al signatario	El PSC o CE debe implementar procedimientos de capacitación que permitan al signatario manejar en forma segura e informada el dispositivo de firma, y además mantener un servicio de atención para responder y solucionar dudas de los signatarios.
Referencias de los cargos en los planes de continuidad de negocios del PSC o CE	Referencia del personal en los planes de continuidad del negocio y los planes de recuperación de desastres y contingencia.
Planes de contingencia	Descripción de planes de contingencia
Descripción de las operaciones	Descripción detallada de los siguientes eventos: 1. Procedimiento certificados seguro de suspensión y revocación de Medidas de control de acceso 2. Procedimientos de respaldo y recuperación
Interacción entre AR del PSC o CE	El documento cubre los procedimientos que involucren la interacción entre la(s) AC y la(s) AR
Requerimientos ETSI TS 102 042, sección 7.3.1	**Registro del signatario** La AC se asegurará de que se evidencie tanto para el suscriptor como para el signatario su identificación, la precisión de sus nombres y los datos asociados a su identificación, sean debidamente examinados y sean exactos como parte del servicio de registro, y que puedan ser certificados a través de fuentes adecuadas y autorizadas. En particular: Se verificará la existencia legal, física y operacional de los suscriptores y signatarios según sea el caso. a) Antes de entrar en una relación contractual con un suscriptor, el PSC o CE deberá informar al suscriptor respecto a los términos y condiciones relacionadas con el uso del certificado. b) Si el signatario es una persona y no es el mismo que el suscriptor, el signatario será informado de sus obligaciones. c) El PSC o CE comunicará esta información a través de medios de comunicación confiables, íntegros y disponibles, y en un lenguaje fácilmente comprensible. d) El PSC o CE deberá recoger ya sea evidencia directa, o a través de fuentes adecuadas y autorizadas, la identidad (por ejemplo, nombre) y, en su caso, cualesquiera otros atributos específicos del signatario a los que se les emita un certificado. La verificación de la identidad del signatario será al momento de la inscripción por medios adecuados y de acuerdo con la legislación nacional. e) Si el signatario es una persona las evidencias de su identidad (por ejemplo, nombre) deberá se comprobada contra la presencia de la persona física, ya sea directa o indirectamente utilizando medios que proporcione una seguridad equivalente a la presencia física. Las evidencia para la verificación de otro tipo de entidades deberán incluir procedimientos que proporcionan el mismo grado de seguridad. f) Si el signatario es una persona física, las evidencias consistirán en: f.1) nombre completo (incluyendo el apellido y nombre de conformidad con la ley aplicable a nivel nacional en prácticas de identificación); f.2) la fecha y lugar de nacimiento, la referencia a un documento de identidad reconocido a nivel nacional, u otros atributos que puede ser utilizado para, en la medida de lo posible, distinguir la persona de otros con el mismo nombre. g) Si el signatario es una persona física que es identificado en asociación con una persona jurídica, o entidad de organización (por ejemplo, el suscriptor), las evidencias consistirá en: g.1) nombre completo (incluyendo el apellido y nombre, en consonancia con la ley aplicable a nivel nacional en prácticas de identificación) del signatario; g.2) la fecha y lugar de nacimiento, la referencia a un documento de identidad reconocido a nivel nacional, o de otros atributos del suscriptor que puede ser utilizado para, en la medida de lo posible, distinguir la persona de otros con el mismo nombre; g.3) el nombre completo y la situación jurídica de la persona jurídica asociada u otra entidad organizativa (por ejemplo, el suscriptor); g.4) cualquier información relevante de registro existente (por ejemplo, registro de la empresa) de la persona jurídica asociada u otra entidad organizativa; g.5) pruebas de que el signatario se asocia con la persona jurídica u otra entidad organizativa. h) Si el signatario es una organización, se proporcionará la siguiente evidencia: h.1) del nombre completo de la entidad u organización (organización privada, entidad gubernamental o no comercial); h.2) referencia a un registro reconocido a nivel nacional, u otros atributos que pueden utilizarse en la medida de lo posible, distinguir la entidad u organización de los demás con el mismo nombre. h.3) Si el sujeto es un dispositivo o sistema operado por o en nombre de una entidad u organizativa, las evidencias consistirán en: h.3.1) identificador del dispositivo por el cual se puede hacer referencia (por ejemplo, nombre de dominio de Internet); Se verificará exhaustivamente el control y registro exclusivo del dominio. Nombre, cargo del contratante del dominio. Nombre, cargo del solicitante y quien aprobó el certificado electrónico. El contratante del dominio debe estar vinculado en los registros legales del suscriptor o del signatario. Se verificará el cumplimiento de: CA/BR G sección 10.6; h.3.2) el nombre completo de la entidad u organización; Requisitos CA/BR G secciones 10.2 y 10.6 h.3.3) un número de identidad reconocido a nivel nacional, u otros atributos que pueden utilizarse para, en la medida de lo posible, distinguir la entidad u organización de los demás con el mismo nombre. j) El PSC o CE deberá registrar toda la información necesaria para verificar la

identidad del signatario y, en su caso, cualquier atributo específico de la materia, incluyendo cualquier número de referencia en la documentación utilizada para la verificación, y cualquier limitación sobre su validez.

k) Si una entidad que no sea el signatario está suscribiendo los servicios de AC (es decir, el suscriptor y signatarios están en entidades separadas), entonces se debe proporcionar evidencia de que el suscriptor está autorizado para actuar en nombre del signatario (por ejemplo, está autorizado para todos los miembros de la organización identificada).

l) El suscriptor deberá proporcionar una dirección física, u otros atributos, que describan cómo puede ser él contactado.

m) El PSC o CE deberá registrar el acuerdo firmado con el suscriptor, incluyendo:

m.1) la aceptación de las obligaciones del suscriptor

m.2) el acuerdo del suscriptor respecto al uso seguro del dispositivo

m.3) el consentimiento para que el PSC o CE (bien sea suscriptor o signatario):

- Mantenga la información utilizada en el registro
- El derecho de proveer el dispositivo del signatario
- Cualquier revocación posterior
- La identidad y los atributos específicos ubicados en el certificado
- Traspaso de dicha información a terceros en las mismas condiciones, si así lo requieren las políticas, en el caso de terminación de los servicios de la AC;

m.4) bajo que condiciones, el suscriptor requiere que el sujeto consienta la publicación del certificado;

m.5) la confirmación de que la información contenida en el certificado es correcta.

m.6) Los requisitos CA/BR G las secciones 10.8 y 10.9;

m.7) Los Requisitos de la CA/BR B sección 10.3.2

n) Los registros identificados anteriormente se conservarán durante el periodo de tiempo establecido en la LSMDFE (10 años) y según sea necesario, para aportar pruebas de certificación en procedimientos judiciales.

o) El PSC o CE se asegurará de que los requisitos de la legislación nacional de protección de datos se cumplen (incluyendo el uso de seudónimos en su caso) dentro de su proceso de registro.

p) La política de la verificación del PSC o CE sólo exigirá la toma de pruebas de identidad suficiente para satisfacer los requisitos de la utilización prevista para el certificado.

r) Los requisitos CA/BR G sección 10.11.1 y 10.11.2

s) Los requisitos CA/BR G sección 12.1.3.

t) Los requisitos CA/BR G sección 7.2.

u) Los requisitos CA/BR G sección 9.2.

v) Los requisitos CA/BR B secciones 10.1, 10.2, 11.3, 11.4, 11.5 y 11.6

w) Los requisitos CA/BR G 6.2.1 punto 1) y 2)

x) Los requisitos CA/BR B sección 7.1

Requerimientos ETSI TS 102 042, sección 7.2.9

Preparación segura del dispositivo de usuario

El PSC o CE se asegurará de que si se distribuyen dispositivos a usuarios finales el mismo debe ser revisado e inicializado, de forma que se pueda garantizar la seguridad y confianza en su uso

Para el caso de firma de código con Certificados de Validación Extendida se debe seguir las recomendaciones del Apéndice H , de la CA/BR G.

a) la preparación dispositivo del usuario será controlada por el PSC o CE

b) El dispositivo de usuario se debe almacenar y se distribuir de forma segura .

c) La desactivación y reactivación debe ser controlada de forma segura

d) Cuando el aseguramiento del dispositivo está asociado a la activación de la data (por ejemplo de código PIN), los datos de activación deben ser preparados de forma segura y distribuidos de forma separada al módulo de creación de firma.

Requerimientos CA/BR G 13.1.5

Razones para Revocación de un Certificado del Suscriptor

El PSC o CE revocará un certificado dentro de 24 horas si se presenta uno o más de los siguientes supuestos:

1. Solicitudes de revocación por escrito del suscriptor a la AC.

2. El suscriptor notifica a la AC que la solicitud de certificado original no fue autorizada y no puede conceder retroactivamente autorización

3. El PSC o CE obtiene pruebas de que la clave privada del signatario correspondiente a la clave pública en el Certificado sufrió un Compromiso o ya no cumple con la requisitos acordados

4. El PSC o CE obtiene pruebas de que el certificado fue mal utilizado;

5. El PSC o CE descubre que un Suscriptor o Signatario ha violado una o más de sus obligaciones de uso acordadas en las condiciones y términos

6. El PSC o CE tiene conocimiento de circunstancias que indican que el uso de un nombre de dominio completo o la IP dirección en el certificado ya no esta legalmente permitida (por ejemplo, un tribunal o árbitro ha revocado un dominio, o el derecho del Titular de utilizar el nombre de dominio, un acuerdo de licencia o servicios relevantes entre el Nombre de dominio y el Solicitante ha terminado, o el "Domain Name Registrante" ha fallado en renovar el nombre de dominio);

7. El PSC o CE se hace consciente de que un Certificado se ha utilizado para autenticar de forma fraudulenta o engañosa Nombres de Dominio Fully-Qualified

8. El PSC o CE observa un cambio material en la información contenida en el Certificado;

9. El PSC o CE observa que el certificado no fue emitido de acuerdo con los requisitos de la Política de Certificado de la AC o Declaración de Prácticas de Certificación

10. El PSC o CE observa o determina que la información que aparece en el Certificado es inexacta o engañosa;

11. El PSC o CE cesa operaciones por cualquier motivo y no ha hecho arreglos para otro PSC pueda proporcionar apoyo, se revoca el Certificado;

12. El derecho del PSC o CE para emitir certificados bajo los requisitos iniciales expira, se revocan o terminan, a menos que el PSC haya hecho arreglos para continuar manteniendo el Repositorio LCR / OCSP;

13. El PSC o CE observa un posible compromiso de la clave privada de la AC utilizada para la emisión del Certificado;

14. La revocación es requerida por la Política de Certificados de la AC y/o Declaración de Prácticas de Certificación;

15. El contenido técnico o el formato del Certificado presenta un riesgo inaceptable para Software o Aplicación provista por terceras partes (por ejemplo, el CA / Browser Forum podrían determinar que el algoritmo criptográfico o el tamaño de las claves presenta un riesgo inaceptable y que dichos Certificados deben ser revocados y sustituidos por las AC en un plazo de tiempo determinado).

5.3.2.4 Modelo de Confianza

5.3.2.4.1 Objetivo

Verificar que el PSC o CE provea a los signatarios de certificados de firma electrónica emitidos por él, un mecanismo de confianza que le permita comprobar la validez de cualquier certificado que reciba.

5.3.2.4.2 Descripción

El certificado de firma electrónica emitido por un PSC o CE acreditado debe permitir a su receptor verificar, en forma directa o mediante consulta electrónica, todos los certificados que reciba, con la finalidad de comprobar la validez del mismo.

De esta forma es factible asegurar la interoperabilidad en el sistema y la propagación de la confianza depositada por el signatario en su PSC o CE hacia el resto del sistema.

5.3.2.4.3 Estándares de Evaluación

Este apartado no aplica

5.3.2.4.4 Documento Solicitado

Documento en el que se describe el modelo de confianza utilizado por el PSC o CE para lograr el objetivo o alternativamente la DPC y PC si contiene dicho punto.

5.3.2.4.5 Detalles de la Evaluación

Aspectos	Evaluación
Modelo de confianza	El modelo de confianza es el esquema por el cual un signatario de un certificado de firma electrónica emitido por un PSC o CE acreditado puede confiar en dicho certificado. El esquema definido en la LSMDFE y su reglamento parcial, deja en manos del PSC implementar el mecanismo por el cual un signatario que confíe en él, pueda confiar en cualquier otro PSC o CE acreditado. El mecanismo propuesto consiste en que cada PSC o CE mantenga en su repositorio de acceso público los certificados de todos los Proveedores acreditados, de tal manera que los signatarios que confíen en él puedan instalar en sus aplicaciones estos certificados. El método debe incluir mecanismos de seguridad para evitar que se puedan reemplazar los certificados en el repositorio o durante su transmisión, sin que ello no pueda ser detectado por el signatario. Este modelo tiene la finalidad de mostrar a los signatarios la cadena de confianza que brinda la Infraestructura Nacional de Certificación Electrónica de Venezuela, es decir, este modelo debe mostrar al signatario toda la estructura de Certificación Electrónica de nuestro país que respalda y le da el valor jurídico a los certificados emitidos pro el PSC o CE acreditado.
Efectividad	Se verifica el mecanismo utilizado para implementar el modelo de Confianza en forma práctica en la Infraestructura Nacional de Certificación Electrónica.
Requerimientos ETSI TS 102 042, sección 7.2.3	**Distribución de claves públicas** Generación y distribución de los certificados La AC se asegurará la verificación de la integridad y la autenticidad de la clave publica, la AC la firma asegurando de esta forma lo anterior, así como cualquier parámetro asociado que se mantenga durante su distribución a las partes que confían . En particular: a) La AC verifica y firma las claves públicas poniéndola de esta forma a disposición de las partes que confían. De esta manera se asegura la integridad de las mismas y se autentica su origen a los efectos de garantizar su distribución confiable.

5.3.3 Administración, Operación y Seguridad de la Infraestructura de Clave Pública

El PSC o CE debe asegurarse que los procesos operaciones y administrativos tengan una adecuada correspondencia con el cumplimiento de estándares.

Los procesos operativos y de control deben ser documentados, implementados y mantenidos.

El SGSI del PSC o CE no puede ser tercerizado, reside bajo su responsabilidad la Seguridad de sus operaciones.

La información manejada por el PSC o CE debe estar clasificada, y de esta forma asegurarse que reciba el adecuado nivel de protección.

5.3.3.1 Revisión de la Evaluación de Riesgos y Amenazas

5.3.3.1.1 Objetivo

Determinar la consistencia del análisis de riesgos y amenazas de la Infraestructura Técnica y Operativa del PSC o CE

5.3.3.1.2 Descripción

Dado que el producto principal de un PSC o CE es la "confianza", el requerimiento fundamental para un PSC o CE es demostrar una clara comprensión de las amenazas de seguridad enfrentadas por el negocio y poder mostrar planes efectivos para reducir el riesgo a un nivel aceptable.

La Evaluación de Riesgos es parte de un proceso más amplio denominado Administración del Riesgo. El objetivo principal de un proceso de administración del riesgo en una organización debe ser proteger la organización y su capacidad de cumplir con su misión, y no sólo sus activos IT.

