PROPUESTA TÉCNICA
CONSORCIO “CEDULA 4.0 RD”

PARA EL PROCESO DESTINADO A LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA NUEVA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI) DE REF.: JCE-CCC-LPI-2024-0001.

Junta Central Electoral
Garantía de Identidad y Democracia

Cliente: Junta Central Electoral

Las informaciones citadas en esta propuesta son de carácter confidencial para uso exclusivo de la JCE y el consorcio 4.0 R.D

Contenido

RESUMEN EJECUTIVO 7

PRESENTACIÓN DEL CONSORCIO 8

ALCANCE GEOGRÁFICO DE LA INFRAESTRUCTURA DE SERVICIOS QUE OPERARÁ EL FABRICANTE DE LA IMPRESORA 9

BENEFICIOS INMEDIATOS PARA LA JUNTA CENTRAL ELECTORAL (JCE) CON LA IMPLEMENTACIÓN DE LA SOLUCIÓN DEL CONSORCIO CÉDULA 4.0 RD 11

CREDENCIALES DE MIEMBROS DEL CONSORCIO CEDULA 4.0 RD 13

VISIÓN DEL PROYECTO, SUGERENCIAS Y RECOMENDACIONES 14

ESPECIFICACIONES TÉCNICAS GENERALES 18

EQUIPAMIENTO PARA LA EMISIÓN DE CÉDULAS 19

INFRAESTRUCTURA PKI – CA 19

CAPACITACIÓN PARA PERSONAL DE LA JCE 19

SEGURIDAD Y PROTECCIÓN DE DATOS 19

ÍTEM I - ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS 21

1. ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS 22

1.1 INTRODUCCIÓN 22

1.1.1 DISEÑO Y PRODUCCIÓN 22

1.1.1.1 IMPRESOR DE ALTA SEGURIDAD 22

1.1.1.2 FABRICACIÓN DE TARJETAS SOBRE DIVERSOS MATERIALES 23

1.1.1.3 CALIDAD Y RESPETO MEDIOAMBIENTAL 23

1.1.2 COMPONENTES ELECTRÓNICOS, SISTEMAS OPERATIVOS Y APLICACIONES 25

1.1.2.1 SEGURIDAD DE LOS COMPONENTES 25

1.1.2.2 TARJETAS ELECTRÓNICAS, INLAYS, E-STICKERS, E-COVERS 25

1.1.3 CERTIFICACIONES 26

1.1.3.1 ISO 9001, 14001, 27001 26

1.1.3.2 ISO 14298:2013 27

1.2 PROCESO DE FABRICACIÓN DE TARJETA 28

1.2.1 DISEÑO / ESTUDIO 28

1.2.2 PRUEBA DE COLOR 29

1.2.3 IMPRESIÓN 29

1.2.3.1 IMPRESIÓN EN OFFSET 29

1.2.3.2 IMPRESIÓN SERIGRÁFICA 31

1.2.4 ENSAMBLADO 31

1.2.5 LAMINADO 32
1.2.6 CORTE 33
1.2.7 PRE PERSONALIZACIÓN 34
1.2.7.1 ELÉCTRICA 34
1.2.7.2 GRÁFICA 34
1.2.8 CONTROL DE CALIDAD 35
1.2.9 EMBALAJE Y ALMACENAMIENTO 35
1.2.10 ENVÍO 36
1.2.11 DESTRUCCIÓN DE LOS PRODUCTOS SENSIBLES 37
1.3 PROPUESTA TARJETAS DE POLICARBONATO 38
1.3.1 LA TARJETA EN POLICARBONATO 38
1.3.1.1 CUERPO DE LA TARJETA 38
1.3.1.2 ESTRUCTURA DE LA TARJETA 39
1.3.2 TARJETA CON CHIP SIN CONTACTO 40
1.3.3 MIDDLEWARE 44
1.3.4 PERSONALIZACIÓN GRÁFICA 47
1.3.5 IMPRESIÓN DE SEGURIDAD 47
1.3.5.1 CERTIFICACIÓN PARA IMPRESORES DE SEGURIDAD 48
1.3.5.2 CREACIÓN DE UN DISEÑO GRÁFICO SEGURO 48
1.3.6 ELEMENTOS DE SEGURIDAD 49
1.3.6.1 NIVEL DE SEGURIDAD 50
1.3.6.2 IMPRESIÓN DE SEGURIDAD 50
1.3.6.2.1 GUILLOCHES 51
1.3.6.2.2 IMPRESIÓN EN ARCOÍRIS 52
1.3.6.2.3 MICROLÍNEAS DE AMPLITUD VARIABLE 53
1.3.6.2.4 MICROTEXTOS (POSITIVOS Y NEGATIVOS) 54
1.3.6.2.5 ERRORES DELIBERADOS 55
1.3.6.2.6 FONDOS NUMISMÁTICOS 56
1.3.6.3 TINTAS UV INVISIBLES 57
1.3.6.3.1 GUILLOCHES EN UV 58
1.3.6.3.2 MICROTEXTOS EN UV 58
1.3.6.3.3 ARCOIRIS EN UV 58
1.3.6.3.4 UV MALLA DE FONDO EN MICROTEXTO 58

1.3.6.4 TINTA ÓPTICAMENTE VARIABLE (OVI) 59
1.3.6.5 ELEMENTOS HOLOGRÁFICOS 60
1.3.6.6 ELEMENTOS TÁCTILES / RELIEVE SUPERFICIAL POSITIVO O NEGATIVO 61
1.3.6.7 MLI / CLI 63
1.3.6.8 VENTANA TRANSPARENTE 64
1.3.6.9 TINTAS INFRARROJAS ABSORBENTES/TRANSPARENTES 65
1.3.6.10 OTROS ELEMENTOS DE SEGURIDAD 66
ÍTEM II - ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN 67
2. ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN LASER 68
2.1 BENEFICIOS DE LA SOLUCIÓN 69
2.2 CRITERIOS DE DESEMPEÑO ÚNICOS 70
2.3 MÓDULO LASER CLM600 71
2.4 CARACTERÍSTICAS ADICIONALES 73
2.5 MÓDULO OPCIONAL PARA IMPRESIÓN A COLOR GET CP500 74
2.6 CONDICIONES DE GARANTÍA 75
GARANTÍA: 75
ÍTEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI - CA 78
3.1 GET TRUST – SOLUCIÓN DE PKI 79
3.1.1 ARQUITECTURA DEL SOFTWARE 79
3.2 GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA 80
3.3 FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER) 90
3.4 PKI CIUDADANA – PKI SUBORDINADA X509 92
3.5 INFRAESTRUCTURA GET TRUST 93
3.5.1 CARACTERÍSTICAS CLAVES 93
3.6 MÓDULO DE SEGURIDAD POR HARDWARE (HSM) 94
ÍTEM IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL 97
4.1 INTRODUCCIÓN - GET MOBILE ID 98
4.1.1 GET MOBILE ID 98
4.1.2 GET MOBILE ADMINISTRATOR 98
4.2 GET MOBILE ID – COMPONENTES 99
4.2.1 GET MOBILE ADMINISTRATOR 99
4.2.1.1 OPCIONES DE INTEGRACIÓN: 100
4.2.1.2 OPCIONES DE FIRMADO DIGITAL 102

4.2.1.3 MODELO DE DATOS Y CODIFICACIÓN. 103
4.2.1.4 PROCEDIMIENTO DE ACTIVACIÓN 103
4.2.2 GET MOBILE ID – APLICACIÓN MÓVIL 106
4.2.2.1 OPCIONES DE PERSONALIZACIÓN 107
4.2.2.2 CONTROL TOTAL Y PROTECCIÓN DE LA PRIVACIDAD 108
4.2.2.3 SIEMPRE ACTUALIZADO 109
4.2.2.4 INTEROPERABILIDAD 109
4.2.3 GET MOBILE VERIFIER 109
4.2.3.1 MODOS DE INTERACCIÓN 112
4.2.4 Herramientas de Desarrollo 113
4.2.5 INFRAESTRUCTURA 113
4.2.5.1 ARQUITECTURA DE ALTA DISPONIBILIDAD 113
4.2.5.2 DISPONIBILIDAD DEL 99.95% DE OPERACIÓN 115
ÍTEM V- KIT PERIFERICOS 116
ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO 127
6 PLAN DE MANTENIMIENTO PARA IMPRESORAS Y PERIFERICOS 128
6.1 PLAN DE MANTENIMIENTO PARA PKI 130
6.1.3 MODELOS DE SERVICIO Y SLA 130
6.1.4 SLA Y TIEMPOS DE RESPUESTA 131
6.1.5 PROCEDIMIENTO PARA LA APERTURA DE INCIDENTES POR PARTE DE LA JCE 132
6.3 MANTENIMIENTO PREVENTIVO Y CORRECTIVO 134
6.4 SEGURIDAD Y CUMPLIMIENTO 135
6.5 KPIS Y MÉTRICAS DE RENDIMIENTO 135
6.6 PLAN DE MANTENIMIENTO PARA TARJETA DIGITAL 136
6.6.1 INTRODUCCIÓN 136
6.6.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA 136
6.6.3 MODELOS DE SERVICIO Y SLA 136
6.7 MANTENIMIENTO PREVENTIVO Y CORRECTIVO 138
6.7.1 ACTIVIDADES PERIÓDICAS 138
6.7.2 ACTIVIDADES DE MANTENIMIENTO PREVENTIVO 139
6.7.3 ACTIVIDADES DE RESPUESTA A INCIDENTES 139
6.7.4 MANTENIMIENTO CORRECTIVO 139
6.8 SEGURIDAD Y CUMPLIMIENTO 139

6.9 KPIS Y MÉTRICAS DE RENDIMIENTO 141
6.10 INVENTARIO 141
ÍTEM VII - CAPACITACIÓN 142
7. PLAN DE CAPACITACIÓN PARA IMPRESORAS 143
7.1 ENTRENAMIENTOS 143
7.11 PLAN DE CAPACITACION PARA PKI 145
7.11.1 CONTENIDO 145
7.11.2 METODOLOGÍA 145
7.11.3 DESCRIPCIÓN 145
7.12 PLAN DE CAPACITACION PARA TARJETA DIGITAL 151
7.12.1 CONTENIDO 151
7.12.2 METODOLOGÍA 151
7.12.3 DESCRIPCIÓN 151
VIII- OTRAS CONDICIONES 154
8. PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) 154
8.1 OBJETIVO DEL PLAN 154
8.2 2. ALCANCE 154
8.3 ANÁLISIS DE RIESGOS 154
8.4 ESTRATEGIAS DE CONTINUIDAD 155
8.4.1 INFRAESTRUCTURA DE RESPALDO: 155
8.4.2 PROTOCOLOS DE RESPALDO DE INFORMACIÓN: 155
8.4.3 GESTIÓN DE PROVEEDORES ESTRATÉGICOS: 155
8.4.4 PLAN DE RECUPERACIÓN ANTE CRISIS: 155
8.5 PROCEDIMIENTOS DE RESPUESTA Y RECUPERACIÓN 155
8.6 REQUISITOS DE PRODUCCIÓN Y TIEMPOS DE ENTREGA 157
8.7 INFRAESTRUCTURA DE PRODUCCIÓN Y UBICACIÓN DE LAS FÁBRICAS 157
8.9 CRONOGRAMA GENERAL DE PRODUCCIÓN Y ENTREGA 158
8.10 CRONOGRAMA DE TRABAJO 158

RESUMEN EJECUTIVO

La Junta Central Electoral (JCE) mediante la convocatoria de la presente Licitación Pública Internacional con el objetivo de modernizar el sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) en la República Dominicana. Esta licitación busca la contratación de una empresa que suministre los equipos, materiales y servicios requeridos para garantizar un sistema de identificación seguro, eficiente y tecnológicamente avanzado.

En respuesta a esta convocatoria, se presenta una solución integral que cumple con los requerimientos técnicos, operativos y de seguridad exigidos en el pliego de condiciones. Nuestro enfoque está basado en la experiencia y capacidad de un equipo altamente especializado, garantizando un sistema confiable y escalable para la JCE.

La propuesta ofrece una serie de beneficios estratégicos para la JCE, alineados con su visión de modernización e innovación:

- Optimización en la emisión de cédulas, reduciendo tiempos y costos operativos.
- Mayor seguridad y confiabilidad, con tecnologías de protección contra fraudes y falsificaciones.
- Interoperabilidad con sistemas gubernamentales, facilitando la integración con otras plataformas digitales.
- Infraestructura de soporte técnico en República Dominicana, EE. UU. y Europa, garantizando mantenimiento y servicio especializado.
- Sostenibilidad operativa, con una red de distribución y mantenimiento ya establecida.

Para la ejecución de este proyecto, el consorcio cuenta con una amplia trayectoria en la implementación de soluciones de identidad seguras a nivel global. Su experiencia abarca la fabricación, integración y operación de sistemas de identificación, garantizando el cumplimiento de los más altos estándares de seguridad y confiabilidad.

A través de esta propuesta, se garantiza la viabilidad y sostenibilidad del proyecto, respaldado por un equipo altamente capacitado y una infraestructura tecnológica de primer nivel.

PRESENTACIÓN DEL CONSORCIO

La Junta Central Electoral (JCE), a través de la presente licitación, busca adquirir una solución integral para la gestión de las cédulas de identidad en la República Dominicana. Esta iniciativa contempla la implementación de una infraestructura avanzada para la emisión de cédulas físicas y digitales, incorporando tarjetas de policarbonato con impresión láser, periféricos modernos y una plataforma PKI – CA que garantice autenticación y seguridad en el acceso a los servicios de identificación.

Para dar respuesta a esta necesidad, el Consorcio Cédula 4.0 RD fue conformado bajo el liderazgo de Copy Solutions International S.A. (CSI), con el objetivo de proporcionar una solución robusta, eficiente y alineada con los estándares tecnológicos y de seguridad establecidos por la JCE.

El Consorcio Cédula 4.0 RD está conformado por seis empresas de reconocimiento internacional, especializadas en la fabricación, integración y operación de sistemas de identificación. Gracias a esta estructura, la solución propuesta abarca desde la producción de credenciales seguras hasta la implementación de plataformas digitales para la gestión de identidad.

Las empresas que conforman el consorcio son:

- **Copy Solutions International S.A. (CSI) –** responsable principal del contrato y con capacidad instalada en la República Dominicana para la logística y operación del servicio.
- **Grupo Get Group:**
  - **GET International FZCO –** Especialista en tecnología de identidad y seguridad digital con experiencia en soluciones de autenticación y verificación de identidad.
  - **GET Group Latin America S.A. –** Enfocada en el desarrollo de plataformas para la emisión de documentos de identidad, pasaportes electrónicos y sistemas biométricos.
  - **GET Secure ID Corp. –** Dedicada a la fabricación de tarjetas de policarbonato con impresión láser y elementos de seguridad de alta resistencia.
  - **Global Enterprise Technologies Corp. –** Proveedor de tecnología y soluciones integradas para la personalización de documentos y autenticación digital.
- **SELP S.A.S. –** Especialista en la producción de documentos de identidad, con experiencia en impresión de alta seguridad y gestión de credenciales.

Cada una de estas empresas aporta su conocimiento en áreas específicas, garantizando una solución sólida, confiable y preparada para responder a los desafíos operativos y de seguridad de la JCE.

ALCANCE GEOGRÁFICO DE LA INFRAESTRUCTURA DE SERVICIOS QUE OPERARÁ EL FABRICANTE DE LA IMPRESORA

La cobertura de apoyo de servicios de CSI abarca, en la actualidad, el **100%** de las Provincias de RD.

PROVINCIAS					
1- Azua	7- Elías Piña	13- Monseñor	19- Romana, La	25- San Juan de la Maguana	31- Valverde
2- Bahoruco	8- Espaillat	14- Montecristi	20- Her. Mirabal	26- San Pedro de Macorís	32- La Vega
3- Barahona	9- Hato Mayor	15- Monte Plata	21- Samaná	27- Santiago	
4- Dajabón	10- Independencia	16- Pedernales	22- San Cristóbal	28- Santiago Rodríguez	
5- Distrito nacional	11- Altagracia, La	17- Peravia	23- Sánchez Ramírez	29- Santo Domingo	
6- Duarte	12- María Trinidad	18- Puerto Plata	24- Ocoa	30- Seibo, El Seibo	

Clientes Actuales	Ubicacion Geografica del Clientes de Impresoras suplidas por CSI donde se cubre el servicio y soporte técnico en la actualidad EN Republica Dominicana																														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Edenorte Dominicana																																
Banco BHD	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Asociación La Nacional de Ahorros y Prestamos				✓	✓	✓	✓	✓	✓		✓	✓		✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Grupo CID	✓				✓										✓							✓					✓		✓			
Banco Promerica					✓						✓		✓						✓						✓		✓		✓			✓
Banco multiple Caribe				✓	✓						✓			✓				✓								✓	✓		✓			
Farmaco Quimico Nacional					✓			✓			✓						✓	✓	✓							✓			✓			
Fenwal International																						✓										
Banco Union de Ahorro y Credito	✓		✓		✓			✓				✓		✓			✓		✓						✓	✓	✓					
Hotelera Bavaro											✓																					
Grupo Propagas																													✓			
Grupo Marti					✓																											
La Aurora (Grupo Leon Jimenes)											✓																					
Grupo SIM											✓																					
Punta Cana Holding (Secret)					✓													✓								✓			✓			
Print City																																
Grupo Ambar(Santo Domingo Motors)					✓								✓																✓			
DP World Caucedo																													✓			
Grupo JMMB					✓						✓																		✓			
Grupo Viamar				✓							✓															✓			✓			
Junta Central Electoral	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Procuraduria general de la Rep. Dominicana	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Senasa	✓	✓			✓			✓			✓	✓		✓				✓			✓						✓		✓			✓
Promipyme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mitur				✓																												
Registro Inmobiliario					✓																								✓			
Medio Ambiente	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Camara de Diputados de la Rep Dom					✓																											
Senado de la Republica Dominicana					✓																											

CSI cuenta con más de 2,000 clientes de impresoras con tecnología láser en la RD y el desplazamiento a brindar el servicio de soporte técnico a sus localidades es tan común, que lo venimos sirviendo desde hace más de 20 años.

En la documentación adjunta detallamos un ejemplo de la infraestructura que disponemos en la actualidad. Lista muy distinguida en la que todos los meses se incluyen nuevas instalaciones

Nuestra presencia en el territorio nacional con seis (6) oficinas y una próxima en Azua, nos posiciona como el principal suplidor de soluciones tecnológicas en equipos de impresión y sistemas llave en

mano en la República Dominicana. Esto nos permite ofrecer el mejor tiempo de respuesta en servicio a nuestros clientes.

Cualquier otra oferta disponible actualmente está diseñada para brindar soporte exclusivamente desde el Distrito Nacional. Para ser realmente comparable, nuevas propuestas de servicio tendrían que replicar una plataforma de atención similar a la de CSI.

A continuación, se desglosa la distribución de nuestros clientes en el territorio nacional en relación con nuestras oficinas operativas, asegurando una cobertura eficiente y tiempos de respuesta óptimos para nuestros servicios.

BENEFICIOS INMEDIATOS PARA LA JUNTA CENTRAL ELECTORAL (JCE) CON LA IMPLEMENTACIÓN DE LA SOLUCIÓN DEL CONSORCIO CÉDULA 4.0 RD

- **Optimización en la emisión de cédulas:** La integración de un sistema holístico permite agilizar el proceso de emisión y renovación de cédulas, reduciendo tiempos y costos operativos.

- **Actualización tecnológica:** La incorporación de tecnología de vanguardia, como la impresión láser y plataformas digitales, asegura la modernización del sistema de identidad.

- **Mayor seguridad y confiabilidad:** La infraestructura robusta, que incluye una plataforma PKI – CA, fortalece la integridad de los datos y la autenticidad de las cédulas, generando mayor confianza en la ciudadanía.

- **Soporte técnico especializado en RD:** Con la red de instalada de soporte técnico de CSI a cargo del Fabricante para operar el mantenimiento, se garantiza un soporte técnico continuo y un mantenimiento eficiente, asegurando la operatividad de la plataforma al nivel más avanzado en SLAs.
- **Soporte técnico especializado en EEUU:** Con la red de instalada de soporte técnico de Get Group, miembro del consorcio CEDULA 4.0 RD y fabricante de la solución de impresoras, hoy suple servicios similares de soporte y mantenimiento al proyecto de Pasaportes de los EEUU desde las ciudades principales, se garantiza un soporte técnico continuo y un mantenimiento eficiente, al parque de impresión de la plataforma en ese país.

- **Soporte técnico especializado en Madrid:** Desde las oficinas de SELP en Madrid C/ Cronos 63,4-4 28037 Madrid, España. miembro del consorcio CEDULA 4.0 RD y suplidor de las tarjetas de Policarbonato, se centralizarán los servicios de soporte y mantenimiento a requerimientos de las impresoras del proyecto de la JCE en Europa.

- **Interoperabilidad con otros sistemas:** La solución digital facilita la integración con otras plataformas y sistemas gubernamentales, promoviendo la eficiencia en la gestión interinstitucional.

- **Reducción de riesgos operativos:** La experiencia y solvencia de las empresas integradas en el consorcio minimizan riesgos, asegurando la continuidad del servicio y la confiabilidad del proceso.

- **Optimización logística:** La amplia infraestructura de soporte y mantenimiento al usuario de la JCE de impresoras Láser será operado por el fabricante de las impresoras, tanto en la Republica Dominicana, en EE. UU. como España garantizando la atención oportuna y el soporte de los equipos y a sus usuarios sin necesidad de implementar e improvisar para el proyecto una infraestructura nueva en ninguna localidad.

- **Mejora en la atención a la ciudadanía:** Un sistema moderno, seguro y eficiente contribuye a elevar la calidad del servicio ofrecido a los ciudadanos, mejorando la imagen institucional de la JCE.
- **Opción de COLOR con impresión Laser en Policarbonato:** Nuestra propuesta contempla la capacidad de incorporar módulo de impresión a color de la fotografía para una combinación de impresión de tintas de pigmento solido e impresión laser utilizando la tecnología de imagen híbrida *LASMENT mediante impresión por re-transferencia* segura con grabado láser, logrando una característica única de personalización a color en tarjetas de policarbonato. El contar con esta opción le permitirá a la JCE redoblar la seguridad en el documento mientras se eleva la seguridad y calidad de este a estándares antes no vistos.

CREDENCIALES DE MIEMBROS DEL CONSORCIO CEDULA 4.0 RD

VISIÓN DEL PROYECTO, SUGERENCIAS Y RECOMENDACIONES

VISIÓN DEL PROYECTO

La modernización del sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) en la República Dominicana responde a la creciente necesidad de un sistema de identidad seguro, eficiente e integrado con las nuevas tecnologías digitales. Esta transformación no solo es una evolución técnica, sino una respuesta a las dinámicas económicas y demográficas del país, que han incrementado la demanda de servicios de identificación y digitalización de procesos gubernamentales.

En las últimas décadas, la República Dominicana ha experimentado un crecimiento sostenido en su población, lo que ha generado una mayor presión sobre los sistemas de emisión de documentos de identidad. A esto se suma la expansión económica del país, con un crecimiento del PIB proyectado entre 4.5% y 5.0% para 2025, impulsado por el turismo, la inversión pública y el fortalecimiento del sector financiero.

Adicionalmente, el auge del turismo y la migración internacional ha elevado la necesidad de sistemas de identificación modernos, interoperables y seguros. Con ingresos turísticos que superan los 10,000 millones de dólares anuales, la República Dominicana se consolida como un hub internacional, albergando a ciudadanos de diversas nacionalidades que requieren servicios automatizados y verificación de identidad en múltiples sectores.

En este contexto, el Consorcio Cédula 4.0 RD presenta una solución que va más allá del cumplimiento de los requisitos del Pliego de Condiciones. Nuestra propuesta se fundamenta en las mejores prácticas internacionales en gestión de identidad, combinando seguridad, eficiencia operativa y facilidad de uso para los ciudadanos.

La implementación de este sistema permitirá a la JCE gestionar la identidad nacional con los más altos estándares de seguridad, interoperabilidad y escalabilidad. A través de la impresión láser en policarbonato, la autenticación digital y un esquema de soporte técnico integral, garantizamos un servicio sin interrupciones, adaptable al crecimiento del país y preparado para la evolución de los servicios digitales en el futuro.

SUGERENCIAS PARA LA IMPLEMENTACIÓN

La modernización del sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) no solo debe responder a exigencias tecnológicas y de seguridad, sino también a las necesidades operativas reales de la Junta Central Electoral (JCE). La estabilidad y eficiencia del servicio dependen de factores estratégicos que van más allá del pedigrí y la experiencia internacional de los proveedores, incorporando factores críticos como la infraestructura nacional, la capacidad de respuesta local y la continuidad operativa garantizada.

En este sentido, el Consorcio Cédula 4.0 RD cuenta con una ventaja diferenciadora clave: la participación de un proveedor local con 21 años de experiencia en servicios tecnológicos y operativos en el país, de los cuales más de la mitad han sido en servicio directo a la JCE. Esta trayectoria no solo respalda la capacidad técnica del consorcio, sino que también aporta un conocimiento profundo de la realidad operativa dominicana, permitiendo la optimización de recursos, reducción de riesgos y una implementación eficiente.

Algunos de los factores clave que garantizan el éxito de la implementación incluyen:

Experiencia operativa comprobada en la JCE: Con más de 10 años de servicio directo a la institución, el proveedor local ha gestionado y mantenido infraestructura crítica para la emisión de documentos de identidad, asegurando continuidad operativa y eficiencia.

Infraestructura de soporte en todo el país: La cobertura a nivel nacional de los servicios técnicos permite una respuesta rápida y eficiente ante cualquier eventualidad, asegurando tiempos mínimos de inactividad.

Estabilidad eléctrica y conectividad garantizada: La infraestructura propuesta toma en cuenta la realidad energética y de telecomunicaciones de la República Dominicana, con planes de contingencia que minimizan el impacto de interrupciones en el servicio.

Capacidades de respuesta inmediata: Gracias a un esquema de reporte diario y monitoreo en tiempo real, la solución garantiza una evaluación constante de la operación, facilitando la identificación y resolución inmediata de cualquier incidencia.

ESTRATEGIAS PARA UNA IMPLEMENTACIÓN EFICIENTE

Para garantizar una transición fluida y sin interrupciones, el Consorcio Cédula 4.0 RD propone una estrategia de implementación escalonada, asegurando la correcta integración de los sistemas y la optimización del servicio.

Fase Piloto: Implementación inicial en una región específica para validar la interoperabilidad de los sistemas, identificar posibles mejoras y ajustar procesos antes de la implementación a nivel nacional.

Capacitación Especializada: Formación a los operadores y técnicos de la JCE sobre el manejo del nuevo sistema, combinando sesiones presenciales y virtuales, acompañadas de documentación técnica completa.

Integración con Otros Sistemas Gubernamentales: Implementación de interfaces de comunicación que permitan la validación en tiempo real de los datos de identidad con otras instituciones estatales, promoviendo la interoperabilidad del sistema.

Estrategia de Respaldo y Continuidad Operativa: Desarrollo de un esquema de redundancia y contingencia, asegurando la operatividad ininterrumpida del sistema ante cualquier evento imprevisto.

RECOMENDACIONES PARA LA JCE

Para maximizar la eficiencia y sostenibilidad del sistema, recomendamos:

Priorización de proveedores con experiencia operativa local comprobada: La experiencia internacional es importante, pero no suficiente cuando se trata de la continuidad operativa de la JCE. La gestión de un sistema de identificación nacional *requiere proveedores* que no solo cumplan con los estándares técnicos, sino que también comprendan las condiciones reales del país. Seleccionar proveedores con infraestructura local establecida y una trayectoria de servicio comprobada evita sobrecostos en adaptaciones, logística y gestión operativa.

Integración de capacidades nacionales para garantizar eficiencia y sostenibilidad: El éxito de la implementación no solo depende de la tecnología instalada, sino también de la capacidad operativa para sostenerla en el tiempo. Aprovechar la experiencia acumulada en el país reduce riesgos, optimiza costos y garantiza la adaptación del sistema a la demanda real de la JCE sin necesidad de inversiones adicionales en infraestructura de soporte.

Evitar proveedores que impliquen costos adicionales de implementación: Seleccionar un proveedor sin presencia establecida en el país podría significar inversiones adicionales en infraestructura, personal de soporte y contingencias operativas. Apostar por un modelo ya probado en la JCE y con capacidad instalada permite reducir el riesgo de fallas en la implementación, evitando gastos innecesarios y garantizando un servicio operativo desde el primer día.

Entrega de un producto final sobresaliente y sostenible: Además de cumplir con los requerimientos técnicos y operativos, el producto final debe representar un salto cualitativo en la identidad digital del país. La implementación de una cédula moderna, con capacidades digitales avanzadas, mecanismos de autenticación segura y opciones de interoperabilidad con otros servicios gubernamentales garantizará un sistema sostenible a largo plazo. La elección de un proveedor con experiencia local permite maximizar la eficiencia en este proceso, asegurando una implementación sin fricciones y con mejoras escalables en el tiempo.

Adopción de la Infraestructura de Seguridad PKI: La integración de la Plataforma de Infraestructura de Claves Públicas (PKI – CA) permitirá la firma digital y autenticación segura de documentos e identidades electrónicas, alineándose con estándares internacionales. Este sistema garantizará mayor seguridad en la identidad digital, reduciendo riesgos de fraude y facilitando la interoperabilidad con servicios gubernamentales y privados.

Optimización de Procesos de Emisión: Implementar medidas para reducir los tiempos de emisión y renovación de documentos, mejorando la experiencia del ciudadano y garantizando procesos más ágiles y eficientes. La reducción de tiempos de espera y la implementación de tecnologías que automaticen los procedimientos serán clave para aumentar la satisfacción del usuario final.

Mantenimiento Preventivo y Correctivo: Aplicar un plan de mantenimiento programado que garantice la disponibilidad y óptimo funcionamiento de los equipos de impresión y autenticación digital. Un mantenimiento preventivo estructurado minimizará tiempos de inactividad y reducirá costos operativos, asegurando que la infraestructura se mantenga en condiciones óptimas a largo plazo.

ESPECIFICACIONES TÉCNICAS GENERALES

La implementación del nuevo sistema de emisión de la Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) representa una transformación clave en la gestión de identidad en la República Dominicana. Más allá de la simple modernización tecnológica, esta iniciativa debe garantizar una transición fluida, una operación ininterrumpida y un servicio ágil para los ciudadanos, minimizando riesgos y optimizando los recursos disponibles.

Este desafío no solo implica la adopción de tecnologías de última generación, sino también la integración efectiva con la infraestructura existente de la Junta Central Electoral (JCE). La propuesta del Consorcio Cédula 4.0 RD ha sido diseñada para ofrecer una solución adaptable, sostenible y alineada con las necesidades operativas reales, asegurando que la implementación no afecte la continuidad del servicio ni genere costos adicionales imprevistos.

Nuestra solución está diseñada para cumplir con los más altos estándares de seguridad, interoperabilidad y eficiencia operativa, garantizando:

- Un sistema robusto y escalable, capaz de responder a la demanda actual y futura de emisión de documentos de identidad.
- Automatización y optimización de procesos, reduciendo tiempos de emisión y mejorando la experiencia del ciudadano.
- Interoperabilidad con otros sistemas gubernamentales, facilitando la validación en tiempo real de los datos de identidad.
- Estrategias de contingencia y respaldo operativo, asegurando la continuidad del servicio ante cualquier eventualidad.