La Administración del Riesgo incluye tres procesos:

1. **Valoración de los riesgos,** incluye la identificación y evaluación de los riesgos e impactos de los riesgos, y medidas recomendadas para reducirlos.
2. **Tratamiento de los riesgos,** se refiere a la priorización, implementación y mantenimiento de las medidas de reducción de riesgo apropiadas recomendadas por el proceso de valoración de riesgos. Este proceso conduce a la definición de un Plan de Seguridad.
3. **Mantenimiento,** corresponde al proceso de evaluación continua para adecuar la valoración de riesgos a condiciones cambiantes del entorno o del negocio.

El resultado debe ser un compromiso razonable entre los costos económicos y operacionales de las medidas de protección, y obtener mejoras en la capacidad de lograr la misión de la organización.

Se debe seguir un proceso similar al descrito en los documentos indicados en las referencias, para realizar el proceso de evaluación de riesgos.

Los esfuerzos de seguridad deberían abordar los riesgos de una manera eficaz y oportuna, donde y cuando sean necesarios. La gestión del riesgo en la seguridad de la información debería ser una parte integral de todas las actividades de gestión de seguridad de la información y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

La gestión del riesgo en la seguridad de la información debería ser un proceso continuo.

El reporte de la valoración de los riesgos debe tener lineamientos dados en la siguiente estructura, un ejemplo se muestra en el Anexo No 2.

5.3.3.1.3 Estándares de Evaluación

Puede considerarse como referencia normativa la ISO 27005, el Magerit u otro estándar ampliamente conocido.

5.3.3.1.4 Documentación Solicitada

Copia del documento correspondiente a la Evaluación de Riesgos o documento equivalente.

5.3.6.5 Detalles de la Evaluación

Aspectos	Evaluación
Reporte de la valoración de riesgos [2]	• Verificar la adecuada identificación de los riesgos; • Verificar que los riesgos considerados sean reales. • Validar que riesgos relevantes no hayan sido omitidos. • Verificar la valoración adecuada de los riesgos. • Constatar si hay un plan de mantenimiento de la valoración . • Verificar que la evaluación de los riesgos esté en términos y en consecuencia con el negocio del PSC o CE • Verificar la adecuada estimación de la probabilidad de su ocurrencia • Verificar el establecimiento de un orden de prioridad para el tratamiento de los riesgos; • Verificar que se haya priorizado las acciones para reducir la ocurrencia de los riesgos; • Verificar que se haya considerado la participación de los interesados cuando se toman las decisiones sobre gestión del riesgo • Verificar la eficacia del monitoreo del tratamiento del riesgo • Verificar el monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos
Estructura del proceso de valoración de riesgos	Verificar si el proceso de valoración ha sido realizado o auditado por un ente externo, independiente y calificado. Verificar que el proceso de valoración de riesgo haya sido revisado y reevaluado al menos una (1) vez al año.

5.3.3.2 Política de Seguridad de la Información (Documentación y mantenimiento)

5.3.3.2.1 Objetivo

Comprobar a través de este documento que la organización tiene claros los objetivos de seguridad relevantes para el negocio y que las instancias de gestión del PSC o CE apoyan formalmente esta política.

5.3.3.2.2 Descripción

La política de seguridad es una declaración de objetivos de seguridad. Solo contiene objetivos de seguridad que son factibles de lograr a través de acciones, procedimientos y mecanismos implementados por el PSC o CE. Si el PSC o CE tiene en otra organización algún aspecto de seguridad o confianza, entonces debe indicarse claramente.

La política de seguridad debe cumplir al menos con los siguientes requerimientos:

1. Los objetivos de seguridad deben ser consecuencia de la Evaluación de Riesgos y Amenazas, de forma tal que los objetivos de la política de seguridad y sus defensas asociadas correspondan al nivel de riesgo requerido para que un PSC o CE sea un ente de confianza.
2. Debe estar basada en las recomendaciones del estándar ISO 27002:2013 control 5, los cuales se transcriben en el Anexo No 3 de este documento de evaluación.
3. Los objetivos de la política son de alto nivel y no técnicos, por tanto debe ser lo suficientemente general para permitir alternativas de implementación tecnológica.
4. Si la complejidad de los objetivos así lo requieren, la política puede estar conformada por más de un documento; esto es, puede haber una política general soportada por políticas específicas.
5. En esta política de seguridad deben estar incluidos los elementos contenidos en la DPC y PC
6. Este documento debe identificar los objetivos de seguridad relevantes y las amenazas potenciales relacionadas a los servicios suministrados, así como las medidas tomadas para evitar o limitar los efectos de estas amenazas.
7. Adicionalmente, la documentación debe describir las reglas, directivas y procedimientos que indican como son provistos los servicios específicos y las medidas de seguridad asociadas.

En el Anexo No 4 de este documento se describen los principales aspectos que una política de seguridad debe considerar.

Para los propósitos de la acreditación o renovación de un PSC o CE, algunos de los aspectos más relevantes han sido incorporados en criterios separados para así facilitar el proceso de evaluación y donde estos se detallan completamente. Por ello, este documento puede expresar en forma general aquellos aspectos de la seguridad organizacional que se tratan en documentos específicos.

5.3.3.2.3 Estándares de Evaluación

- ISO/IEC 27002:2013

5.3.3.2.4 Documentación Solicitada

Copia del documento correspondiente a la política de seguridad de la organización.

Documento en el cual se describa formalmente la estructura organizativa del PSC o CE, aprobada por las autoridades de la Institución.

2 * Risk Management Guide for Information Technology Systems, Special Publication 800-30, Recommendations of the National Institute of Standards and Technology, October 2001
* Handbook 3, Risk Management, Version 1.0, Australian Communications Electronic Security Instruction 33 (ACSI 33)

5.3.3.2.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ISO 27002:2013 control 5.1.1	Verificar que los requerimientos de la control 5.1.1 descritos en el Anexo No 3, están incorporados.
Conformidad con el estándar ISO 27002:2013 control 5.1.2	Verificar que se ha incluido un procedimiento de revisión y evaluación periódico de la política de seguridad.
Consistencia entre la política de seguridad y la DPC y PC	Constatar la consistencia de la política de seguridad con la DPC y PC .
Relación entre la Evaluación de Riesgos y la política de seguridad	Verificar que los principales aspectos de la política de segundad son coherentes con los niveles de riesgo determinados en la evaluación formal de riesgos.
Inclusión de lo indicado en el Anexo 4	Chequear que los elementos fundamentales de una política de seguridad (que apliquen al PSC o CE) están incluidos en el documento.
Claridad de los objetivos de seguridad	Verificar que se establecen objetivos de seguridad claros relacionados con la protección de los procesos de negocios, activos y servicios del PSC o CE.

5.3.3.3 Plan de Continuidad del Negocio y Recuperación ante Desastres

5.3.8.1 Objetivo

Comprobar a través de este documento que la organización tiene planes establecidos para disminuir a un nivel aceptable el efecto de interrupciones del servicio del PSC o CE, mediante una combinación de controles preventivos y planes de contingencia.

5.3.8.2 Descripción

El Plan de Continuidad del Negocio y de Recuperación de Desastres, debe describir cómo los servicios serán restaurados en el evento de desastre, una caída de los sistemas o fallas de seguridad.

Dicho plan debe ser mantenido y probado periódicamente y debiera ser parte integral de los procesos de la organización.

En particular, el documento describe la prioridad de restauración para asegurar la continuidad de los negocios de terceros que sean dependientes de la operación del PSC o CE.

Este documento debe seguir los lineamientos brindados por:

- Estándar ISO 27002:2013 en su control 17 y
- Estándar ETSI TS 102 042 V2.4.1 en su sección 7.4.8

Este documento también debe describir los procedimientos de contingencia a ser seguidos en al menos los siguientes eventos:

- Desastre que afecte el funcionamiento de los productos de software en el cual el PSC o CE basa sus servicios.
- Incidente o posible incidente de seguridad que afecte la operación del sistema en el cual el PSC o CE basa sus servicios.
- Compromiso de la clave privada de firma del PSC o CE.
- Falla de los mecanismos de Auditoría.
- Falla en el hardware donde se ejecuta el producto en el cual el PSC o CE basa sus servicios, este debe incluir los servidores, dispositivos criptográficos, dispositivos de seguridad y dispositivos de comunicaciones.

Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales y operacionales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información, esto según la ISO 27002:2013.

El plan debe además incluir mecanismos para la preservación de evidencia de mal uso de los sistemas, cuyo propósito es proporcionar evidencia admisible en una corte judicial en alguna fecha posterior.

5.3.8.3 Estándares de Evaluación

- ISO 27002:2013
- ETSI TS 102 042

5.3.8.4 Documentación Solicitada

- Documento de Planes de Continuidad del Negocio y Recuperación de Desastres.
- Documento de Evaluación de Riesgo.

5.3.8.5 Detalles de la Evaluación

Aspectos	Evaluación
Conformidad con el estándar ISO 27002:2013 controles 17.1.1 y 17.1.2	Verificar que los requerimientos del control 17 indicados en el Anexo No 3, están incorporados.
Conformidad con el estándar ISO 27002:2013 controles 17.1.3	Verificar que los requerimientos del control 17 indicados en el Anexo No 3, están incorporados.
Conformidad con el estándar ETSI TI 102 042 sección 7.4.8	El PSC o CE debe asegurar que las operaciones deben restaurarse tan pronto como sea posible ante la ocurrencia de un desastre, incluyendo el caso del compromiso de la clave privada utilizada para la firma de certificados. Otras situaciones de desastre incluyen la falla de componentes críticos de los sistemas del PSC o CE, incluyendo hardware y software. En particular: a) El PSC O CE debe definir y mantener un plan de continuidad del negocio en caso de un desastre b) El plan de continuidad de negocios del PSC o CE deberá considerar como un desastre el compromiso o sospecha de compromiso de la clave privada de firma del PSC o CE y los procesos de recuperación deben estar disponibles y probados. c) A continuación de un desastre el PSC o CE deberá. en la medida que sea posible, tomar las medidas que eviten su repetición. d) En el caso de compromiso de su clave privada, el PSC o CE deber como mínimo tomar las siguientes medidas: 1. Informar del compromiso a todos los suscriptores y sus contrapartes así como a los otros PSC o CE con quienes tiene acuerdos de interoperabilidad, certificación cruzada u otras formas de colaboración. 2. Indicar que los certificados e información del estado de revocación emitidos usando la clave del PSC o CE puede no ser válida, porque ha sido comprometida. Se e recomienda a los terceros que confían, con la cual se tiene un acuerdo de colaboración, sean informados del compromiso de la clave privada. El PSC o CE debiera revocar cualquier certificado de la AC que haya sido emitido.
Evaluación del riesgo	Esta evaluación debiera considerar los procedimientos comerciales y operacionales y no se debieran limitar a los medios de procesamiento de la

	información. También se debe verificar que la evaluación del riesgo identifique, cuantifique y establezca prioridad de los riesgos en comparación con los criterios y objetivos relevantes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, tiempos de desabastecimiento permitidos y prioridades de recuperación.
Viabilidad de las facilidades computacionales alternativas	Chequear que las facilidades computacionales alternativas consideradas en el plan, cumplen con los requerimientos mínimos para la operación del PSC o CE.
Elementos de Auditoría	Verificar que el sistema en el cual el PSC o CE basa sus servicios provee mecanismos de preservación de los elementos de Auditoría.

5.3.3.4 Plan de Seguridad de la Información

5.3.3.4.1 Objetivo

Comprobar a través de este documento que la organización tiene un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.3.4.2 Descripción

El Plan de Seguridad de la información tiene como propósito describir los requerimientos de seguridad de la información y los controles desplegados o planificados para satisfacer dichos requerimientos. Adicionalmente, debe delinear las responsabilidades y conductas esperadas de los individuos que acceden a los sistemas.

Por lo tanto, el Plan de Seguridad de la información debe describir las acciones operacionales, procedimientos y mecanismos que permitan lograr los objetivos indicados en la Política de Seguridad del PSC o CE.

El plan de seguridad debe considerar al menos los controles 6 a la 14, 16, 17 y 18 del estándar ISO 27002:2013. Sin embargo, en este requisito se evalúan en particular los siguientes aspectos:

- Organización de la Seguridad de la Información (control 6)
- Seguridad Ligada a los Recursos Humanos (control 7)
- Gestión de activos (control 8)
- Control del acceso (control 9)
- Criptografía (control 10)
- Seguridad Física y del Ambiente (control 11)
- Seguridad de las Operaciones (control 12)
- Gestión de las comunicaciones (control 13)
- Adquisición, desarrollo y mantenimiento de los sistemas de información (control 14)
- Gestión de incidentes de seguridad de la información (control 16)
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio (control 17)
- Cumplimiento (control 18)

En el anexo No. 5 se mencionan otros elementos a considerar para la evaluación del plan de seguridad de la información. Se considera que este Plan es una declaración de intenciones del PSC o CE, por lo que la evaluación bajo este requisito no es una certificación de su nivel de seguridad. El proceso de evaluación bajo este requisito indica el nivel de confiabilidad del PSC o CE si este cumple con el plan de seguridad de la información.

El PSC o CE debe asegurar que el acceso físico y lógico a los servicios que manejan información sensible esté controlado y los riesgos físicos para los activos estén reducidos a su valor residual. Esto debe estar basado en el estándar ETSI 102 042 secciones 7.4.4 y 7.4.6.

ACCESO FISICO

Ubicación de las instalaciones

La ubicación de los sistemas de certificación no debe estar públicamente identificada. No debe haber ambientes compartidos que permitan la visibilidad de las operaciones críticas de emisión o revocación de certificados. Esas operaciones deberán ser realizadas en espacios cerrados, que no permitan visibilidad desde el exterior y estar físicamente protegidos.

El PSC o CE se asegurará de que el acceso físico a los servicios críticos deben estar controlados y debe reducir al mínimo el riesgo de sus activos.

Acceso físico a las instalaciones

a) El acceso físico a las instalaciones que están relacionadas el ciclo de vida del certificado, deberán limitarse a personas debidamente autorizadas.

b) Se debe aplicar controles para evitar la pérdida, el daño o el compromiso de los activos o la interrupción de las actividades del negocio; y

c) Se debe aplicar controles para evitar el compromiso o el robo de información.

En base a lo dicho anteriormente se recomienda:

Zonas de acceso físico:

Zona 1: Las instalaciones destinadas a la gestión del ciclo de vida de los certificados deberán encontrarse en un ambiente protegido físicamente con la finalidad de evitar el compromiso de los servicios a través del acceso no autorizado a los sistemas o datos. En esta zona todas las personas ajenas a las operaciones deberán ingresar acompañadas de personal autorizado, así como el personal autorizado debe ser identificado.