El Consorcio Cédula 4.0 RD presenta una solución efectiva y probada, con una ejecución estructurada que prioriza la estabilidad del sistema y el cumplimiento de los entregables exigidos en el Pliego de Condiciones Específicas, garantizando así un sistema de identidad seguro, eficiente y preparado para el futuro.

CUMPLIMIENTO DE NORMATIVAS Y ESTÁNDARES INTERNACIONALES

El sistema propuesto cumple con las siguientes normativas:

NORMAS DE IDENTIFICACIÓN Y SEGURIDAD

- OACI Doc 9303 – Normativa internacional para documentos de viaje electrónicos.
- ISO/IEC 14443 A y B – Tarjetas de proximidad sin contacto.
  CWA 15374 y CWA 14641 – Documentos de seguridad e identidad digital.

NORMAS DE SEGURIDAD DE LA INFORMACIÓN

- ISO 27001 – Seguridad de la información en sistemas de identidad.
- ISO 14298 – Seguridad en la impresión de documentos de alta sensibilidad.

NORMAS DE PRODUCCIÓN Y CALIDAD

- ISO 9001 – Gestión de calidad en la producción y personalización.
- ISO 14001 – Sostenibilidad y reducción de impacto ambiental.

ENTREGABLES Y CANTIDADES EXIGIDAS

A continuación, se presentan los entregables en cantidad, de acuerdo con los requisitos del Pliego de Condiciones Específicas:

- Producción y Personalización de Cédulas
- **Cantidad total de tarjetas a emitir**: 8 millones de cédulas en un período de 18 meses.
- **Material:** Policarbonato multicapa con grabado láser.
  Chip sin contacto: Compatible con autenticación biométrica y validación PKI.

EQUIPAMIENTO PARA LA EMISIÓN DE CÉDULAS

- **Impresoras láser de personalización**: Cantidad requerida según demanda nacional.
- **Sistemas de captura biométrica:** Con capacidad de integración en centros de emisión.
- **Servidores y software de gestión:** Infraestructura optimizada para emisión, almacenamiento y validación de datos de identidad.

INFRAESTRUCTURA PKI – CA

- **Implementación de la Plataforma de Infraestructura de Claves Públicas (PKI – CA)** para firma digital y autenticación segura de identidades.
- **Compatibilidad con estándares ICAO y gobierno digital**.

MANTENIMIENTO Y SOPORTE TÉCNICO

- **Cobertura**: Presencial y remota en todo el territorio nacional.
- **Tiempo de respuesta:** Cumple con los niveles de servicio (SLA) exigidos por la JCE.
- **Soporte técnico:** 24/7 con capacidad de monitoreo y diagnóstico remoto.

CAPACITACIÓN PARA PERSONAL DE LA JCE

- **Modalidad:** Presencial y virtual.
- **Documentación:** Manuales técnicos y operativos detallados.
- **Certificación**: Asegurando la correcta operación y mantenimiento del sistema.

SEGURIDAD Y PROTECCIÓN DE DATOS

- La solución garantiza altos niveles de seguridad mediante:
- Cifrado de datos AES-256 y RSA-4096.
- Autenticación biométrica y multifactor.
- Protección contra ataques cibernéticos y falsificación de identidad.
- Gestión de accesos con trazabilidad y auditoría continua.

PLAN DE IMPLEMENTACIÓN Y ENTREGABLES EN FASES

- **Fase 1 – Prueba Piloto:** Implementación inicial en una región específica para validar la interoperabilidad y ajustar procesos.
- **Fase 2 – Despliegue Nacional**: Expansión de la infraestructura a nivel nacional, garantizando estabilidad operativa.
- **Fase 3 – Soporte Continuo:** Mantenimiento y optimización del sistema tras su implementación.

ÍTEM I - ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

1. ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

1.1 INTRODUCCIÓN

1.1.1 DISEÑO Y PRODUCCIÓN

1.1.1.1 IMPRESOR DE ALTA SEGURIDAD

SELP es una imprenta de alta seguridad, certificada por Intergraf y por la norma internacional ISO 14298. Esta certificación garantiza un entorno de alta seguridad, y permite la fabricación de documentos de alto valor.

Como impresor de alta seguridad, SELP también tiene acceso a software de diseño gráfico fiduciario. Nuestros diseñadores integran elementos de seguridad (guilloches, arco iris, marcas ocultas, fondos numismáticos...) en los visuales que envían a nuestros clientes.

Nuestro sistema de producción es moderno y eficiente. SELP imprime fundamentalmente en offset y serigrafía, utilizando tintas que cumplen con la norma ISO 18745 (durabilidad) y con una solidez a la luz mayor a 4 en la escala de las lanas azules. Entre las tintas utilizadas, están las de formulación específica para el sistema de impresión offset (Pantone, UV, etc). Para la impresión de ciertos elementos de seguridad, se tienen las de seguridad con pigmento sólido, las tintas ópticas variables, entre otras.

Las diferentes capas que componen las tarjetas se ensamblan, laminan y cortan siguiendo un procedimiento muy preciso y perfectamente controlado.

La impresión es frecuentemente complementada con un hot-stamping de elementos de seguridad como: material de scratch seguro o banda magnética.

1.1.1.2 FABRICACIÓN DE TARJETAS SOBRE DIVERSOS MATERIALES

SELP está especializada en la producción de tarjetas plásticas (PVC, PET, Policarbonato), pero nuestros talleres también manejan una gran variedad de materiales alternativos como cartón, PLA y estructuras de madera.

SELP tiene una sólida experiencia con este tipo de substratos, gracias a la producción de grandes pedidos por los diferentes proyectos realizados.

1.1.1.3 CALIDAD Y RESPETO MEDIOAMBIENTAL

SELP está ampliamente reconocida por la calidad de sus productos y servicios. Esta notoriedad es el resultado de un compromiso total de la empresa.

Durante la producción, nuestras tarjetas se controlan de tres maneras diferentes: por medios mecánicos (cámaras, sistemas de rechazo automáticos en las máquinas), muestreos sistemáticos según nuestros procedimientos internos y muestreos aleatorios según las especificaciones de los productos.

SELP está certificada ISO 9001 (sitios de Angulema, Puy-Guillaume, Mareuil y Mumbai) por su gestión de calidad, ISO14001 (sitio de Angulema) por su gestión medioambiental, e ISO 27001 (sitio de Angulema) por la seguridad en el manejo de datos.

Respetuosas con el medio ambiente, nuestras fábricas destruyen los restos y mermas de manera programada y maximizan el reciclado de materiales en bruto y deshechos.

1.1.2 COMPONENTES ELECTRÓNICOS, SISTEMAS OPERATIVOS Y APLICACIONES

1.1.2.1 SEGURIDAD DE LOS COMPONENTES

SELP produce tarjetas de fidelización, tarjetas prepago, tarjetas bancarias y todo tipo de tarjetas de identificación.

La seguridad, el volumen de datos para almacenar y las aplicaciones necesarias definen la estructura de tarjeta a usar en cada caso (banda magnética, Mifare, chip de contacto, sin contacto, interface dual...) así como la normativa ISO a cumplir.

1.1.2.2 TARJETAS ELECTRÓNICAS, INLAYS, E-STICKERS, E-COVERS

El componente se incorpora en la tarjeta (mediante ensamblado / laminado / encartado)

De manera alternativa, también puede ser integrado:

- Junto a un adhesivo para la producción de e-stickers (trazabilidad de vehículos),
- En una lámina plástica flexible para la fabricación de inlays (en colaboración con diferentes proveedores),
- Sobre papel o teslín para la producción de e-covers (Pasaportes electrónicos).

1.1.3 CERTIFICACIONES

Todas las certificaciones originales, así como las traducciones de éstas, se encuentran en la sección de Documentos Adicionales, **"Certificaciones SELP"**

1.1.3.1 ISO 9001, 14001, 27001

Bureau Veritas Certification

SELP

RUE LOUIS PERGAUD
16000 ANGOULEME
FRANCE

Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :

ISO 9001:2015

Domaine d'activité

FABRICATION, IMPRESSION & PERSONNALISATION DE CARTES BANCAIRES, CARTES A PUCES ET DOCUMENTS D'IDENTITE.

DESIGN, MANUFACTURING & PERSONALIZATION OF BANKING, IDENTITY & SMART CARDS.

Date de début du cycle de certification : 16 septembre 2023
Sous réserve du respect des dispositions contractuelles et des résultats positifs des surveillances réalisées, ce certificat est valable jusqu'au : 15 septembre 2026
Date d'expiration du cycle précédent : 07 juin 2023
Date d'audit de certification/recertification : 26 mai 2023
Date de certification originale : 16 septembre 2020
(Organisme certifié par un autre organisme de certification avant le 02/03/23)

Certificat n° : FR082608-1
Affaire n° : 18363737 *Date de révision :* 01 août 2023

Samuel DUPRIEU - Président

Adresse de l'organisme certificateur : Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du référentiel peuvent être obtenues en consultant l'organisme.
Pour vérifier la validité de ce certificat, veuillez utiliser le QR Code.

1/1

Bureau Veritas Certification

SELP

RUE LOUIS PERGAUD
16000 ANGOULEME
FRANCE

Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :

ISO 14001:2015

Domaine d'activité

FABRICATION, IMPRESSION & PERSONNALISATION DE CARTES BANCAIRES, CARTES A PUCES ET DOCUMENTS D'IDENTITE.

DESIGN, MANUFACTURING & PERSONALIZATION OF BANKING, IDENTITY & SMART CARDS.

Date de début du cycle de certification : 16 septembre 2023
Sous réserve du respect des dispositions contractuelles et des résultats positifs des surveillances réalisées, ce certificat est valable jusqu'au : 15 septembre 2026
Date d'expiration du cycle précédent : 07 juin 2023
Date d'audit de certification/recertification : 26 mai 2023
Date de certification originale : 16 septembre 2020
par un autre organisme de certification avant le 02/03/23)

Certificat n° : FR082609-1
Affaire n° : 18363737 *Date de révision :* 01 août 2023

Samuel DUPRIEU - Président

Adresse de l'organisme certificateur : Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du référentiel peuvent être obtenues en consultant l'organisme.
Pour vérifier la validité de ce certificat, veuillez utiliser le QR Code.

1/1

Bureau Veritas Certification

SELP ANGOULEME

RUE LOUIS PERGAUD 16000 ANGOULEME - France

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2022

Scope of certification

SECURE ARTWORK DESIGN, EMBEDDING AND INITIALIZATTION OF SMART CARDS

CONCEPTION DE VISUELS SECURITAIRES, ENCARTAGE ET PERSONNALISATION DE CARTES A PUCES

Original cycle start date:	12 November 2015
Expiry date of previous cycle:	11 November 2024
Certification / Recertification Audit date:	18 December 2024
Certification / Recertification cycle start date:	12 November 2024
Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on:	11 November 2027

Certificate No.: FR094191 Version: 1 Issue date: 17 January 2025

Contrat number: 23090509

UKAS MANAGEMENT SYSTEMS 0008

Samuel DUPRIEU - President
Signed on behalf of BVCH SAS UK Branch

Certification Body Address: 5th Floor, 100 Lower Thames Street, London, EC3R 6DL, United Kingdom

Local Office: 1 place Zaha Hadid - 92400 Courbevoie

Further clarifications regarding the scope of this certificate the applicability of the management system requirements may be obtained by consulting the organization.
To check this certificate validity, please use the QR Code.

1/1

1.1.3.2 ISO 14298:2013

INTERGRAF Certificate for Management of Security Printing Processes

Intergraf hereby certifies that, based on the results of the audit conducted by SQS, Swiss Association for Quality and Management Systems, Switzerland,

SELP SECURE (SELP SAS)

Rue Louis Pergaud, 16000 Angoulême, France

complies with ISO 14298:2021 "Management of Security Printing Processes" and with the relevant Intergraf requirements for this standard.

Certification Level:	Governmental Level
Markets of Operation:	National, International, Governmental, Non-Governmental organisations
Scope:	Manufacturing and personalization of banking, identity and smart cards.

Reference Number of the Certificate: 202403693
Expiration Date: 13 April 2027

Brussels, 16 April 2024

For Intergraf — INTERGRAF — **Beatrice Klose**, Secretary General

For SQS — SQS — **Felix Müller**, CEO

1.2 PROCESO DE FABRICACIÓN DE TARJETA

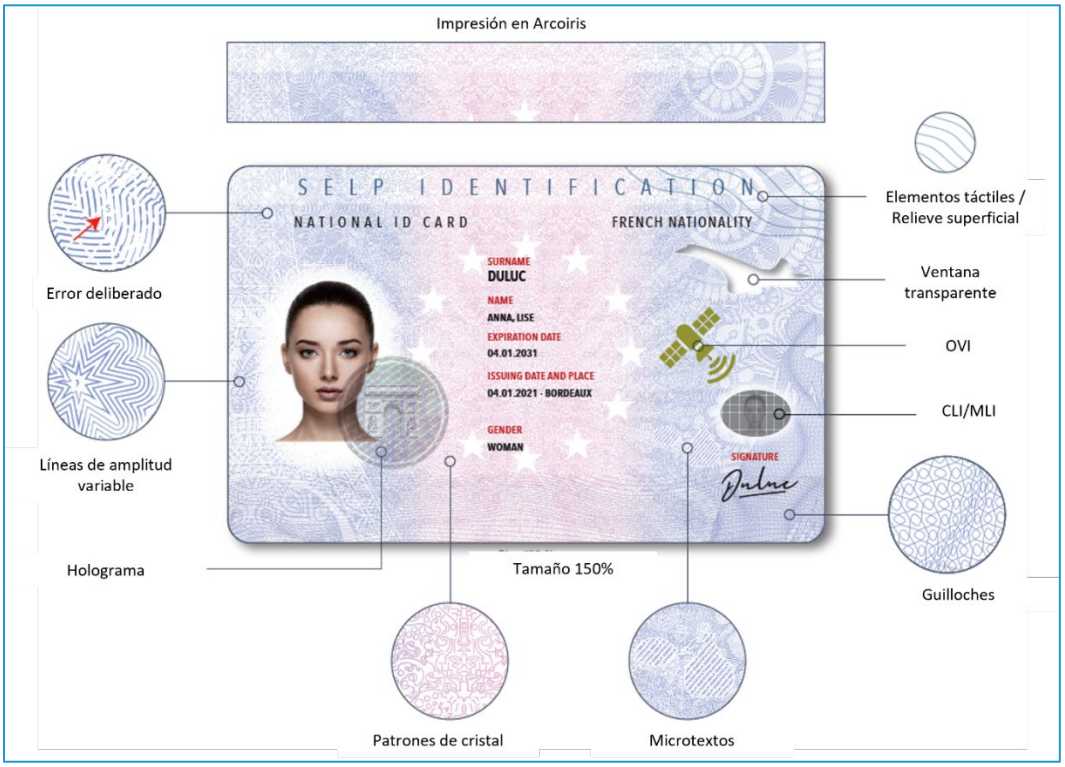
La fabricación de una tarjeta en SELP se divide generalmente en los siguientes pasos:

1.2.1 DISEÑO / ESTUDIO

El equipo DTP de SELP está al servicio de sus clientes para ofrecerles un diseño adaptado a sus necesidades. El diseño puede ser proporcionado por el cliente y adaptarse a las limitaciones de plástico, las dimensiones de la tarjeta, tintas offset, etc.

También podemos ofrecer un diseño original que luego se vuelve a trabajar en base a la retroalimentación del cliente, hasta obtener un visual satisfactorio. Cada planta de producción cuenta con una sala de DTP con varias estaciones de computadoras. Estas están equipadas con Adobe Suite (Illustrator, InDesign, Photoshop, Distiller 9 Pro y Acrobat 9 Pro), así como el software Prinergy Evo 5.1, Suitcase Fusion 3 Preps 6, QuarkXPress, XMF, Platón, FreeHand MX, Fortuna, EFI Colorproof XF.

El diseño es enviado como documento electrónico de baja resolución al cliente. Todos los elementos de seguridad se exponen. Elementos de seguridad especiales, tales como la exposición a lámparas UV se simulan en el documento. El cliente puede enviar rápidamente sus observaciones si los ajustes deben hacerse a nivel visual.



Para este proyecto en específico, un diseño exclusivo para la tarjeta CIE y CI han sido creados de acuerdo con las especificaciones incluidas en el punto I.8 Características detalladas del ITEM I ESPECIFICACIONES TECNICAS DE LAS TARJETAS y de acuerdo a lo mencionado en el punto 1.27.7.1 Fases de diseño y puesta en marcha: “Cada oferente en su oferta debe entregar una propuesta de diseño gráfico de las nuevas tarjetas de República Dominicana en formato impreso y electrónico”.
Ambos diseños se están entregando junto con nuestra propuesta técnica, de manera física en formato booklet y en archivo electrónico.

1.2.2 PRUEBA DE COLOR

Una vez que el modelo visual es validado por el cliente, SELP crea un archivo de impresión completa del diseño en alta resolución (2400 ppp y superiores). Durante esta etapa, el diseño completo y cada elemento de seguridad se genera utilizando el software de seguridad dedicado y accesible sólo por organizaciones certificadas como Impresoras de alta seguridad (ISO 14298 INTERGRAF).

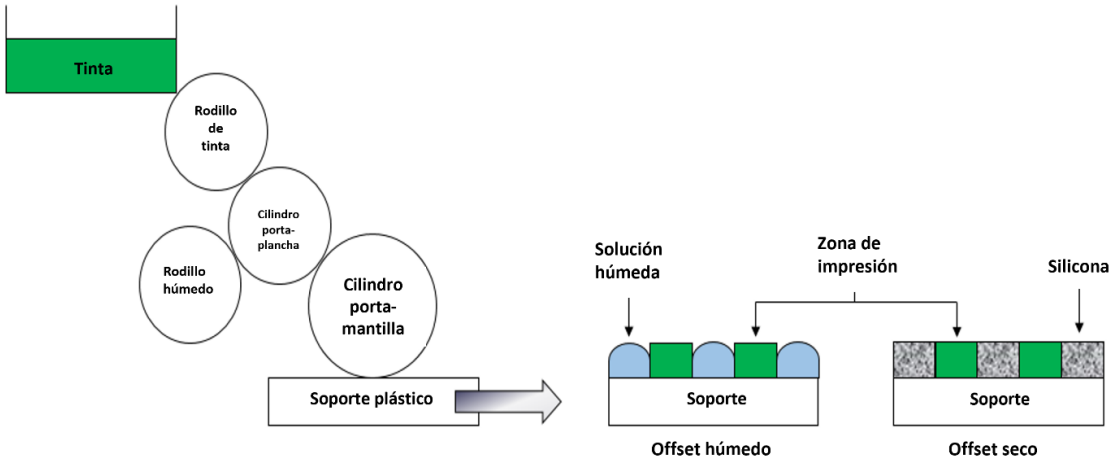
Este visual se imprime en papel satinado usando una impresora de alta calidad, calibrada de manera que los colores sean representados lo más cerca posible del resultado en el soporte de plástico.
Antes del inicio de la producción, esta primera hoja de plástico impresa con el diseño final se envía al cliente para ser validado y firmado.
Este paso también se puede realizar por el cliente directamente en la planta de producción SELP.

1.2.3 IMPRESIÓN

1.2.3.1 IMPRESIÓN EN OFFSET

Las características de seguridad gráficas son impresas en el soporte de plástico con la tecnología de impresión en offset, que requiere para su uso personal especializado. La calidad general de la impresión en offset está estrechamente relacionada con diversos parámetros que requieren un ajuste fino, tales como: hacer coincidir el color de tinta especificado (utilizando tintas de formulación específicas), minimizar el movimiento del soporte de plástico, minimizar la distorsión o el ruido de la imagen, tal como el polvo, verificar que las planchas impresas se soportan entre sí correctamente, etc.

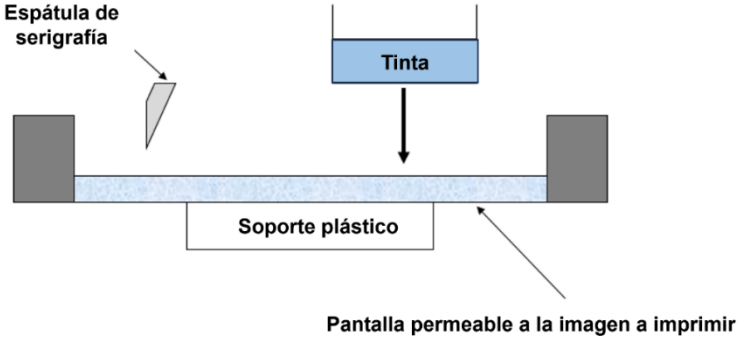
El nombre "offset" proviene del principio básico de esta técnica de impresión: la tinta es transferida de una plancha (imagen positiva) a una mantilla de caucho (imagen negativa) y luego al soporte a imprimir (como un positivo nuevamente). Cuando se hace una plancha de impresión, la imagen de impresión se convierte en receptora de tinta y repelente de agua, mientras que las áreas sin impresión son receptoras de agua y repelentes de tinta. Se pueden usar dos técnicas, "offset húmedo" u "offset sin agua", tal como está ilustrado abajo.



En la prensa de impresión, la plancha es montada en un cilindro portaplancha el cual, a medida que, rota, se pone en contacto con rodillos húmedos con agua (o solución humectante) y rodillos húmedos con tinta. La solución humectante humedece las áreas sin impresión e impide que la tinta penetre estas áreas. La tinta humedece las áreas de imagen, que son transferidas al cilindro portamantilla intermedio. El soporte de plástico capta la imagen a medida que este pasa debajo del cilindro portamantilla.

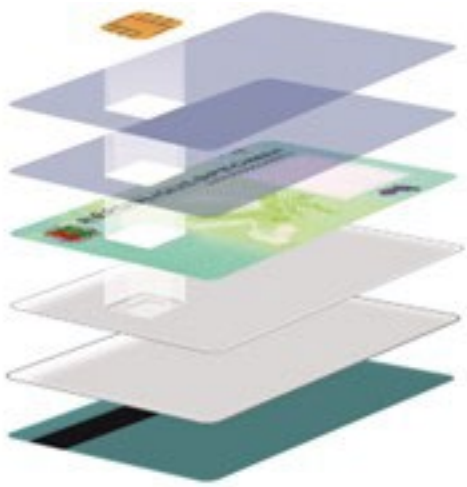
1.2.3.2 IMPRESIÓN SERIGRÁFICA

La serigrafía se usa para aplicar barnices o tintas especiales en el cuerpo de la tarjeta inteligente, una vez que el fondo principal ha sido impreso con offset. Una plantilla es aplicada a una pantalla de nailon o poliéster, mediante un procedimiento fotográfico, esparciéndola sobre un marco. Luego se escurre la tinta a través de la pantalla, depositándose la tinta sobre el soporte de plástico. Se necesita una pantalla distinta para cada color deseado.



1.2.4 ENSAMBLADO

Las tarjetas se componen generalmente de 5 a 8 capas de plástico u otros materiales, unidas entre sí. Las diferentes capas se ensamblan entre sí en un orden específico (dos capas externas, incrustaciones en el interior, y los componentes eléctricos en caso necesario. La composición de la estructura dependerá del material utilizado (PVC, policarbonato, PET, etc.), del tipo de tarjeta y del tipo de personalización que tendrá.



En nuestras soluciones, la construcción del cuerpo de la tarjeta está diseñada sin capas/materiales patentados que pudieran limitar el abastecimiento de materiales para cumplir con la producción de tarjetas de este proyecto.

1.2.5 LAMINADO

Cuando se tienen ensambladas las distintas láminas de material, se pegan entre sí mediante un proceso conocido como laminado. Se trata de un proceso durante el cual las láminas se calientan a cierta temperatura y presión para permitir que las diferentes capas, que inicialmente eran individuales, se adhieran entre sí y se unan permanentemente para formar un bloque sólido de material. Es durante el laminado que se puede dar a la tarjeta un acabado especial, como un efecto mate, espejo o satinado. Las tarjetas pueden grabarse incluso empleando placas de laminación. Esto se utiliza en los documentos de identidad para garantizar una seguridad aún mayor.

1.2.6 CORTE

Una vez realizado el laminado, se procede al corte para obtener las tarjetas. Los formatos pueden variar según el documento.

1.2.7 PRE PERSONALIZACIÓN

El propósito de un documento de identidad es almacenar información personal que permita identificar a una persona con certeza. La certeza con la que se puede identificar a una persona no solo se deriva de la seguridad de la propia tarjeta, sino también de la forma en que los datos se almacenan de forma segura en la tarjeta.

1.2.7.1 ELÉCTRICA

Para las tarjetas que tienen un chip o una incrustación eléctrica, SELP realiza la pre personalización eléctrica de estos componentes. En general, esto consiste en cargar la aplicación que va a gestionar posteriormente los datos personales de cada individuo.
Esta pre personalización se puede realizar antes del montaje de la tarjeta, o después de este paso.

También tenemos, para las tarjetas bancarias, una máquina Datacard que permite hacer múltiples pasos en línea. Las tarjetas se montan y se cortan de antemano. A continuación, se colocan en la máquina que corta una ventana en la tarjeta, coloca el chip, lleva a cabo la pre personalización eléctrica del mismo, y prueba el componente en el extremo de la cadena.

1.2.7.2 GRÁFICA

En muchas ocasiones, se requiere hacer también una pre personalización gráfica. Normalmente consiste en imprimir algún número de serie utilizado para control de las tarjetas. Para este proyecto, cada tarjeta se identificará de manera individual durante el proceso de manufactura, mediante un número de serie en grabado láser.

1.2.8 CONTROL DE CALIDAD

SELP es reconocida por la calidad de sus productos y servicios. Esta notoriedad es la culminación del compromiso total de la empresa.

En la producción, nuestros productos se controlan de tres maneras distintas: mediciones automáticas (cámaras y sistemas de expulsión de máquinas), muestreo sistemático de acuerdo con nuestros procedimientos internos y muestreo aleatorio de acuerdo con las especificidades de los productos.

A lo largo de toda la fabricación, se realizan diferentes pruebas para corroborar la calidad de nuestros productos: dimensiones exactas (longitud, anchura y grosor), que el diseño de las tarjetas sea bien respetado, que la impresión no presente errores, pruebas de los componentes eléctricos, pruebas de materiales (resistencia física y química).

1.2.9 EMBALAJE Y ALMACENAMIENTO

De manera estándar, las tarjetas son empaquetadas en bandejas de 500 unidades. Posteriormente, estas bandejas se cubren con un film transparente y se embalan en paquetes de 10 unidades en cajas de cartón. Las cajas se sellan con un adhesivo SELP y se encintan para enseguida colocarlos en palés. Estos se recubren con una película transparente o negra, según las indicaciones del cliente, y se encintan. Finalmente, los palés se sellan para garantizar su inviolabilidad y trazabilidad.

Como la seguridad es una prioridad, particularmente en los sectores bancarios y de identidad, los palés se almacenan en una cámara de seguridad. SELP Secure dispone de amplios dispositivos de seguridad (cámaras de vídeo, enlaces con empresas de vigilancia, etc.) que le permiten manejar documentos sensibles.

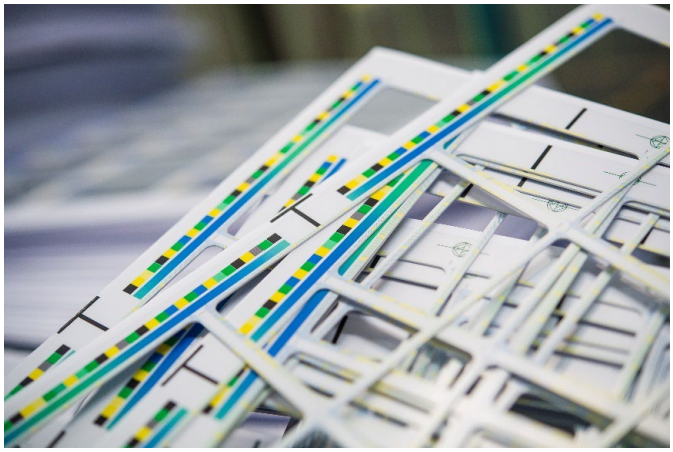
Para este proyecto en particular, se hará de acuerdo con lo especificado en las bases de la licitación. Las tarjetas serán empaquetadas en cajas que contendrán mil unidades correlativas, debidamente embaladas y selladas.

1.2.10 ENVÍO

Según el producto enviado, se elige el tipo de transporte (seguro o no). Para asegurar el transporte, tenemos varias esclusas entre la bóveda y el área de carga de tarjetas. No hay contacto entre el transportista y el interior de la planta de producción. Los palés se depositan en una esclusa intermedia; una vez que la esclusa se ha cerrado, el transportista carga los palés. El camión es liberado una vez que esté cerrado.

1.2.11 DESTRUCCIÓN DE LOS PRODUCTOS SENSIBLES

Todos los residuos se procesan dentro de la planta de producción. Los materiales reciclables son recogidos para su reutilización y el resto de los residuos se destruyen en nuestro incinerador.



1.3 PROPUESTA TARJETAS DE POLICARBONATO

1.3.1 LA TARJETA EN POLICARBONATO

1.3.1.1 CUERPO DE LA TARJETA

Las tarjetas basadas en policarbonato propuestas por SELP cumplen con los más altos requerimientos de seguridad, cuando se escoge el grabado por láser para la personalización. El cuerpo multicapas de la tarjeta de policarbonato, laminado en caliente, se caracteriza por su alta durabilidad, seguridad y flexibilidad para esta tarjeta de última generación. Además, este tipo de material de tarjeta ofrece resultados de personalización superiores en términos de resolución y contraste entre el grabado por láser negro y los colores de fondo.

La tarjeta es laminada a partir de varias capas de películas, las cuales están todas hechas de materiales homogéneos. Este material es particularmente resistente al desgaste por uso y a la exposición a temperaturas altas. Comparado con otros materiales poliméricos, el policarbonato ofrece alta resistencia al esfuerzo mecánico, químico y térmico, así como a las influencias ambientales, lo que asegura una larga durabilidad de todas sus características.

Las composiciones del material y la tarjeta han sido optimizadas para satisfacer los requisitos de las técnicas de personalización por láser. Las películas exteriores en cada lado de la tarjeta son transparentes y protegen la impresión y personalización en las capas interiores.

Las características físicas de la tarjeta son, hasta donde es aplicable, totalmente conformes con las normas internacionales mencionadas más adelante. Esto se refiere a características tales como dimensiones de la tarjeta, rigidez a la flexión, resistencia a productos químicos, estabilidad dimensional de la tarjeta y deformación por temperatura/ humedad y por el uso normal, la exposición a la luz, la delaminación, la adhesión o el bloqueo y la transmisión luminosa.

El mejoramiento de la estructura del material brinda mejores resultados en la etapa de laminado, haciéndolo mucho más seguro. Después de 50,000 ciclos de torsión/flexión, la resistencia a la ruptura para la solución con material de policarbonato únicamente, es de ~ 200 N.

Las principales ventajas del policarbonato son las siguientes:

- Alta durabilidad,
- Alta flexibilidad y por lo tanto menor esfuerzo volumétrico.

1.3.1.2 ESTRUCTURA DE LA TARJETA

Las características físicas de la tarjeta son, hasta donde es aplicable, totalmente conformes con las siguientes normas internacionales mencionadas:

- ISO/IEC 7810
- ISO/IEC 7501-1
- ISO/IEC 7501-3
- ISO/IEC 10373-1
- ISO/IEC 7816

Las dimensiones de la tarjeta son las definidas por ISO/IEC 7810 capítulo 5. El tamaño y espesor corresponden al tipo de tarjeta ID-1 con las siguientes dimensiones:

- Largo: entre 85.47 mm y 85.72 mm
- Ancho: entre 53.92 mm y 54.03 mm
- Espesor: entre 0.68 mm y 0.84mm.

El cuerpo de la tarjeta y sus características de impresión están diseñados para una vida útil de 10 años en condiciones normales de desgaste y almacenamiento. Las tarjetas que fabricamos son conformes al perfil 3D de la norma ISO24789.

La tarjeta de policarbonato grabable por láser es un compuesto multicapas, es decir que es producido "fundiendo" entre sí varias capas durante un proceso de laminado en caliente. Las características de las capas y el proceso de laminado en caliente en sí aseguran una unión duradera, segura y flexible del compuesto. La tarjeta terminada tiene un espesor según los requisitos de ISO 7810 y, junto con las características especiales del material, ofrece una gran flexibilidad.

Por lo mismo, la deformación que se pudiera presentar es una deformación causada por el uso normal de la tarjeta. Nuestras tarjetas se someten a una fase de calificación durante su desarrollo, que resulta en pruebas de flexión/torsión de acuerdo a la norma ISO10373. Posteriormente en la fase de producción, las muestras se toman en lotes y se someten a las mismas pruebas de flexión/torsión, para asegurar su conformidad a las normas.

La durabilidad del material laminado excede las especificaciones de la norma ISO 10373. También excede la durabilidad y resistencia a la delaminación convencional.

Hablando de toxicidad, las tarjetas no presentan ningún riesgo tóxico en su uso normal de acuerdo a la norma ISO 7810. Las tarjetas, al cumplir con la norma ISO 10373 e ISO 7810, son resistentes a los efectos químicos inherentes al manejo y uso normales.

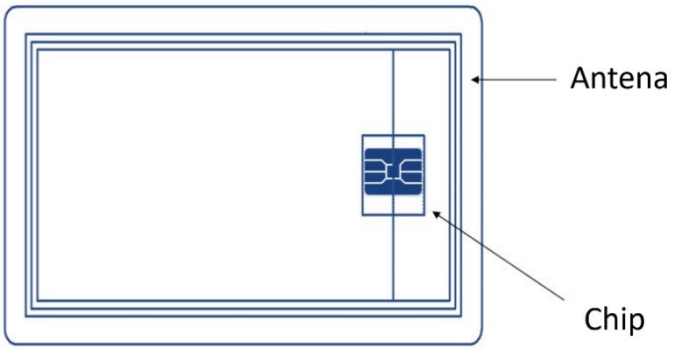
En cuanto a la estabilidad térmica, la tarjeta se mantendrá legible mecánicamente a temperaturas que oscilen entre -10°C y +50°C. La tarjeta no perderá su funcionalidad en caso de quedar expuesto a temperaturas que oscilen entre -35°C y +80°C.

Con respecto a la humedad, la tarjeta será legible mecánicamente a una humedad ambiente relativa del 5% al 95% y una temperatura máxima de bulbo húmedo de 25 °C. La tarjeta no perderá su fiabilidad en caso de quedar almacenada o expuesta a una humedad relativa ambiente del 0% al 100% (sin condensación).

1.3.2 TARJETA CON CHIP SIN CONTACTO

Las tarjetas con chip sin contacto tienen las mismas características funcionales que las tarjetas con microprocesador, pero con tecnología RFID (Identificación por radiofrecuencia) que permite intercambiar datos simplemente acercando la tarjeta a un lector compatible, sin necesidad de contacto físico. Están alimentadas por inducción (la inducción es un principio físico que transforma la energía mecánica [movimiento] colocada en un campo magnético en energía eléctrica) y equipados con una antena para comunicarse a distancias de unos pocos centímetros por radiofrecuencia (usualmente 13,56 MHz).

- El chip está conectado a la antena. Ambos están incrustados en el cuerpo de la tarjeta
- La comunicación con el chip se realiza únicamente a través de la antena
- La tarjeta se lee a distancia (de 0 a 10 cm)



En términos de fabricación, la estructura utilizada está compuesta por un prelam de policarbonato (incluido el chip y la antena) insertado entre varias capas de policarbonato. Las tarjetas con chip sin contacto cumplen, hasta donde es aplicable, con la norma ISO 14443.

El chip sin contacto para las tarjetas de esta licitación será conforme a las especificaciones detalladas en la Tabla 3.2 (NXP JCOP 4 o equivalente).

Las características principales del chip son:

- El mejor de su clase en términos de rendimiento y una excelente comunicación por radiofrecuencia
- Java Card v3.0.5 Edición Clásica
- GlobalPlatform:
  - Configuración de la identificación de GP v2.2
  - GP v2.2 Configuración de las directrices de mapeo v1.0.1
  - GP v2.3 Configuración de la implementación común v2.0
- ISO 7816-3 T=0, T=1
- ISO 14443 (hasta 848kbps)
- Soporte de doble interfaz

- Compatibilidad con DES, 3DES, AES, RSA, ECC y SHA mediante coprocesadores dedicados basados en hardware
- Sistema operativo ubicado en ROM que potencia el rendimiento de ejecución
- Memoria no volátil (NVM) disponible para aplicaciones y datos de personalización de hasta 180kB
- Certificación EAL 6+ de criterios comunes
- Aprobación EMVco
- Certificación FIPS

Aplicaciones incluidas:

- Documento nacional de identidad electrónico
- ePKI
- Firma Digital

Otras aplicaciones que se pueden cargar en este chip:

- Pasaporte electrónico
- Tarjeta electrónica de permiso de conducir
- Tarjetas electrónicas sanitarias y de prestaciones sociales
- Servicios electrónicos
- Pago y micropago
- Transporte público
- Acceso lógico y físico

Este chip albergará los aplicativos de Documento de viaje electrónico de acuerdo con ICAO 9303, Firma electrónica e Identificación Ciudadana.

Respecto a las especificaciones técnicas solicitadas para el chip, se presenta a continuación la información solicitada:

TABLA 3.2

	Respuesta	**Comentarios adicionales**
9.1 Características del chip sin contacto		
CPU de 16/32 bits	Cumplimos	
Certificación CC EAL5+ o superior (o equivalente)	Cumplimos	La certificación incluida es EAL6+ Favor de dirigirse a la sección de Documentos Adicionales, “Documentación Técnica Adicional”, donde se incluye la certificación solicitada.
Criptoprocesador hardware para operaciones criptográficas	Cumplimos	
Clave simétrica (Triple DES con clave de hasta 168 bits, AES hasta 256 bits)	Cumplimos	

Clave pública (RSA con longitud de clave de hasta 4096 y ECC con clave de hasta 512 bits)	Cumplimos	
Hash SHA1 y SHA2	Cumplimos	
Generador de números aleatorios de acuerdo a AIS31	Cumplimos	
Protección contra descargas ESD.	Cumplimos	
Número de serie único	Cumplimos	
Reloj interno asíncrono	Cumplimos	
Firewalls de seguridad entre particiones de memoria	Cumplimos	
Memoria no volátil necesaria para la incorporación de las aplicaciones requeridas y los datos especificados en el presente punto 1.2.4. Características electrónicas y del sistema operativo	Cumplimos	La memoria no volátil incluida en el chip es de 180k. Se considera suficiente de acuerdo a la información compartida por la JCE en los diferentes documentos de la presente licitación.
Retención de datos en memoria no volátil de al menos 10 años	Cumplimos	
Al menos 500.000 ciclos de lectura / escritura garantizados	Cumplimos	Típicamente 100.000.000 ciclos de lectura/escritura.
Interfaz de RF ISO/IEC 14443 A/B de hasta 848kbits/s, pudiendo ofrecer modos de transmisión RF mejorados	Cumplimos	Tipo A solamente. Compatible con VHBR (velocidad de transmisión muy alta)
9.2Características del Sistema Operativo		
Protocolo de transmisión de acuerdo con ISO/IEC 14443 A/B Interfaz de comandos de acuerdo a ISO/IEC 7816-4 y PCSC.	Cumplimos	
UID / PUPI aleatorio	Cumplimos para el UID	UID de 7 octetos. PUPI no aplica para Tipo A.
Certificación Common Criteria EAL4+ o superior (o equivalente).	Cumplimos	Favor de dirigirse a la sección de Documentos Adicionales, “Documentación Técnica Adicional”, donde se incluyen las certificaciones solicitadas del OS.
En caso de que el Sistema Operativo sea basado en JavaCard, se deberá bloquear la posibilidad del agregado de nuevas aplicaciones una vez incorporadas las aplicaciones requeridas.	Cumplimos	
Documento de Viaje Electrónico de acuerdo con ICAO 9303		
SAC (Supplemental Access Control).	Cumplimos	
EAC (Extended Access Control).	Cumplimos	
AA (Active Authentication)	Cumplimos	
Funcionalidad de Firma Electrónica		
Acceso protegido mediante PIN / PUK	Cumplimos	
Algoritmos de firma RSA y ECDSA	Cumplimos	
Soporte para claves RSA en formato CRT y en formato normal (exponente privado, exponente público y módulo).	Cumplimos	
Claves RSA con soporte para componentes p y q de longitud variable	Cumplimos	
Capacidad de almacenar, generar y usar claves RSA de, como mínimo, 4096 bits de longitud Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Para el caso del tamaño de llaves de la Autoridad Ciudadana, tanto la Autoridad Raíz como la Autoridad Subordinada deben tener un tamaño de llaves de 4096 bits.	Cumplimos	

Para el caso de los certificados de usuario (ciudadanos) será de 2048 bits. Las claves que componen la "PKI de Firma Digital" y la "PKI de Firma de Documentos" deben estar basadas en los estándares X.509v3 y RFC 5280.		
Soporte de diversas curvas ECDSA, incluyendo las más habituales (NIST P-256, Brainpool, etc Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Se debe tener la capacidad de soportar curvas elípticas NIST P-256, BrainpoolP256r1, entre otras, conforme con los estándares: • TR-03111 Elliptic Curve Cryptography (ECC) based on ISO 15946. Technical Guideline TR-03111, Version 2.0 • ISO15946-1 ISO/IEC. 15946-1. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 1: General. 2002. • ISO15946-2 ISO/IEC. 15946-2. Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures. 2002. • ISO15946-3 ISO/IEC. 15946-3: Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 3: Key establishment. 2002.	Cumplimos	
Operaciones de firma digital	Cumplimos	
Intercambio de claves de sesión o simétricas entre dos entidades basado en RSA/ECDSA/ECDH	Cumplimos	
Claves almacenadas en ficheros/elementos independientes	Cumplimos	
Condiciones de acceso independientes para cada clave/elemento	Cumplimos	
Estructura interna de ficheros según el estándar ISO/IEC 7816-15 (PKCS#15)	Cumplimos	
Deberá disponer de capacidad de memoria suficiente para almacenar hasta 4 certificados, con sus correspondientes claves, incluyendo el caso de claves RSA 4096 Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: El eID debe ser capaz de almacenar certificados x.509 que permitan a los ciudadanos gozar de los servicios de criptografía	Cumplimos	
Securización de los mensajes transmitidos entre la tarjeta y el terminal mediante canal seguro de acuerdo a CEN14890 o equivalente	Cumplimos	
Confidencialidad de los datos transmitidos mediante triple DES / AES	Cumplimos	
Autenticación de la información intercambiada entre las dos partes; incorporación de checksum criptográfico de tipo MAC según ANSI X9.19 y DES	Cumplimos	

Protocolo de establecimiento de las claves de sesión basado en el esquema propuesto en ISO/IEC 9798-3 Authentication SASL Mechanism Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Para mayor claridad, la "Aplicación de Firma Electrónica" debe estar certificada según CC EAL5+, compatible con el conjunto y comandos ISO-7816	Cumplimos	
Claves de sesión derivadas a partir de información generada por las partes involucradas en el establecimiento del canal seguro; el cálculo de las claves se realiza según ANSI X9.63 Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: Para mayor claridad, la "Aplicación de Firma Electrónica" debe estar certificada según CC EAL5+, compatible con el conjunto y comandos ISO-7816	Cumplimos	
Software de gestión y drivers		
Drivers de la tarjeta (PKCS#11, CSP, Card Module, etc)	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
Software de gestión que permita gestionar las operaciones más habituales con la tarjeta; por ejemplo, cambio de PIN, desbloqueo de PIN, borrado de certificados, etc. Deberá garantizar el funcionamiento del documento en distintos sistemas operativos (Windows, Linux, MacOS). Deberá garantizar el funcionamiento del documento en distintos navegadores	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
Se deberán aportar librerías o SDKs que faciliten el desarrollo de aplicaciones para dispositivos móviles, con sistemas operativos Android e IOS	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
El software suministrado deberá ser actualizado, adecuándolo a nuevos SO, Navegadores, corrección de bugs, etc., durante el tiempo de vida del proyecto	Cumplimos	Punto 1.3.3 del Anexo "Especificaciones técnicas ITEM 1: Propuesta Técnica de las Tarjetas de Identidad en Policarbonato"
Funcionalidad de Identificación Ciudadana		
Se almacenarán los datos de filiación del ciudadano de manera estructurada	Cumplimos	De acuerdo con el estándar ISO7816-4 file system
El acceso a los mismos se realizará por medios seguros	Cumplimos	Existen muchos mecanismos de seguridad estándar disponibles para garantizar la integridad, confidencialidad y autenticidad
Preferiblemente, de acuerdo con la Guía Técnica TR-03110 del BSI o similar Se añade el siguiente texto de las respuestas recibidas por parte de la JCE: No es necesario control de acceso basado en roles basado EAC2 y/o Identificación Restringida para la función de elecciones.	Cumplimos	Cumplimos con la normativa eIDAS y somos compatible con TR-03110 v2.21, dentro del alcance implementado que incluye PACEv2 (incluyendo PACE con PIN), EACv1 y EACv2

Favor de referirse a la sección de Documentos Adicionales, "Documentación técnica adicional", donde se encontrará información adicional sobre el chip, así como las certificaciones Common Criteria solicitadas.

1.3.3 MIDDLEWARE

En la vida cotidiana existe una creciente necesidad de realizar acciones digitales con restricción de seguridad, que permita al ciudadano tener una burocracia inteligente y menos pérdida de tiempo. Las aplicaciones típicas se resumen en “Autenticación de sitio web” y “Firma digital”.

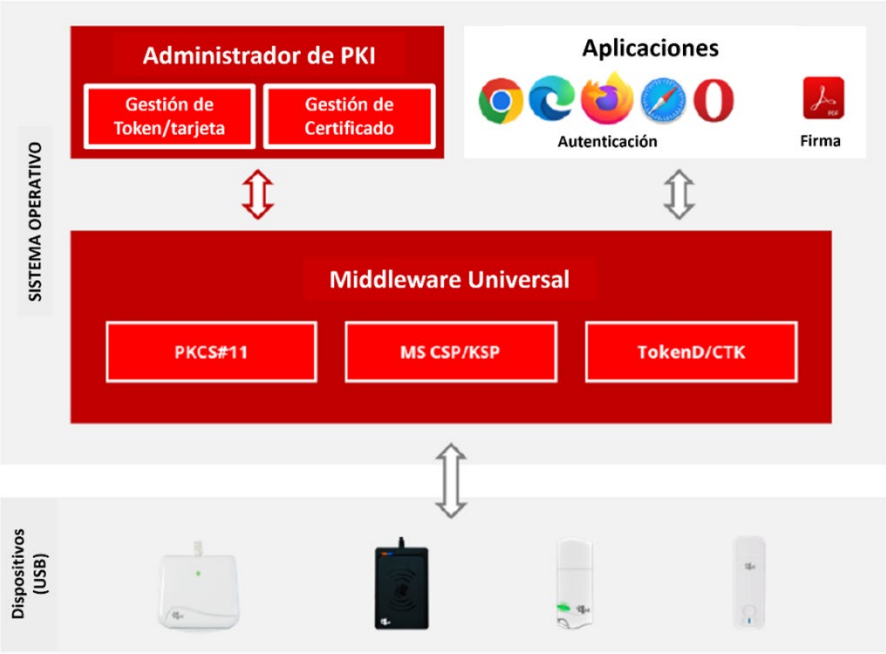
Con el fin de dar al ciudadano la posibilidad de utilizar la infraestructura digital, se le proveen tarjetas inteligentes / token, cuyo núcleo es un elemento seguro que contiene un certificado digital. Este certificado es accesible mediante un PIN, y por esta razón existe la necesidad de permitir también las funcionalidades de “Desbloquear PIN”, “Cambiar PIN”, “Cambiar PUK”.

Dado que hay muchos sistemas operativos diferentes y una gran variedad de tarjetas inteligentes y tokens, no es posible interconectarlos sin un componente de software externo. Todas las aplicaciones que se ejecutan en el sistema operativo utilizan la interfaz PKCS#11 (o CSP/TokenD) para ejecutar comandos criptográficos. Cada tarjeta inteligente habla en su propio idioma. De tal forma que el middleware es el traductor entre las aplicaciones (SO) y las tarjetas inteligentes.

Para esta licitación se contempla el Middleware Universal “UMW” u otro equivalente. El UMV es un conjunto de bibliotecas y herramientas estándar para interconectar varios dispositivos criptográficos, como tarjetas inteligentes y tokens PKI, con otros dispositivos (como PC de escritorio). UMW permite al usuario gestionar sistemas basados en certificados sin necesidad de tener un alto conocimiento de los mismos.

ESTRUCTURA DE MIDDLEWARE UNIVERSAL

El UMW consta de 2 componentes:



- **Administrador de PKI:**

Es una aplicación multiplataforma para la gestión de tarjetas que permite operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtención de información sobre la tarjeta, importación o exportación de certificados.

- **Bibliotecas del Middleware Universal:**

Son una colección de archivos que contiene la implementación de los principales estándares criptográficos, por ejemplo, PKCS#11, MS CSP, MS CSP-NG, TokenD, CryptoTokenKit.

Las bibliotecas del UMW están compuestas por:

a) Un módulo de biblioteca que expone una API compatible con PKCS#11 v2.40/v3.0, totalmente compatible con los siguientes sistemas operativos: Windows, Linux y Mac OS X
b) Un módulo del sistema que expone una API compatible con la especificación del Proveedor de Servicios Criptográficos de Microsoft (MS CSP) (CryptoSPI / 2006) y con la API de criptografía de próxima generación (CNG o CSP-NG)
c) Un módulo del sistema "almacén de certificados" que implementa un mecanismo para la importación automática de certificados en el almacén "Personal" del usuario de Windows. Este mecanismo es compatible con el servicio de propagación de certificados de Windows.
d) Un módulo del sistema que expone una API compatible con el Apple TokenD para MacOS hasta 10.13.
e) Un módulo del sistema que expone una API compatible con Apple CryptoTokenKit para MacOS 10.13 o superior.

Dichos módulos proporcionan varias interfaces de programación, lo que permite en aplicaciones de terceros el uso de tarjetas inteligentes criptográficas y tokens.

Favor de referirse a la sección de Documentos Adicionales, “Documentación técnica adicional”, al documento “Datasheet Universal Middleware” donde se tiene información adicional sobre el Middleware.

1.3.4 PERSONALIZACIÓN GRÁFICA

La tarjeta propuesta puede ser personalizada gráficamente con una foto de alta resolución en escala de grises y el texto de los datos variables, con una impresora de grabado por láser.

El grabado por láser es un proceso mediante el cual, las capas de policarbonato del cuerpo de la tarjeta químicamente modificadas son carbonizadas con un haz de láser de alta precisión. Esta tecnología permite imprimir datos debajo de la superficie de la tarjeta. Combinado con el policarbonato, el grabado por láser también abre el camino a características de seguridad variables únicas, tales como grabado táctil, imagen fantasma perforada, impresión de microtexto variable o imagen láser cambiable/múltiple (CLI/MLI).

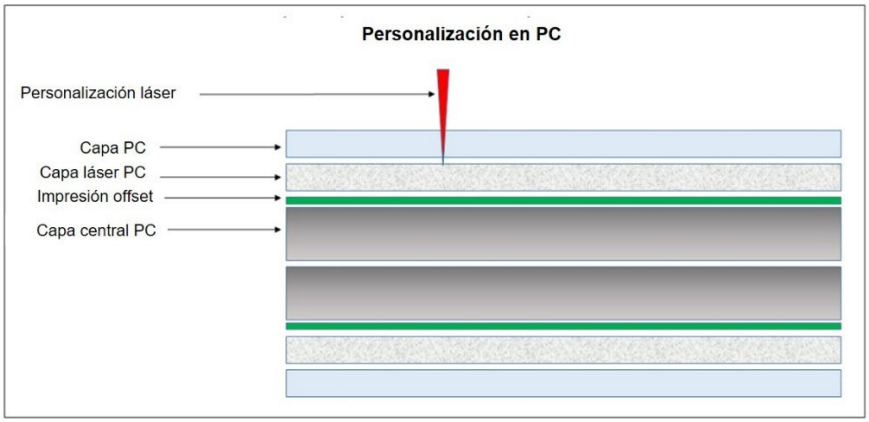


IMAGEN EXCLUSIVAMENTE ILUSTRATIVA

La tarjeta no debe ser expuesta al agua u a otros solventes que puedan debilitar su construcción, dejar rastros forenses o dañar el componente de microchip que pudiese tener. Tampoco debe ser conectada a dispositivos o sistemas para los cuales no está diseñada.

En las soluciones que ofrecemos, el cuerpo de la tarjeta en blanco y el proceso de personalización de esta, en combinación, no constituyen una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización.

1.3.5 IMPRESIÓN DE SEGURIDAD

SELP tiene acceso a una experiencia única en la impresión de seguridad de diseños y de elementos de seguridad.

Esta sección presenta una lista de diversas certificaciones de seguridad que SELP puede reunir para diseñar un documento de identidad de alta seguridad personalizado basado en soportes de plástico tales como tarjetas inteligentes y páginas de datos electrónicas de pasaportes.

1.3.5.1 CERTIFICACIÓN PARA IMPRESORES DE SEGURIDAD

La certificación CWA 14641 para impresores de seguridad es un procedimiento implementado por la “International Confederation for Printing and Allied Industries” ("Confederación internacional para las industrias de la impresión y asociadas") (Intergraf). Esta da fe de que se han cumplido las reglas y reglamentos estrictos correspondientes a la seguridad del producto y la producción y de que satisfacen a los auditores.

Los criterios de certificación incluyen:

Seguridad del edificio, control de admisión, vigilancia por video, administración de llaves, elección y vigilancia de los empleados, comportamiento en caso de emergencias, contacto directo con la policía en caso de una alarma, gestión de productos y trazabilidad de los procesos de producción, el almacenamiento y la entrega, destrucción de maculación, seguridad EDP y gestión de datos, monitoreo de visitantes, etc.

SELP está certificado como un **Sistema de gestión de alta seguridad para impresión segura** con el ámbito de impresión de plásticos, fabricación e integración de tarjetas de alta seguridad.

1.3.5.2 CREACIÓN DE UN DISEÑO GRÁFICO SEGURO

Para la creación del diseño gráfico seguro que será impreso en el fondo de la tarjeta, SELP proporciona a su cliente toda su experiencia como impresor de plásticos de alta seguridad.

Creación del diseño gráfico y maqueta digital

La integración de diversas características de seguridad distintas dentro de un solo diseño gráfico requiere personal formado, tanto con experiencia técnica como con sensibilidad artística. El diseño gráfico final debe satisfacer a las limitaciones y requerimientos exclusivos de cada cliente, respetando las normas solicitadas (como ICAO para ciertos documentos), presentando elementos gráficos tales como:

- Diseño gráfico de un documento o tarjeta ya existente,
- Estándar internacional o regional,
- Monumentos nacionales,
- Jefes de Estado,
- Sitios geográficos excepcionales,
- Escudo y bandera,
- Mapa del país,
- Etc.

El diseño gráfico es enviado electrónicamente al cliente en forma de un archivo gráfico vectorial (en pdf) con cada elemento de seguridad detallado. Se simulan iluminaciones especiales - como la exposición a la luz UV. El cliente puede entonces rápidamente enviar su retroalimentación y si es necesario realizar cualquier ajuste al diseño gráfico.

Listo para imprimir e impresión en color real

Una vez que el diseño gráfico modelo es validado por el cliente, SELP crea un archivo de impresión completo del diseño gráfico en muy alta resolución (2400 dpi y superior). En esta etapa, todo el diseño gráfico y cada característica de seguridad son generados usando software de seguridad dedicado, solo accesible a organizaciones certificadas como Impresores de alta seguridad (CWA 14641) por la confederación internacional de impresores e industrias asociadas.

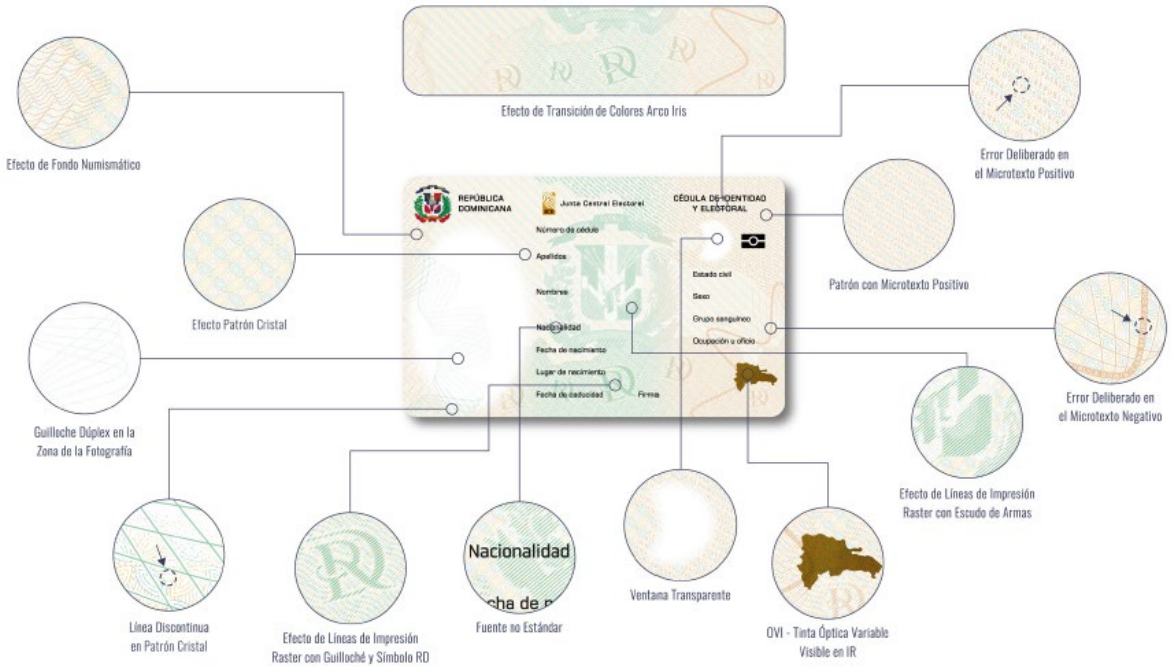
Este diseño gráfico es impreso en papel brillante con una impresora de alta calidad que ha sido calibrada para representar los colores lo más fielmente posible a cómo serán representados durante la producción en serie. Es encuadernado en dos folletos de presentación que son enviados al cliente para su aprobación.

Una vez aprobados, los diseños serán entregado en ficheros vectoriales de formato electrónico a la JCE, quien será la propietaria de todos los derechos sobre estos diseños.

Firma en la lámina lista para imprimir e inicio de la producción

Antes del inicio de la producción en volumen, la primerísima lámina de plástico impresa con el diseño gráfico final es enviada al cliente para validación y firma. Este paso también puede ser realizado por el cliente directamente en la fábrica SELP.

1.3.6 ELEMENTOS DE SEGURIDAD



En esta sección se describen los diferentes niveles de seguridad disponibles en el universo de elementos de seguridad utilizados en los documentos de identidad, así como la descripción detallada de cada uno de aquellos solicitados para las tarjetas de identidad en policarbonato. Todos estos elementos de seguridad se incluyen en los diseños exclusivos creados para la CIE y CI, objetos de esta licitación.

1.3.6.1 NIVEL DE SEGURIDAD

Los niveles de seguridad de autenticación de tarjetas son un enfoque estructurado para verificar la autenticidad de un documento, asegurando que cumpla con estándares estrictos en diferentes etapas de la inspección. Los niveles de seguridad y medios de verificación son los siguientes:

1.3.6.2 IMPRESIÓN DE SEGURIDAD

La impresión de seguridad utiliza técnicas de impresión gráfica sencillas, que son difíciles de reproducir, con el propósito de limitar la posibilidad de que los defraudadores copien o escaneen la tarjeta y recreen una

falsa. Estos elementos gráficos especiales constituyen la base de la seguridad de una tarjeta, y son los elementos de seguridad más utilizados en el sector de la identidad.

Incluyen guilloches, fondos iridiscentes, fondos numismáticos, motivos de cristal, microtextos, microlíneas.

1.3.6.2.1 GUILLOCHES

Los guilloches son elementos de seguridad gráficos elaborados exclusivamente con software de diseño de seguridad.

Un guilloche es un motivo compuesto de líneas muy delgadas entretejidas que forman una imagen única que solo puede ser recreada con el software del equipo y los parámetros usados en la creación del diseño original. El estilo gráfico del motivo guilloche consta de la interacción de líneas delgadas en motivos geométricos en aspectos positivo, negativo, radiante, deformación, marco o fondo.

El patrón cristal, el cual se puede visualizar en el diseño propuesto de CIE y CI, es un tipo de guilloche.

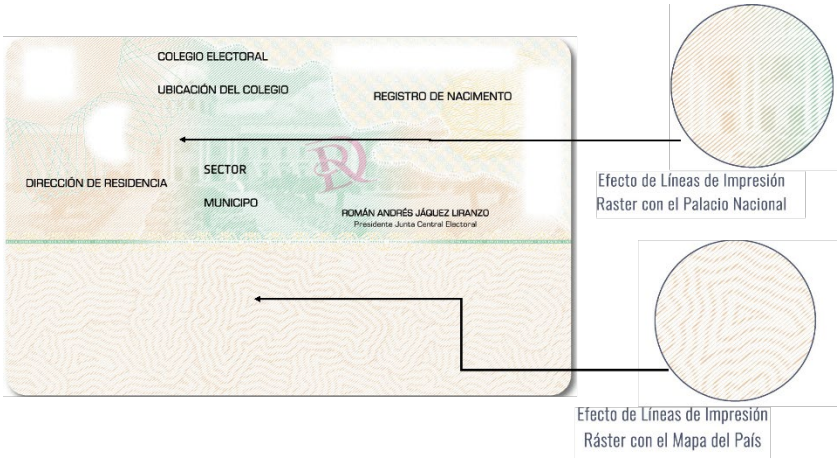
1.3.6.2.2 IMPRESIÓN EN ARCOÍRIS

Un fondo en arco iris se crea mezclando dos o cuatro colores sobre toda la superficie de la tarjeta. Los gradientes de color visibles o fluorescentes bajo radiación UV cambian continuamente de un color a otro. Es por ello que los bordes de color mezclándose entre sí representan una característica de seguridad que no puede ser copiada con las tecnologías de fotocopia o de digitalización en alta resolución.