Zona 2: La protección física de esta zona se logra a través de la creación de perímetros de seguridad claramente definidos (es decir, barreras físicas). No se permite compartir con otras organizaciones esta zona por lo que deberán estar fuera de este perímetro cualquier otra actividad no relacionada con la AC. Al acceso del personal autorizado debe quedar registrado y debe contar con al menos un (1) factor de seguridad (tarjeta electrónica, biometría y/o clave)

Zona 3: Los controles de seguridad física y ambiental se aplicarán para proteger los sistemas y las instalaciones, por lo que se deberán tener controles de protección contra desastres naturales, controles de seguridad contra incendios, controles ante fallas de servicios públicos (por ejemplo, energía, telecomunicaciones), colapso de la estructura, fugas en las tuberías, protección contra el robo, allanamiento de las instalaciones, etc. El acceso del personal autorizado y las actividades que en la misma se desarrollen debe estar registradas con un sistema de circuito cerrado de TV. Así mismo el acceso debe quedar registrado y debe contar con al menos un (1) factor de seguridad (tarjeta electrónica, biometría y/o clave)

Zona 4: En esta zona se llevan a cabo las actividades críticas del PSC o CE, las funciones de la AC(s) y AR(s), la instalación física de la infraestructura de clave pública y equipos de comunicación, hardware criptográfico de la AC(s), hardware criptográfico de los signatarios. El acceso del personal autorizado a esta zona debe quedar registrado y debe ser dual, al menos contar con dos (2) factores de autenticación simultáneos (tarjeta electrónica, biometría y clave). Debe quedar registrada la actividad a través de circuito cerrado de TV.

Para entrar a la Zona 1, todo individuo deberá ser identificado y su ingreso registrado por personal autorizado.

Acceso Lógico a los sistemas

Los controles se llevarán a cabo para proteger los equipos, información, medios de comunicación y el software relacionado con la Servicios de la AC. El PSC o CE se asegurará de que el acceso al sistema se limita a las personas debidamente autorizadas. Debe quedar registrados los acceso y actividades en los sistemas, deben habilitarse los logs de auditorías en base de datos y servicios relacionados a la ICP. Los mismos deben resguardarse como parte de la política de respaldo.

Los controles (por ejemplo, servidores de seguridad) se aplicarán para proteger a los dominios de la red interna de la ICP de accesos no autorizados por terceros en la red.

Se recomienda configurar los cortafuegos para evitar accesos no autorizados dentro de las operaciones de la AC

a) Los datos sensibles deberán estar protegidos contra el acceso o modificación no autorizada. Los datos sensibles serán protegidos (Por ejemplo, mediante el cifrado y un mecanismo de integridad) cuando se intercambian a través de redes que no son seguras. Los datos sensibles incluye información de registro.

b) La AC deberá asegurar una gestión eficaz del usuario (esto incluye a los operadores, administradores y cualquier usuario que tiene acceso directo a los sistema) para mantener la seguridad del sistema, se recomienda incluir la gestión de cuentas de usuario, auditoría y la modificación puntual o eliminación del acceso en caso de ser necesario.

c) La AC deberá garantizar que el acceso a la información, sistemas o aplicaciones están restringidas de acuerdo con la política de control de acceso y controles de seguridad informática suficientes para la separación de funciones según los roles identificados en las prácticas de AC, incluyendo le administrador de seguridad y operación. En particular, el uso de programas o aplicaciones estará restringido y estrechamente controlado. Se limitará sólo a permitir el acceso a los recursos necesarios para llevar a cabo las funciones asignadas a ese usuario.

d) El personal de la AC deberán estar identificado y autenticado antes de utilizar aplicaciones críticas relacionadas con la gestión de certificados.

e) El personal de la AC deberán rendir cuentas de sus actividades, por ejemplo mediante el registros de eventos.

f) Los datos sensibles deberán estar protegidos de usuarios no autorizados, en caso de ser revelados a través de objetos de almacenamiento reutilizados (por ejemplo archivos borrados).

Implementación del Sistema de Confianza y Mantenimiento

El sistema de la AC debe asegurarse de usar sistemas y productos que aseguren la protección a alteraciones.

a) Un análisis de los requisitos de seguridad se llevará a cabo en la etapa de diseño y la especificación de los requisitos de cualquier proyecto de desarrollo de sistemas realizado para la AC o en nombre de la AC para garantizar que la seguridad

b) Deben existir procedimientos de control de cambios para nuevas versiones, modificaciones y correcciones de software de operacional

Cumplimiento de normas legales

El PSC o CE deberá garantizar que se cumplen todos los requisitos legales aplicables de acuerdo al marco normativo nacional establecido (LSMDFE y su Reglamento, así como las normas SUSCERTE de carácter sub legal y cualquier otro marco regulatorio relacionado, para la protección de pérdida, destrucción y/o falsificación de los registros. Algunos registros pueden necesitar ser retenidos de manera segura para cumplir con los requisitos legales.

Resguardo de la información relacionada con el PSC o CE

El PSC o CE se asegurará de que toda la información relevante al ciclo de vida de los certificados electrónicos sea resguardada por al menos diez (10) años, de acuerdo a lo establecido en el marco legal vigente (LSMDFE y su Reglamento), así como aquella que pueda servir como evidencia y/o prueba para propósitos legales.

5.3.3.4.3 Estándares de Evaluación

ISO/IEC 27002:2013

ETSI 102 042 V 2.4.1

5.3.3.4.4 Documentación Solicitada

Copia del documento correspondiente al Plan de Seguridad de Información.

5.3.3.4.5 Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados	Verificar que el PSC o CE pueda justificar la disponibilidad de los recursos y capacidades para implementar los mecanismos y los recursos asignados por el procedimiento de seguridad (según el NIST SP800-18 y el NIST SP800-53A)
Relación entre el Plan de Seguridad y Evaluación de Riesgos	Comprobar que los procedimientos y mecanismos de seguridad permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Relación entre Plan de Seguridad y Política de Seguridad	Confirmar que los procedimientos y mecanismos de seguridad permiten lograr los objetivos de la Política de Seguridad.
Mantenimiento del Plan de seguridad	Verificar que el Plan de Seguridad incluya los procedimientos que garanticen que la segundad del PSC o CE se mantiene en el tiempo ante cambios en:
	amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con las prácticas y política de certificación	Verificar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través del Plan de Seguridad.
Requerimientos ISO 27002:2013, Control 6	Confirmar que los controles de Organización de la Seguridad de la información del estándar ISO 27002:2013 están considerados (indicados en el Anexo No 3 de este documento).
Requerimientos ISO 27002:2007, Control 7	Verificar que se han tomado en cuenta los controles de Gestión de Activos del estándar ISO 27002:2013 (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 8	Verificar que se han tomado en cuenta los controles de Gestión de Activos del estándar ISO 27002:2013 (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 9	Verificar la inclusión de los controles de la cláusula de Control de Acceso del estándar ISO 27002:2013 (indicados en el Anexo No 3 de este documento)
Requerimientos ISO 27002:2013, Control 10	Verificar la inclusión de los controles de la cláusula de Criptografía del estándar ISO 27002:2013 (indicados en el Anexo No 3 de este documento)
Requerimientos ISO 27002:2007, Control 11	Verificar que los controles de Seguridad Física y de Ambiente del estándar ISO 27002:2013 están presentes (ver Anexo No 3)
Requerimientos ISO 27002:2007, Control 12	Rectificar que los controles de Seguridad de las Operaciones del estándar ISO 27002:2013 están considerados (ver Anexo No 3)
Requerimientos ISO 27002:2007, Control 13	Rectificar que los controles de Seguridad de las Comunicaciones del estándar ISO 27002:2013 están considerados (ver Anexo No 3)
Requerimientos ISO 27002:2007, Control 14	Comprobar que se han tomado en cuenta los controles de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información del estándar ISO 27002:2013 (ver Anexo No 3)

Requerimientos ISO 27002:2013, Control 16	Verificar que los controles de Gestión de incidentes de seguridad de la información estén considerados (ver Anexo No 3)
Administración de claves Criptográficas	Verificar que el Plan de Seguridad contiene un Plan de Administración de Claves Criptográficas para todo el ciclo de vida de estas claves.
Protección del repositorio de acceso público	Verificar que el Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Asegurarse de que el plan incluye medidas de protección de información privada recaudada durante el proceso de registro.
Acceso a la información	Cumplimiento de los lineamientos sobre acceso físico y lógico

5.3.3.5 Implementación del Plan de Seguridad de la Información

5.3.10.1 Objetivo

Comprobar que la organización tiene implementado un plan de seguridad coherente con su Política de Seguridad, que permita mostrar un nivel de confianza consistente con los objetivos del negocio.

5.3.10.2 Descripción

El PSC o CE debe mostrar que sus procedimientos de administración de la seguridad y la capacidad de disponer de las instalaciones, están de acuerdo con el Plan de Seguridad.

Se evalúan:

- Acciones operacionales, procedimientos y mecanismos que permiten lograr los objetivos indicados en el Plan de Seguridad del PSC o CE.
- Controles desplegados o planificados para satisfacer dichos requerimientos.
- Que estos controles sean coherentes con los requerimientos del estándar ISO 27002:2013 En particular los planes correspondientes a los siguientes aspectos:
  1. Organización de la seguridad de la información
  2. Gestión de activos
  3. Seguridad de las comunicaciones
  4. Seguridad de las operaciones
  5. Control del acceso
  6. Adquisición, desarrollo y mantenimiento de los sistemas de información

La evaluación combinará entrevistas con el personal del PSC o CE y Auditorías que incluirán visitas a las instalaciones del PSC o CE para verificar la implementación práctica del plan.

5.3.10.3 Estándares de Evaluación

- ISO 27002:2013

5.3.10.4 Documentación Solicitada

Documento descriptivo de la implementación del Plan de Seguridad de la Información del solicitante a PSC o CE, el cual será validado al momento de la auditoría.

5.3.10.5 Detalles de la Evaluación

Aspectos	Evaluación
Relación entre el Plan de Seguridad y los recursos asignados	Verificar que el PSC o CE dispone de los recursos y capacidades para implementar los mecanismos y procedimientos de seguridad (según el NIST SP800-18 y el NIST SP800-53A)
Relación entre el plan de seguridad y política de seguridad	Comprobar que los procedimientos y mecanismos de seguridad implementados permiten lograr los objetivos de la política de seguridad.
Relación entre Plan de Seguridad y Evaluación de Riesgos	Verificar que los procedimientos y mecanismos de seguridad implementados permiten lograr el riesgo residual determinado en la Evaluación de Riesgos.
Mantenimiento del Plan de Seguridad	Confirmar que la implementación del Plan de Seguridad incluye los procedimientos que garanticen que la seguridad del PSC o CE se mantiene en el tiempo ante cambios en: amenazas, personal, servicios, componentes tecnológicos, etc.
Relación del Plan de Seguridad con prácticas y la Política de Certificados	Verificar que los objetivos de seguridad enunciados en la DPC y PC del PSC o CE se logran a través del Plan de Seguridad.
Requerimientos ISO 27002:2013, Control 6	Verificar que los controles de Organización de la Seguridad de la Información recomendados por el estándar ISO 27002:2013 están implementados (indicados en el Anexo No 3)
Requerimientos ISO 27002:2013, Control 7	Verificar que los controles de Seguridad Ligada a los Recursos Humanos recomendados por el estándar ISO 27002:2013 están implementados (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 8	Comprobar que los controles de Gestión de Activos recomendados por el estándar ISO 27002:2013 están implementados (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 9	Verificar la implantación de los controles de la cláusula de Control del Acceso recomendados por el estándar ISO 27002:2013 (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 10	Confirmar la inclusión de los controles de la cláusula de Criptografía del estándar ISO 27002:2013 (indicados en el Anexo No 3 de este documento)
Requerimientos ISO 27002:2013, Control 11	Confirmar la implementación de los controles de Seguridad y Física y de Ambiente recomendados por el estándar ISO 27002:2013 (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 12	Validar que los controles de Seguridad de las Operaciones recomendados por el estándar ISO 27002:2013 están implementados (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 13	Validar que los controles de Seguridad de las Comunicaciones recomendados por el estándar ISO 27002:2013 están implementados (ver Anexo No 3)
Requerimientos ISO 27002:2013, Control 14	Confirmar que los controles de adquisición, desarrollo y mantenimiento de los sistemas de información recomendados por el estándar ISO 27002:2013 están implementados (ver Anexo No 3)
Protección del repositorio de acceso público	Verificar que la implementación del Plan de Seguridad contiene medidas especiales de protección del repositorio público de certificados.
Protección de información privada	Comprobar que la implementación del plan incluye medidas de protección de información privada recolectada durante el proceso de registro.

5.3.3.6 Evaluación de la Plataforma Tecnológica

5.3.3.6.1 Objetivo

Evaluar los elementos de seguridad de la plataforma tecnológica utilizada para la generación, publicación y administración de certificados de firma electrónica y LCR.

5.3.3.6.2 Descripción

Evaluar la seguridad de los elementos que constituyen la plataforma tecnológica del PSC o CE. Se debe considerar componentes hardware y software que conforman la infraestructura PKI del PSC o CE, así como, todos los elementos de apoyo a su operación e interrelación, como protocolos y servicios.

Los elementos a considerar son:

- Módulo criptográfico.
- Módulo de Operación AC (Autoridad de Certificación)
- Módulo de Operación AR (Autoridad de Registro)
- Módulo de Almacenamiento y Publicación de Certificados.
- Protocolos de comunicación entre AC y AR.
- Elementos de administración de logs y Auditoría.

5.3.3.6.3 Estándares de Evaluación

- FIPS 140-2
- ISO/IEC 15408 o equivalente.

5.3.3.6.4 Documentación Solicitada

Documento descriptivo de la implementación de la infraestructura tecnológica.

Este documento debe incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica.

Manuales del fabricante de los productos hardware y software relevantes.

Documentación del fabricante que acredite el correspondiente nivel de seguridad.

5.3.3.6.5 Detalles de la Evaluación

Aspectos	Evaluación
Módulo criptográfico	1. Funcionalidad y operación: • Generar pares de clave privada y pública con claves de al menos 4096 bits • Capacidad de FIPS 140-2 Nivel 3 • Capacidad de firma y cifrado 2. Seguridad
	• Existencia de sistema de control de acceso para acceder a la clave privada • Existencia de controles de acceso para acceder a funcionalidades de firma y cifrado 3. Ciclo de vida • Capacidad de respaldar la clave privada, en forma segura • Capacidad de recuperar la clave privada de respaldo (back-up) 4. Auditoría • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos 5. Documentación • Manuales de operación, configuración y puesta en marcha • Procedimiento de recuperación ante contingencia
Módulo de Operación AC (Autoridad de Certificación)	1. Funcionalidad y operación: • Servicios que presta la AC • Interrelación de los servicios • Capacidad para generar certificados con claves de al menos 2048 / 4096 bits, según corresponda al tipo de certificado emitido. • Capacidad de suspensión y revocación de certificados • Capacidad para generar LCRs • Indicar fecha de publicación y de nueva renovación de la LCR. • Capacidad para generar certificados de firma electrónica • Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura (Specifies The Functions Needing A Trusted Channel CC P2 FTP_ITC.1). • Capacidad de entregar certificados y LCR a directorios públicos X500. 2. Seguridad. • Existencia de sistema control de acceso para acceder a la generación de certificados (Generation of Secrets CC P2 FIA_SOS.2) • Existencia de sistema de control de acceso para acceder a los sistemas de administración y Auditoría (User authentication before any action CC P2 FIA_UAU.2) 3. Ciclo de vida. • Capacidad de emitir, suspender y revocar certificados • Capacidad de revocar certificado raíz y generar uno nuevo 4. Auditoría. Capacidad de generar log auditable para administración de contingencia. Actividades del personal autorizado y accesos maliciosos. 5. Documentación. • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de Operación AR (Autoridad de Registro)	1. Funcionalidad y operación: • Servicios que presta la AC • Interrelación de los servicios • Capacidad de recibir requerimientos de certificados (Cryptographic key distribution CC P2 FCS_CKM.2).
	• Solicitar certificado a la AC. 2. Seguridad: • Existencia de sistema control de acceso para acceder a la generación de certificados. • Existencia de sistema de control de acceso para acceder a los sistemas de administración y Auditoría. 3. Ciclo de vida: • Capacidad de validación de datos de los certificados y solicitud de certificados a la AC. 4. Auditoría: • Capacidad de generar log auditable para administración de contingencia y accesos maliciosos. 5. Documentación: • Manuales de operación, configuración y puesta en marcha. • Procedimiento de Recuperación ante contingencia.
Módulo de Almacenamiento y Publicación de Certificados	Almacenamiento de certificados en base de datos X500, y publicación a través de protocolos LDAP v2.0 y/o OCSP V1,0.
Protocolos de comunicación entre AR y AC	Capacidad de generar certificados de comunicación segura, entre AC y AR, si corresponde a la arquitectura, utilizando un protocolo estándar de la industria (Inter-TSF trusted channel CC P2 FTP_ITC.1)
Elementos de administración de log y Auditoría	Deben existir módulos de log y de Auditoría, que permitan verificar los intentos de acceso, los accesos y las operaciones dañinas, sean estas intencionadas o no.