1.3.6.2.3 MICROLÍNEAS DE AMPLITUD VARIABLE

Las microlíneas de amplitud variable, llamadas también Raster, son líneas muy pequeñas que se utilizan para crear tramas destinadas a impedir la copia de documentos de identidad, mediante el cambio de grosor y la distancia de las líneas, manteniendo constante la cobertura de tinta.

La idea detrás de este enfoque es que el proceso de falsificación no sería tan preciso y se verían diferentes tonos de color debido a la variación en el grosor del trazo y la distancia entre las líneas individuales.



1.3.6.2.4 MICROTEXTOS (POSITIVOS Y NEGATIVOS)

El microtexto es un texto muy pequeño que se extiende sobre el fondo de la tarjeta. Sólo puede leerse con una lupa y es imposible reproducirlos con las técnicas de impresión convencionales. Generalmente se utilizan para escribir el nombre de un país, su moneda, la autoridad que emite el documento o un mensaje. El objetivo de esta técnica es evitar la duplicación mediante fotocopia o escaneado.

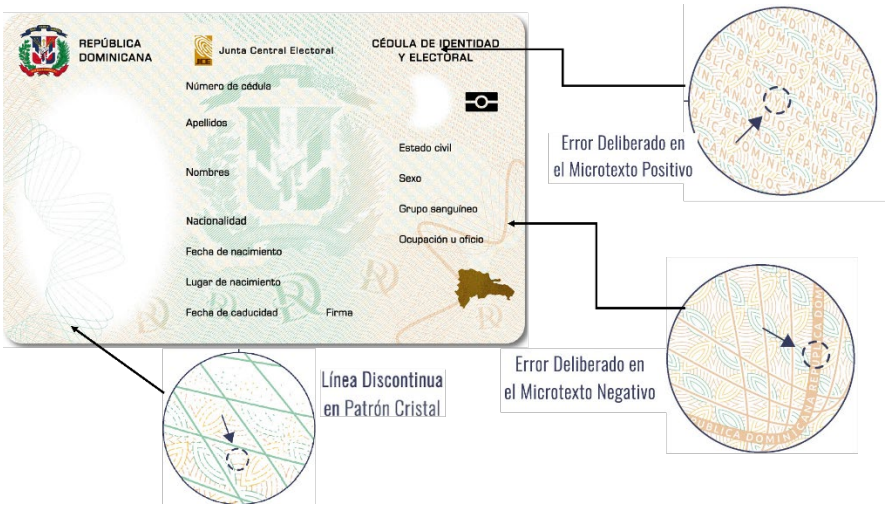
Reproducir microtextos con un alto grado de precisión y detalle es extremadamente complicado, ya que la finura de la impresión dificulta su producción y, por tanto, su reproducción. Al ser parte integrante del grafismo de la tarjeta y estar impreso al mismo tiempo que ésta, el microtexto es fácil de ocultar.

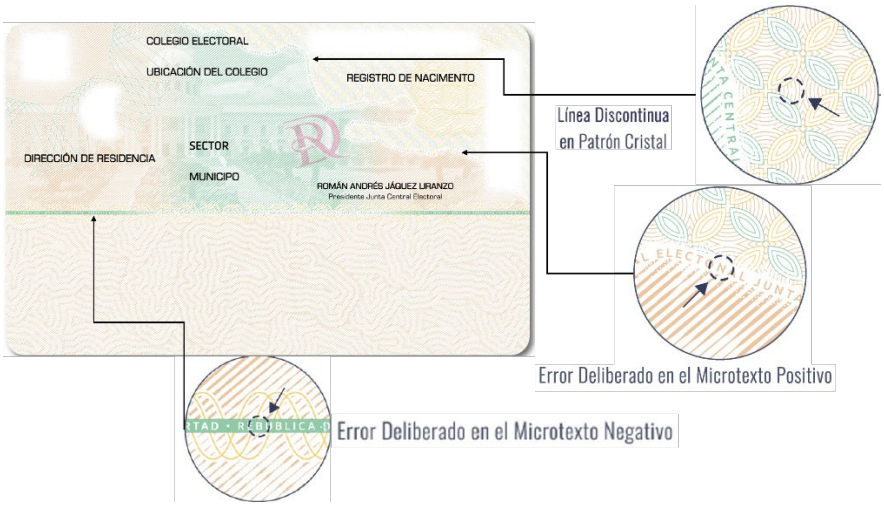
El microtexto suele ir unido a errores deliberados para crear zonas en la tarjeta que sean reconocibles y, por tanto, fáciles de comprobar.

1.3.6.2.5 ERRORES DELIBERADOS

Un error deliberado está pensado para eludir al falsificador: ya sea haciéndole creer que el documento que está copiando contiene un error de impresión, por lo cual no lo reproducirá en el documento falso (por ejemplo: un carácter no bien formado, un punto añadido, un corte en una línea delgada) o, por el contrario, ocultando un error deliberado que no será detectado por el falsificador, de modo que éste no lo reproducirá (por ejemplo: un carácter invertido en un microtexto, o una letra faltante).

Los errores deliberados son elementos de seguridad fáciles de incorporar y ocultar, pero también fáciles de comprobar por las autoridades competentes.

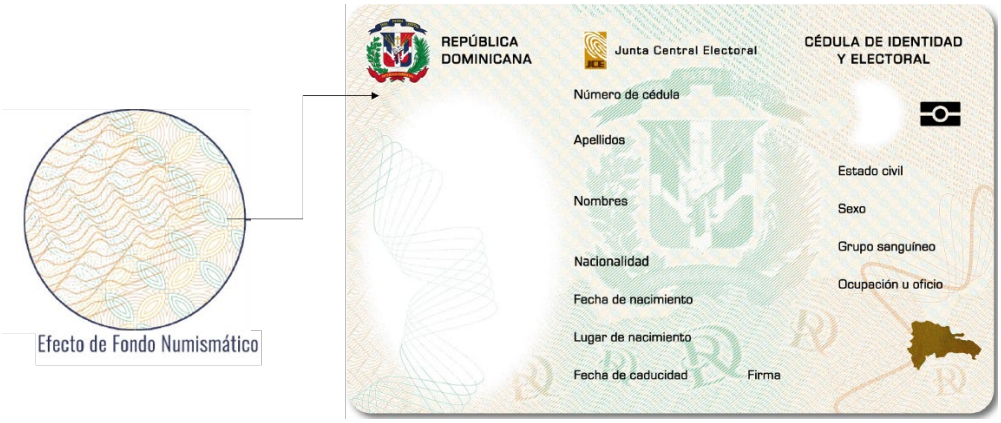




1.3.6.2.6 FONDOS NUMISMÁTICOS

Un fondo numismático usa una onda modulada que consta de líneas paralelas delgadas cuya orientación, grosor y espaciado varían a fin de generar un efecto de relieve y crear imágenes y / o texto de estas superficies elevadas. Una segunda serie de líneas a un ángulo de orientación distinta a la del primero (normalmente de un color diferente) puede reforzar eficazmente la impresión de relieve y crear un efecto tridimensional.

Esta característica gráfica ayuda a detectar la alteración de datos variables y documentos falsificados puesto que es difícil crear ambas líneas delgadas y los tonos de color que componen los diseños mediante escáneres y fotocopiadoras.



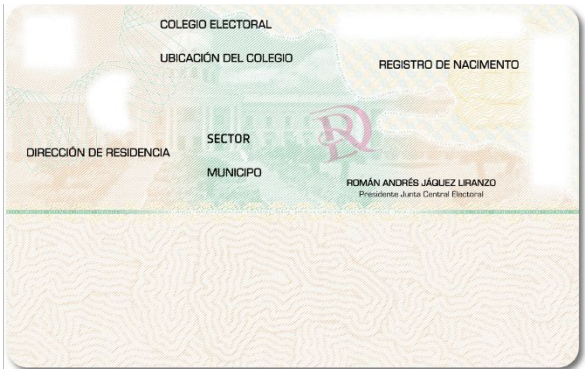
1.3.6.3 TINTAS UV INVISIBLES

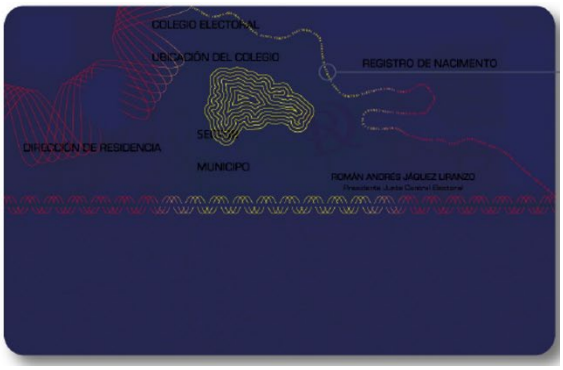
Las tintas especiales con propiedades que reaccionan a la luz ultravioleta (UV) son una parte importante de la protección de un documento de identidad. Cuando se exponen a la luz UV, estas tintas cambian de color y se vuelven reflectantes.

Esta tecnología abre posibilidades creativas para mejorar la seguridad de los documentos impresos. Al incorporar estas tintas especiales durante el proceso de impresión, se pueden incorporar detalles ocultos en el documento, creando nuevos patrones estéticos o resaltando rasgos distintivos como escudos, lemas y otras sutilezas.

Este proceso de seguridad de segundo nivel ofrece una sólida protección contra la imitación y la falsificación. Combinando el uso de estas tintas reactivas a los rayos UV con complejos guilloches, la seguridad de los documentos aumenta aún más.

En resumen, el uso de tintas UV reactivas representa una forma segura y estéticamente discreta de añadir elementos de seguridad a los documentos impresos. Estas tintas ofrecen una solución rentable para combatir la falsificación y reforzar la integridad de los documentos oficiales.





1.3.6.3.1 GUILLOCHES EN UV

Finas líneas entrelazadas, generalmente de naturaleza geométrica, crean una imagen única que impide la reproducción sin las herramientas y configuraciones originales que reaccionan a la luz UV.

1.3.6.3.2 MICROTEXTOS EN UV

Los microtextos son elementos textuales sutiles y detallados. Es posible hacer microletras que reaccionan a la luz ultravioleta. Por ejemplo, cuando pasa una fuente de luz UV, se puede mostrar el nombre del país emisor, la moneda nacional, la entidad emisora o un mensaje específico.

1.3.6.3.3 ARCOIRIS EN UV

Un degradado sutil y gradual de dos a cuatro colores en todo el sustrato, similar al efecto visual de un arco iris reaccionando a la luz ultravioleta. Este proceso solo se puede llevar a cabo a través de prensas offset especializadas.

1.3.6.3.4 UV MALLA DE FONDO EN MICROTEXTO

Realizando una combinación de microtextos dispuestos sobre un fondo guilloche con cierta disposición y utilizando tintas UV invisibles, se puede tener una Malla de fondo en microtexto UV.

1.3.6.4 TINTA ÓPTICAMENTE VARIABLE (OVI)

La tinta ópticamente variable (OVI por Optical Variable Ink) es una tecnología de seguridad poco común pero muy eficaz para proteger los documentos de identidad, los billetes de banco y otros documentos oficiales como los carnés profesionales. Esta tinta contiene pigmentos que tienen la particularidad de presentar dos colores distintos según el ángulo desde el que se mire el documento. Por ejemplo, según la orientación del observador, el color de la tinta puede cambiar de dorado a azul, de magenta a verde, o muchas otras combinaciones.

El fenómeno del cambio de color en estas tintas se debe a la forma en que reflejan diferentes longitudes de onda de la luz blanca en función del ángulo de incidencia sobre su superficie.

Esto las convierte en una medida muy eficaz contra la falsificación, ya que esta característica dificulta la copia o el escaneado precisos de documentos seguros mediante dispositivos como fotocopiadoras o escáneres en color, ya que necesitan un ángulo específico para reproducir el cambio de color. El OVI puede tener diferentes opciones de seguridad y complejidad, para una máxima protección del documento. Todos los OVI son visibles a la radiación IR.

1.3.6.5 ELEMENTOS HOLOGRÁFICOS

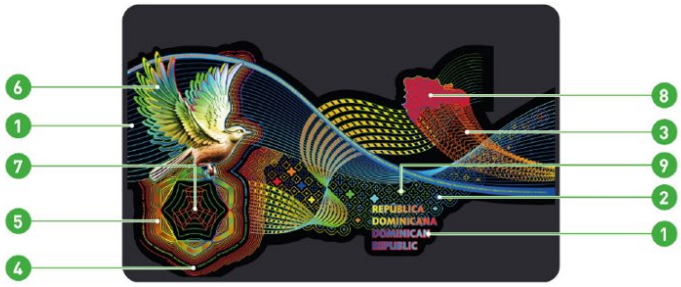
Un holograma de seguridad es un componente impreso que reduce la posibilidad de fraude gracias a su diseño y tecnología, que son complejos y caros. Se crea mediante la superposición de capas impresas que se hacen visibles o no en función de los ángulos de visión. El holograma destaca como uno de los elementos más predominantes de los dispositivos utilizados para reforzar la seguridad de los documentos sensibles. En concreto, se utiliza mucho para autenticar documentos y tarjetas de identidad, billetes de banco y tarjetas de crédito o débito. Con estos hologramas pueden conseguirse diversos efectos, de color, estructura o visuales, lo que convierte a los hologramas en un importante detalle estético del documento.

Hay que tener en cuenta que los hologramas pueden ser extremadamente complejos, con diferentes niveles de seguridad en su interior, que van desde simples cambios de color y texto cromático, o la aparición/desaparición de un visual, hasta nanotextos que sólo pueden observarse con herramientas de laboratorio. Un holograma es imposible de duplicar con un escáner o una fotocopiadora en color. Tampoco puede imitarse mediante procesos de impresión estándar.

Para las tarjetas en policarbonato, se tienen diferentes opciones. Una de éstas son los hologramas 3D, que forman parte de los DOVID (dispositivo difractivo de imagen ópticamente variable). Estos introducen imágenes tridimensionales y son capaces de incorporar visuales que cambian en respuesta al ángulo con que los mira la persona, así como variaciones cromáticas. El DOVID es un elemento holográfico incrustado dentro de un documento de policarbonato. Los DOVID transparentes protegen la fotografía grabada con láser de modificaciones o sustituciones.

Una capa holográfica es un holograma de mayor tamaño y puede llegar a estar presente en todo el documento seguro (holograma de borde a borde). Esta es, con mucho, la versión más agradable estéticamente porque el holograma se puede adaptar al diseño gráfico del producto agregando detalles y colores, al tiempo que mantiene una importante utilidad protectora porque cubre datos más confidenciales.

Para esta licitación, el holograma propuesto es un DOVID 3D transparente de borde a borde, el cual se muestra a continuación. Este cumple con los requisitos especificados en el punto I.4, I.8.1.1 y I.8.1.4.



1. Efecto cinético lineal: este efecto aparece como una transición de un color a lo largo de la forma cuando se inclina el holograma.
2. Rejilla difractiva directa: el efecto es visible sólo en un ángulo determinado como una forma o superficie coloreada
3. Efecto cinético de expansión: este efecto aparece como una expansión de un color a lo largo de la forma cuando se inclina el holograma.

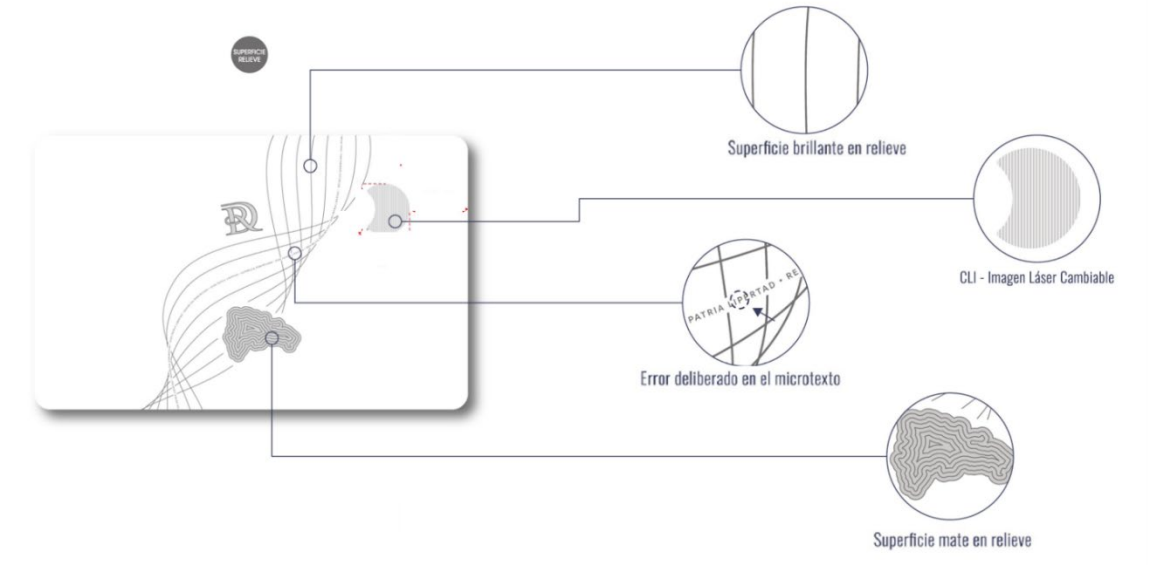
4. Efecto cinético lineal en un microtexto de 400 micras
5. Elemento óptico especial Axicona modificada: Aparece como múltiples líneas de colores que giran alrededor de su punto central y es visible desde cualquier dirección.
6. Bajorrelieve Pastel: Este se presenta coma un bajorrelieve 30 en color pastel reflectante con un alto nivel de detalle. La superficie de color pastel con brillo variado es muy visible bajo cualquier tipo de iluminación, incluida la luz diurna difusa. Es un elemento de seguridad muy fuerte. Se aplica al palmito que es el ave nacional de la República Dominicana
7. Rotación profunda: Un efecto 3D nítido sabre un motivo ornamental. Este efecto holográfico real, extremadamente brillante, aparece coma un objeto colorido de estructura alámbrica en 3D que flota de 3 a 5 mm por encima o por debajo de la superficie del holograma, incluido un objeto giratorio en 2D. La rotación del objeto es observable con una inclinación horizontal. IQ CHECK proporciona una autenticación inequívoca de un documento de identidad físico mediante un smartphone.
8. Efecto Ghost3D: El efecto holográfico real aparece coma un objeto de estructura alámbrica en 3D que flota a 100 mm por debajo de la superficie del holograma. El objeto es observable cuando se inclina horizontal y verticalmente. Solo es visible cuando el holograma se ilumina con una luz monocromática lateral. Este es un fuerte elemento de seguridad.
9. Imagen nanográfica y nanotextos: Este efecto permite la inscripción directa de una estructura de mapa de bits con una resolución de 254.000 dpi. Se utiliza para inscribir una imagen pequeña y nanotextos, que sólo son legibles con el uso de un microscopio forense

1.3.6.6 ELEMENTOS TÁCTILES / RELIEVE SUPERFICIAL POSITIVO O NEGATIVO

Los elementos táctiles de los documentos de identidad, como los contornos del país emisor, un emblema o cualquier otro elemento de diseño, se crean grabando las placas de laminación, aportando un terminado de alto o bajo relieve, así como una terminación mate o brillante. Estos pueden detectarse de forma táctil y visual cuando se inclina el documento. Esta técnica disuade la adición de capas fraudulentas, ya que cualquier modificación interfiere con la continuidad táctil del relieve.

Los microtextos son elementos textuales sutiles y detallados. Es posible hacer micro letras táctiles. Por ejemplo, se puede mostrar el nombre del país emisor, la moneda nacional, la entidad emisora o un mensaje específico. Los microtextos en relieve se colocan generalmente en forma de guilloche, pero se pueden controlar fácilmente con una lupa. También es posible incorporar errores deliberados. En nuestra propuesta se incluye un microtexto con error deliberado, tal y como se muestra en la figura siguiente.

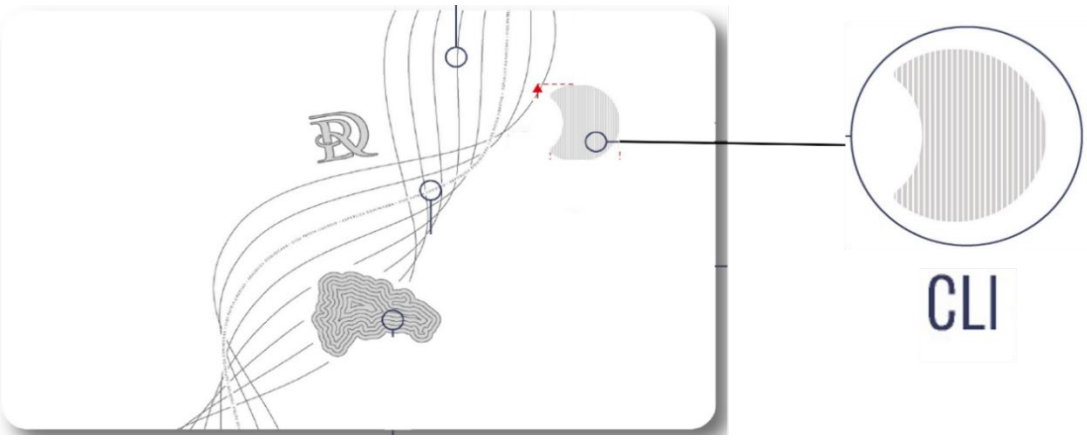
Superficie con Elementos en Relieve - Frente



1.3.6.7 MLI / CLI

El MLI o el CLI (Multiple Laser Image o Changeable Laser Image, respectivamente, por sus siglas en inglés), consisten en numerosas pequeñas lentes horizontales o verticales, respectivamente, incorporadas a la superficie de la tarjeta con placas de laminación especiales. Estos elementos de seguridad son personalizados posteriormente con láser. Según el ángulo de visión, el titular puede ver distintas partes de la información de la tarjeta, como la fecha de nacimiento, una pequeña foto, la firma, etc.

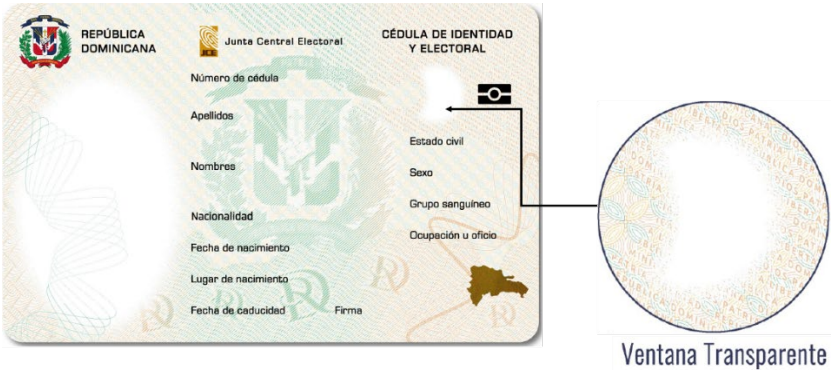
El CLI / MLI es el elemento de seguridad más eficaz contra la copia y la falsificación. No es posible reproducir los datos CLI / MLI grabados utilizando técnicas tradicionales como la fotocopia. La función CLI / MLI proporciona medios visuales y táctiles para verificar la autenticidad de la tarjeta.

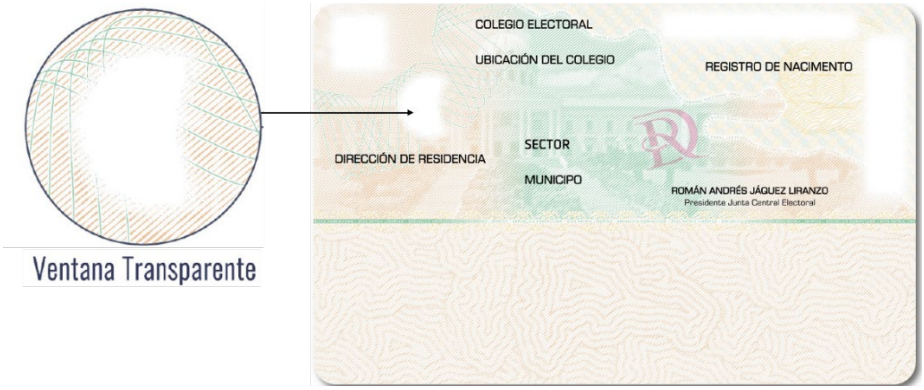


1.3.6.8 VENTANA TRANSPARENTE

La ventana transparente es un área transparente realizada en el material mediante un proceso de producción específico y avanzado. Su integración en el documento complica cualquier intento de infracción, en particular al impedir la adición ilegítima de capas de materiales que contienen datos falsificados.

La ventana transparente puede incorporar elementos de seguridad adicionales como la integración del retrato del titular del documento, tintas específicas o elementos táctiles, aumentando su seguridad. Tal y como se puede distinguir en nuestra propuesta de diseño, un CLI está incorporado dentro de la ventana transparente.





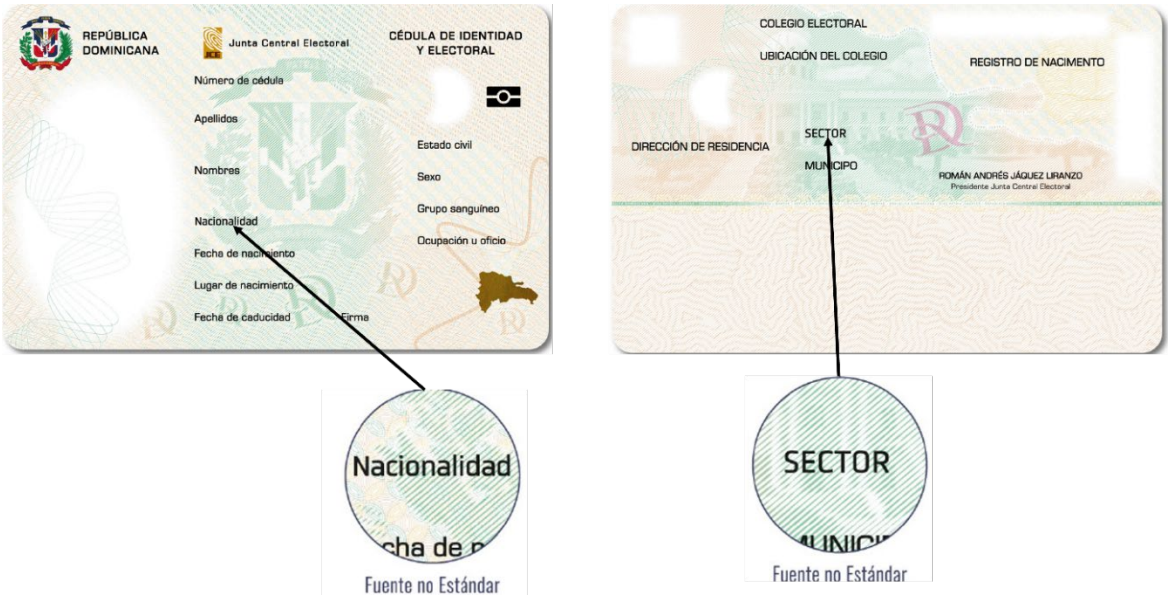
1.3.6.9 TINTAS INFRARROJAS ABSORBENTES/TRANSPARENTES

Las tintas infrarrojas (IR) transparentes y absorbentes mantienen un aspecto uniforme bajo iluminación normal y son claramente visibles sin ayudas ópticas. Cuando se someten a una fuente de luz infrarroja específica, solo las tintas IR absorbentes revelan su presencia, lo que permite una detección selectiva. Lo contrario sucede con las tintas IR transparentes, las cuales son invisibles al someterlas a una fuente de luz infrarroja específica. Esto permite la lectura mecánica del documento, como requisito ICAO.

Este atributo hace que las tintas IR sean especialmente eficaces como defensa adicional contra la copia ilegal.

1.3.6.10 OTROS ELEMENTOS DE SEGURIDAD

En el contexto de un proyecto de muy alta seguridad, SELP puede utilizar una fuente no estándar, lo que hará aún más difícil de copiar el documento.



Para esta licitación, SELP ha realizado una proposición de diseño para la Cédula de Identidad y Electoral (CIE) y otro para la Cédula de identidad (CI), los cuales incluyen todas las características de seguridad mencionadas en el punto I.8.1 “Características de seguridad de la tarjeta”. Favor de referirse al Booklet “Proposición de diseño CIE y CI” donde se muestran cada uno de los elementos de seguridad, tanto en el anverso como en el reverso de cada documento.

Nota: La construcción del cuerpo de la tarjeta esta diseñada sin capas /materiales patentados que limitarían al abastecimiento de materiales de producción de tarjetas a proveedores dedicados. A su vez el cuerpo de la tarjeta en blanco y el proceso de personalización de la misma en combinación no constituirán una solución dependiente o patentada que excluya a los proveedores de tarjetas y/o sistemas de personalización.

ÍTEM II - ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN

2. ESPECIFICACIONES TÉCNICAS SOLUCION DE IMPRESIÓN LASER

GET GROUP ofrece una solución modular de personalización de tarjetas que combina la impresión avanzada con capacidades de grabado láser para producir tarjetas láser en blanco y negro y a color en un proceso de personalización unificado para producir tarjetas de identificación gubernamentales seguras con características de seguridad complejas que no pueden manipularse ni sustituirse.

La solución de personalización CLM600 está disponible en un diseño compacto y liviano, y personaliza tarjetas de policarbonato en colores seguros con láminas holográficas personalizadas. Utiliza la tecnología de imagen híbrida LASMENT mediante impresión por re-transferencia segura con grabado láser.

Unidad de Impresión GET CLM600

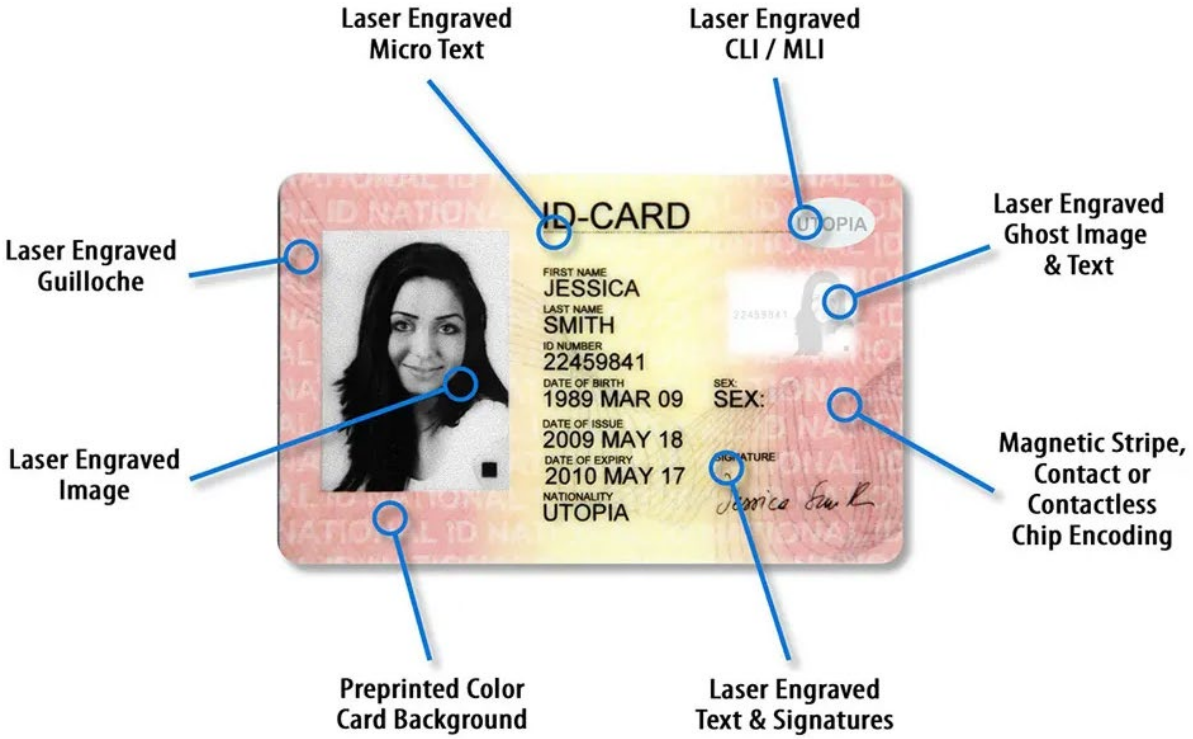
El CLM600 es una unidad láser de fibra de 20 W confiable que brinda un rendimiento y una calidad óptimos en el grabado láser de tarjetas. El control del láser está integrado en una única placa altamente integrada con una pantalla gráfica a color para monitorear el estado y las operaciones.