5.3.4.- Declaración de Prácticas de Certificación y Políticas de Certificado

5.3.4.1 Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC)

5.3.4.1.1 Objetivo

Verificar que el PSC o CE disponga de un documento, que señale los procedimientos de gestión de certificados y los diferentes tipos de certificados a otorgar, según se establece en la LSMDFE, su Reglamento Parcial, y los estándares internacionales ETSI 102 042, Webtrust for CA y EV. El enfoque de una Política de Certificado es significativamente diferente al de una Declaración de Prácticas de Certificación. Una Política de Certificados se define independientemente de los detalles específicos del entorno operativo específico de una entidad de certificación, mientras que una Declaración de Prácticas de Certificación se adapta a la estructura organizativa, los procedimientos de operación, instalaciones y el entorno computacional de una entidad de certificación.

5.3.4.1.2 Descripción

Los elementos principales que debe contener la DPC, son las delimitaciones de responsabilidad y las obligaciones tanto del PSC o CE, como del signatario.

Además debe quedar explícito, tanto el ciclo de vida de los certificados, desde su solicitud hasta el término de su vida útil, como el ciclo de vida del PSC o CE, desde el inicio hasta el fin del mismo.

Este requisito es relevante no sólo para el signatario del certificado sino para todas las entidades involucradas, incluyendo quienes reciben un documento firmado electrónicamente.

La DPC y PC deben ser revisadas y actualizadas anualmente, y aprobadas por las autoridades del PSC.

5.3.4.1.3 Estándares de Evaluación

- RFC 3647
- ETSI TS 102 042
- CA/BR B
- CA/BR G

5.3.4.1.4 Documentación Solicitada

Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) con los diferentes tipos de estructura de campos de certificados. (Norma 022 de SUSCERTE).

5.3.4.1.5 Detalles de la Evaluación

Aspectos	Evaluación
Verificar estructura	Verificar que la DPC contiene al menos los tópicos indicados en la Norma 022 de SUSCERTE apartado 5.5
Signatarios	Se debe indicar a quien se le puede otorgar un certificado de firma electrónica.
Usos del certificado	Se debe indicar los propósitos para el cual fue emitido el certificado y sus limitaciones, indicando cuales usos son permitidos y cuales no.
Publicación de información de la AC y Repositorios de los Certificados	Se debe verificar la publicación de los certificados, LCR, y DPC, su frecuencia de publicación, así como la disponibilidad de los repositorios y sus controles de acceso.
Identificación y Autenticación	Se debe comprobar el registro del nombre del signatario, la validación inicial de su identidad, así como la identificación y autenticación de las solicitudes de renovación y revocación de la clave.
Ciclo de vida de los certificados	Confirmar que para cada etapa del ciclo de vida de los certificados (emisión/revocación/suspensión/renovación) estén establecidos los procedimientos y deberes del PSC o CE.
Controles de seguridad física, de gestión y de operaciones	Se debe comprobar la existencia de los controles de seguridad física, funcionales, de seguridad personal, los procedimientos de control de seguridad, los archivos de informaciones y registros. Además se debe contemplar que exista la documentación de procedimientos de la recuperación en caso de desastre y en caso del cese de la actividad del PSC o CE, que incluyan los procedimientos de término y de traspaso a otro PSC u organismo que asuma la responsabilidad de mantener la continuidad de los servicios, en tanto existan certificados vigentes.
Controles de Seguridad técnica	Comprobar la existencia de las medidas de seguridad adoptadas por el PSC o CE para la generación e instalación de las claves privada y pública, la protección de la clave privada, los datos de activación. Además se debe verificar los siguientes controles de seguridad: del computador, del ciclo de vida y de la red, así como los controles de ingeniería de los módulos criptográficos.
Perfiles de certificados, OSCP y LCR	Se verificará que el perfil de los certificados cumpla con los estándares internacionales vigentes, aplicables para las infraestructuras de claves públicas y los certificados electrónicos. En forma similar se verificará que el perfil de la LCR y el OCSP se adapten al estándar correspondiente.
Auditoría de conformidad	Se debe verificar que el PSC o CE cumpla con la frecuencia de la realización de auditorías internas.
Aranceles y responsabilidad financiera	Se refiere a las tasas establecidas para la emisión, renovación y revocación de certificados.
Confidencialidad de la información de los signatarios /protección de datos	Existencia de procedimientos de protección de la información de los signatarios.
Obligaciones AC, AR, signatario	Descripción de las obligaciones que contraen las entidades involucradas en la emisión y utilización de un certificado.
Las obligaciones y responsabilidades del PSC o CE	Comprobar que exista una declaración de las obligaciones y deberes del PSC o CE.
Las obligaciones y responsabilidades del signatario	Verificar que existan definiciones de los deberes y obligaciones de los signatarios.
Renuncias de garantías y limitación de responsabilidades	Concordancia de la DPC y PC con los procedimientos operacionales.
Modificaciones	Entre los requisitos comerciales y legales, todo PSC o CE debe tener procedimientos que especifiquen una autoridad que apruebe los cambios aplicables a su DPC, así como su publicación y notificación.
Validación Extendida	La Declaración de Prácticas de Certificación de la AC, deberá incluir los puntos relacionados a "Implementación" y "Compromiso" correspondientes a las políticas de validación extendida del Estándar de la CA/Browser Forum (CA/Brower Forum Baseline Requeriments).
Organizaciones externas	La Declaración de Prácticas de Certificación de la AC deberá identificar las obligaciones de todas las organizaciones externas de apoyo a los servicios de AC, incluyendo las políticas y prácticas aplicables.
Actualización y aprobación	La Declaración de Prácticas de Certificación y las Políticas de Certificado será revisadas y actualizadas una vez al año, así mismo debe ser aprobada por los representantes legales de la organización o aquella persona que tenga bajo su responsabilidad legal a la AC.

5.3.5. Organización

5.3.5.1 Evaluación del Personal.

5.3.5.1.1. Objetivo

Verificar que el PSC o CE emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión, con el fin de minimizar los riesgos de errores humanos, robos o mal uso de los atributos del cargo.

5.3.5.1.2. Descripción

Se evaluará en conformidad al análisis de riesgos del PSC o CE que el personal que maneja o tiene acceso a sistemas e información sensible cumpla al menos con las siguientes condiciones:

a) Que tenga la calificación técnica o profesional requerida para el cargo o función que desempeña.
b) Que tenga la experiencia mínima requerida para el cargo y función que desempeña.
c) Que esté instruido en los procedimientos mínimos de seguridad que debe guardar en su función.

Se evalúa el procedimiento que utiliza el PSC o CE para reclutar, seleccionar, evaluar y contratar personal crítico.

El personal de operaciones y sistemas no debería tener acceso a funciones de confianza, hasta que todos sus antecedentes hayan sido razonablemente verificados.

Los empleados que manejen información sensible, deben ser personal fijo, y deben existir contratos de confidencialidad que se extiendan más allá de la vigencia del contrato del empleado y/o empresa externa. Este documento debe estar basado en el estándar ETSI TS 102 042, sección 7.4.3

5.3.5.1.3 Estándares de Evaluación

- ISO 27002:2013
- ETSI TS 102 042

5.3.5.1.4 Documentación Solicitada

Perfiles de los cargos del personal que maneja información o sistemas sensibles Currículos de las personas que ocupan los cargos y funciones sensibles.

Evidencia de Identificación del personal calificado como crítico, durante la visita del experto designado por la Superintendencia, en la forma que él lo solicite (Presentación de CV, foto, huella biométrica, etc.)

5.3.5.1.5 Detalles de la Evaluación

Aspectos	Evaluación
Experiencia profesional del personal crítico	Se valida la experiencia del personal crítico que trabaja para el PSC o CE, verificando la concordancia de los perfiles en cada cargo y función, con el análisis de riesgos.
Capacitación del personal crítico en aspectos de seguridad acorde a su función y cargo.	Se confirma que el personal crítico esté capacitado en las prácticas de seguridad que debe observar de acuerdo a su cargo y función.
Procedimiento de contratación del personal crítico	Se valida el procedimiento definido por el PSC o CE para la contratación del personal crítico.
Requerimientos ETSI TS 102 042, sección 7.4.3	**Seguridad del Personal:** El PSC o CE se asegurará que el personal y las prácticas de contratación apoyaran a mejorar la fiabilidad de las operaciones de la AC. En particular: a) El PSC o CE deberá emplear un número suficiente de personas que posean el conocimiento y la experiencia necesaria para garantizar calidad en los servicios que ofrecen y que sean calificados para la funciones de trabajo. El personal del PSC o CE puede cumplir con el requisito de "conocimiento experto, experiencia y calificación" a través de capacitación formal, experiencia actualizada o la combinación de ambas. b) Deberán existir sanciones disciplinarias apropiadas que se aplicarán al personal que viole las políticas o procedimientos de la AC. c) Las funciones y responsabilidades sobre seguridad, tal como se especifican en la política de seguridad de la AC, se documentarán en la descripción del cargo. Las funciones sobre tareas de confianza, en el que la seguridad de la operación de la AC es dependiente, deberán ser claramente identificadas. d) El personal de la AC (contratados y fijos) deberán tener las descripciones de sus cargos definidos desde el punto de vista de: separación de funciones y los mínimos privilegios, determinación de la sensibilidad del cargo basada en sus funciones y niveles de acceso, investigación de antecedentes y conocimientos del empleado. En su caso, éstas se establecerán diferencias entre las funciones generales y las funciones específicas CA Las descripciones de trabajo pueden incluir habilidades y requisitos de experiencia. e) El personal deberá ejercer la administración y gestión de procedimientos que están en línea con los procesos de seguridad de la información. **NOTA 3:** Véase la norma ISO / IEC 27002 [11] para la orientación. **El registro, generación de certificados, prestación de servicios con dispositivos, gestión de la revocación** f) El personal directivo deberá emplear o contratar a quienes posean experiencia o capacitación en tecnología de firma

	electrónica y estén familiarizados con los procedimientos de seguridad para el personal con responsabilidades de protección, seguridad de la información y la evaluación del riesgo suficiente para llevar a cabo las funciones de gestión. g) Todo el personal del PSC o CE en los roles de confianza deberán estar libres de intereses que pudieran perjudicar la imparcialidad de las operaciones. *h) Los roles de confianza* incluyen roles relacionados con las siguientes responsabilidades: 1) Oficiales de Seguridad: la responsabilidad general de la administración de la aplicación de las prácticas de *seguridad. Adicionalmente aprobar* la generación / revocación / suspensión de certificados; 2) Los administradores del sistema: autorización para instalar, configurar y mantener los sistemas de la AC para el registro, generación de certificados, *la provisión prestación* de servicios con dispositivos, gestión de la revocación. 3) Los operadores del sistema: responsables de la operación diaria de los sistemas de la AC. Está autorizado
	para realizar la copia de seguridad y recuperación del sistema; 4) Los auditores del sistema: autorizado para ver los archivos y registros de auditoría de los sistemas de la AC. i) La alta dirección sera la responsable de nombrar oficialmente al personal con roles de confianza. j) El PSC o CE no nombrará en roles de confianza a personas que tienen una condena por un delito grave u otro delito que afecta a su idoneidad para el cargo. El personal no tendrán acceso a las funciones de confianza hasta que se completen todas las comprobaciones necesarias. 1) En algunos países no puede ser posible para la AC obtener información sobre las condenas anteriores. Cuando sea así, se recomienda que al empleador le pida al candidato proporcionar dicha información y rechazar la solicitud en caso de que sea negativa;

5.3.6. Reconocimiento de los Certificados de la Cadena de Confianza

5.3.6.1. Inclusión de Certificado Raíz de PSC o CE en Herramientas Tecnológicas

5.3.6.1.1 Objetivo

Verificar el cumplimiento por parte del PSC o CE en la inclusión del Certificado Raíz en herramientas y aplicaciones tecnológicas, que permita establecer confianza en la identidad de los certificados utilizados.

5.3.6.1.2 Descripción

Dado que el producto principal de un PSC o CE es la confianza en la identidad digital, esta se debe garantizar en el ámbito nacional al momento del empleo de herramientas y aplicaciones para navegar en páginas web, procesamiento de palabras, correo electrónico, entre otras; que implementen certificados emitidos por los PSC o CE.

La inclusión del Certificado Raíz en herramientas y aplicaciones tecnológicas requiere lo siguiente:

1. Estudio de factibilidad de inclusión en las distintas herramientas y aplicaciones tecnológicas, tanto privativas como no privativas, garantizando así el cumplimiento del Decreto 3.390 en materia de Tecnologías Libres.
2. Contar con la validación de **SUSCERTE**, para continuar con el proceso de incorporación en las herramientas y aplicaciones validadas.
3. Crear la petición de solicitud de inclusión en cada herramienta o aplicación requerida.
4. Someterse a un proceso de verificación de las políticas, estándares y documentación relacionada con el Certificado Raíz del PSC o CE, por parte de la organización donde se desea incluir el Certificado de la AC.
5. Reunir los requisitos exigidos por parte de la organización donde se solicita la inclusión, tales como:
   1. **Generales**. Información sobre el PSC o CE: creación, naturaleza, misión, visión, objetivos, sector atendido, entre otros.
   2. **Técnicos.** Información sobre el Certificado Raíz, Nombre del Certificado, Nombre Común, Resumen, URL del Certificado, Huella, Validez, Versión, Parámetros de las llaves de firma, URL página web, Certificados de ejemplo, CRL, OCSP, Solicitud de bits de confianza, Validación SSL, Jerarquía, Firmas Cruzadas, entre otros.
   3. **Documentación de políticas y prácticas.** Información referente a la operación del PSC o CE, disponible tanto en idioma nativo como en idioma inglés que incluye: DPC, PC, acuerdos para firmas cruzadas, auditorías, procedimientos de verificación de SSL y de correo electrónico, procedimientos de firma de código, entre otros; así como cualquier otro que sea requerido por la organización donde se procese la inclusión.
   4. **Informar mensualmente a SUSCERTE** sobre el estatus del reporte, a partir de la creación de la petición de inclusión.
   5. **Disponer del recurso humano y tecnológico**, para el logro de la meta en el tiempo mínimo dispuesto por la organización referente para la inclusión; así como para la consecución de los objetivos del Estado, en materia de certificación electrónica.
   6. **Cumplir con todas las condiciones** que no se encuentren en este apartado, pero que sean exigidas por la organización a quien se solicita la inclusión, siempre y cuando no se contradiga lo dispuesto en las normativas legales y sublegales que apliquen en materia de certificación electrónica.