2.1 BENEFICIOS DE LA SOLUCIÓN

Calidad, seguridad y simplicidad todo en un solo paso para impresión a doble cara.

Equipo modular para ser integrado en diferentes opciones de personalización laser.

- Funcionalidad de impresión a blanco y negro en laser de alta calidad.
- Resolución de 600 dpi para escala de grises.
- Sistema de personalización de escritorio ideal para personalización descentralizada.
- Diseño industrial de gran robustez para trabajo de alto tráfico de impresión, incluso por 24 horas.
- Grabación Laser que permite la máxima seguridad de la tarjeta a través de funciones de Nivel 1, Nivel 2 y Nivel 3:
    - Microtextos
    - Imagen fluorescente a todo color.
    - Grabado en Relieve (táctil) personalizable.
    - Código de Barra de 1D y 2D.
    - Impresión de imágenes, imagen fantasma y logotipos.
- Funciones de seguridad de ventana CLI/MLI.
- El control del láser integrado con una pantalla gráfica en color para supervisar el estado y las operaciones.
- Tecnología de imagen híbrida LASMENT.
- Personalización y Codificación de tarjetas en cumplimiento del estándar ICAO Documento 9303.
- Impresión personalizada de acuerdo con las especificaciones del formato solicitado Pliego de Condiciones, según punto II.2.1 Formato (Lay out) de las tarjetas CIE y punto II.2.2 Formato (Lay out) de las tarjetas CI.
    - Datos personales.
    - Fotografía a blanco y negro en escala de grises.
    - Firma y Foto fantasma.
    - Personalización CLI.
    - Zona de Lectura Mecánica (MRZ)
    - Códigos de Barras 1D y 2D.
- Capacidad de incluir componentes adicionales para controles de calidad adicionales que permiten garantizar una inspección completa de inicio a fin del proceso de impresión:
    - Control de posicionamiento de la tarjeta, mediante cámara, iluminación y software dedicado para reconocer los elementos de referencia.
    - Lectura OCR/OCV para verificación de los elementos impresos en la tarjeta.
    - Lectura de códigos de barras en la tarjeta.
    - Codificador para tarjetas:
        - Chip sin contacto: Antena y conectividad para interactuar con tarjetas RFID según ISO 14443 Parte I a IV, tipo A/B, CL y Mifare (opcional). La opción se puede conectar en un puerto USB y mediante protocolo PC/SC o a través del SDK.
        - Antena para verificación de calidad, para comprobación de calidad.



2.2 CRITERIOS DE DESEMPEÑO ÚNICOS

- Adaptación descentralizada: la configuración descentralizada de GET CLM600 ofrece al cliente las siguientes ventajas clave:
    - Escalabilidad: Fácilmente escalable a la demanda de producción de cada ubicación.
    - Operación: Cargas equilibradas y más bajas en cada sitio mantendrían un rendimiento de producción garantizado durante toda la duración del proyecto.
    - Riesgo distribuido: Los riesgos están distribuidos; por lo tanto, es muy poco probable que falle todo el sistema.
    - Entrega: La emisión dentro de la misma provincia garantizará plazos de entrega inmediatos o más cortos que una impresión centralizada.
    - Solución de problemas: fácil de definir, localizar y solucionar errores o problemas.
    - Configuración del sitio: pequeñas ubicaciones propiedad del gobierno podrían albergar el sistema de emisión.
    - Seguridad: La entrega directa de documentos seguros personalizados a los ciudadanos dentro de cada provincia minimiza cualquier riesgo de mal manejo.
    - Monitoreo: Esfuerzos moderados de monitoreo y supervisión.
    - Equipada con un sistema de alimentación ininterrumpida (UPS), asegurando al menos dos minutos de autonomía en caso de interrupciones eléctricas. Este respaldo permite la finalización segura de los procesos de impresión en curso, minimizando riesgos de fallas o pérdida de datos.

2.3 MÓDULO LASER CLM600

El CLM600 es un sistema modular compacto de personalización de tarjetas de escritorio que ejecuta personalización de gráficos mediante grabado láser y ofrece opciones de codificación para banda magnética y chip de contacto y sin contacto.

El CLM600 es una unidad láser de fibra confiable de 20 W que proporciona un rendimiento y calidad óptimos en el grabado láser de tarjetas. El control láser está integrado en una única placa altamente integrada con una pantalla gráfica en color para monitorear el estado y las operaciones.

Las características relevantes del CLM600 son las siguientes:

CLM600	
Rendimiento (TPH)	Diseño industrial de hasta 60 tarjetas por hora (TPH) a doble cara, dependiendo del diseño, composición de la tarjeta y los requerimientos de codificación y verificación QA. Eficiencia productiva de más del 95%.
Personalización	Grabado Laser (Class 1), codificación de chip, banda magnética
Tecnología de personalización	Laser de Fibra 20W refrigerado por aire
Area de trabajo	Mayor a la especificada en el ID1/CR80, con un borde de 1.5 mm

Seguridad en Operación	Sistemas de bloque interno para evitar la apertura durante las operaciones.
Seguridad ambiental	Extractor de aire con filtro de carbón activo
CLI/MLI	MLI/CLI mediante desviación óptica (espejos)
Codificación de Banda magnética	Tracks 1, 2, 3 HiCo/LoCo read/write per ISO/IEC 7810, 7811
Codificación Chip de Contacto	Estación de contacto para ISO/IEC 7816 lectura y escritura, PC/SC
Codificación Chip sin Contacto	ISO 14443 Part I a IV, tipo A/B, CL y Mifare (opcional), PC/SC
Aseguramiento de calidad	Cámara con auto posicionamiento (5 Mpx, standard), Verificación OCR para lectura y códigos de barras (SW opcional)
Bandeja de alimentación de tarjetas	Alimentador de tarjetas con capacidad para entre 100 y 300 tarjetas
Administración de la tarjeta	Transporte sin rayones, modular, con volteo integrado
Bandeja de salida de tarjetas	Bandeja de 100 tarjetas Bandeja de rechazo de 10 tarjetas
Monitor de estado	Pantalla gráfica en color de 128x64 píxeles para acceso a operador.
Integración de Software	Integración de software multiplataforma mediante SDK propietario con licencia gratuita. Código fuente de ejemplo de integración. PC integrado WINDOWS. Incluye los elementos necesarios para desarrollar, compilar, depurar y probar las aplicaciones de personalización en un entorno de pruebas.
Control de Láser	Aplicación de control láser integrada (basada en PC, integrada)
Diagnóstico y Personalización	iCube (Id IDInterface), aplicación de configuración y monitoreo basada en web (web-based) para informes de producción. Personalización de datos personales almacenados de manera temporal, acorde a configuración.
Tamaño y peso	300 x 300 x 500(a) mm 29 Kgs./ Largo por ancho (0.09m²).;
Fuente de Alimentación	110/240V AC, 50/60Hz, 300W
Conectividad	Ethernet LAN

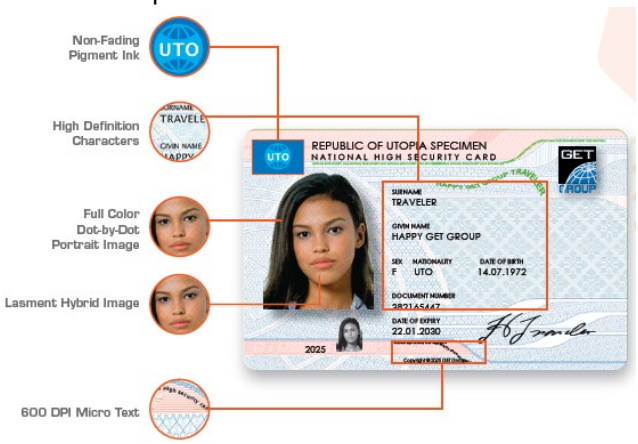
2.4 CARACTERÍSTICAS ADICIONALES

Las características relevantes del CLM600 son las siguientes:

CLM600	
El sistema de posicionamiento automático XY	El sistema de posicionamiento automático XY tiene como objetivo asegurar la posición exacta del grabado y consta de un conjunto de cámara en escala de grises, iluminación con LED múltiple y software dedicados a capturar la imagen, reconocer los elementos de referencia y medir su posición (orientación), ya sea para la tarjeta relativa al sistema, y para los elementos relativos a los otros elementos de la tarjeta.
Lectura OCR/OCV	Esta es una herramienta de software que permite implementar la lectura y verificación de texto impreso en documentos, por anverso y reverso de la tarjeta. La herramienta actualiza las funcionalidades del kit de cámara. Validación de textos impresos y ZLM (MRZ)
Lectura de códigos de barra	Esta es una herramienta de software que permite leer códigos de barras 2D/3D en documentos. La herramienta actualiza las funcionalidades del kit de cámara.
Aseguramiento de Calidad	El conjunto de lectura de OCR y/o códigos de barras, normalmente utilizado para identificar las tarjetas entrantes, también puede abordar el control de calidad, comprobando la coherencia de los datos gráficos y verificando la legibilidad de los datos grabados. Rechazo por la ausencia de los datos requeridos.
Codificación Chip sin Contacto	La opción de codificación de chip sin contacto proporciona la antena y la conectividad para interactuar con tarjetas RFID según ISO 14443 Parte I a IV, tipo A/B, CL y Mifare (opcional). La opción se puede conectar a un puerto USB y mediante protocolo PC/SC o mediante SDK. Opción también disponible desde el módulo de impresión a color CP500. Integrado al componente de Middleware incluido en esta propuesta. Control de Lectura a la entrada, que permite verificar la tarjeta a ser grabada antes de su proceso de codificación (ATS). Opcional: Control de lectura al final del proceso de codificación e impresión, por antena adicional.
Codificación Chip de Contacto	La opción de codificación de chip de contacto proporciona la conexión mecánica a tarjetas con chip ISO7816. El módulo de chip de contacto se puede conectar a un puerto USB y mediante el protocolo PC/SC o mediante el SDK.
Codificación de Banda Magnética	Este es un módulo dedicado capaz de codificar y leer TRK1, 2 y 3 (2 pistas en una sola pasada), separado del transporte principal, que funciona cargando la tarjeta desde la estación de volteo.
MLI/CLI Grabado inclinado	El grabado inclinado se realiza mediante un método patentado que utiliza espejos para desviar el rayo láser en un ángulo adecuado. La principal ventaja de esta solución es reducir el impacto de MLI/CLI en la productividad, ya que la tarjeta no se mueve de la posición de grabado estándar y el tiempo de ejecución corresponde al tiempo necesario para grabar dos entidades.

2.5 MÓDULO OPCIONAL PARA IMPRESIÓN A COLOR GET CP500

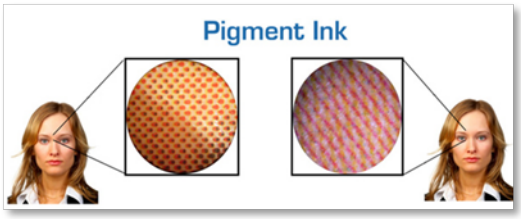
El módulo laser GET CLM600, tiene la opción de poder ser integrado con un módulo de impresión a color por re-transferencia térmica, lo que evoluciona al equipo denominado GET CP500LE. La CP500LE es una solución modular integrada de personalización de tarjetas que combina la impresión por re-transferencia inversa avanzada de la CP500 con capacidades de grabado láser de la GET CLM600 en un proceso de personalización unificado que produce tarjetas de identificación gubernamentales seguras con características de seguridad complejas que no se pueden manipular ni sustituir. La solución está disponible en un diseño compacto y liviano, y produce tarjetas de policarbonato a color seguras con láminas holográficas personalizadas en un solo paso.



1. Imágenes a full color en 600 dpi sobre tarjetas en policarbonato.
2. Estabilidad del color a largo plazo con tintas pigmentadas resistentes a la decoloración.
3. Opciones avanzadas de grabado láser.
4. Tecnología de imagen híbrida LASMENT.
5. Máxima seguridad de la tarjeta a través de funciones de Nivel 1, Nivel 2 y Nivel 3:

5.1 Personalización variable UV
5.2 Tinta variable reflectante Plus (RVI+)
5.3 Microtextos
5.4 Patrón de impresión único punto por punto
5.5 Imagen fluorescente a todo color.

6. 10 años de resistencia a la decoloración.
7. Opción de Película holográfica de retransferencia segura.
8. Funcionalidad de impresión a blanco y negro en laser de alta calidad.



2.6 CONDICIONES DE GARANTÍA

Marcador láser CLM600

GARANTÍA:

- Reemplazar o reparar las piezas que se demuestren defectuosas durante el período de garantía, excepto las piezas sujetas a desgaste normal y las piezas consumibles.
- La garantía estándar cubre todas las piezas mecánicas y eléctricas.
- Tiempo de Garantía: 5 años posteriores a la entrega de equipos a la JCE.
- Tiempo de vida útil: Hasta 10 años, siempre y cuando se sigan las instrucciones y recomendaciones del fabricante en cuanto a instalación, operación, mantenimiento y uso de partes originales.

LIMITACIONES:

- La garantía cubre fallas de fabricación o mal funcionamiento durante el funcionamiento normal de la máquina.
- El Consorcio no se hace responsable de los defectos causados por una mala instalación, en los casos donde el consorcio no realice la instalación (ejemplo: luego de un mantenimiento), o por un uso incorrecto de la máquina o el desgaste de las piezas.
- La garantía no cubre los mal funcionamientos resultantes del grabado de cualquier otro material que no sea PC. Las tarjetas que no sean de policarbonato deben probarse y aprobarse con anticipación.

CONDICIONES QUE ANULA LA GARANTÍA:

A) Condiciones ambientales:

- humedad elevada
- temperatura elevada
- cualquier condición ambiental fuera de las Especificaciones Técnicas

B) Falta de mantenimiento regular.

C) La cantidad de ciclos o documentos producidos durante el uso normal de la máquina. (**ver clasificación de repuestos)**

CLASIFICACIÓN DE REPUESTOS:

Description
FUSE 5X20 10A (F)
EUROPEAN POWER CORD
POWER SUPPLY RWS300B-24
ON/OFF SWITCH
MAIN POWER PLUG AND FILTER
IDC 16G CONTROL BOARD ASSEMBLY
JPT FIBER LASER 20W WITH RED PILOT BEAM
IDC SCAN HEAD

“SCAPS” USC-1 BOARD WITH SOFTWARE
F-THETA LENS 160 1064 M39
Ø25.4mm MIRROR, BROADBAND 603&1064 nm
2.0 A-B 0,6m USB CABLE
CARD TRANSPORT SIGNAL CABLE IDC6
USC1-SCAN HEAD CABLE IDC6
USC1-DB37-IDX_CTRL CABLE IDC6
LASER SOL-IDX_CTRL CABLE IDC6
IDC CARD TRANSPORT
IDX INTERFACE BOARD 1
REPETEABLE TRANSPORT PARTS
BELT 60MXL025-75D ENCODER
MXL Z180 025 BELT
O-RING BELT Ø2.62X133
IDC RUBBER ROLLER Ø15
IDC O-RING PULLEY
IDC INPUT LOWER ROLLERS KIT
IDC PINCH ROLLER KIT
IDC OUPUT LOWER ROLLERS KIT
IDC FLIP OVER KIT
CARD TRANSPORT ELECTRICAL PARTS
CARD TRANSPORT PHOTOSENS. W\CABLE CARD
TRANSPORT STEP MOTOR W\CABLE
IDC DC MOTOR W/CABLE
*** VISION ***
IDX & IDC XY AUTOPOSITIONING GREYSCALE CAMERA KIT
CAMERA ILLUMINATOR
**** VISION CAMERA LICENSES ***
OCR/OCV READING TOOL (SINGLE LICENSE, 1 FOR EACH CAMERA)
BARCODE READING TOOL (SINGLE LICENSE, 1 FOR EACH CAMERA)
**** CLI / MLI MIRRORS *****
CLI/MLI MIRROR SPARE PART
**** MISCELLANEOUS ***
IDX INTERFACE BOARD 1
USB FEED THROUGH CONNECTOR
CENTRIFUGAL FAN 51x51 24Vdc
FAN 92x92x25 12Vdc
REED SWITCH SENSOR WITH UL CABLE
INTERLOCK MAGNET
DONGLE EXTERNAL INTERLOCK
LOCK ASSEMBLY + KEY
*** MACHINE KIT CABLE ***

IDC20 CABLES KIT
**** CONSUMABLE ***
ACTIVE CARBON FILTER FOR IDC

A) Corredores (RUN): piezas sujetas a desgaste y por tanto relacionadas con la carga de trabajo, por ejemplo:

- Rodillos
- Correas

B) Repetidores (RPT): piezas con vida limitada o con vida menor o cercana a la vida de la máquina, por ejemplo:

- Iluminador Led para Sistema de visión: 15.000hrs
- Diodo Láser: 30.000hrs
- Integridad de Datos Disco SSD: 15.000hrs
- Módulo Magnético: 750.000 Ciclos

C) Extraños (STR): piezas con tasa de fallos impredecible o con vida útil comparable a la vida del sistema, por ejemplo:

- Conjunto de Transporte de Tarjetas
- Resonador Láser
- Cabezal de Escáner Láser
- Láser de Radio Frecuencia
- Láser de Fibra
- Tarjetas Electrónicas

D) Consumibles (CNS): piezas que necesitan ser reemplazadas a intervalos regulares, por ejemplo:

- Filtro de carbón activo

NOTA:

Las horas de vida útil dependen en gran medida de las condiciones ambientales de trabajo y los parámetros de salida.

ÍTEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI - CA

3.1 GET TRUST – SOLUCIÓN DE PKI

En nuestra búsqueda de una solución de infraestructura de clave pública (PKI) sólida y segura, hemos implementado "GET Trust", que es compatible con los estándares de la ICAO (OACI). Este sistema PKI de vanguardia ha sido meticulosamente diseñado y ejecutado por nuestro equipo de PID (Departamento Comercial de Pasaportes e Identificación) para cumplir con los más altos estándares de seguridad y garantizar la integridad y autenticidad de las transacciones digitales.

3.1.1 ARQUITECTURA DEL SOFTWARE

GET Trust establece una estructura clara y jerárquica para nuestros certificados digitales. Incluye una Autoridad de Certificación de Firma de País (CSCA) de primer nivel para seguridad a nivel nacional, así como Autoridades de Certificación Técnica (CA Técnicas) para manejar certificados SSL y otros certificados técnicos.

Sus módulos se componen de varios submódulos propietarios de PKI de la OACI que se pueden utilizar para firmar información de forma segura en documentos electrónicos y proteger datos confidenciales como identidades digitales.

- **Extensible**

GET Trust es altamente extensible. Ofrece soporte para múltiples API criptográficas y se integra perfectamente con una variedad de dispositivos de módulo de seguridad de hardware (HSM), lo que garantiza adaptabilidad y compatibilidad en diversos entornos operativos.

- **Escalable**

GET Trust ha sido ingeniosamente diseñado como una arquitectura de microservicios, lo que garantiza flexibilidad y escalabilidad. Este sistema puede escalarse horizontalmente fácilmente agregando sin esfuerzo firmantes de datos adicionales cuando surja la necesidad.

- **Registro**

GET Trust, con su arquitectura de microservicios, también prioriza capacidades de registro sólidas. Proporciona funciones de registro amplias y configurables, lo que permite un seguimiento y análisis exhaustivos de las actividades del sistema para mejorar la seguridad y la resolución de problemas.

- **Gestión de usuarios**

La gestión de usuarios es un aspecto fundamental del conjunto de funciones de GET Trust. El sistema incluye sólidas funcionalidades de administración de usuarios, lo que permite a los administradores crear, administrar y controlar de manera eficiente el acceso, los permisos y los procesos de autenticación de los usuarios para operaciones seguras y sin inconvenientes.

- **Mecanismo de confianza en la máquina (Machine Trust)**

GET Trust incorpora un sofisticado mecanismo Machine Trust que aprovecha las autoridades de certificación técnicas (Technical CA) para emitir certificados SSL. Las claves generadas dentro de este mecanismo se almacenan de forma segura en Módulos de plataforma segura (TPM) y están diseñadas para no ser

exportables. Esta estricta medida de seguridad garantiza la máxima protección de los materiales criptográficos confidenciales, mejorando la postura de seguridad general del sistema.

3.2 GET AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA – CSCA

La Autoridad de Certificación de Firma de País (CSCA) de GET Trust permitirá las siguientes funcionalidades:

- Confidencialidad: garantía con certificados de cifrado
- Integridad: garantía con certificados de firma.
- Autenticación: garantía con certificados de autenticación
- No repudio: garantía con certificados de firma y autenticación
- Control de acceso: garantía con certificados de autenticación

El software ID-CA actúa en la solución propuesta como CSCA, como fabricante de certificados gestionando su ciclo de vida.

El objetivo del componente ID-CA es permitir una gestión centralizada y segura del ciclo de vida de los certificados gracias a las siguientes funcionalidades:

- Creación de autoridades de certificación.
- Creación de certificados de usuario (entidad final) por parte de las autoridades de certificación.
- Revocación de certificados por parte de las autoridades certificadoras.
- Creación automática de CRL (listas de revocación de certificados) para cada autoridad certificadora.
- Publicación de certificados de usuario (entidad final) y CRL en un directorio LDAP.

Una característica interesante de ID-CA es la multi entidad, que permite crear instancias de un número ilimitado de particiones (dominios), capaces de alojar una jerarquía PKI completa con CA raíz e intermedia. Estas particiones actúan como dominios separados y, por lo tanto, es posible implementar entornos de confianza de clientes completamente independientes dentro de la misma instancia de software.

Centrándose en la capacidad de abordar todo tipo de segmentos del mercado de identidad digital, ID-CA también ha sido diseñado para satisfacer todos los requisitos de las necesidades de Seguridad Corporativa y, en particular:

- Proporcionar una variedad de conectores de interfaz, permitiendo la integración en el sistema de TI de la empresa.
- Implementar una configuración altamente empaquetada y, por lo tanto, eliminar la complejidad de las implementaciones de PKI.
- Instalación y configuración del sistema fáciles de usar.

Como enfoque general, su desarrollo tuvo mucho cuidado en facilitar al máximo el uso de PKI. Por lo tanto, se han revisado todos los aspectos, desde los procedimientos de instalación hasta las tareas administrativas diarias, donde se guía y apoya al administrador durante la configuración y ejecución de la aplicación.

Considerando los esquemas de evaluación de seguridad de terceros como garantía de calidad, seguridad y robustez, ID-CA se somete a un proceso de certificación Common Criteria, dirigido al nivel EAL4+. Este enfoque es una apuesta clara por mantener continuamente el nivel de seguridad del software, como lo demuestran las certificaciones EAL3+ y EAL4+ obtenidas por productos anteriores.

GESTIÓN DEL ALMACÉN DE CLAVES

Un KeyStore es la configuración para acceder al contenedor de claves criptográficas de hardware o software.

Permite generar pares de claves criptográficas basadas en servicios criptográficos proporcionados por bibliotecas de software, tokens de tarjetas inteligentes (a través del middleware PKCS11) o mediante un Crypto Server (capa de abstracción de hardware), conectado a un HSM.

El tipo de algoritmos, parámetros y longitudes de clave dependen únicamente del recurso elegido. Por lo tanto, con el software o hardware adecuado, ID-CA admite RSA hasta 4096 bits y ECDSA hasta 512 (curvas NIST, Brain Pool y otros parámetros).

Los HSM compatibles son de la familia EVIDEN Trustway Proteccio, Safenet y Thales (nCipher). Cualquier otro HSM estándar basado en PKCS#11 puede ser compatible después de la calificación.

La gestión del KeyStore consiste en Creación, Edición, Actualización y Eliminación.

GESTIÓN DE DEPOSITOS EN GARANTIA

ID-CA integra la gestión de depósitos en garantía (Escrow Management) como función principal.

El depósito de claves es un acuerdo en el que las claves necesarias para descifrar datos cifrados se mantienen en depósitos de garantía y, en determinadas circunstancias, el propietario o un tercero autorizado puede obtener acceso a esas claves. El depósito en garantía se utiliza a menudo con la generación de claves centralizada (es decir, emisión de pares de claves en el lado de PKI), para limitar el riesgo de filtración de la clave.

La clave maestra para escrow, la clave simétrica y la clave de usuario final se generan en un recurso criptográfico de hardware, cada vez que existe una solicitud de generación de clave centralizada.

De forma predeterminada, la clave maestra es una clave RSA de 3072 bits y la CLAVE simétrica es una clave AES de 256.

Están disponibles las siguientes funciones:

- **Creación de configuración de generación de claves:** cree una configuración de generación de claves para la partición actual.
- **Habilitar la generación centralizada de pares de claves en el perfil de certificado:** habilite la generación de pares de claves mediante PKI (generación centralizada de pares de claves) para un perfil de certificado en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.

- **Habilitar depósito en garantía en perfil de certificado:** habilite el depósito en garantía para un perfil de certificado en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- **Clave de depósito en garantía:** deposita en custodia una clave para un certificado en una partición de destino.
- **Recuperar clave en custodia:** recupere una clave que ha sido en custodia para un certificado en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.

AUTORIDAD DE CERTIFICACIÓN DE CONFIANZA

ID-CA permite una gestión de autoridades de certificación muy sofisticada y eficaz.

Una Autoridad de Certificación (CA) es la parte esencial de un sistema PKI. Su función principal es emitir certificados y gestionar su ciclo de vida. Una CA puede tener varios certificados, que deben tener el mismo DN (Domain Name).

Con ID-CA están disponibles las siguientes funciones de gestión de CA disponibles en el mercado:

- **Generación de pares de claves de CA:** genere un par de claves para un certificado de CA
- **Creación de certificado de CA firmado localmente/renovación de certificado con nueva clave:** crear un certificado de CA para una configuración de CA
- **Creación de certificado de CA firmado externamente/renovación de certificado con nueva clave:** cree una CSR para firmarlo externamente e importar el certificado resultante.
- **Importar certificado de CA/renovación de certificado:** importar un certificado de CA a una CA

ID-CA implementa una característica particular, el concepto *CA Group*, que permite una gestión de CA altamente flexible y segura.

CA Groups permite a los administradores gestionar varias CA en una sola entidad. En general, los *CA Groups* están formados por una sola CA y, por lo tanto, el concepto de grupo se oculta en aras de la simplicidad. Los *CA Groups* permiten:

- Garantizar que el servicio de firmas permanezca disponible incluso cuando el tráfico de firmas esté en su nivel más alto: una CA definida en un *CA Group* puede tener una cuota de firmas. Cuando una CA alcanza la cuota de firmas, el servicio de firma cambia a la siguiente *CA Group* que aún no ha alcanzado la cuota de firmas.
- Administrar las CRL (listas de revocación de certificados) para todas las CA dentro del *CA Group*.
- Predefina las CA antes de crear certificados de CA: los *CA Groups* se pueden crear y configurar antes de que se hayan creado los certificados de CA; luego los certificados de CA se pueden cargar cuando estén disponibles.

La función *CA Groups* es de particular interés para proyectos de identidad a gran escala donde se necesita producir una gran cantidad de certificados de ciudadanos (usuarios). De hecho, *CA Groups* evita ataques criptoanalíticos a una única clave privada de CA. *CA Group* se administra fácilmente mediante configuración y mecanismos GUI.

En detalle, están disponibles las siguientes funciones de *CA Group*:

- Creación de *CA Group* mediante la importación de un certificado: Cree un *CA Group* en la Partición actual o cualquier Partición en un nivel inferior de la rama del árbol, con dentro, una CA y un certificado importado.
- Creación de *CA Group* con certificado firmado localmente: cree un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol, con una CA interna y su certificado firmado por una CA local.
- Creación de *CA Group* con certificado firmado externamente: cree un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol, con dentro, una CA y su certificado firmado por una CA externa.
- Edición de *CA Group*: edite el *CA Group* en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- Importación de *CA Group*: cree un *CA Group* en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol, desde un archivo XML.
- Exportación de *CA Group*: exportación XML de un *CA Group* en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- Eliminación de *CA Group*: elimine un *CA Group* que no tenga un certificado de CA en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.

ADMINISTRACIÓN DE PERFILES DE CERTIFICADOS

La principal tarea de una Autoridad de Certificación es, por definición, producir certificados digitales.

ID-CA realiza esta tarea con un enfoque particular en el rendimiento y la facilidad de uso, para permitir una rápida definición del perfil de certificado y la producción de certificados en gran volumen.

En lo que a tareas de administración se refiere, se puede:

- Crear/Editar perfiles de certificados
- Importar/exportar perfiles de certificados

La estructura de un certificado se puede crear de una manera muy sencilla mediante soporte GUI, en un proceso guiado que permite al usuario ingresar solo valores que no están predefinidos.

Además, y para poder combinarlo con productos anteriores de CA, es posible importar perfiles de certificados también en formato XML.

Para configurar rápidamente varios entornos, como ensayo, preproducción y producción, también se pueden exportar perfiles de certificados, así como otros datos de configuración, en formato XML.

Un perfil de certificado está asociado con una CA o un grupo de CA. Determina las propiedades del certificado, como el tamaño de la clave pública, el período de validez, el DN y los usos de clave para todos los certificados emitidos por la CA o el grupo de CA asociado con el perfil del certificado.

A través de la GUI, se puede definir, editar y modificar casi todos los elementos dentro de un perfil de certificado. La gestión del perfil del Certificado IDnomic ID-CA permite, en particular, definir libremente:

- El formato del certificado
- El algoritmo utilizado para el certificado.
- La firma del Grupo CA
- La información del certificado y cómo obtener esta información.

ADMINISTRACIÓN DE LISTAS DE REVOCACIÓN DE CERTIFICADOS

Periódicamente se genera y publica una lista de revocación de certificados (CRL), a menudo en un intervalo definido.

ID-CA implementa todas las funciones de gestión de CRL necesarias para producir y distribuir información de revocación a todas las aplicaciones relevantes. Además de la publicación (automática), también se puede recuperar la CRL manualmente a través de la GUI.

Una CRL también se puede publicar inmediatamente después de que se haya revocado un certificado. La CRL siempre la emite la CA que emite los certificados correspondientes. Todas las CRL tienen una vida útil durante la cual son válidas. Durante el período de validez de una CRL, una aplicación habilitada para PKI puede consultarla para verificar un certificado antes de su uso.

También es posible generar una CRL Delta, que es la lista de cambios desde la última CRL.

Las funciones de Gestión de CRL de ID-CA consisten en:

- **Configuración de generación de CRL en grupo CA:** configure la información de CRL de un grupo CA para producir CRL (y opcionalmente Delta CRL).
- **Producción automática de CRL:** produzca periódicamente una CRL completa (y opcionalmente una CRL Delta) para todas las CA válidas de un grupo de CA.
- **Producción automática de Delta CRL:** produzca una Delta CRL periódicamente para todas las CA válidas en un grupo de CA.
- **Producción manual de CRL:** produzca periódicamente una CRL completa (y opcionalmente una CRL Delta) para todas las CA válidas de un grupo de CA.
- **Descarga de CRL mediante GUI:** descarga mediante GUI, la última CRL completa o Delta CRL de una CA en la partición actual o cualquier partición en un nivel inferior de la rama del árbol.
- **Descarga de CRL vía HTTP:** Descarga vía HTTP, última CRL completa o Delta CRL de CA.

ADMINISTRACIÓN DE PUBLICACIÓN

La publicación de la información producida (certificados y CRL) es una tarea clave en los sistemas PKI para hacer que los datos públicos estén disponibles para verificar la identidad digital y su validez. La publicación en ID-CA está disponible tanto para Certificados como para CRL al ser datos públicos de una CA.

ID-CA tiene una gestión de publicaciones muy fácil de usar, que consiste en un proceso de configuración basado en GUI combinado con elementos de configuración. La publicación se puede realizar de forma automática o manual.

En particular, las características de ID-CA Publication Management consisten en todas las funciones del ciclo de vida, como creación, edición y eliminación para terminales, estrategia de publicación y política de publicación.

Además, ID-CA admite de forma nativa la política de publicación de enlaces para la publicación de certificados y CRL, así como la publicación automática.

Para configurar una publicación se necesitan varias configuraciones (Endpoint, Estrategia de publicación, Política de publicación).

ADMINISTRACIÓN DE CA DE CONFIANZA (TRUSTED CA)

El paradigma de seguridad de ID-CA se basa en el más alto nivel de confianza. Por lo tanto, una CA interna sólo se puede utilizar si es de confianza. Las CA confiables se utilizan para la autenticación de usuarios y la verificación de firmas de solicitudes de servicios web.

El concepto Trusted CA se implementa en toda la aplicación para permitir y controlar la comunicación segura y el acceso a las funciones del producto.

Los certificados de autenticación de usuario que permiten conexiones a la aplicación ID-CA deben haber sido emitidos por una autoridad de certificación (CA) en la que la aplicación ID-CA confíe para la autenticación de actores. ID-CA también debe poder verificar la cadena de confianza del certificado hasta un ancla de confianza.

Para la firma de solicitudes de certificados, las CA que emiten certificados que firman solicitudes de certificados deben ser confiables para la firma de solicitudes y la CA de ID debe poder verificar la cadena de confianza del certificado hasta un ancla de confianza.

Cuando se confía en una CA en una partición, también se confía en todas las particiones debajo de esta partición.

Trusted CA Management consiste en:

- **Creación de CA de confianza externa:** cree una CA de confianza en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- **Edición de CA de confianza externa:** edite la CA de confianza en la partición actual o en cualquier partición en un nivel inferior de la rama del árbol.
- **Edición de CA de confianza interna:** edite la CA de confianza interna en la partición actual o inferior

ADMINISTRACIÓN DE NOTIFICACIONES

En modo operativo, esta función de notificación es esencial para garantizar un alto nivel de disponibilidad de la aplicación PKI.

ID-CA ha integrado de forma nativa la gestión de notificaciones dirigidas a sus administradores.

El módulo de Notificación se utiliza para advertir a una persona sobre los diferentes eventos que ocurren en la plataforma o sobre entidades administradas por una CA. Las funcionalidades de Notificación ID-CA consisten en:

- **Notificación de caducidad:** notifica a un usuario acerca de un certificado que caducará pronto en la partición de destino.
- **Configuración de notificación:** configure la notificación para la partición actual y cualquier partición en un nivel inferior de la rama del árbol.

ADMINISTRACIÓN DE ACTORES

Los actores son Personas, Máquinas o Dispositivos que pueden acceder al sistema, normalmente identificados y autenticados mediante un certificado. Disponible para la asignación de doble factor de autenticación mediante OTP.

Están autorizados a realizar Acciones dependiendo del Rol que se les asigne en una Partición específica y sus hijos.

- Los **roles** (roles) son una colección de derechos. Los roles se definen para casos de uso específicos identificados de la aplicación y para garantizar la separación de funciones.
- Los **permisos** (rights) son una colección coherente de posibles acciones en el sistema para una característica específica. Actualmente, no es posible editar derechos ni crear roles (los roles y derechos son estáticos).

En resumen, el **triplete** de Rol, Partición y Actor es necesario para determinar si una acción está autorizada o no en el sistema, en una partición específica.

Rol	Descripción
Super Administrator	Posee todos los roles
Rights Administrator	Puede ver certificados y usuarios.
Connector Enroll	Puede crear y editar usuarios.
Connector Revoke	Puede realizar la inscripción de certificados a través del servicio web (SOAP)
Connector Recovery	Puede realizar la revocación de certificados a través del servicio web (SOAP)
Configuration Administrator	Puede realizar recuperación de claves a través del servicio web (SOAP)
Certificate Administrator	Puede realizar todas las tareas de configuración, así como ver certificados
Revocation Administrator	Puede realizar búsquedas, inscripciones y revocaciones de certificados a través de GUI
Recovery Administrator	Puede ver todos los ajustes de configuración, excepto los clústeres criptográficos. Puede ver, suspender, revocar y reactivar/reanudar certificados. Puede suspender, revocar y reactivar/reanudar certificados mediante servicios web
Key Administrator	Puede realizar la recuperación de claves a través de GUI
Audit Administrator	Puede gestionar funciones de generación de claves.

Tabla 1. Roles y Permisos.

ADMINISTRACIÓN DE AUDITORIA, REPORTES Y SUPERVISIÓN

ID-CA registra todos los eventos funcionales y técnicos. Los registros de auditoría se utilizan para monitorear la plataforma tanto a nivel de proceso comercial como a nivel técnico.

Se pueden diferenciar dos tipos de trazas:

- **Seguimientos técnicos:** Estos seguimientos son generados por los componentes internos (servidor web Apache, base de datos PostgreSQL, directorio LDAP, etc.) implicados en el funcionamiento de ID-CA. Accesibles como un archivo de texto a través del sistema de archivos, estos seguimientos proporcionan indicadores sobre el estado de ejecución de cada uno de estos componentes. Estos rastros son generados por los propios componentes según su propia lógica de aplicación.
- **Seguimientos de aplicaciones:** Para garantizar la trazabilidad y la rendición de cuentas, ID-CA genera seguimientos completos de las aplicaciones para cada una de las acciones realizadas. Cada rastro tiene un número único que permite seguir los eventos que originaron la emisión de este rastro y seguir las acciones realizadas posteriormente. Por ejemplo, a partir de un seguimiento generado durante la validación de una solicitud de tarjeta, será posible:

- Volver a la solicitud inicial.
- Seguimiento del futuro de la solicitud.

En general, cada rastro se compone de datos que especifican "quién" hizo "qué", "cuándo", "dónde" y "el resultado". Un seguimiento suele ir acompañado de los datos correspondientes (solicitudes, certificados, etc.).

Los seguimientos de aplicaciones de ID-CA se pueden interconectar con la herramienta Syslog.

La Gestión de Auditoría consiste en:

- Normalización de auditoría: normalice periódicamente los eventos de auditoría en la base de datos para realizar consultas en la base de datos.
- Vista de auditoría: vea información de auditoría en la partición actual o debajo
- Búsqueda de auditoría: busque registros de auditoría disponibles en la partición actual o debajo
- Exportación de auditoría: exporta registros de auditoría en la partición actual o debajo

En términos de funciones de informes, ID PKI puede manejar la siguiente información:

1. Para una fecha determinada, una tabla muestra el número total de certificados (emitidos antes de esta fecha) por partición o perfil y por estado:

- válido (no revocado en un período de validez)
- revocado (en un período de validez)
- aún no válido y no revocado
- aún no válido y revocado
- caducado y no revocado
- caducado y revocado

2. Por rango de tiempo, una lista de eventos relacionados con certificados por perfil o partición

- Inscribirse
- Revocación
- Vencimiento

A nivel global, cada administrador de sistemas necesita verificar el estado de las aplicaciones en ejecución.

ID-CA proporciona información básica sobre el estado de las aplicaciones y expone varios indicadores basados en los procesos de Monitoreo del sistema y Monitoreo de aplicaciones.

Los elementos de monitoreo del sistema son:

- CPU, RAM, uso del disco, tiempo de actividad del servidor,
- Estado de salud del repositorio LDAP, la base de datos y el agente JMS.

Los elementos de monitoreo de aplicaciones PKI son:

- Tiempo de actividad y estado del servidor
- Estado de salud de HSS (capa de abstracción de hardware criptográfico)
- Caducidad de CA
- Información de gestión de CRL
  - Producción de CRL
  - Publicación CRL
  - Alerta de publicación de CRL

ADMINISTRACIÓN DE PARTICIONES

El sistema de partición permite implementar fácilmente el arrendamiento múltiple dentro de ID PKI. Permite configurar varios entornos CA completamente independientes dentro de una única instancia del software.

Las particiones se definen en una estructura de árbol, siendo cada nodo una partición en la que se pueden adjuntar recursos (por ejemplo, configuraciones, certificados, etc.). Según las necesidades del cliente podemos aislar o compartir recursos comunes.

Debido a la asociación de los roles y acciones del actor a una partición y sus hijos, es posible dedicar una partición completa a un cliente. Puede actuar como un entorno PKI individual.

El principio de partición lógica se describe a continuación:

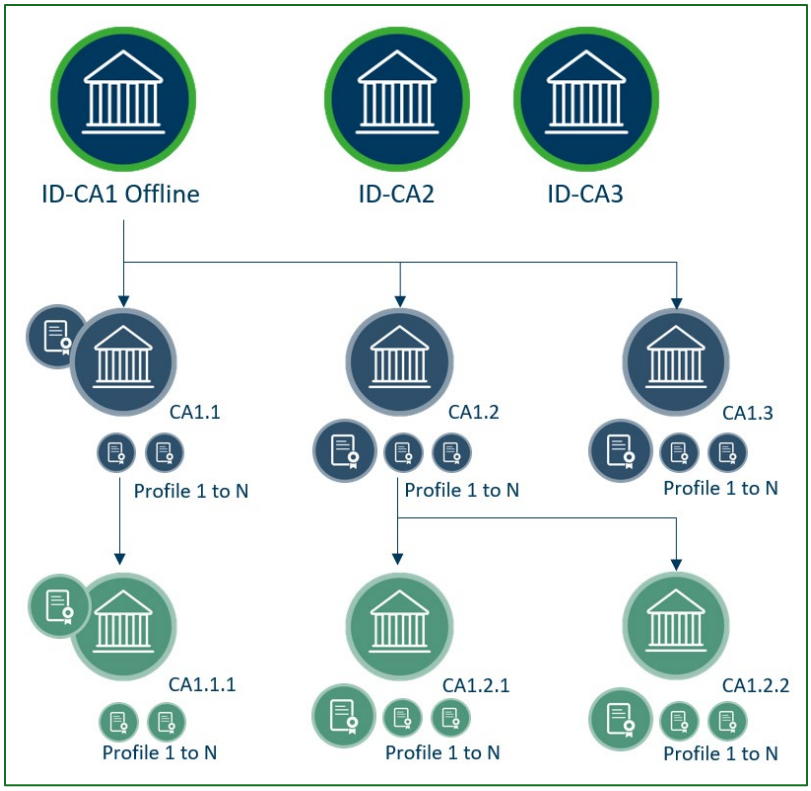


Ilustración 1. Principios de partición de datos.

La gestión de particiones consiste en:

- **Creación de partición:** creación de una nueva partición (son posibles estructuras anidadas)
- **Edición de partición:** edición de la partición actual o cualquier partición en un nivel inferior de la rama.

Es posible **compartir** (colocar recursos más arriba en el árbol) y **aislar** (crear ramas en el árbol de partición).

La gestión de particiones se realiza de una manera extremadamente fácil de usar, a través de una sencilla GUI mediante mecanismos de hacer clic, arrastrar y soltar. Para una mayor visibilidad, se puede asociar un logotipo a cada partición para resaltar mejor unas de otras.

SELLADO DE TIEMPO

El producto Time Stamping nos permite proporcionar tokens de tiempo certificados y fiables.

En combinación con una fuente de tiempo y un medio de firma digital, esto permitirá a los clientes garantizar, por ejemplo, la existencia de un documento en un momento preciso en el tiempo.

En términos de implementación, un cliente transmite solicitudes de sellado de tiempo a la plataforma, que determina con gran precisión la hora y la fecha, firma y envía esta información de vuelta al cliente.

El protocolo de comunicación subyacente para este procedimiento está definido en RFC 3161, al que el producto Time Stamping cumple plenamente.

La firma de los tokens de tiempo se basa en dispositivos criptográficos (módulos de seguridad de hardware) que admiten la interfaz PKCS#11.

El producto consta de dos servidores:

- Un servidor de administración, encargado de proporcionar servicios de gestión basados en GUI para operadores acreditados.
- Un servidor de firma, encargado de producir técnicamente los tokens (de tiempo) firmados.

Se admiten las siguientes funciones:

- Administración basada en GUI del servicio de sellado de tiempo
- Gestión de los espacios de trabajo del cliente, incluido el manejo de pares de claves criptográficas asociadas
- Gestión de entidades de sellado de tiempo, sus políticas y extensiones aceptadas
- Gestión de actores
- Auditoría y estadísticas

El acceso a los servidores solo se concede mediante autorización basada en autenticación mutua (HTTPS SSL/TLS).

Además, el sellado de tiempo ofrece las siguientes ventajas:

- Tokens producidos totalmente compatibles con IETF RFC 3161 e IETF RFC 5816
- Gestión flexible de particiones de clientes (cada una dedicada a un espacio de trabajo de sellado de tiempo)
- Máximo rendimiento
- Cumplimiento de la normativa Eidas

3.3 FIRMADO DE DOCUMENTOS GET TRUST (DOCUMENT SIGNER)

ADMINISTRACIÓN BASADA EN WEB

La interfaz de administración basada en web ofrece las siguientes funcionalidades:

- Gestión de espacios de trabajo (dominio del cliente)
- Gestión de entidades firmantes (comúnmente denominadas “Firmantes de documentos” o DS)
- Gestión de claves de firma (claves de firma de respuestas y sus certificados asociados)
- Gestión de los usuarios del servicio.
- Auditoría de operaciones de administración
- Consulta de estadísticas de producción.

Solo se puede acceder al sitio de administración mediante un certificado de usuario final (UE), que se puede almacenar en una tarjeta inteligente. El servidor web frontal autentica a la UE que se conecta. Para que la UE esté autorizada a acceder al sitio, la CA que emitió su certificado debe estar definida como una CA confiable del servidor web frontal.

Una vez que el Usuario Final haya sido autenticado por el servidor Web frontal, se abrirá la página de inicio de la plataforma DS. Dependiendo del perfil de Usuario final utilizado para conectarse al sitio, tendrá acceso a ciertas funcionalidades, pero no a todas.

Están disponibles los siguientes perfiles:

- Perfil **"Gestión del espacio de trabajo":** Otorga acceso al menú "Gestión del espacio de trabajo". Un Usuario Final con este perfil puede crear, seleccionar, ver o modificar un espacio de trabajo.
- Perfil **"Gestión de claves":** Otorga acceso al menú "Gestión de claves". Un Usuario Final con este perfil puede generar un par de claves en el equipo criptográfico y recuperar la solicitud de certificado emitido (CSR en formato PKCS#10).
- Perfil **"Administración DS":** Otorga acceso al menú "Administración DS". Un Usuario Final con este perfil puede registrar, ver, activar, desactivar y bloquear certificados DS.
- Perfil **"Gestión de usuarios":** Otorga acceso al menú "Gestión de usuarios". Un Usuario Final con este perfil puede registrar, activar, desactivar o bloquear usuarios y gestionar los derechos de los usuarios registrados.
- Perfil **"Gestión de Auditoría":** Otorga acceso al menú "Auditoría". Un usuario final con este perfil puede ver información relacionada con la auditoría, así como estadísticas de producción.

INTERFACE CON LA PLATAFORMA DE DS

La interfaz de la plataforma DS se basa en el enfoque de servicios web (XML sobre HTTP(S)) y permite, por lo tanto, una interfaz sencilla e independiente del contexto.

IDnomic proporciona al Cliente:

- Una documentación para la interfaz de especificación
- Apoyo a la integración

ESPECIFICACIONES DE LA PLATAFORMA DE DS

Software	Especificaciones
ICAO - DOCUMENT SIGNER®	La plataforma DS se suministra y puede configurarse. Normalmente se instala en el sitio de producción en interfaz directa con la cadena de personalización. **Funciones principales:** • Verificación de certificados DS. • Enrutamiento de una solicitud de firma a una clave disponible con control de cuota (número máximo de firmas por clave). • Generación de un lote de claves y DS CSR. • Realiza codificación ASN.1 y firma de SOD. Interfaz DS: servicio web (XML) sobre protocolo HTTP(S)

ALGORITMOS

- RSA 2048 y 4096
- SHA-1, SHA-256 y SHA-512
- ECDSA 256

3.4 PKI CIUDADANA – PKI SUBORDINADA X509

CA SUBORDINADA DE LA CA ROOT

Una CA subordinada es una CA que obtiene su certificado de una CA raíz (también conocida como CA principal). La CA subordinada podrá emitir certificados a otras entidades (ciudadanos), pero su certificado es verificado por la CA raíz.

PROCESO DE EMISIÓN DE CERTIFICADOS

El proceso de emisión de certificados en la PKI Ciudadana con una CA subordinada es el siguiente:

1. Solicitud de certificado: Una entidad (Ciudadano) solicita un certificado a la CA subordinada.
2. Verificación de identidad: La CA subordinada verifica la identidad de la entidad (Ciudadano) que solicita el certificado. (Tarea delegada al sistema de verificación de identidad de la JCE)
3. Generación de clave pública: La entidad genera un par de claves (pública y privada).
4. Solicitud de certificado a la CA raíz: La CA subordinada solicita un certificado a la CA raíz para la entidad.
5. Emisión de certificado x509: La CA raíz emite un certificado para la CA subordinada, que a su vez emite un certificado para la entidad.
6. Firma del certificado: El certificado es firmado digitalmente por la CA subordinada y la CA raíz.

ESTRUCTURA DEL CERTIFICADO X.509

Un certificado X.509 tiene la siguiente estructura:

- **Número de versión:** Indica la versión del certificado.
- **Número de serie:** Un número único que identifica el certificado.
- **Algoritmo de firma:** El algoritmo utilizado para firmar el certificado.
- **Emisor:** La entidad que emitió el certificado (CA subordinada).
- **Sujeto:** La entidad a la que se emitió el certificado.
- **Clave pública:** La clave pública de la entidad.
- **Validez**: La fecha de inicio y fin de validez del certificado.
- **Extensiones:** Información adicional sobre el certificado.

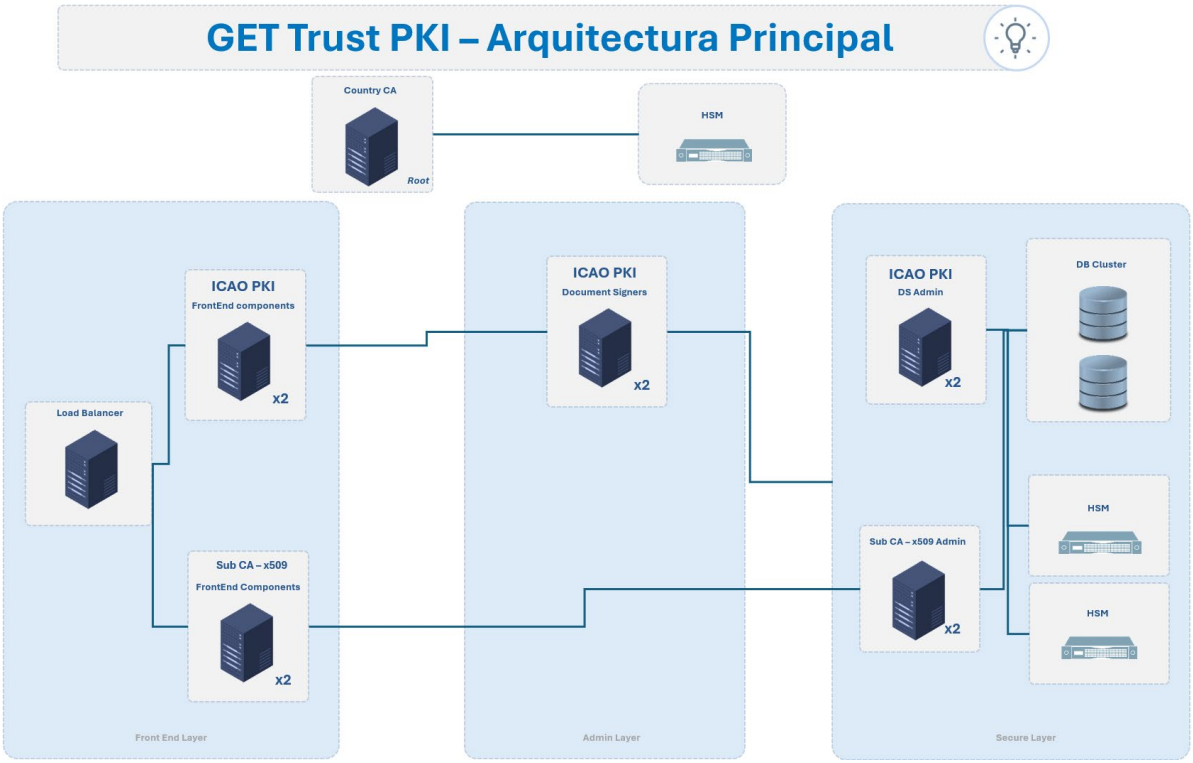
VENTAJAS DE LA PKI CON CA SUBORDINADA

La PKI con CA subordinada ofrece varias ventajas, como:

- **Mayor flexibilidad:** La CA subordinada puede emitir certificados para entidades específicas.
- **Mejora la seguridad**: La CA raíz puede revocar el certificado de la CA subordinada si es necesario.
- **Reducir costos:** La CA subordinada puede reducir los costos de emisión de certificados.

3.5 INFRAESTRUCTURA GET TRUST

La infraestructura de GET Trust está diseñada para permitir la comunicación digital segura, la autenticación y la protección de datos durante todo el proceso de personalización. La infraestructura que se describe a continuación comprende componentes esenciales del sistema y la intercomunicación entre ellos. Abarca la Autoridad de Certificación de Firma de País (CSCA), la Autoridad de Certificación Técnica (CA Técnica) responsable de los certificados SSL, los firmantes de datos y los sitios de emisión.



3.5.1 CARACTERÍSTICAS CLAVES

GET Trust cuenta con la notable capacidad de operar en entornos Windows y Linux y, al mismo tiempo, se adapta a diferentes estándares de API criptográfica, incluidos PKCS11, CNG y CSP. Además, la excepcional flexibilidad de GET Trust se extiende a su compatibilidad con módulos de seguridad de hardware (HSM) y soluciones de software HSM como el 'DB Crypto Engine'. Esta interoperabilidad dinámica garantiza que GET Trust pueda integrarse perfectamente en una amplia gama de infraestructuras de TI, brindando a las organizaciones la libertad de elegir las herramientas y plataformas que mejor se adapten a sus necesidades de seguridad.

- Máxima seguridad probada, Modulo CA certificado en CC EAL4+

- Multi-tenant por diseño: implemente, configure y administre varias PKI de forma independiente con una instancia de software.
- Cumplimiento de normas y estándares:
    - Cumplimiento del formato del certificado: X.509v3, RFC 5280 y RFC 3739
    - Solicitudes de certificados: PKCS#10, CSR, SPKAC
    - Algoritmos de firma RSA (1024 - 4096), (RSA PKCS#1 v1.5, RSA PSS PKCS#1 v2.1), ECDSA (192-521)
    - Algoritmos hash SHA-224, SHA-256, SHA-384, SHA-512, SHA-256 MGF1, SHA-384 MGF1, SHA512 MGF1
    - Contenido del certificado: UTF8, T61, imprimible, correo electrónico,
    - SAN (RFC822, UPN), etc.
- Cumplimiento:
    - Certificado RGS considerando todos los usos de los certificados y para todas sus clasificaciones (1, 2 y 3). LSTI N° 8029-1318-V3.0 / EN319411-1 V1.1.1
    - Cumple con eIDAS: obtención del Certificado LSTI N° 8029-1318-V3.0.

3.6 MÓDULO DE SEGURIDAD POR HARDWARE (HSM)

Nos permitimos ofrecer el modelo Eviden Trustway Crypt2pay, el cual presenta las siguientes características.

Eviden Trustway Crypt2pay ™ es un Módulo de Seguridad Hardware (HSM) que ofrece soluciones de software en un entorno altamente seguro y de alto rendimiento, permitiendo la ejecución de operaciones criptográficas muy sensibles. Este HSM combina medidas sólidas de seguridad física con un núcleo criptográfico que cumple con los estándares de seguridad más estrictos, lo que lo convierte en uno de los módulos criptográficos más certificados del mundo para integrarse en sistemas de información corporativos y servicios en la nube. Su implementación simplificada, diseñada para despliegue independiente, proporciona a los entornos críticos una solución ideal para garantizar la seguridad absoluta de sus datos sensibles, todo a un precio competitivo.

Algunas características clave de Eviden Trustway Crypt2pay incluyen:

- Nivel de seguridad alto: Diseño a prueba de manipulaciones (Anti-tampering) con un alto nivel de certificación.
- -Gestión sencilla: Fácil instalación y administración intuitiva.
- Disponibilidad alta: Mecanismos nativos para alta disponibilidad, conmutación por error y copias de seguridad.

- Protección de datos: Soluciones de protección de datos que le permiten cifrar, gestionar y controlar el acceso a sus datos, independientemente de su ubicación (local, virtual y en la nube).
- Autenticación: Eleva la seguridad de su aplicación mediante el control de acceso a sus datos y la protección de generadores de claves.
- Seguridad en la nube: Proporciona una raíz de confianza para servicios en la nube al asegurar la comunicación entre la nube privada y el sitio local, la encriptación de datos para soluciones locales y basadas en la nube, y servicios criptográficos bajo demanda.

- **APIs:**
  - PKCS#11
  - OpenSSL
  - Java Cryptography Architecture/Extension (JCA/JCE)
  - Microsoft Crypto API (CSP), Cryptography Next Generation (CNG)
- **Diseño Anti-Tampering certificado en:**
  - Common Criteria EAL4+ en cumplimiento con CWA 14167-2-PP
  - NATO SECRET
  - Cumple con eIDAS.
  - Qualification Renforcée (la más alta calificación de la ANSSI)
  - FIPS 140-2 level 3.
- **Algoritmos**
  - DES: Triple DES
  - RSA: Keys up to 4069bits
  - 5 and PSS signature
  - SHA-1, SHA-2, SHA-3
  - HMAC
  - AES: 128, 192 and 256 bit keys
  - ECDSA: ANSI and Brainpool named curves
  - CHACHA & Poly1305
  - EdDS
- **Interfaces y características físicas**
  - Performance: Crypt2pay XT: 100 to 3600 PVV tps
  - Voltage: 85 – 264 Vac
  - Red: 3 x 1Gb
  - 2 Hot Plug PSU
  - Frecuencia: 47 – 63 Hz
  - Humedad: 30% – 70% noncondensing
  - Temperatura de Operación: 10/45°C
  - Dimensiones: Crypt2pay XT: 442x346x76mm
  - Peso: Crypt2pay XT: 14 kg
- **Tipos de Llaves**
  - Payment Industry keys.
  - Smart metering Industry keys.
  - PKCS#11 keys.

- Generic secret keys.
- Import / Export keys feature.

ÍTEM IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL

4.1 INTRODUCCIÓN - GET MOBILE ID

La solución de identidad digital GET Mobile ID proporciona una identidad de alta seguridad en el dispositivo móvil de un usuario, que representa una alternativa conveniente, segura e instantánea a los documentos de identificación físicos tradicionales, y utiliza formidables algoritmos de cifrado de datos y medidas de seguridad de comunicación para reducir el robo de identidad y mejorar la privacidad de los ciudadanos.

4.1.1 GET MOBILE ID

Los ciudadanos quieren que sus documentos de identificación sean móviles y esperan poder administrar sus datos de identidad mejor que con las tarjetas de identificación físicas. GET Mobile ID brinda control de identificación por parte del usuario y permite una verificación de edad y una comprobación de identidad rápida y segura en todo tipo de negocios.

GET Mobile ID es el único producto en el mercado compatible con Android e iOS. Los gobiernos pueden emitir cualquier documento de identificación en GET Mobile ID. También permite que las organizaciones de todos los sectores (educación, empresa, comercio minorista y finanzas, así como instituciones públicas) acepten identificaciones digitales de alta seguridad. La autenticación es instantánea, las identidades son seguras, las interacciones están estandarizadas. Es la base para una amplia gama de servicios de identidad.

- La aplicación Direct to Consumer permite el control ciudadano del mID
- Tu identificación oficial en tu teléfono
- Totalmente compatible con ISO 18013-5
- Cambia cómo se protege la identidad
- No se puede falsificar

4.1.2 GET MOBILE ADMINISTRATOR

GET Mobile Administrator permite a los emisores de tarjetas de identificación del gobierno, hacer el cambio a lo digital de forma rápida y segura. Los gobiernos con visión de futuro podrán digitalizar sus documentos de identidad y dar a los ciudadanos el control de sus propios datos de identidad. GET Mobile ID cumple con la norma ISO/IEC 18013-5 de cinco estrellas con todos los canales de comunicación y modos de interacción estandarizados, dando como resultado la mejor experiencia de usuario y aceptación en la mayor cantidad de ubicaciones y casos de uso.