5.3.6.1.3 Estándares de Evaluación

1. X.509v3
2. ETSI 102 042 v2.4.1
3. RFC 4346
4. CA/BR G
5. CA/BR B

5.3.6.1.4 Documentación Solicitada

- Copia electrónica del documento correspondiente a la evaluación de la documentación del PSC o CE y pruebas técnicas requeridas.
- Copia electrónica de la tramitación, aprobación o negación, tal sea el caso, de la inclusión del Certificado Raíz en los Navegadores Web.

5.3.6.1.5 Detalles de la Evaluación

Aspectos	Evaluación
Generales	• Verificar la información propia del PSC o CE facilitada a los Navegadores Web. • Validar la petición o solicitud de inclusión en los navegadores web.
Técnicos	• Verificar la información del Certificado Raíz suministrada por el PSC o CE a la organización que provee el navegador web. • Validar la disponibilidad de LCR y el servicio de OCSP del PSC o CE.
Documentación	• Verificar que la documentación relacionada con el Certificado Raíz del PSC o CE requerida por el Navegador Web este en idioma ingles.
Personal	• Verificar que exista un personal asignado al seguimiento de la solicitud de inclusión.

5.4 Descripción del Procedimiento

Ver Norma SUSCERTE No 027, la cual presenta una Guía para la Acreditación o Renovación de Proveedores de Servicios de Certificación.

6 PARTE FINAL

6.1. Disposiciones transitorias

A partir de la fecha de publicación en gaceta de esta Norma, el PSC o Caso Especial, deberá iniciar un proceso de adecuación de hasta un máximo de 12 meses contados a partir de la fecha de publicación. Durante ese lapso el PSC deberá consignar ante la SUSCERTE informes trimestrales donde se evidencie el alcance y avance de esta actualización.

6.2. Disposiciones finales

Si los estándares y recomendaciones internacionales utilizados para la elaboración de esta norma son actualizados o reemplazados, SUSCERTE podrá solicitar a los PSC aplicar dichos cambios a fin de garantizar el funcionamiento óptimo de la Infraestructura Nacional de Certificación Electrónica.

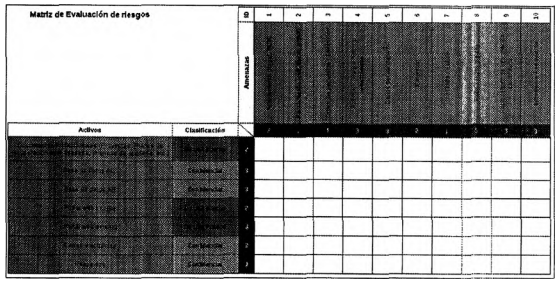
7 ANEXOS NORMATIVOS

Anexo No 1 Resumen de Recaudos Técnicos para la Acreditación o Renovación

N°	Nombre de Recaudo	Normas y Guías	Documentación Solicitada
T01 Infraestructura de Clave Pública. Perfiles de Certificado y Servicios de Publicación			
T01.1	Estructura e información del Certificado Electrónico	- ITU-T Rec. X.509 / ISO/IEC 9594-8 - ITU-T X.690 - Norma SUSCERTE 032	Modelos de Certificado tipo de firma electrónica, emitido por el PSC o CE en evaluación y el Modelo de la solicitud de firma del certificado (CSR), en caso de acreditación. Y modelos de certificados electrónicos emitidos por el PSC o CE (DPC y PC).
T01.2	Estructura de la Lista de Certificados Revocados (LCR) y OCSP – Online Certificate Status Protocol	- RFC 6818 - Norma SUSCERTE No 032 - RFC 2560	- DPC y PC del PSC o CE - LCR emitida por el PSC o CE en evaluación y el certificado de firma electrónica de la AC que la emite - Reportes de solicitudes y/o peticiones al servicio
T01.3	Registro de acceso público	Este apartado no aplica	Documento descriptivo que contenga al menos la siguiente información: • Detalle del sitio Web donde publicara la información. • Descripción de la tecnología. • Disponibilidad, accesibilidad, conexión, esquemas y diagramas de funcionamiento. • Medidas de seguridad. • Sitio Web de prueba con las funcionalidades requeridas. • Publicación y vigencia de DPC y PC • Publicación y vigencia de la LCR
T01.4	Modelo de confianza	Este apartado no aplica	Documento en el que se describe el modelo de confianza utilizado por el PSC o CE para lograr el objetivo o alternativamente la DPC y PC si contiene dicho punto.
T02 Seguridad			
T02.1	Evaluación de riesgos y Amenazas	Puede considerarse como referencia normativa la ISO 27005, el Magerit u otro estándar ampliamente conocido	Copia del documento correspondiente a la Evaluación de Riesgos o documento equivalente.
T02.2	Política de seguridad de la información	- ISO/IEC 27002:2013	Copia del documento correspondiente a la política de seguridad de la organización. Documento en el cual se describa formalmente la estructura organizativa del PSC o CE, aprobada por las autoridades de la Institución
T02.3	Plan de continuidad del negocio y recuperación ante desastres.	- ISO/IEC 27002:2013 - ETSI TI 102 042	Documentación Solicitada • Documento de Planes de Continuidad del Negocio y Recuperación de Desastres. • Documento de Evaluación de Riesgo
T02.4	Plan de seguridad de la información	- ISO/IEC 27002:2013 - ETSI TS 102 042	Copia del documento correspondiente al Plan de Seguridad de Información.
T02.5	Implementación del plan de seguridad de la información.	- ISO/IEC 27002:2013	Documento descriptivo de la implementación del Plan de Seguridad de la Información del solicitante a PSC o CE, el cual será validado al momento de la auditoría
T02.6	Plan de administración de claves criptográficas.	- ETSI TS 102 042 - FIPS 140-1 - FIPS 140-2 - CABR B - CABR G	Documento descriptivo de la implementación del Plan de Administración de Claves Criptográficas de la Organización
T03 Plataforma Tecnológica			
T03.1	Evaluación de la plataforma tecnológica	- FIPS 140-2 - ISO/IEC 15408 o equivalente	Documento descriptivo de la implementación de la infraestructura tecnológica. Este documento debe incluir al menos, planos de interconexión de sistemas, cableado de red de datos, cableado de poder principal y auxiliar, dispositivos de seguridad y control de acceso, y todo aquello relevante que permita demostrar la confiabilidad de la infraestructura tecnológica. Manuales del fabricante de los productos hardware y software relevantes. Documentación del fabricante que acredite el correspondiente nivel de seguridad
T04 Políticas de Certificación			
T04.1	Declaración de prácticas de certificación y políticas de certificados	- RFC 3647 - ETSI TS 102 042 - CA/BR B - CA/BR G	Documento de la Declaración de Prácticas de Certificación (DPC) y Política de Certificados (PC) con los diferentes tipos de estructura de campos de certificados. (Norma 022 de SUSCERTE)
T04.2	Modelo y Manual de Operación de la Autoridad de Certificación (AC) del PSC o CE	- ETSI TS 102 042 - CA/BR - RFC 3647	Modelo y Manual de operación de la AC principal y/o subordinadas del PSC o CE Manual del Hardware Criptográfico usados para la generación y protección de las claves privadas de la(s) autoridades de certificación
T04.3	Modelo y Manual de Operación de la Autoridad de Registro (AR)	- ETSI 102 042 - CA/BR B - CA/BR G - RFC 3647	Modelo y Manual de Operación de la AR Manual técnico de los dispositivos seguros de firma electrónica

T05 Modelo Organizacional			
T05.1	Estructura organizativa	- ISO/IEC 27002:2013 - ETSI TI 102 042	Describiendo las unidades y cantidad de personas dedicadas a las labores relacionadas a la solicitud
T05.2	Evaluación del personal	- ISO/IEC 27002:2013 - ETSI TI 102 042	Perfiles de los cargos del personal que maneja información o sistemas sensibles Currículos de las personas que ocupan los cargos y funciones sensibles. Evidencia de identificación del personal calificado como crítico, durante la visita del experto designado por la Superintendencia, en la forma que él lo solicite (Presentación de CV, foto, huella biométrica, etc.)

Anexo N° 2 Ejemplo Matriz de Riesgos



Anexo N° 3 Controles del Estándar ISO/IEC 27002:2013, Controles 5 al 18, Aplicables

CONTROL 5 Política de Seguridad

5.1 Orientación de la dirección de la seguridad de la información

Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.

5.1.1 Políticas de seguridad de la información

Control: Definir un conjunto de políticas de seguridad de la información, ser aprobadas por la dirección, publicadas y comunicadas a los empleados y a las partes externas relevantes.

Guía de implementación

La política de seguridad de la información deben abordar los requisitos creados por:

a) Estrategias de negocios

b) Reglamentos, leyes y contratos

c) Entorno de amenazas de seguridad de la información

La política de seguridad de la información deben contener declaraciones respecto a:

a) Definición de la seguridad de la información, los objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información

b) Asignación de responsabilidades generales y específicas para la gestión de seguridad de la información a los roles definidos

c) Procesos para el manejo de desviaciones y excepciones

5.1.2 Revisión de las políticas de seguridad de la información

Control: las políticas de seguridad de la información deberían revisarse a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficiencia continuación

Guía de implementación

Cada política debe tener un propietario con responsabilidad de gestión aprobada para el desarrollo, la revisión y la evaluación de las políticas. La revisión debería incluir la evaluación de las oportunidades de mejora de las políticas de la organización y el enfoque a la gestión de seguridad de la información en respuesta a cambios en el ambiente de la organización, a las circunstancias del negocio, a las condiciones legales o al ambiente técnico.

La revisión de las políticas de seguridad de la información debería tomar en cuenta los resultados de las revisiones por la dirección.

Debe obtenerse la aprobación de la dirección para la política revisada.

CONTROL 6 Organización de la Seguridad de la Información

6.1 Organización interna

Objetivo: Iniciar, controlar la implementación y la operación de la seguridad de la información dentro de la organización.

- Funciones y responsabilidades de la seguridad de la información (6.1.1).
- Separación de funciones (6.1.2).
- Contacto con autoridades (6.1.3).
- Seguridad de la información en la gestión de proyectos (6.1.5).

CONTROL 7 Seguridad Ligada a los Recursos Humanos

7.1 Previo al empleo[3]

Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y que sean aptos para los roles para los cuales están siendo considerados.

- Selección (7.1.1)
- Términos y condiciones de empleo (7.1.2)

7.2 Durante el empleo

Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con las responsabilidades de seguridad de la información.

- *Responsabilidades de la Dirección* (7.2.1)
- Toma de conciencia, educación y formación en la seguridad de la información (7.2.2)
- Proceso disciplinario (7.2.3)

7.3 Finalización o cambio de empleo

Objetivo: *Proteger los intereses de la organización como parte del proceso de finalización o cambio de empleo.*

- Responsabilidades de terminación (7.3.1)

CONTROL 8 Gestión de Activos

8.1 Responsabilidad por los Activos

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

- Inventario de activos (8.1.1)
- Propiedad de los activos (8.1.2)
- Uso aceptable de los activos (8.1.3)
- Devolución de los activos (8.1.4)

8.2 Clasificación de la Información

Objetivo: Asegurar que la información reciba un apropiado nivel de protección de acuerdo a su importancia dentro de la organización.

3 Explicación: La palabra "Empleo" significa cubrir todas las diferentes situaciones siguientes: empleo de personas (temporal o permanente), la asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos y la terminación de cualquiera de estos arreglos

- Clasificación de la información (8.2.1)
- Etiquetado de la información (8.2.2)
- Manejo de los activos (8.2.3)

8.3 Manejo de los Medios

Objetivo: Evitar la divulgación no autorizada, la modificación, Eliminación o destrucción de la información almacenada en medios.

- Gestión de medios extraíbles (8.3.1)
- Eliminación de medios (8.3.2)
- Transferencia de medios físicos (8.3.3)

CONTROL 9 Control de Accesos

9.1 Requisitos de negocio para el control de acceso

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

- Política de control del accesos (9.1.1)
- Acceso a las redes y a los servicios de red (9.1.2)

9.2 Gestión del Acceso de usuarios

Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.

- Registro de usuarios y cancelación del registro (9.2.1)
- Gestión de acceso a los usuarios (9.2.2)
- Gestión de derechos de acceso privilegiados (9.2.3)
- Gestión de la información de autenticación secreta de los usuarios (9.2.4)
- Revisión de derecho de acceso a usuario (9.2.5)
- Remoción o ajuste de los derechos de acceso (9.2.6)

9.3 Responsabilidades del usuario

Objetivo: Hacer a los usuarios responsables de salvaguardar su información de autenticación.

- Uso de la información de autenticación secreta (9.3.1)

9.4 Control de Acceso al Sistema y a las Aplicaciones

Objetivo: Impedir el acceso no autorizado a los sistemas y las aplicaciones.

- Restricción de acceso a la información (9.4.1)
- Procedimientos de conexión seguros (9.4.2)
- Sistema de gestión de contraseñas (9.4.3)
- Uso de programas de utilidad privilegiados (9.4.4)
- Control de acceso al código de programas fuente (9.4.5)

CONTROL 10 Criptografía

10.1 Controles Criptográficos

Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

- Políticas sobre el empleo de controles criptográficos (10.1.1)
- Gestión de claves (10.1.2)

CONTROL 11 Seguridad Física y del Ambiente

11.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, daño e interferencia a las instalaciones de procesamiento de información y la información de la organización.

- Perímetro de seguridad física (11.1.1)
- Controles físicos de entrada (11.1.2)
- Seguridad de oficinas, despachos e instalaciones 11.1.3)
- Protección contra las amenazas externas y del ambiente (11.1.4)
- Trabajo en áreas seguras (11.1.5)
- Áreas de entrega y carga (11.1.6)

11.2 Equipamiento

Objetivo: Prevenir pérdidas, daños, robo o comprometer los activos e interrupción de las actividades de la organización.

- Ubicación y protección del equipamiento (11.2.1)
- Elementos de soporte (11.2.2)
- Seguridad en el cableado (11.2.3)
- Mantenimiento del equipamiento (11.2.4)
- Retiro de bienes (11.2.5)
- Seguridad del equipamiento de los activos fuera de las instalaciones (11.2.6)
- Seguridad en la reutilización o eliminación de equipos (11.2.7)
- Equipamiento desatendido por el usuario (11.2.8)
- Política de escritorio y pantalla limpios (11.2.9)

CONTROL 12 Seguridad de las Operaciones

12.1 Procedimientos Operacionales y Responsabilidades

Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.

- Procedimientos documentados de operación (12.1.1)
- Gestión de cambios (12.1.2)
- Gestión de la capacidad (12.1.3)
- Separación de los ambientes para desarrollo, prueba y operación (12.1.4)

12.2 Protección ante software malicioso

Objetivo: Garantizar que la información y las instalaciones de procesamiento de la información se encuentren protegidos contra el software malicioso.

- Controles ante software malicioso (12.2.1)

12.3 Respaldo

Objetivo: Evitar la pérdida de información.

- Respaldo de la información (12.3.1)

12.4 Registros y Supervisión

Objetivo: Registrar eventos y generar evidencias.

- Registro de eventos (12.4.1)
- Protección de la información de registros logs (12.4.2)
- Registros del administrador y operador (12.4.3)
- Sincronización de relojes (12.4.4)

12.5 Control del Software en Producción

Objetivo: Garantizar la integridad de los sistemas operativos.

- Instalación de software en los sistemas operativos (12.5.1)

12.6 Gestión de Vulnerabilidad Técnica

Objetivo: Prevenir la explotación de vulnerabilidades técnicas.

- Gestión de vulnerabilidades técnicas (12.6.1)
- Restricciones en la instalación de software (12.6.2)

12.7 Consideraciones sobre la auditoría de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

- Controles de auditoría de sistemas de información (12.7.1)

CONTROL 13 Seguridad de las Comunicaciones

13.1 Gestión de la Seguridad de Red

Objetivo: Asegurar la protección de la información en redes y la protección de infraestructura de soporte.

- Controles de red (13.1.1)
- Seguridad de los servicios de red (13.1.2)
- Separación de redes (13.1.3)

13.2 Intercambio de Información

Objetivo: Mantener la seguridad de la información intercambiada dentro de la organización y con cualquier otra entidad.

- Políticas y procedimientos de intercambio de información (13.2.1)
- Acuerdos de intercambio de información (13.2.2)
- Mensajería electrónica (13.2.3)
- Acuerdos de confidencialidad o no divulgación (13.2.4)

CONTROL 14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad es una parte integral de los sistemas de información en todo su ciclo de vida, incluyendo los sistemas de información de servicios a través de redes públicas.

- Análisis y especificación de los requisitos de seguridad (14.1.1)
- Aseguramiento de los servicios de aplicación en las redes públicas (14.1.2)
- Transacciones en línea (14.1.3)

14.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: Garantizar que la seguridad de la información ha sido diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información.

- Política de desarrollo seguro (14.2.1)
- Procedimiento de control de cambios del sistema (14.2.2)
- Revisión técnica de las aplicaciones después de cambios de las plataformas operativas (14.2.3)
- Restricciones sobre cambios a paquetes de software (14.2.4)
- Principios de la ingeniería de sistemas seguros (14.2.5)
- Ambiente de desarrollo seguro (14.2.6)
- Pruebas de seguridad del sistema (14.2.8)
- Pruebas de aceptación del sistema (14.2.9)

14.3 Datos de Prueba

Objetivo: garantizar la protección de los datos utilizados para las pruebas.

- Protección de datos de prueba (14.3.1)

CONTROL 15 RELACIONES CON LOS PROVEEDORES: No Aplica

CONTROL 16 Gestión de incidente de seguridad de la información

16.1 Gestión de incidente y mejoras de seguridad de la información

Objetivo: Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades.

- Responsabilidades y procedimientos (16.1.1)
- Reporte de eventos de seguridad de la información (16.1.2)
- Reporte de debilidades de seguridad de la información (16.1.3)
- Evaluación y decisión sobre los eventos de seguridad de información (16.1.4)
- Respuesta a incidentes de seguridad de información (16.1.5)
- Aprendiendo de los incidentes de seguridad de información (16.1.6)
- Recolección de evidencia (16.1.7)

CONTROL 17 Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

17.1 Continuidad de la Seguridad de la Información

Objetivo: La continuidad de seguridad del negocio debe estar integrada en los sistemas de gestión de continuidad del negocio de la organización

- **Planificación de la continuidad de la seguridad de la información (17.1.1)**

Control: la organización debe determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Guía de Implementación:

Una organización debe determinar si la continuidad de la seguridad de la información está incluida dentro del proceso de gestión de continuidad del negocio o en el proceso de gestión de recuperación ante desastres. Deben determinarse los requisitos de seguridad de la información al planificar la continuidad del negocio y la recuperación ante desastres.

Si no existe una continuidad del negocio formal ni planificación de recuperación ante desastres, la gestión de seguridad de la información debe asumir que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones de funcionamiento normales. Alternativamente una organización puede realizar un análisis de impacto en el negocio para que los aspectos de seguridad de la información determinen si los requisitos de seguridad de la información son aplicables a las situaciones adversas.

- **Implementación de la continuidad de la seguridad de la información (17.1.2)**

Control: la organización debe establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.

Guía de Implementación:

Una organización debería asegurarse que:

a) Se establezca una estructura de gestión adecuada para estar preparados para, mitigar y responder a un evento disruptivo utilizando personal con la autoridad, experiencia y competencias necesarias

b) Designar personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para gestionar un incidente y mantener la seguridad de la información

c) Desarrollar y aprobar los planes documentados, los procedimientos de respuesta y recuperación, detallando cómo la organización va a gestionar un evento disruptivo y mantener su seguridad de la información en un nivel predeterminado, basados en los objetivos de continuidad de seguridad de la información aprobados por la gestión (Ver 17.1.1)

De acuerdo con los requisitos de continuidad de la seguridad de la información la organización debe establecer, documentar, implementar y mantener:

a) Los controles de seguridad de la información dentro de los procesos, procedimientos y sistemas de apoyo y herramientas de continuidad del negocio o de recuperación ante desastres

b) Los procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa

c) Los controles de compensación para los controles de seguridad de la información que no pueden ser mantenidos durante una situación adversa.

- **Verificar, revisar y evaluar la continuidad de la seguridad de la información (17.1.3)**

Control: La organización debe verificar los controles de continuidad de seguridad de la información establecidos e implementados a intervalos a fin de asegurar que son válidos y eficaces durante situaciones adversas

Guía de Implementación:

Las organizaciones deben verificar su gestión de la continuidad de la seguridad de la información:

a) Ejercitando y probando la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para asegurar que son coherentes con los objetivos de continuidad de seguridad de la información

b) Ejercitando y probando el conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información para asegurar que su desempeño es coherentes con los objetivos de continuidad de seguridad de la información

c) Revisando la validez y eficacia de las medidas de continuidad de la seguridad de la información cuando los sistemas de información, los procesos, procedimientos y controles de seguridad de la información o los procesos de gestión de continuidad del negocio/gestión de recuperación ante desastres y las soluciones para el cambio

17.2 Redundancia

Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de información

- Disponibilidad de las instalaciones de procesamiento de información (17.2.1)

CONTROL 18 Cumplimiento

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control: todos los requisitos estatutarios, reguladores y contractuales relevantes y el enfoque de la organización para cumplir estos requisitos debería definirse explícitamente, documentarse y mantenerse al día para cada sistema de información y para cada organización

Guía de Implementación:

Los directores deberían identificar todas la layes aplicables a su organización a fin de cumplir con los requisitos para su tipo de negocio. Si la organización realiza negocios en otros países los directores deberían considerar el cumplimiento en todos los países pertinentes.

18.1.2 Derechos de la Propiedad Intelectual

Control: deberían implantarse los procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reguladores y contractuales relacionados sobre los derechos de propiedad intelectual y sobre el uso de los productos de software propietario.

Guía de Implementación:

Deberían considerarse las siguientes recomendaciones para proteger cualquier material que pueda ser considerado propiedad intelectual:

a) Publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos de software de información.

b) Adquirir software solo de fuentes conocidas y de buena reputación, para asegurar que los derechos de copia del software no han sido violados.

c) Mantener la concientización de las políticas de proteger los derechos de propiedad intelectual y publicando la intención de adoptar medidas disciplinarias para el personal que los viole.

d) Mantener un registro apropiado de activos e identificar todos los activos con requisitos protegidos por el derecho de propiedad intelectual.

e) Mantener los documentos que acrediten la propiedad de licencias, discos originales, manuales, etc.

f) Implementar controles para asegurar que no se sobrepasa el numero máximo de usuarios permitidos de la licencia.

g) Llevar a cabo revisiones que solo son instalados productos de software autorizados y con licencia.

h) Establecer una política de mantenimiento de las condiciones adecuadas de la licencia.

i) Establecer una política de eliminación de software o de su transferencia a terceros

j) Cumplir con los términos y condiciones de uso del software y de la información obtenida de redes públicas

k) No duplicar, ni convertir a otro formato o extraer información de las grabaciones comerciales (película, audio) con excepción de los permitidos por los derechos de copia

l) No copiar total o parcialmente libros, artículos, informes u otros documentos con excepción de los permitidos por los derechos de copia.

18.1.3 Protección de los Registros:

Control: deberían protegerse los registros frente a su perdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada de acuerdo a los requisitos estatutarios, reguladores, contractuales y del negocio.

Guía de Implementación:

Para alcanzar los objetivos de salvaguardar los registros, deberían tomarse las siguientes medidas dentro de una organización:

a) Deberían publicarse directrices sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información.

b) Debería establecerse un calendario de retenciones que identifique los registros y los períodos de tiempo que deberían retenerse.

c) Debería mantenerse un inventario de las fuentes de información clave.

18.1.4 Protección de los datos y privacidad de la información personalmente

Control: debería asegurarse la protección y la privacidad de los datos de acuerdo con la legislación y las regulaciones pertinentes, cuando corresponda.

Guía de Implementación:

El cumplimiento de esta política y de toda la legislación y regulaciones relevantes a la protección de la privacidad de las personas y de los datos personales requiere una apropiada estructura de gestión y control. Este objetivo suele alcanzarse con mayor facilidad designando una persona responsable, por ejemplo un oficial de protección de datos, que oriente a los directores, usuarios y proveedores de servicios sobre sus responsabilidades individuales y sobre los procedimientos específicos que deberían seguirse. La *responsabilidad de manejar la información personal y de asegurar el conocimiento de los principios de privacidad debería establecerse de acuerdo con la legislación y las regulaciones relevantes. Deberían implantarse medidas técnicas y organizacionales apropiadas para proteger la información personal.*

18.2 Revisiones de Seguridad de la Información

18.2.1 Revisión independiente de la seguridad de la información

Control: el enfoque de la organización para gestionar la seguridad de la información y su implementación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos de seguridad de la información) deberían revisarse de forma independiente a intervalos planificados o cuando se producen cambios significativos.

Guía de Implementación:

La dirección debería iniciar la revisión independiente, tal revisión es necesaria para asegurar la conveniencia, adecuación y eficacia continua del enfoque de la organización para gestionar la seguridad de la información. La revisión debería incluir oportunidades de evaluación para la mejora y la necesidad de cambios en el enfoque de seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería realizarse por personas independientes del área bajo revisión, por ejemplo, la función de auditoría interna, un administrador independiente o una organización de tercera parte especializada en este tipo de revisiones. Las personas que llevan a cabo estas revisiones deberían tener las habilidades y experiencia apropiadas.

Los resultados de una revisión independiente deberían registrarse y comunicarse a la gestión que inició la revisión. Estos registros deberían mantenerse.

Si la revisión independiente identifica que el enfoque de la organización y la implementación para gestionar la seguridad de la información son inadecuados, por ejemplo, los requisitos y objetivos documentados no se cumplen o no cumplen con la dirección de seguridad de la información establecida en las políticas de seguridad de la información, la dirección debería considerar las acciones correctivas

18.2.2 Cumplimiento de la política y las normas de seguridad

Control: los directores deberían revisar regularmente el cumplimiento del procesamiento de la información y los procedimientos dentro de su área de responsabilidad con las políticas de seguridad apropiadas, las normas y cualquier otro requisito de seguridad.

Guía de Implementación:

Los directores deberían identificar como revisar si se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y otras regulaciones aplicables. Debería considerarse la medición automática y las herramientas de informes para una revisión periódica eficiente. Si algún incumplimiento se encuentra como resultado de la revisión, los directores debería:

a) Identificar las causas del incumplimiento

b) Evaluar la necesidad de tomar medidas para lograr el cumplimiento

c) Implementar las acciones correctivas apropiadas

d) Revisar la acción correctiva tomada para comprobar su eficacia e identificar las deficiencias y debilidades

Los resultados de las revisiones y de las acciones correctivas realizadas por los directores deberían registrarse y estos registros deberían mantenerse. Los directores deberían reportar los resultados a las personas que realizar las revisiones independientes cuando la revisión independiente se realice en el área de su responsabilidad

18.2.3 Revisión del Cumplimiento Técnico

Control: los sistemas de información deberían revisarse regularmente para verificar el cumplimiento con las políticas y las normas de seguridad de la información de la organización

Guía de Implementación:

El cumplimiento técnico debería revisarse preferentemente con la ayuda de herramientas automatizadas que generen un informe técnico para su posterior interpretación por parte de un especialista técnico. Alternativamente un ingeniero de sistemas experimentado podría realizar revisiones manuales (con el apoyo de herramientas de software apropiadas, si es necesario)

Si se realizan pruebas de intrucción o evaluaciones de vulnerabilidad, debería tenerse cuidado pues estas actividades podrían comprometer la seguridad del sistema. Tales pruebas deberían planificarse, documentarse y repetirse.

Cualquier revisión del cumplimiento técnico debería realizarse solamente por personas competentes, autorizadas o bajo supervisión de tales personas.

Anexo N° 4 Documento Estándar de una Política de Seguridad

Según la ISO 27002:2013: una política de seguridad debe contener enunciados relacionados con:

- Una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información
- Un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales.
- Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.
- Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización.
- Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información .
- Referencias a la documentación que fundamenta la política

Aunque cada organización debe crear su política y destacar los aspectos que le apliquen, a continuación se mencionan algunos de los considerados más relevantes:

Organización de la seguridad de la información

- Se debe establecer un marco referencial gerencial para iniciar controlar la implementación de la seguridad de la información.
- La gerencia debe aprobar la política de seguridad de la información,asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización.
- Si fuese necesario, se debe establecer una fuente de consultoría sobre seguridad de la información.
- Se debe fomentar un enfoque multi-disciplinario para la seguridad de la información.

Gestión de Activos

- Todos los activos debieran ser inventariados y contar con un propietario nombrado.
- Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados.

Seguridad de recursos humanos

- Especifica los requerimientos de selección del personal de seguridad y como estos serán logrados.
- En caso de no ser necesaria una selección formal por un departamento de seguridad, esta sección detalla la política de verificación indirecta de antecedentes del personal, para asegurar que sea empleado en posiciones de confianza sólo personal adecuado.
- Proveer directrices bajo las cuales personal, contratistas, consultores y/o auditores pueden acceder a las dependencias de la organización, darle acceso a información de los sistemas internos, etc.
- También es importante un plan mediante el cual al personal se le da acceso privilegiado a los sistemas críticos.
- Esta sección también debe detallar las responsabilidades asociadas con el uso de los sistemas de la organización y los requerimientos que permitan asegurar que los signatarios estén conscientes de sus responsabilidades y efectos de las violaciones.