- Conectividad simple al sistema del JCE.
- Diseñado para Alta Disponibilidad.
- Conecta a los emisores para emitir identidades digitales en teléfonos móviles.
- Habilita todos los modos de interacción ISO 18013-5 en línea y fuera de línea
- Mantener actualizadas las identidades digitales
- Administrar el ciclo de vida de la identificación digital móvil

4.2 GET MOBILE ID – COMPONENTES

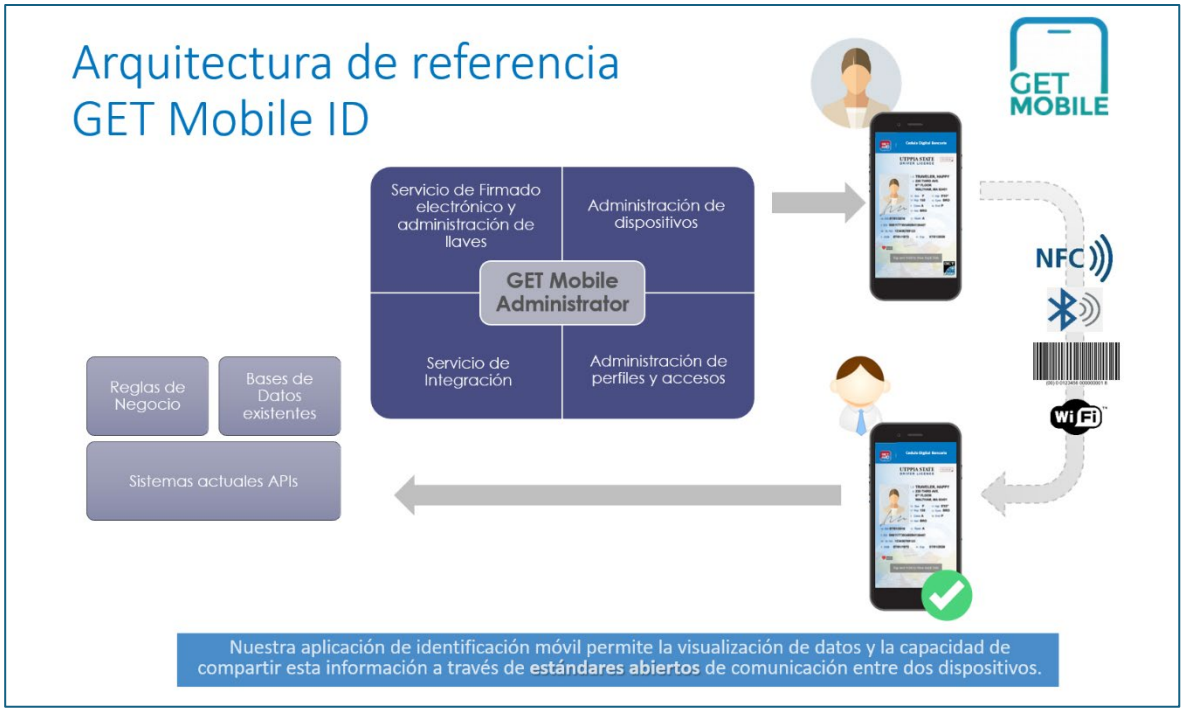
4.2.1 GET MOBILE ADMINISTRATOR

El módulo GET Mobile Administrator es fundamental para el concepto de producto mID, puesto que proporciona a la autoridad expedidora los siguientes servicios y funciones:

- Conectividad sencilla con el sistema de Identidad y Emisión del JCE.
- Diseñado para alta disponibilidad al 99,99% cuando se aloja en plataformas en nube o centros de datos redundantes y distantes.
- Conecta a los Emisores (el JCE) para que puedan emitir documentos de identidad firmados ISO 18013-5 en Teléfonos Móviles para sus ciudadanos.
- Incluye la más alta seguridad a nivel de pasaportes para la firma de datos mID a partir de su estructura de claves o de claves generadas
- Valida a los ciudadanos para garantizar que sólo reciben su documento de identidad.
- Permite solicitudes de verificadores compatibles con ISO 18013-5 en línea (WebAPI u OIDC).
- Mantiene los mID actualizados con los cambios de datos del Sistema del Emisor.

Los servicios prestados por GET Mobile Administrator son:

- Servicio de firma y gestión de claves: firma de forma segura los mID en nombre del emisor para transmitirlos a los dispositivos de los ciudadanos. Mediante la integración con la solución de PKI propuesta para el proyecto, se realizan los procesos de encripción sugeridos por la norma ISO 18013-5.
- Personalización y gestión de dispositivos: portal del consumidor para gestionar dispositivos, incluidos teléfonos perdidos, nuevos o actualizados.
- Fácil integración con sistemas de registro: conexiones API seguras con sistemas de registro que mantienen los datos actualizados.
- Gestión de Identidad y Acceso - Inicio de sesión y registro para verificadores que necesitan acceso a servicios ISO en línea.
- Caché mID – Puede mantener los datos mID durante un tiempo predeterminado para aligerar las solicitudes de los verificadores en la base de datos SOR.



4.2.1.1 OPCIONES DE INTEGRACIÓN:

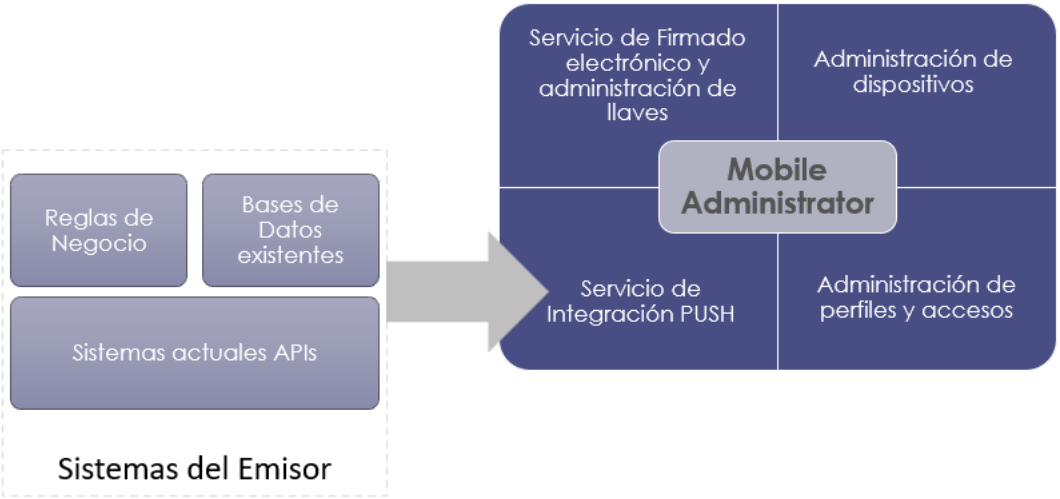
GET Mobile Administrator provee diferentes métodos de integración, buscando que la integración con el sistema de emisión del Emisor se pueda realizar de la forma más eficiente, y de esa manera, permitir un escalamiento progresivo en el desarrollo de casos de uso:

- **Modelo sin integración:** El modelo sin integración se basa únicamente en el aprovisionamiento diligenciado y aprobado por el administrador, se pueden aprobar nuevas solicitudes para Mobile ID sin una integración con la base de datos. El Administrador es responsable de revisar las solicitudes de mID, corregir cualquier error de datos, verificar la identidad y la confianza del solicitante y aprobar el mID que se proporcionará. Los datos mID están autocontenidos en la caché mID y el sistema se ejecuta basándose únicamente en esos datos.

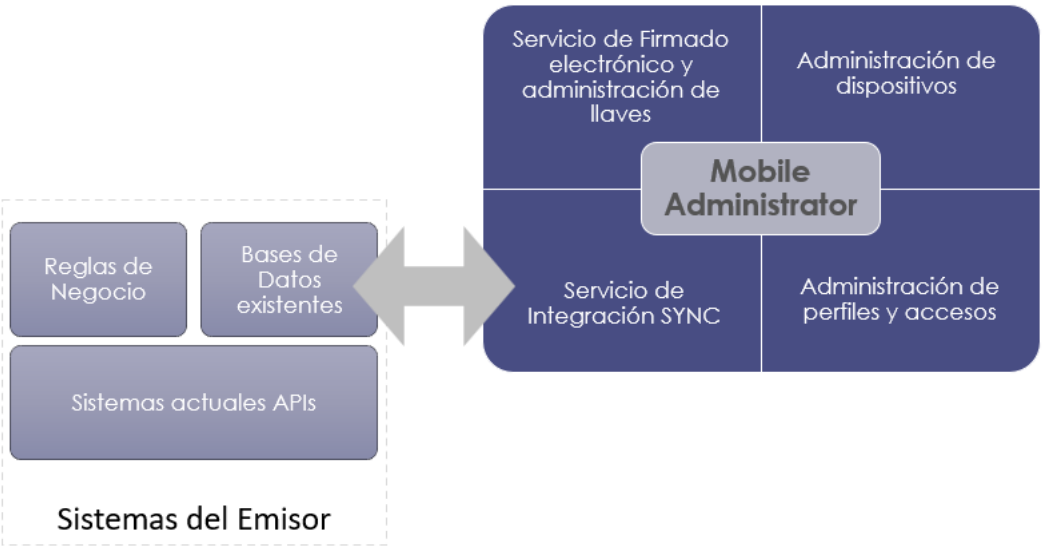
- **Modelo Push:** En el modelo Push, el sistema del emisor, como parte de su lógica empresarial, determina los momentos adecuados para llamar a GET Mobile Administrator con a través del API, usando un método de Creación de Licencia según los documentos de swagger para su instancia del software GET Mobile Administrator.

- **Los documentos Swagger están disponibles al navegar a la URL de la instancia de la página GET Mobile Administrator Services del Emisor**. Este modelo Push brinda el máximo control al entorno del sistema del emisor a expensas del tiempo de programación para la integración (el uso de la API es sencillo, rápido y fácil de usar según un enfoque tecnológico popular; el esfuerzo de programación puede variar dependiendo de la integración necesaria con los sistemas existentes).

El JCE puede crear sus propios informes a partir del software cuando utiliza este modelo porque tiene pleno conocimiento de qué mID están activos.

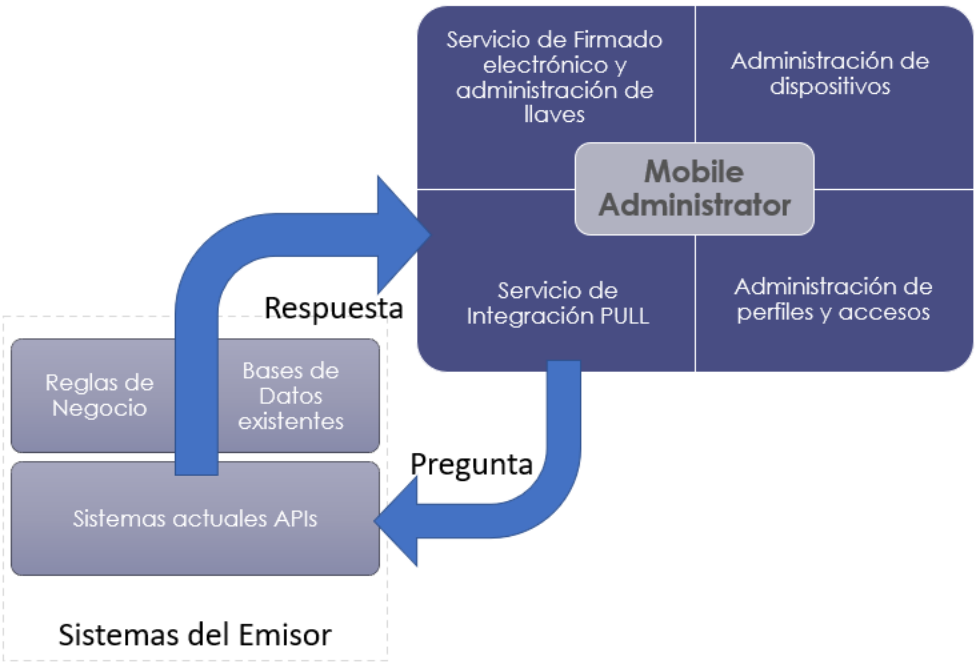


- **Modelo SYNC:** Para el modelo de sincronización, es posible realizar una conexión ODBC o similar entre el sistema del emisor y GET Mobile Administrator, cache que sincroniza el último registro del ciudadano en su registro en caché mID. La rutina de sincronización se puede configurar para sincronizar solo registros SOR estatales aprobados para mID, o para sincronizar todos los registros.



- **Modelo Pull:** En el modelo Pull, el administrador de GET Mobile se puede configurar para llamar a una API del sistema del emisor que busca registros actuales pendientes de emisión. La caché mID retiene registros de identidad para que el número de llamadas al sistema del emisor sea limitado.

La caché mID también se puede configurar para que no retenga datos. Si el sistema del emisor puede manejar los altos volúmenes de transacciones de los verificadores en el momento de uso, y existen requisitos contra el almacenamiento en caché de los registros más recientes detrás de la API en línea ISO (consulte la sección Medidas de seguridad para la API en línea a continuación), se puede configurar GET Mobile Administrator para llamar una API del sistema del Emisor que busca registros actuales. La carga completa de tráfico mID en el momento de uso (consulte la sección Tiempo de verificación (uso de mID) a continuación) alcanzará el SOR del emisor en esta configuración. (Cuando se hace referencia a SOR (Sistemas del Emisor), también puede ser un espejo local sincronizado de SOR).



4.2.1.2 OPCIONES DE FIRMADO DIGITAL

La implementación de una identidad digital móvil ISO 18013-5 requiere llaves privadas del emisor que firmen los datos mID antes de que se aprovisionen en los dispositivos móviles. Estas llaves privadas pueden generarse a partir de la CA estatal. La CA no tiene que ser pública porque no existe una verificación de la cadena de certificados. Si se utiliza una CA estatal, se deben planificar ceremonias de certificación segura en el proyecto para obtener la clave privada en el servicio de firma o HSM. El Certificado Público IACA puede distribuirse por separado de la jurisdicción o colocarse en una "Lista Maestra" (también conocida como VICAL) con otros certificados confiables y ser distribuido por cualquier entidad. Los verificadores son responsables de garantizar que obtengan Listas Maestras confiables.

4.2.1.3 MODELO DE DATOS Y CODIFICACIÓN.

JSON Identity Suite es el modelo de objetos sobre el que se construye Open ID Connect. Sus estructuras de datos JSON Web Token (JWT) están definidas en https://tools.ietf.org/html/draft-ietf-oauth-json-web-token-19 especificaciones IETF, con los campos de datos registrados en el registro JWT de la Autoridad de Números http://www.iana.org/assignments/jwt/jwt.xhtml. El estándar ISO 18013-5 ha ampliado el modelo de datos JWT con atributos de identidad específicos de las tarjetas de identificación (+ privilegios de conducción).

Este mismo modelo de datos JWT estándar se ejecuta a través de ISO 18013-5 y grupos de trabajo de OpenID Foundation (OIDF) para que las identidades digitales puedan ser utilizadas ampliamente y confiables por la más amplia gama de dispositivos autenticadores y dispositivos POS posible. La transmisión de datos "fuera de línea" ISO 18013-5 utiliza una representación compacta de objetos binarios (CBOR por sus siglas en ingles) de este modelo de datos JWT. Esto une los casos de uso en línea y en persona.

La codificación de los datos mID ha ser codificados en el dispositivo móvil, serán codificados de acuerdo al numeral 7.2 del estándar ISO 18013-5, campos que serán discutidos y coordinados con el JCE para que su integración tenga una correlación a los campos mencionados en el estándar. La definición de campos adicionales conlleva un análisis adicional para su inclusión y lectura por parte de los verificadores ISO 18013-5.

4.2.1.4 PROCEDIMIENTO DE ACTIVACIÓN

Para el aprovisionamiento, o emisión y descarga de la identidad móvil en el dispositivo del ciudadano, GET Mobile Administrator presenta estas opciones de activación:

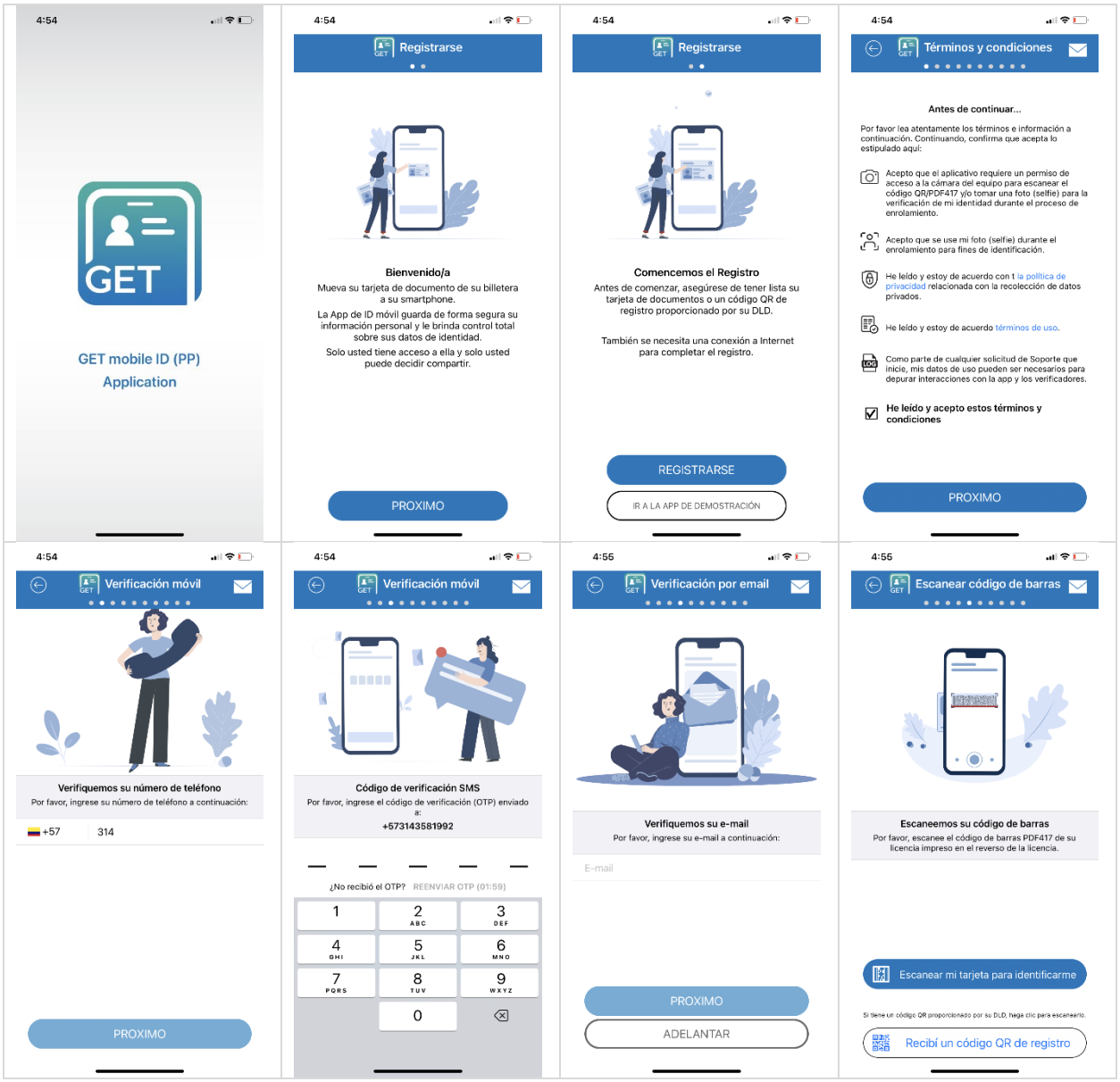
- **Aprobador por Administrador:** Para el aprovisionamiento aprobado por el administrador, los datos se ingresan a través de GET Mobile Administrator. El Administrador aprueba el registro verificando la identidad del solicitante e ingresa la información en el Administrador de GET Mobile ya sea de forma manual o automática desde el sistema del emisor (ver opciones de integración arriba). Una vez que se inserta el registro, los datos mID están listos para publicarse en la aplicación móvil. Es opción es ideal para un programa piloto, donde el titular puede recibir una invitación por correo electrónico para descargar la aplicación y luego completar un breve formulario para personalizar su aplicación con los datos de mID.

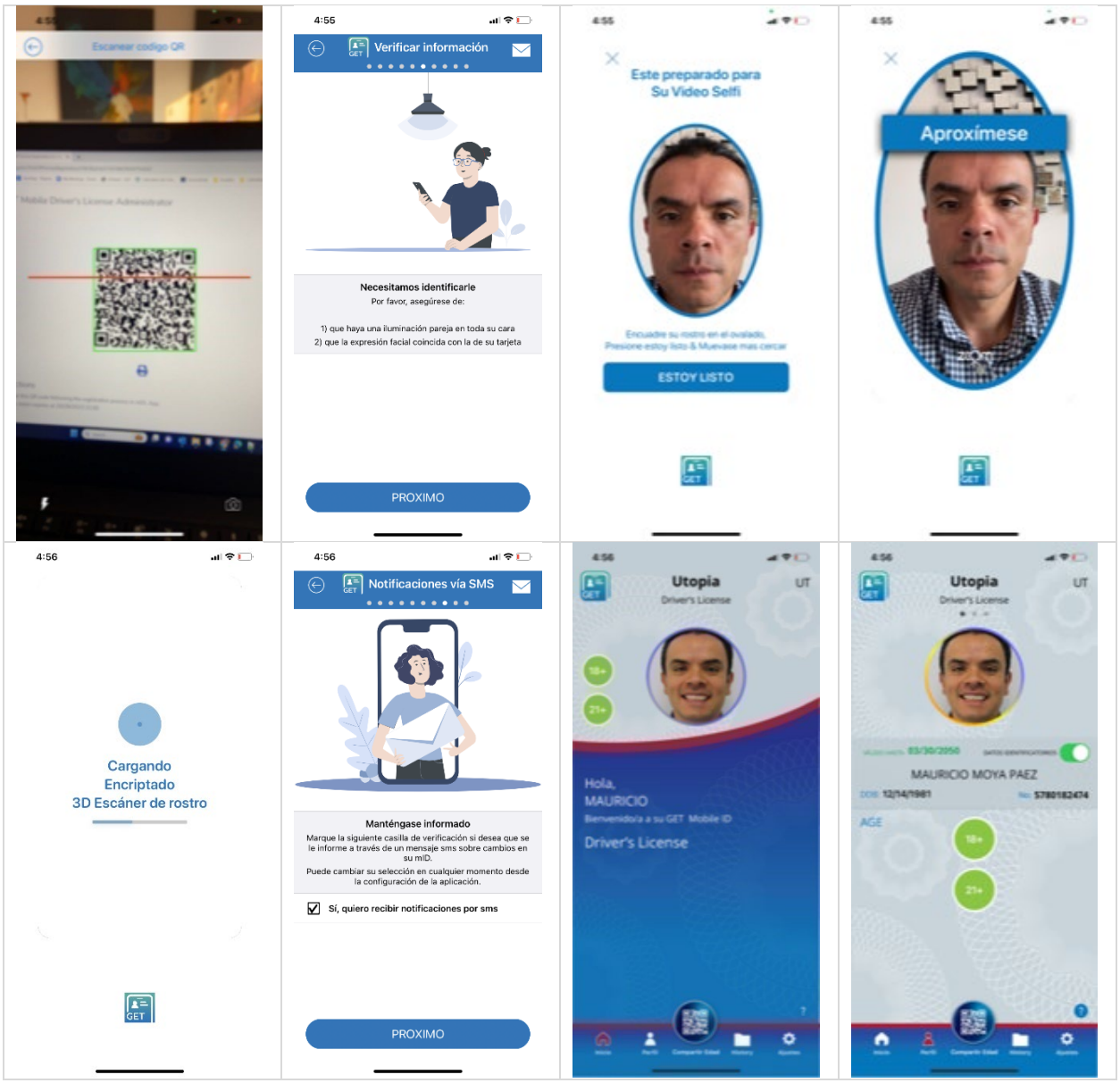
- **Aprovisionamiento en Persona:** Para el aprovisionamiento en persona supervisado por un operador, el administrador de GET Mobile o la aplicación del sistema del emisor del operador pueden mostrar un código QR que identifica un registro mID adecuado y permite que la aplicación GET Mobile ID acceda a ese registro mID adecuado para descargarlo en el dispositivo móvil. (personalización). Alternativamente, el titular puede rellenar un breve formulario para personalizar su aplicación con los datos mID.

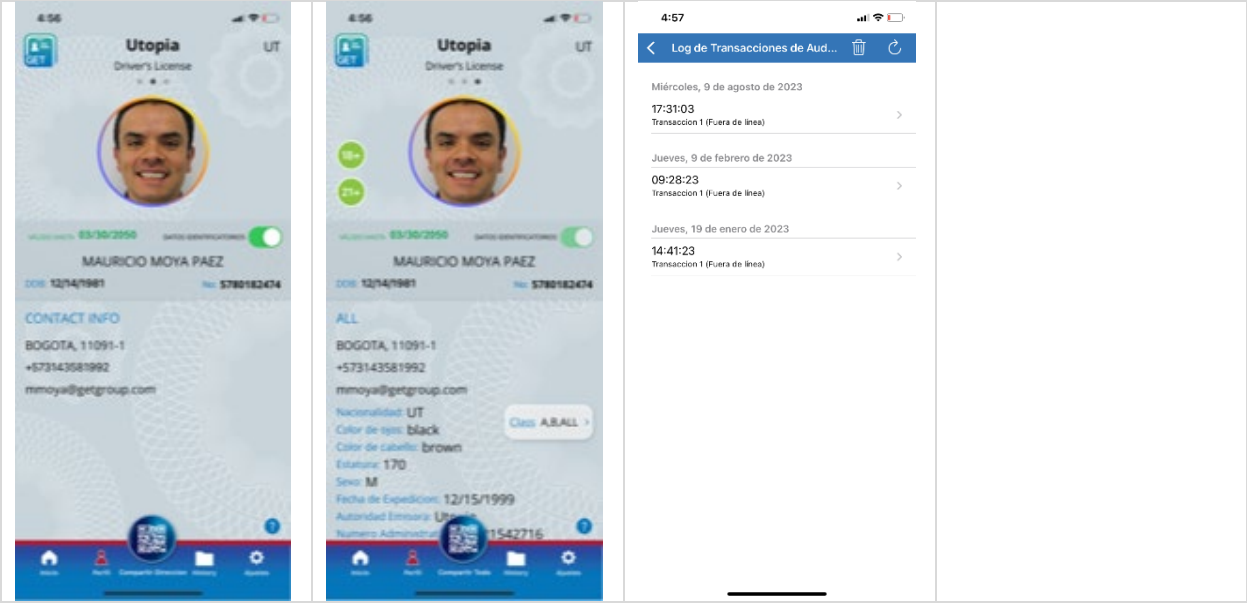
- **Aprovisionamiento remoto:** Para el aprovisionamiento remoto/selfie + liveness, la función del GET Mobile Administrator es verificar a una persona basándose en un escaneo de su identificación estatal emitida por el gobierno, o mediante la lectura de un código QR enviado por correo

electrónico, y una selfie en vivo, incluyendo validación de vida certificada ISO 30107-3 , ambas tomadas en el momento del proceso de inscripción de la aplicación GET Mobile ID. Esta opción incluye la instalación de un componente de que facilita la verificación de datos biométricos y demográficos durante el proceso de registro de emisión de mID. Luego de la emisión, se solicita al usuario digitar un PIN Personal, para permitir la apertura de la aplicación de forma segura. Se cuenta con la funcionalidad de Apple FaceID para realizar este proceso de autenticación.

DEMOSTRACIÓN DE APROVISIONAMIENTO REMOTO:




Escanear codigo QR
Verificar información
Necesitamos identificarle
Por favor, asegúrese de:
1) que haya una iluminación pareja en toda su cara
2) que la expresión facial coincida con la de su tarjeta
PROXIMO
Este preparado para
Su Video Selfi
ESTOY LISTO
Aproximese
Cargando
Encriptado
3D Escáner de rostro
Notificaciones vía SMS
Manténgase informado
Marque la siguiente casilla de verificación si desea que se le informe a través de un mensaje sms sobre cambios en su miID.
Puede cambiar su selección en cualquier momento desde la configuración de la aplicación.
Sí, quiero recibir notificaciones por sms
PROXIMO
Utopia
Driver's License
Hola,
MAURICIO
Driver's License
MAURICIO MOYA PAEZ



4.2.2 GET MOBILE ID – APLICACIÓN MÓVIL

GET Mobile ID estará disponible en las tiendas de aplicaciones públicas de cada plataforma móvil en el momento del lanzamiento. Dado que es una aplicación de consumo, se espera que las características del producto se aceleren continuamente y se les dé prioridad según las solicitudes de los ciudadanos/usuarios y lo que esté sucediendo en el mercado mID. El uso de una aplicación de las tiendas de aplicaciones proporciona la experiencia de aplicación que los usuarios esperan de sus bancos, emisores de tarjetas de crédito, proveedores de atención médica y entretenimiento. Todos los usuarios de la aplicación en todas las jurisdicciones experimentarán el mismo conjunto de funciones y se podrán implementar nuevas funciones en todo el país.

El CONSORCIO trabajará con el JCE para configurar ("personalizar") el interior de la aplicación GET Mobile ID cuando un ciudadano lleva su credencial digital como mID. El sello estatal, los patrones de fondo entrecruzado, las fuentes de encabezado y las banderas, así como los tipos de licencia, están disponibles como configuraciones. El GET Mobile ID no es una tarjeta y no tiene una representación de tarjeta; está diseñado para ser intervenido, compartido y utilizado electrónicamente porque la prueba criptográfica de identidad es fácil de presentar utilizando ISO 18013-5.

El CONSORCIO se asegurará de que los campos de la credencial digital estén asignados a los campos ISO 18013-5. Si alguno permanece sin asignar, se puede agregar opcionalmente según se define en los campos específicos de las jurisdicciones, pero no podrán ser leídos por todos los dispositivos o aplicaciones lectores estandarizados. Por lo general, esto no es un problema en los casos de uso de identidad, ya que los campos específicos de la jurisdicción no suelen ser necesarios para aprobar transacciones generalizadas.

Soporte de cumplimiento y estándares

- Cumple con las especificaciones y directrices de la AAMVA
- Certificado de cumplimiento de las normas ISO/IEC18013
- Comunicación entre pares compatible con NFC, Bluetooth y WiFi nativos
- Manejo de llaves conforme a ICAO 9303
- Protección de acceso básica mejorada mediante clave de acceso dinámica

Soporte de comunicaciones

- HTTP/S
- Modo par NFC
- Modo Bluetooth Peer to Peer
- Wifi aware
- Código de barras 2D

Funciones de control de seguridad

- Seguridad redundante mediante almacenes de claves respaldados por hardware.
- Encripción de datos en reposo y transmisión encriptada basada en sesiones.
- Los datos de mID están firmados por la autoridad emisora de confianza a prueba de manipulaciones.
- La ofuscación de aplicaciones significa que el código ejecutable no se puede piratear.
- Protección de análisis estático y dinámico. Se logran protecciones integrales de análisis estático y dinámico a través de técnicas de encriptación y ofuscación en capas complementadas con verificaciones RASP automatizadas y defensas antimalware integradas. Protección contra jailbreaking y rooting.
- OAuth habilitado para autorización de agentes del orden.
- Revocación automática desde el GET Mobile Administrator.
- Criptografía soportada: RSA y Eliptic Curves.

4.2.2.1 OPCIONES DE PERSONALIZACIÓN

GET utilizará componentes existentes sobre una base de desarrollo personalizado para crear una aplicación de emisor personalizada que funcione según los requisitos y el diseño del emisor. Una vez determinado el tamaño y el alcance de los requisitos de la aplicación, se procede con los ajustes de personalización. Además, si el JCE desea publicar la aplicación a través de su propia tienda de aplicaciones (también conocida como marca blanca), se requerirá una coordinación significativa con el personal de Desarrollo de productos de GET para coordinar las actualizaciones del servicio con las actualizaciones de la aplicación.

GET trabajará en conjunto con el JCE para presentar una propuesta de diseño que cumpla con los requerimientos de diseño de la marca JCE y de la marca PAIS.

Así mismo, el sistema GET Mobile Administrator, en conjunto con las aplicaciones móviles, permiten la generación de notificaciones PUSH, permitiendo la comunicación con los ciudadanos portadores del GET Mobile ID.

4.2.2.2 CONTROL TOTAL Y PROTECCIÓN DE LA PRIVACIDAD

Todos los ciudadanos tienen el derecho básico a controlar su información de identidad. Deberían poder elegir qué datos comparten, ser transparentes en su uso y tener un registro claro de dónde han compartido sus datos. En línea o fuera de línea, GET Mobile ID permanece bajo el control del ciudadano y siempre se requiere su consentimiento para compartir datos, proporcionando un registro claro para el titular del mID de dónde se utilizaron los datos del mID y, cuando sea posible, por quién.