Seguridad ambiental y física

- Especifica los objetivos de seguridad física incluyendo, pero no limitado a, eliminación de elementos en desuso, guardias, alarmas de seguridad física, tiempos de respuesta, claves físicas, y estructura de la seguridad física de todas las dependencias relevantes.
- Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.
- Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

Gestión de las comunicaciones y operaciones

- Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.
- Chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer los requerimientos acordados por la tercera persona .
- Realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.
- Establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.
- Tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.
- Establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de la data y practicar su restauración oportuna.
- Los medios se deben controlar y proteger físicamente.
- Se debe establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), input/output de data y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción .
- Considerar las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo las transacciones en línea, y los requerimientos de controles.
- También se debe considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de los sistemas públicamente disponibles.
- Monitorear los sistemas y se debieran reportar los eventos de seguridad de la información. Utilizar bitácoras de operador y registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información.

Control de Acceso

- Controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.
- Especifica los niveles de clasificación de la confidencialidad e importancia de la información que será manipulada o que podría ser accesada por el personal autorizado de los sistemas de información de la organización.

Adquisición, desarrollo y mantenimiento de los sistemas de información

- Identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información .
- Desarrollar una política sobre el uso de controles criptográficos.
- Controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI y las actividades de soporte se debieran realizar de una manera segura .
- Controlar estrictamente los ambientes del proyecto y soporte.
- Los gerentes responsables por los sistemas de aplicación también deben asegurar que todos los cambios propuestos para el sistema, sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación.
- Implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable .

Gestión de un incidente en la seguridad de la información

- Establecer procedimientos formales de reporte y de la identificación de un evento.
- Establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debiera aplicar un proceso de mejoramiento continuo para la respuesta a, monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información .

Gestión de la continuidad del negocio

- Desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales .
- Debe incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debe limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales y operacionales.
- La evaluación del riesgo de la continuidad el negocio se debiera llevar a cabo con la participación total de los propietarios de los recursos y procesos comerciales y operacionales.

Cumplimiento

- El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.
- Durante las auditorías de los sistemas de información deben existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.
- Los gerentes deberán asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

Anexo No 5 Elementos de Evaluación de un Plan de Seguridad

La evaluación es una valoración de los siguientes aspectos:

- ¿Existe un administrador de la seguridad de Tecnología de la Información in situ?
- ¿Tiene el administrador de seguridad en Tecnología de la Información un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Está el personal de soporte que se identifica en el Plan de Seguridad disponible?

- ¿Tiene el personal de soporte un conocimiento adecuado de su rol, consistente con aquel descrito en el Plan de Seguridad y el Manual de Operación?
- ¿Es el conjunto de signatarios privilegiados del sistema AC o AR consistente con el conjunto de signatarios privilegiados descritos en el plan de seguridad?
- ¿Está la infraestructura computacional y de red instalada y operando de acuerdo a lo descrito en: el Plan de Seguridad, el Manual de Operación, la DPC y PC y el Plan de Continuidad de Negocios y Recuperación ante Desastres?
- ¿Están los mecanismos de seguridad y procedimientos descritos en el Plan de Seguridad instalados y configurados o implementados de acuerdo con el Plan? Se verificará principalmente:

1. Mecanismos de control de acceso
2. Captura y revisión de datos de Auditoría
3. Monitoreo de incidentes de seguridad
4. Administración de incidentes y procedimientos de respuesta ante incidentes
5. Mantenimiento y uso de la información acerca de vulnerabilidades de las instalaciones de la AC o AR
6. Plan de administración de claves criptográficas
7. Administración de cuentas de signatarios
8. Control de media removible
9. Respaldo y recuperación de datos y sistemas, incluyendo almacenamiento de segundas copias fuera de las instalaciones
10. Control de inventario, incluyendo procedimientos de registro para controlar ubicación y acceso de los activos críticos.
11. Administración del FW Internet
12. Procedimientos y mecanismos que tengan un rol relevante en reducir las amenazas a las operaciones de la AC o AR.
13. Provee la confianza mediante la comprobación en terreno de que la seguridad operacional del PSC o CE se mantendrá en el tiempo dadas las condiciones siguientes:
    - ¿Después que el grupo evaluador se ha retirado?
    - ¿Después de cambios en las amenazas de seguridad, personal, servicios ofrecidos, tecnología e infraestructura?

Artículo 3. Con la publicación en Gaceta Oficial de esta Providencia queda sin efecto la **NORMA SUSCERTE 040-01/12 edición 3.1 de fecha 30-01-2012.**

Artículo 4. La Norma N° **040-06/17 edición 4.1, "GUÍA DE ESTÁNDARES TECNOLÓGICOS Y LINEAMIENTOS DE SEGURIDAD PARA LA ACREDITACIÓN Y RENOVACIÓN COMO PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN o CASOS ESPECIALES",** se encuentra a disposición en la sede de La Superintendencia de Servicios de Certificación Electrónica así como en la página Web www.suscerte.gob.ve.

Artículo 5. La presente Providencia Administrativa entrará en vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y Publíquese.

LUIS FERNANDO PRADA FUENTES

Resolución Nº 095 del 19 de junio de 2.017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.177 de fecha 21 de junio de 2.017. Resolución Nº 106 de fecha 13 de julio de 2.017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.195 en fecha 18 de julio de 2.017

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR
PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 023
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, al ciudadano: **CARLOS HUMBERTO MARTÍNEZ FIGUERA**, titular de la cédula de identidad Nº **V-3.049.528**, de **Sesenta y Dos (62)** años de edad, con Diecisiete (17) años y Once (11) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Director**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **DOSCIENTOS OCHENTA Y CINCO MIL SETECIENTOS CINCUENTA BOLÍVARES CON DIECINUEVE CÉNTIMOS (Bs. 285.750,19)** mensuales, equivalente al Cuarenta y Cinco por Ciento (45%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR
PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 024
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **GLADYS EPIFANIA MORALES BRITO**, titular de la cédula de identidad Nº **V-3.473.959**, de **Setenta (70)** años de edad, con Diecisiete (17) años y Ocho (8) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Profesional II**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **CIENTO CUARENTA Y CINCO MIL CUATROCIENTOS SESENTA Y DOS BOLÍVARES CON CUARENTA Y SIETE CÉNTIMOS (Bs. 145.462,47)** mensuales, equivalente al Cuarenta y Cinco por Ciento (45%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 025
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial Nº 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **MIRIAM MIROCLE TOVAR BLANCO**, titular de la cédula de identidad Nº **V-3.845.762**, de **Sesenta y Tres (63)** años de edad, con Dieciocho (18) años y Seis (6) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Profesional I**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **CIENTO CUARENTA Y DOS MIL SEISCIENTOS SESENTA Y DOS BOLÍVARES CON TRECE CÉNTIMOS (Bs. 142.662,13)** mensuales, equivalente al Cuarenta y Cinco por Ciento (45%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 026
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial Nº 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **ARMINDA JOSEFINA CARDOZO GODOY**, titular de la cédula de identidad Nº **V-3.903.902**, de **Sesenta y Cuatro (64)** años de edad, con Veintiún (21) años y Nueve (9) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Director de Línea**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **TRESCIENTOS SETENTA Y TRES MIL NOVECIENTOS VEINTIOCHO BOLÍVARES CON OCHENTA CÉNTIMOS (Bs. 373.928,80)** mensuales, equivalente al Cincuenta y Cinco por Ciento (55%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 027
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial Nº 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **CRUZ DEL CARMEN CALDERÓN VICUÑA**, titular de la cédula de identidad Nº **V-3.982.767**, de **Sesenta y Cuatro (64)** años de edad, con Dieciocho (18) años y Tres (3) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Contratada**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **CIENTO CATORCE MIL CIENTO DIECISIETE BOLÍVARES CON OCHENTA Y NUEVE CÉNTIMOS (Bs. 114.117,89)** mensuales, equivalente al Cuarenta y Cinco por Ciento (45%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 028
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, al ciudadano: **ENRIQUE JOSÉ LUQUE ORDOÑEZ**, titular de la cédula de identidad Nº **V-4.171.592**, de **Setenta (70)** años de edad, con Diecisiete (17) años y Tres (3) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Contratado**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **CIENTO TREINTA Y SEIS MIL NOVECIENTOS SETENTA Y SEIS BOLÍVARES CON SESENTA Y NUEVE CÉNTIMOS (Bs. 136.976,69)** mensuales, equivalente al Cuarenta y Dos Punto Cinco por Ciento (42.5%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 029
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **MIRNA YASMIN MORENO JIMÉNEZ**, titular de la cédula de identidad Nº **V-4.846.910**, de **Cincuenta y Nueve (59)** años de edad, con Diecinueve (19) años y Nueve (9) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Auxiliar de Servicio de Oficina**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **CIENTO TREINTA Y UN MIL CIENTO TRESCIENTOS OCHENTA BOLÍVARES CON SESENTA Y SEIS CÉNTIMOS (Bs. 131.380,66)** mensuales, equivalente al Cincuenta por Ciento (50%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 030
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **JOSEFA CHACON BAUTISTA**, titular de la cédula de identidad Nº **V-5.406.311**, de **Cincuenta y Nueve (59)** años de edad, con Diecisiete (17) años y Cinco (5) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Técnico I**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **DOSCIENTOS CINCUENTA Y UN MIL CUATROCIENTOS QUINCE BOLÍVARES CON VEINTRÉS CÉNTIMOS (Bs. 251.415,23)** mensuales, equivalente al Cuarenta y Dos Punto Cinco por Ciento (42.5%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 031
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **MARIA YSABEL CASTELLANOS MARTÍNEZ**, titular de la cédula de identidad Nº **V-5.749.314**, de **Cincuenta y Seis (56)** años de edad, con Dieciocho (18) años y Tres (3) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Bachiller I**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **CIENTO VEINTRÉS MIL SETENTA Y SEIS BOLÍVARES CON SETENTA Y UN CÉNTIMOS (Bs. 123.076,71)** mensuales, equivalente al Cuarenta y Cinco por Ciento (45%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

REPÚBLICA BOLIVARIANA DE VENEZUELA

MINISTERIO DEL PODER POPULAR PARA HÁBITAT Y VIVIENDA

DESPACHO DEL MINISTRO
CONSULTORÍA JURÍDICA
RESOLUCIÓN N° 032
CARACAS, 09 DE FEBRERO DE 2018
207°, 158° Y 19°

El Ministro del Poder Popular para Hábitat y Vivienda, designado mediante Decreto 3.177 de fecha 26 de noviembre de 2017, publicado en Gaceta Oficial Extraordinaria Nº 6.343 de fecha 26 de noviembre de 2017, en ejercicio de la competencia conferida en el artículo 5, numeral 2 de la Ley del Estatuto de la Función Pública, en concordancia con el artículo 78, numerales 3 y 19 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 6.147 Extraordinario de fecha 17 de noviembre de 2014, las previsiones de los artículos 5 y 21 del Decreto con Rango, Valor y Fuerza de Ley Sobre el Régimen de Jubilaciones y Pensiones de los Trabajadores y las Trabajadoras de la Administración Pública Nacional, Estadal y Municipal publicado en Gaceta Oficial N° 6.156 de fecha 19 de noviembre de 2014 y lo previsto en el artículo 12 del Instructivo que establece las Normas que regulan los Requisitos y Trámites para la Jubilación Especial de los Funcionarios y Funcionarias, Empleados y Empleadas de la Administración Pública Nacional, de los Estados y los Municipios y para los Obreros y Obreras al Servicio de la Administración Pública Nacional, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 40.510 de fecha 02 de octubre de 2014.

RESUELVE

ARTÍCULO ÚNICO: Otorgar el beneficio de **Jubilación Especial,** aprobado por el Vicepresidente Ejecutivo de la República mediante Planilla FP-026 de fecha 18/03/2016, a la ciudadana: **YENIFER ERNESTINA MACHADO**, titular de la cédula de identidad Nº **V-6.385.778**, de **Cincuenta y Siete (57)** años de edad, con Dieciocho (18) años y Ocho (8) meses de servicio prestado en la Administración Pública Nacional, siendo su último puesto desempeñado **Profesional II**, en el **Ministerio del Poder Popular para Hábitat y Vivienda,** la cual se hará efectiva a partir del Primero (01) de marzo del Dos Mil Dieciocho (2018). El monto de la Jubilación Especial es por la cantidad **DOSCIENTOS SETENTA Y UN MIL DOSCIENTOS NOVENTA Y UN BOLÍVARES CON SESENTA Y CUATRO CÉNTIMOS (Bs. 271.291,64)** mensuales, equivalente al Cuarenta y Siete Punto Cinco por Ciento (47.5%) de su remuneración promedio mensual de los últimos 12 meses y siendo homologado al salario mínimo nacional vigente.

Comuníquese y Publíquese,

Ildemaro Moisés Villarroel Arismendi
Ministro del Poder Popular para Hábitat y Vivienda

MINISTERIO DEL PODER POPULAR PARA LOS PUEBLOS INDÍGENAS

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LOS PUEBLOS INDÍGENAS
DESPACHO DE LA MINISTRA
208°, 159° y 19°

Resolución Nro.008

Caracas, 12 de marzo de 2018

La Ministra del Poder Popular para los Pueblos Indígenas, **Aloha Joselyn Núñez Gutiérrez**, titular de la cédula de identidad N° **V-16.355.466**, según Decreto Presidencial N° 3.236 de fecha 04 de enero de 2018, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 41.313 de fecha 04 de enero de 2018, conforme a las atribuciones que le confiere lo dispuesto en el artículo 65 y 78 en sus numerales 3º, 19º, 26º y 27º del Decreto Con Rango, Valor y Fuerza de la Ley Orgánica de la Administración Pública, publicada en la Gaceta Oficial Extraordinaria de la República Bolivariana de Venezuela N° 6.147, en concordancia con lo previsto en el numeral 2, del artículo 5 de la Ley del Estatuto de la Función Pública, publicada en Gaceta Oficial Nº 37.522 de fecha 06 de septiembre de 2002.

RESUELVE

ARTÍCULO 1: Se designa a el ciudadano **FERNANDO CUTUSIWA SILVA,** titular de la cédula de identidad **N° V.-13.617.199,** como **DIRECTOR GENERAL DEL TERRITORIO COMUNAL INDÍGENA RÍO, SIERRAS Y BOSQUES DE LA SELVA AMAZÓNICA (ENCARGADO),** del Ministerio del Poder Popular para los Pueblos Indígenas.

ARTÍCULO 2: El ciudadano designado ejercerá las funciones establecidas en el artículo 25 del Reglamento Orgánico dei Ministerio del Poder Popular para los Pueblos Indígenas, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.176 Extraordinaria, de fecha 20 de febrero de 2015, mediante Decreto Presidencial 1.626 de la misma fecha.

ARTICULO 3°: Se le autoriza para la firma de actos y documentos que a continuación se indican:

- Las circulares, memorandos, oficios y comunicaciones inherentes a su dirección, dirigida a las oficinas dependientes del Ministerio del Poder Popular para los Pueblos Indígenas.
- La correspondencia inherente a su dirección, dirigida a funcionarios subalternos, administrativos, judiciales, de investigación científica y policiales a nivel nacional.
- La correspondencia de cualquier naturaleza inherente a su dirección, en respuesta a solicitudes dirigidas a su despacho por los particulares.
- La certificación de la documentación correspondiente a la dirección a su cargo.

ARTICULO 4°: La presente resolución entrará en vigencia a partir de su publicación en Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y publíquese

Por el Ejecutivo Nacional

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR
PARA LOS PUEBLOS INDÍGENAS

Aloha Joselyn Núñez Gutiérrez
Ministra del Poder Popular para los Pueblos Indígenas

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LOS PUEBLOS INDÍGENAS
DESPACHO DE LA MINISTRA
208°, 159° y 19°

Resolución Nro.010

Caracas, 20 de marzo de 2018

La Ministra del Poder Popular para los Pueblos Indígenas, **Aloha Joselyn Núñez Gutiérrez,** titular de la cédula de identidad N° **V-16.355.466,** según Decreto Presidencial N° 3.236 de fecha 04 de enero de 2018, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 41.313 de fecha 04 de enero de 2018, conforme a las atribuciones que le confiere lo dispuesto en el artículo 65 y 78 en sus numerales 3º, 19º, 26º y 27º del Decreto Con Rango, Valor y Fuerza de la Ley Orgánica de la Administración Pública, publicada en la Gaceta Oficial Extraordinaria de la República Bolivariana de Venezuela N° 6.147, en concordancia con lo previsto en el numeral 2, del artículo 5 de la Ley del Estatuto de la Función Pública, publicada en Gaceta Oficial Nº 37.522 de fecha 06 de septiembre de 2002.

RESUELVE

ARTÍCULO 1: Se designa a el ciudadano **JÓSE MANUEL LARREAL,** titular de la cédula de identidad **N° V.-3.266.616,** como **DIRECTOR GENERAL DE FORMACIÓN Y EDUCACIÓN INTERCULTURAL BILINGÜE,** del Ministerio del Poder Popular para los Pueblos Indígenas**.**

ARTÍCULO 2: El ciudadano designado ejercerá las funciones establecidas en el artículo 11 del Reglamento Orgánico del Ministerio del Poder Popular para los Pueblos Indígenas, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.176 Extraordinaria, de fecha 20 de febrero de 2015, mediante Decreto Presidencial 1.626 de la misma fecha.

ARTICULO 3°: Se le autoriza para la firma de actos y documentos que a continuación se indican:

- Las circulares, memorandos, oficios y comunicaciones inherentes a su dirección, dirigida a las oficinas dependientes del Ministerio del Poder Popular para los Pueblos Indígenas.
- La correspondencia inherente a su dirección, dirigida a funcionarios subalternos, administrativos, judiciales, de investigación científica y policiales a nivel nacional.
- La correspondencia de cualquier naturaleza inherente a su dirección, en respuesta a solicitudes dirigidas a su despacho por los particulares.
- La certificación de la documentación correspondiente a la dirección a su cargo.

ARTICULO 4°: La presente resolución entrará en vigencia a partir de su publicación en Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y publíquese

Por el Ejecutivo Nacional

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR
PARA LOS PUEBLOS INDÍGENAS

Aloha Joselyn Núñez Gutiérrez
Ministra del Poder Popular para los Pueblos Indígenas

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LOS PUEBLOS INDÍGENAS
DESPACHO DE LA MINISTRA
208°, 159° y 19°

Resolución Nro.011

Caracas, 20 de marzo de 2018

La Ministra del Poder Popular para los Pueblos Indígenas, **Aloha Joselyn Núñez Gutiérrez**, titular de la cédula de identidad N° **V-16.355.466**, según Decreto Presidencial N° 3.236 de fecha 04 de enero de 2018, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 41.313 de fecha 04 de enero de 2018, conforme a las atribuciones que le confiere lo dispuesto en el artículo 65 y 78 en sus numerales 3º, 19º, 26º y 27º del Decreto Con Rango, Valor y Fuerza de la Ley Orgánica de la Administración Pública, publicada en la Gaceta Oficial Extraordinaria de la República Bolivariana de Venezuela N° 6.147, en concordancia con lo previsto en el numeral 2, del artículo 5 de la Ley del Estatuto de la Función Pública, publicada en Gaceta Oficial Nº 37.522 de fecha 06 de septiembre de 2002.

RESUELVE

ARTÍCULO 1: Se designa a el ciudadano **TITO LUCIANO POYO CASCANTE,** titular de la cédula de identidad **N° V.-5.550.679,** como **DIRECTOR GENERAL DE SABERES ANCESTRALES,** del Ministerio del Poder Popular para los Pueblos Indígenas**.**

ARTÍCULO 2: El ciudadano designado ejercerá las funciones establecidas en el artículo 12 del Reglamento Orgánico del Ministerio del Poder Popular para los Pueblos Indígenas, publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 6.176 Extraordinaria, de fecha 20 de febrero de 2015, mediante Decreto Presidencial 1.626 de la misma fecha.

ARTICULO 3°: Se le autoriza para la firma de actos y documentos que a continuación se indican:

- Las circulares, memorandos, oficios y comunicaciones inherentes a su dirección, dirigida a las oficinas dependientes del Ministerio del Poder Popular para los Pueblos Indígenas.
- La correspondencia inherente a su dirección, dirigida a funcionarios subalternos, administrativos, judiciales, de investigación científica y policiales a nivel nacional.
- La correspondencia de cualquier naturaleza inherente a su dirección, en respuesta a solicitudes dirigidas a su despacho por los particulares.
- La certificación de la documentación correspondiente a la dirección a su cargo.

ARTICULO 4°: La presente resolución entrará en vigencia a partir de su publicación en Gaceta Oficial de la República Bolivariana de Venezuela.

Comuníquese y publíquese

Por el Ejecutivo Nacional

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR
PARA LOS PUEBLOS INDÍGENAS

Aloha Joselyn Núñez Gutiérrez
Ministra del Poder Popular para los Pueblos Indígenas

CONTRALORÍA GENERAL DE LA REPÚBLICA

REPÚBLICA BOLIVARIANA DE VENEZUELA

CONTRALORÍA GENERAL DE LA REPÚBLICA

207°, 159° y 19°

Caracas, 23 de febrero de 2018.

RESOLUCIÓN

N.° 01-00-000095

MANUEL E. GALINDO B.
Contralor General de la República

En ejercicio de las atribuciones que me confiere el artículo 289 numeral 6 de la Constitución de la República Bolivariana de Venezuela, y el artículo 14, numeral 10 de la Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal, así como lo dispuesto en los artículos 4 y 26 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública.

CONSIDERANDO

Que conforme lo previsto en el artículo 290 de la Constitución de la República Bolivariana de Venezuela, la ley determinará lo relativo a la organización y funcionamiento de la Contraloría General de la República y del Sistema Nacional de Control Fiscal.

CONSIDERANDO

Que de acuerdo a las Líneas Generales del Plan de la Patria, Proyecto Nacional Simón Bolívar, Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, sancionado por la Asamblea Nacional, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N.° 6.118 Extraordinario, de fecha 04 de diciembre de 2013, en su Objetivo General 2.4.1.2 señala que es fundamental desarrollar una batalla frontal contra las diversas formas de corrupción, fortaleciendo las instituciones del Estado, fomentando la participación protagónica del Poder Popular, promoviendo la transparencia y la automatización de la gestión pública, así como los mecanismos legales de sanción penal, administrativa, civil y disciplinaria contra las lesiones o el manejo inadecuado de los fondos públicos.

RESUELVE:

PRIMERO: Designar al ciudadano **DOUGLAS RAFAEL CARVAJAL,** titular de la cédula de identidad N.° V-9.278.580, como Contralor Interventor de la Contraloría del municipio Andrés Eloy Blanco del estado Sucre, en sustitución del ciudadano **JOSÉ LUIS ROSALES MARCANO,** titular de la cédula de identidad N.° V-17.538.631, quien por razones de servicio, cesa en las funciones asignadas mediante la Resolución N.° 01-00-000152 de fecha 02 de marzo de 2017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N.° 41.132 de fecha 17 de abril de 2017. Dicha designación tendrá vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

SEGUNDO: El contralor interventor tendrá las atribuciones y deberes siguientes:

1. Exigir al contralor municipal saliente, que haga entrega de la dependencia mediante acta, de conformidad con la normativa que regula la materia.
2. Ejercer las funciones de control que la Constitución de la República Bolivariana de Venezuela, la Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal, la Ley Orgánica del Poder Público Municipal, las Ordenanzas Municipales y demás normativas le asignen a los órganos de control fiscal externo municipales.
3. Presentar al contralor general de la República:
   a) Los informes mensuales de su gestión.
   b) Un informe sobre los resultados de su gestión, dentro de los diez (10) días hábiles siguientes a la culminación de la intervención.

Dada en Caracas, a los veintitrés (23) días del mes febrero de dos mil dieciocho (2018). Año 207° de la Independencia, 159° de la Federación y 19° de la Revolución Bolivariana.

Comuníquese, notifíquese y publíquese, en la Gaceta Oficial de la República Bolivariana de Venezuela y/o en el portal web de la Contraloría General de la República www.cgr.gob.ve.

MANUEL E. GALINDO B.
Contralor General de la República

REPÚBLICA BOLIVARIANA DE VENEZUELA

CONTRALORÍA GENERAL DE LA REPÚBLICA

207°, 159° y 19°

Caracas, 02 de marzo de 2018.

RESOLUCIÓN

N.° 01-00-000141

MANUEL E. GALINDO B.
Contralor General de la República

En ejercicio de las atribuciones que me confiere el artículo 289 numeral 6 de la Constitución de la República Bolivariana de Venezuela, y el artículo 14, numeral 10 de la Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal, así como lo dispuesto en los artículos 4 y 26 del Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública.

CONSIDERANDO

Que conforme lo previsto en el artículo 290 de la Constitución de la República Bolivariana de Venezuela, la ley determinará lo relativo a la organización y funcionamiento de la Contraloría General de la República y del Sistema Nacional de Control Fiscal.

CONSIDERANDO

Que de acuerdo a las Líneas Generales del Plan de la Patria, Proyecto Nacional Simón Bolívar, Segundo Plan Socialista de Desarrollo Económico y Social de la Nación 2013-2019, sancionado por la Asamblea Nacional, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N.° 6.118 Extraordinario, de fecha 04 de diciembre de 2013, en su Objetivo General 2.4.1.2 señala que es fundamental desarrollar una batalla frontal contra las diversas formas de corrupción, fortaleciendo las instituciones del Estado, fomentando la participación protagónica del Poder Popular, promoviendo la transparencia y la automatización de la gestión pública, así como los mecanismos legales de sanción penal, administrativa, civil y disciplinaria contra las lesiones o el manejo inadecuado de los fondos públicos.

RESUELVE:

PRIMERO: Designar a la ciudadana **SONIA ENRIQUETA BITRIAGO RIVERO,** titular de la cédula de identidad N.° V-12.504.221, como Contralora Interventora de la Contraloría del municipio Aragua del estado Anzoátegui, en sustitución del ciudadano **YENNER JOSÉ AMARAL CARMONA,** titular de la cédula de identidad N.° V-16.480.658, quien por razones de servicio, cesa en las funciones asignadas mediante la Resolución N.° 01-00-000152 de fecha 02 de marzo de 2017, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N.° 41.132 de fecha 17 de abril de 2017. Dicha designación tendrá vigencia a partir de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

SEGUNDO: La contralora interventora tendrá las atribuciones y deberes siguientes:

1. Exigir al contralor municipal saliente, que haga entrega de la dependencia mediante acta, de conformidad con la normativa que regula la materia.
2. Ejercer las funciones de control que la Constitución de la República Bolivariana de Venezuela, la Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal, la Ley Orgánica del Poder Público Municipal, las Ordenanzas Municipales y demás normativas le asignen a los órganos de control fiscal externo municipales.
3. Presentar al contralor general de la República:
   a) Los informes mensuales de su gestión.
   b) Un informe sobre los resultados de su gestión, dentro de los diez (10) días hábiles siguientes a la culminación de la intervención.

Dada en Caracas, a los dos (02) días del mes marzo de dos mil dieciocho (2018). Año 207° de la Independencia, 159° de la Federación y 19° de la Revolución Bolivariana.

Comuníquese, notifíquese y publíquese, en la Gaceta Oficial de la República Bolivariana de Venezuela y/o en el portal web de la Contraloría General de la República www.cgr.gob.ve.

MANUEL E. GALINDO B.
Contralor General de la República

GACETA OFICIAL
DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

DEPÓSITO LEGAL: ppo 187207DF1

AÑO CXLV - MES VI Número 41.365

Caracas, miércoles 21 de marzo de 2018

Esquina Urapal, edificio Dimase, La Candelaria
Caracas – Venezuela

Tarifa sujeta a publicación de fecha 14 de noviembre de 2003 en la Gaceta Oficial Nº 37.818
http://www.minci.gob.ve

Esta Gaceta contiene 48 páginas, costo equivalente a 19,65 % valor Unidad Tributaria

DEFENSORÍA DEL PUEBLO

REPÚBLICA BOLIVARIANA DE VENEZUELA
DEFENSORÍA DEL PUEBLO
DESPACHO DEL DEFENSOR DEL PUEBLO

CARACAS, 19 DE MARZO DE 2018
207° y 159°
RESOLUCIÓN Nº DdP-2018-010

ALFREDO JOSÉ RUIZ ANGULO, venezolano, mayor de edad, titular de la cédula de identidad Nº V-6.444.336, Defensor del Pueblo de la República Bolivariana de Venezuela, en ejercicio del cargo desde el 05 de agosto de 2017, según consta en Gaceta Oficial de la República Bolivariana de Venezuela Nº 41.212 de fecha 11 de agosto de 2017, conforme a lo dispuesto en el numeral 4º del artículo 33 de la Ley Orgánica de la Defensoría del Pueblo, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.995 de fecha 05 de agosto de 2004, ratificado en el cargo por la Asamblea Nacional Constituyente de la República Bolivariana de Venezuela, en fecha 17 de agosto de 2017, según consta en Gaceta Oficial de la República Bolivariana de Venezuela N° 41.216, de fecha 17 de agosto de 2017, actuando de conformidad con el artículo 280 de la Constitución de la República Bolivariana de Venezuela, así como en ejercicio de las atribuciones conferidas por el artículo 29 numeral 19 de la Ley Orgánica de la Defensoría del Pueblo, en concordancia con los artículos 11, 66 y 67 del Estatuto de Personal de la Defensoría del Pueblo, contenido en la Resolución N° DdP-2016-048, de fecha 03 de agosto de 2016, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 40.959 del día 04 de agosto de 2016.

RESUELVE:

Designar a la ciudadana **DIANORKA RITA MALAVÉ MORAO**, titular de la cédula de identidad N° **V-14.768.746**, como Defensora Delegada del estado Vargas de la Defensoría del Pueblo de la República Bolivariana de Venezuela, desde el 19 de marzo de 2018, en calidad de encargada, por comisión de servicio.

Comuníquese y Publíquese,

ALFREDO JOSÉ RUIZ ANGULO
DEFENSOR DEL PUEBLO