Actualmente, cuando una persona quiere acceder a un colegio de abogados, por ejemplo, está obligada a demostrar su edad. Sin embargo, al presentar un documento de identificación físico, el individuo se ve obligado a exponer toda su información personal (incluida la dirección y otros datos personales sensibles), algunos de los cuales tal vez desee mantener en privado. Al escanear los códigos de barras se crea un registro permanente de sus datos. Con el mID compatible con ISO de GET, un ciudadano puede proteger su privacidad eligiendo la cantidad y el tipo de datos que pueden transferirse a los verificadores. Sólo ciertos verificadores necesitan acceso a todos los elementos de datos. GET Mobile Verify puede limitar los niveles de acceso a datos según la función, la suscripción y la autorización del verificador.

4.2.2.3 SIEMPRE ACTUALIZADO

Las aplicaciones móviles son dinámicas, a diferencia de las credenciales físicas estáticas, lo que permite definir una frecuencia para actualizar los datos mID. El Administrador de GET Mobile permite al Emisor establecer una política de actualización y aplica e implementa automáticamente esa política para que todos los mID conectados dentro de GET Mobile ID se actualicen de forma natural. Ni el ciudadano ni el administrador necesitan preocuparse por mantenerse al día. Además, GET Mobile Administrator admite múltiples mecanismos, a elección del Emisor, para transmitir datos de identificación modificados desde el sistema de registro (SOR) a los usuarios con mID.

Cuando el emisor cambia el estado de una identificación, el emisor transmite ese cambio al administrador de GET Mobile para que lo transmita inmediatamente al dispositivo móvil del usuario. Si un ciudadano reporta la pérdida de una tarjeta o un teléfono, es posible que se le dé de baja de forma remota. Más convenientemente, las funciones de teléfono perdido o extraviado disponibles en cada plataforma están completamente disponibles. Los usuarios pueden borrar los datos del teléfono utilizando sus inicios de sesión individuales en la plataforma. Estas funcionalidades de actualización también aplican en los escenarios de revocación que la Administración decida implementar.

4.2.2.4 INTEROPERABILIDAD

El concepto de interoperabilidad en el marco de la norma ISO 18013-5 hace referencia la capacidad que deben tener las identidades móviles en poder ser usadas dentro de la jurisdicción del emisor (en este caso, la Republica Dominicana) y cualquier otra jurisdicción que requiere poder leer la información de una identidad digital.

Con relación a lo anterior, la norma ISO 18013-5 es la guía para que los gobiernos puedan emitir identidades móviles a sus ciudadanos de manera que están puedan ser leídas, comprobadas y verificadas dentro de otras jurisdicciones. Por ejemplo, en Colombia, país que ha implementado la identidad móvil digital desde el año 2020, a razón de haber implementado el estándar ISO 18013-5, es ahora permitido viajar en los diferentes países de la CAN y MERCOSUR con tan solo mostrar su identidad móvil en su teléfono inteligente, puesto que, al ser una identidad estandarizada, la interoperabilidad le permite identificar que la identidad sigue siendo original y sin modificaciones.

Es así que al decir que una solución de emisión de identidades móviles digitales se encuentra CERTIFICADA para el estándar ISO 18013-5, confirma que esta solución permite la interoperabilidad de las identidades emitidas por esta solución, en conjunto con las diferentes opciones de integraciones y API disponibles para acceder a información adicional y verificaciones.

4.2.3 GET MOBILE VERIFIER

Contrariamente a lo que se cree erróneamente, aceptar identificaciones móviles no significa mirar la pantalla del teléfono de sus clientes ni manipular su teléfono en absoluto. Las herramientas de manipulación de fotografías hacen que el uso visual no sea confiable y usted nunca debe asumir la responsabilidad de manipular el teléfono de su cliente.

Los mecanismos de transmisión ISO 18013-5 permiten modos de interacción flexibles que mantienen a su cliente en control de su dispositivo y sus datos, al tiempo que le brindan al verificador prueba criptográfica indiscutible de la identidad de su cliente, incluso sin sobrecarga de datos.

Cuando intercambia datos electrónicos y valida pruebas criptográficas, ya no está sujeto a los requisitos de "línea de visión" de las tarjetas de identificación físicas.

A medida que la identificación se vuelve cada vez más digital, el mercado debe estar preparado para aceptar rápidamente identificaciones móviles desde cualquier parte del mundo como forma legal de identidad o verificación de edad. La aplicación GET Mobile Verify le proporcionará una transacción de cliente más fácil y segura.

- Aplicación directa a la parte que confía: verificar la edad y la identidad del titular.
- Lectura estándar ISO 18013-5 en línea y fuera de línea.
- Trabaja con todas las jurisdicciones a nivel mundial a través de una lista confiable
- Disponible para iOS y Android: GET Mobile Verify admite NFC, BLE, Wi-Fi Aware y WebAPI en plataformas iOS y Android. Disponible como motor para dispositivos Windows y POS.
- Reduce la complejidad de la inspección de documentos de identificación globales: mantenerse al día con los cambios de los documentos de identificación en constante cambio es difícil. ¿Cómo puedes saber qué es real o qué es simplemente una muy buena tarjeta de identificación falsa? Las identificaciones móviles mID presentan su prueba de identificación electrónicamente y de la misma manera siempre: grande, en negrita, mostrando prueba de edad o identificación. No requiere del entrenamiento laborioso del personal y hay menos errores cuando los documentos parecen ser legítimos.
- Obtiene una prueba criptográfica de identificación: el simple hecho de mirar los documentos de identificación, especialmente en dispositivos móviles, no descarta las identificaciones falsas. GET Mobile Verify solo acepta documentos de emisores de identificación gubernamentales conocidos, lo que reduce su responsabilidad y exposición.
- Respeta la confidencialidad de sus clientes: reducir los datos intercambiados durante las transacciones de identificación mejora la privacidad de sus clientes y alivia sus preocupaciones sobre privacidad y seguridad, al tiempo que reduce su exposición y responsabilidad de recopilar y almacenar datos personales.
- Transacciones de identidad más saludables: proteja la salud de sus empleados y clientes con transacciones de identificación sin contacto. Un toque o un escaneo desde la distancia social garantiza que no esté manipulando documentos de identidad ni asumiendo responsabilidad por el manejo de los teléfonos móviles de sus clientes. GET Mobile Verify permite a tus clientes comprobar su identidad desde una distancia segura y saludable.

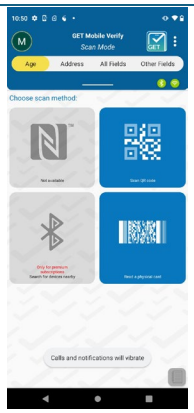
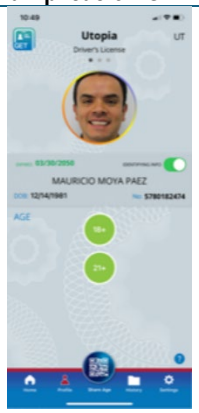
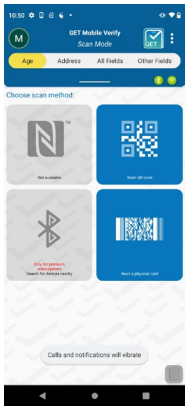
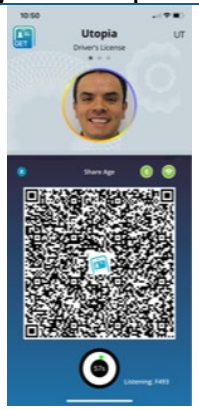
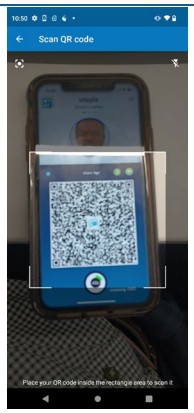
El estándar ISO/IEC 18013-5 introduce dos pasos en una interacción mID: La interacción del dispositivo (Device engagement) es cuando el mID y el dispositivo lector negocian cómo conectarse en el intercambio de datos mID en línea; Y fuera de línea, a través de un canal de transmisión mutuamente compatible. Una vez elegido un canal, los dispositivos realizan la transmisión de datos mediante solicitud-respuesta.

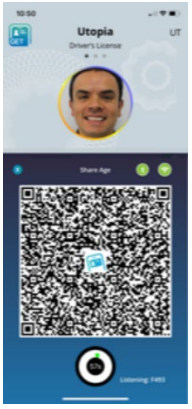
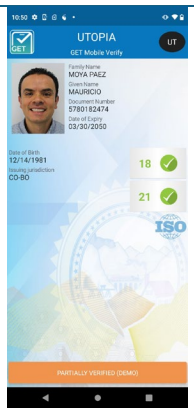
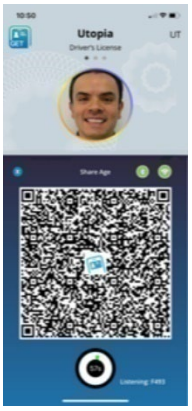
Se admiten dos modelos: verificación offline (sin necesidad de Internet) y verificación de búsqueda en línea.

Los métodos de interacción con dispositivos admitidos: NFC, QR, BLE (según la extensión en evolución del borrador del estándar internacional ISO).

Canales de transmisión de datos admitidos: NFC sin conexión (Android completo e iOS en alfa), BLE, WIFI Aware (en versión beta disponible solo en Android 10 o posterior), en línea a través de WebAPI y Open ID Connect.

Simulación de Verificación de mID

Aplicación mID	Aplicación Mobile Verifier
 Se inicia la Aplicación GET Mobile ID	 **Se inicia la aplicación GET Mobile Verifier**
 **El usuario elije los datos que desea compartir**	
 **El usuario selecciona Compartir**	 **Se escanea el QR compartido**

	 **Se transfieren los datos compartidos y se visualizan**
	**Se verifican los datos de los certificados digitales**

4.2.3.1 MODOS DE INTERACCIÓN

Las combinaciones de interacción con el dispositivo, transferencia de datos y en línea/fuera de línea crean “interacciones” únicas que, si se implementan por completo, permitirán a los verificadores reconfigurar el flujo de trabajo para adaptarlo a su negocio y brindar un servicio ampliado y más personalizado a los clientes de mID en comparación con lo que se ofrece tradicionalmente con Tarjetas físicas.

Estos modos de interacción combinados se pueden resumir a continuación. El soporte de todos los modos de interacción pasa a ser responsabilidad del Emisor al elegir la tecnología mID. Múltiples modos de interacción brindarán la experiencia de usuario óptima para los titulares de mID y brindarán la mejor opción para los verificadores de mID.

Los verificadores deberían poder elegir el modo de interacción que mejor respalde su negocio.

Modo de Interacción	Vinculación de Dispositivo	Transferencia de Datos	Autorización de Usuario [Si es no atendida]	Descripción
Tap & Go	NFC	BLE		El toque NFC establece BLE para la transferencia de datos y el usuario puede alejar el mID mientras transfiere datos al lector
Tap & Request	NFC	Online		NFC contiene un token WebAPI que devuelve datos con el retrato (fotografía) para el operador
Tap & Hold	NFC	NFC		Interacción y transferencia de datos complete por NFC

Scan & Go	QR	BLE	El usuario sostiene el código QR mID frente a la cámara del lector y luego puede mover el mID mientras se transfieren datos a través de un método cercano
Scan & Request	QR	Online	El usuario sostiene el código QR mID en la cámara del Reader y los datos aparecen en el Reader después de una rápida recuperación en línea

Dar soporte a estos múltiples modos de interacción no requiere ningún esfuerzo por parte del JCE más allá de elegir e implementar la tecnología de aplicación GET Mobile ID y realizar una opción de integración estándar como se describe en este documento. Será una opción clave para los ciudadanos y para construir una plataforma en la que la identidad móvil pueda florecer verdaderamente.

4.2.4 Herramientas de Desarrollo

GET Mobile ID tiene la posibilidad de brindar un soporte adicional con relación a las herramientas de desarrollo disponibles para la implementación de la emisión de una identidad digital móvil basada en estándar ISO 18013-5, dentro de las cuales se encuentran:

- SDK's para la emisión de identidades, para Android y iOS.
- API para la conexión e integración en el proceso de emisión de identidades móviles.
- SDK's disponibles para la verificación de identidades móviles, basadas en estándares, para su implementación en Android, iOS, Windows o sistemas POS.

Durante el proceso de análisis de requerimientos se establecerán los compromisos necesarios para realizar la entrega de los SDK's solicitados de acuerdo con la necesidad de implementación del JCE.

4.2.5 INFRAESTRUCTURA

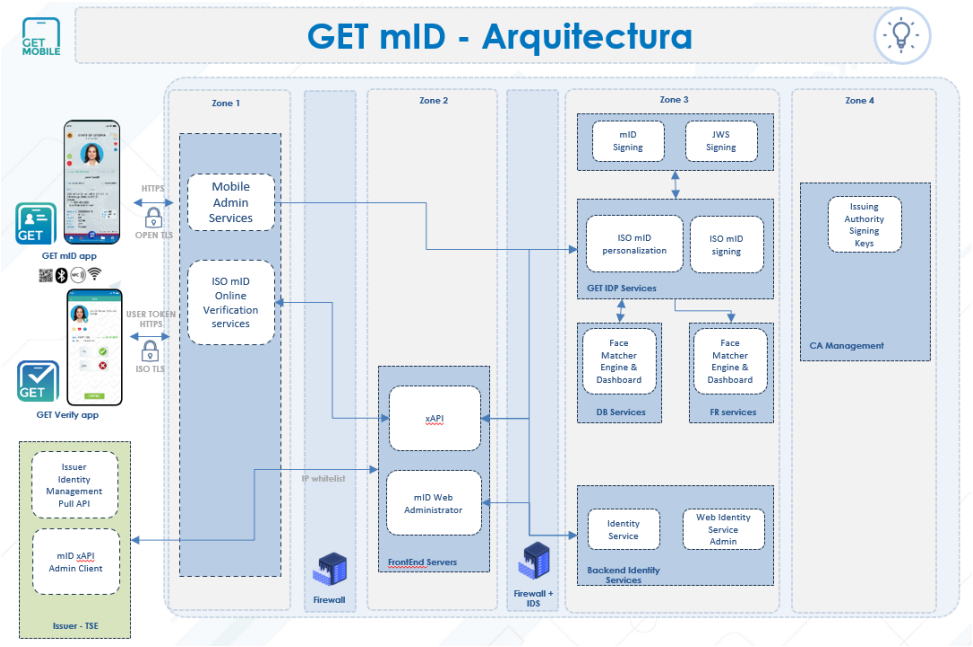
4.2.5.1 ARQUITECTURA DE ALTA DISPONIBILIDAD

El diseño de la solución GET Mobile ID es un diseño innovador que está basado en la Alta Disponibilidad de cada uno de los componentes, en conjunto con el uso de diferentes zonas de seguridad para garantizar la implementación segura. El diseño de solución acá propuesto incluye la capacidad requerida para emitir al menos 5.000 GET Mobile ID por día.

Los módulos que componen la arquitectura de la solución son:

- Mobile Admin services: API para la Administración de la emisión en los teléfonos móviles.
- ISO mID Online Verification services: API para la verificación de identidades Mobile ID en línea.
- xAPI: API para el control de la emisión de identidades Mobile ID.
- mID Web Administrator: Modulo Web que permite la administración de la solución, su configuración, visualizar de eventos y auditoria, gestor de reportes.
- mID Signing: Modulo de firma de documentos digitales, utiliza las llaves del PKI para su función.
- JWS Signing: Modulo de firmado para archivos JSON.
- ISO mID Perso: API para emisión de identidades estándar ISO 18013-5
- ISO mID signing: API para el firmado ISO.

- Face matcher: Módulos de comparación y base de datos para la verificación biométrica y reconocimiento de vida.
- Identity Service: Modulo de administración de identidades.
- Web Identity Service Admin: Administración de usuario para módulos web.
- Issuing Authority Signing Keys: Solución PKI.



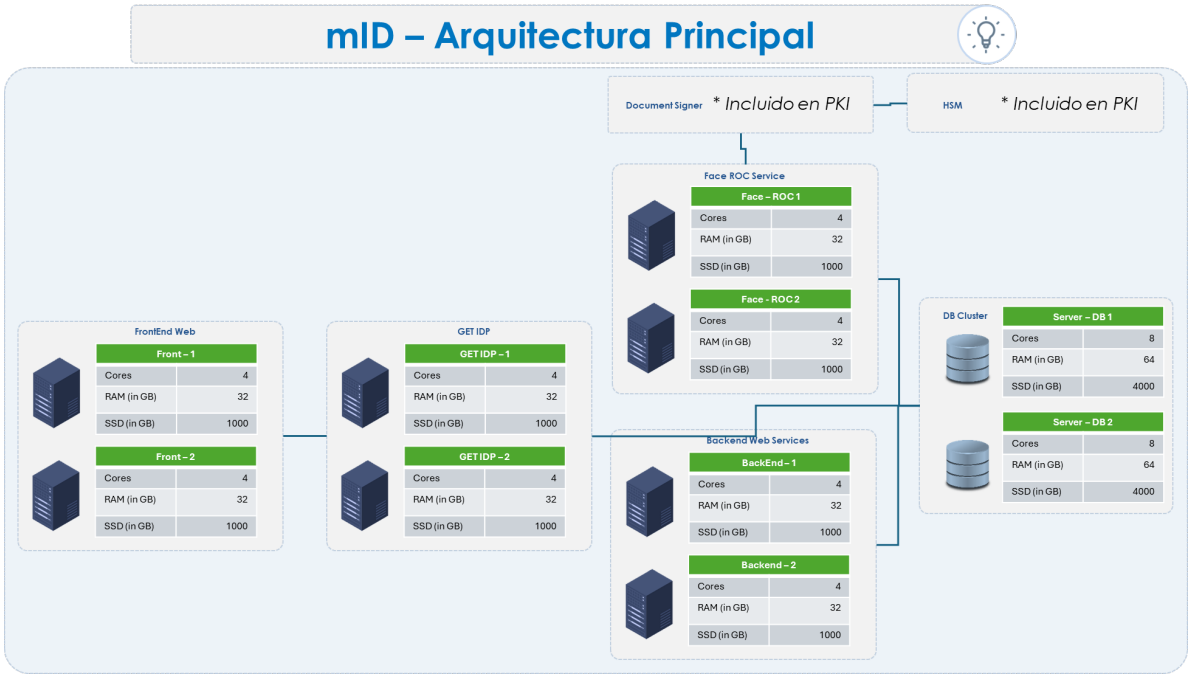
Se han tomado todas las previsiones del caso para poder brindar a la JCE una plataforma con mecanismos de alta disponibilidad del servicio tanto en hardware como en software contemplando los siguientes aspectos a nivel de diseño de la infraestructura para garantizar la continuidad de la operación:

Se dispondrá de una infraestructura Hiperconvergente el cual está diseñado con 4 nodos para brindar una redundancia y alta disponibilidad, además de una capa de interconexión media con dos switches en HA para realizar la configuración del ambiente de producción requerido. Esta solución de hiperconvergencia contempla una configuración vSAN para brindar alta disponibilidad a nivel de almacenamiento.

Esta solución contempla un esquema de respaldos sobre las máquinas virtuales requeridas para desplegar el servicio, el cual se define en 1 respaldo Full diario con retención de 30 días.
Además, se incluye una capa de red de borde compuesta por dos switches en configuración de alta disponibilidad y redundancia para brindar la interconexión entre la infraestructura de hiperconvergencia, la capa de seguridad dimensionada y la conexión hacia la infraestructura de la JCE.

A nivel de seguridad se contempla un diseño de alta disponibilidad de NG Firewalls, este es un componente crítico en la arquitectura de seguridad de redes modernas. Estos dispositivos desempeñan un papel fundamental en la protección de una organización contra amenazas cibernéticas, por lo que garantizar su continuidad operativa es esencial. Para lograr una alta disponibilidad, se implementan redundancias en la infraestructura del NG Firewall, lo que incluye configuraciones en clúster, así como elementos en su arquitectura física, como fuentes de poder redundantes.

Referente a la implementación del Web Application Firewall (WAF), el mismo es un elemento virtual dentro de la solución ofertada. De esta manera, teniendo lo anterior en consideración, es posible brindar todas las bondades de los ambientes de virtualización desarrollados en el presente diseño, lo que permite que el WAF tenga una alta disponibilidad en su infraestructura. Un Web Application Firewall (WAF) virtual de Alta Disponibilidad (HA) es una parte esencial de la estrategia de seguridad cibernética para proteger aplicaciones web y sitios web.



4.2.5.2 DISPONIBILIDAD DEL 99.95% DE OPERACIÓN

Con el fin de garantizar un esquema de alta disponibilidad de operación durante las horas efectivas de producción definidas por el JCE el consorcio considera conveniente la inclusión de un recurso especializado en los equipos de procesamiento y seguridad en sitio para garantizar la atención inmediata de incidentes que se puedan presentar y reducir los tiempos de atención de la solución, esto en conjunto con los diseños explicados en el apartado de Infraestructura buscan garantizar al JCE el menor impacto posible en la operación y la continuidad del servicio.

ÍTEM V- KIT PERIFERICOS

5 INTRODUCCION

Como parte del compromiso del Consorcio Identidad 4.0 RD con la modernización y optimización del sistema de identificación de la Junta Central Electoral (JCE), se ha realizado un análisis exhaustivo de los dispositivos disponibles en el mercado, priorizando la eficiencia, seguridad y compatibilidad con la infraestructura existente.

En base a la amplia experiencia del consorcio en la implementación de soluciones tecnológicas para la gestión de identidad, se ha seleccionado el Canon imageFORMULA P-208II como el escáner ideal para la digitalización de documentos dentro del proceso de emisión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI).

Este escáner portátil de alto rendimiento destaca por su precisión en la captura de documentos oficiales, incluyendo tarjetas de identificación, licencias de conducir, contratos, fotografías y otros archivos esenciales para la personalización y validación de identidad. Su diseño compacto y su capacidad de escaneo a doble cara optimizan los tiempos de procesamiento, reduciendo significativamente los errores en la captura de datos.

El Canon imageFORMULA P-208II ha sido elegido estratégicamente debido a los siguientes factores clave:

- Experiencia del consorcio en la implementación de sistemas de escaneo de alta precisión, garantizando su integración óptima con los procesos de la JCE.
- Compatibilidad comprobada con los sistemas operativos y plataformas en la nube utilizadas en proyectos de identidad digital.
- Cumplimiento con estándares internacionales de calidad y seguridad, incluyendo normativas de protección de datos y eficiencia energética.
- Fiabilidad en entornos de alto volumen de escaneo, respaldada por casos de éxito en la implementación de este modelo en otros organismos gubernamentales y entidades de identificación ciudadana.

El imageFORMULA P-208II permite un escaneo intuitivo y eficiente mediante su función de "Conectar y Escanear", eliminando la necesidad de instalación de software adicional. Además, su tecnología de Reconocimiento Óptico de Caracteres (OCR) facilita la conversión de documentos físicos en archivos digitales estructurados, garantizando una gestión documental ágil y segura.

Debido a su compatibilidad con sistemas operativos Windows y Mac, así como su integración con plataformas en la nube como Google Drive™, OneDrive™ y Microsoft® SharePoint®, este escáner representa una solución flexible y escalable, perfectamente alineada con los requerimientos tecnológicos y operativos de la JCE.

Con una trayectoria comprobada en la integración de soluciones tecnológicas para identidad digital, el Consorcio Identidad 4.0 RD garantiza que la incorporación del Canon imageFORMULA P-208II fortalecerá la infraestructura de emisión de cédulas, asegurando una transición eficiente hacia un sistema moderno, seguro y de alta precisión.

DESCRIPCIÓN DE LOS PERIFÉRICOS

5.1 ESCÁNER DE DOCUMENTOS - CANON IMAGEFORMULA P-208II

El Canon imageFORMULA P-208II es un escáner de documentos compacto y portátil que permite la digitalización rápida de documentos de identidad, fotografías, contratos y otros archivos relevantes. Es ideal para su uso en entornos de oficina o en movilidad.

ESPECIFICACIONES TÉCNICAS

- Tipo: Escáner de documentos portátil.
- Alimentación de documentos: Automática o manual.
- Tamaño de documentos:
- Anchura: 2.0” a 8.5”
- Longitud: 2.8” a 14.0”
- Capacidad del alimentador: 10 hojas.
- Modos de escaneo: Color, escala de grises y blanco y negro.
- Resolución óptica: 600 ppp.
- Velocidades de escaneo:
- Blanco y negro: Hasta 8 páginas por minuto (ppm) / 16 imágenes por minuto (ipm).
- Escala de grises: Hasta 8 ppm / 16 ipm.
- Color: Hasta 8 ppm / 16 ipm.
- Interfaz: USB 2.0 de alta velocidad.
- Compatibilidad con sistemas operativos: Windows (XP, Vista, 7, 8, 10) y Mac OS X 10.6 en adelante.
- Software integrado:
- CaptureOnTouch: Optimización de escaneo con opciones avanzadas.
- OCR (Reconocimiento Óptico de Caracteres): Convierte documentos físicos en texto digital.
- Integración con la nube: Compatible con Google Drive™, Evernote™, Microsoft® SharePoint®, OneDrive™ y Dropbox™.

OTRAS CARACTERÍSTICAS:

- Detección automática de color y tamaño de documento.
- Corrección de desviación y eliminación de sombras.
- Detección de alimentación doble para evitar pérdida de datos.

BENEFICIOS

- Escaneo rápido y eficiente, optimizando el procesamiento de documentos en la JCE.
- Compacto y portátil, ideal para estaciones de trabajo con espacio limitado.
- Integración con los sistemas de la JCE, facilitando el almacenamiento seguro de documentos digitales.
- Alta calidad de imagen, asegurando legibilidad en documentos oficiales.

5.2 TABLETA DE FIRMA DIGITAL WACOM STU-540

Como parte de esta estrategia, y en base a la amplia experiencia del consorcio en la implementación de soluciones de autenticación digital y biométrica, se ha seleccionado la tableta de firma digital Wacom STU-540. Este dispositivo representa la opción más avanzada y confiable en la captura de firmas electrónicas manuscritas, asegurando precisión biométrica, seguridad criptográfica y una integración fluida con los sistemas existentes de la Junta Central Electoral (JCE).

La elección del Wacom STU-540 responde a los siguientes criterios estratégicos:

- Experiencia del consorcio en la implementación de sistemas de firma electrónica en entornos gubernamentales y de alta seguridad.
- Cumplimiento con estándares internacionales de cifrado y autenticación, garantizando la validez jurídica de las firmas electrónicas.
- Compatibilidad con infraestructuras de escritorio virtual (VDI), permitiendo su integración con plataformas como Citrix XenDesktop y XenApp.
- Fiabilidad y durabilidad en entornos de alto tráfico, asegurando un rendimiento óptimo en oficinas de atención al ciudadano.
- Autenticidad en la representación de la firma manuscrita, mediante la tecnología WILL™ (Wacom Ink Layer Language), que proporciona una apariencia natural y precisa de cada trazo.

El Wacom STU-540 ha sido seleccionado como la solución óptima para la captura de firmas electrónicas en el proceso de emisión de la Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI), gracias a su combinación de precisión biométrica, seguridad avanzada y robustez operativa.

Su pantalla LCD de 5 pulgadas con vidrio endurecido proporciona una experiencia de firma natural y ergonómica, replicando la sensación del papel y garantizando una durabilidad superior ante el uso intensivo en entornos de alta demanda. Además, su tecnología de captura con 1024 niveles de presión permite registrar con exactitud cada trazo de la firma manuscrita, asegurando una autenticación precisa, única y verificable.

Desde una perspectiva de seguridad y cumplimiento normativo, el Wacom STU-540 incorpora cifrado AES-256 y RSA-2048, garantizando la integridad y confidencialidad de cada transacción. Su Identificador Único de Hardware (UID) permite asociar de forma inalterable cada firma al dispositivo donde fue generada, fortaleciendo los mecanismos de auditoría, trazabilidad y prevención de fraude dentro del sistema de identidad de la Junta Central Electoral (JCE).

En términos de integración y escalabilidad, su conectividad flexible mediante USB, Virtual COM Port (VCP) y RS-232 facilita su implementación en infraestructuras de escritorio virtual (VDI), garantizando una interoperabilidad sin fricciones con los sistemas actuales de la JCE. Adicionalmente, su capacidad para almacenamiento y despliegue de imágenes permite utilizar el dispositivo como un canal de comunicación institucional, optimizando la difusión de información relevante para los ciudadanos.

La incorporación del Wacom STU-540 en la solución propuesta por el Consorcio Identidad 4.0 RD refuerza el compromiso con la innovación tecnológica y la seguridad en la gestión de identidad, asegurando un sistema de identificación digital eficiente, confiable y alineado con los más altos estándares internacionales.

5.3 LECTOR DE HUELLAS DIGITALES DIGITALPERSONA 4500

La autenticación biométrica es un pilar esencial en la modernización de los sistemas de identidad. Por ello, el DigitalPersona 4500 es el dispositivo ideal para garantizar la identificación precisa y segura en los procesos de emisión de la Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI). Este lector de huellas dactilares se distingue por su capacidad de capturar imágenes con alta fidelidad, su resistencia operativa y su compatibilidad con diversas plataformas tecnológicas.

El DigitalPersona 4500 destaca por sus características avanzadas:

- **Escaneo óptico de alta precisión:** Su tecnología óptica permite la captura de huellas con resolución de 500 dpi, asegurando un alto nivel de detalle y calidad en cada lectura.
- **Fiabilidad en entornos exigentes:** Equipado con una carcasa metálica robusta y un recubrimiento de silicona que mejora la adherencia de la huella, permite la identificación efectiva incluso con dedos húmedos, secos o rugosos.
- **Seguridad criptográfica integrada:** Implementa cifrado propietario de 32 bits con clave de rotación, protegiendo la integridad de los datos biométricos transmitidos.
- **Interoperabilidad y escalabilidad:** Compatible con múltiples sistemas operativos como Windows, Linux y Android, y optimizado para integrarse con los SDK de DigitalPersona.
- **Facilidad de uso e implementación:** Su interfaz USB 2.0 y su diseño compacto permiten una instalación sencilla y una experiencia de usuario intuitiva, ideal para entornos de alta demanda.

Desde el punto de vista normativo, el DigitalPersona 4500 cumple con certificaciones internacionales como FCC Class B, CE, ICES, BSMI, MIC, USB y WHQL, asegurando su idoneidad para sistemas de identidad gubernamentales. Su capacidad de rechazo de huellas falsas y latentes refuerza aún más la seguridad en el proceso de autenticación.

La implementación del DigitalPersona 4500 en la solución del Consorcio Identidad 4.0 RD representa un avance estratégico en la protección y validación de la identidad de los ciudadanos, alineado con los estándares internacionales de seguridad y eficiencia tecnológica.

5.4 IMPRESORA TÉRMICA STAR BSC10UD-24

En el marco de la optimización de los procesos de venta y servicio en entornos de retail y hospitalidad, la impresora térmica STAR BSC10UD-24 se posiciona como una solución esencial para la emisión rápida y fiable de tickets y recibos. Su diseño simple y robusto, junto con la innovadora tecnología de carga de papel sin mecanismos complicados, garantiza un rendimiento óptimo en condiciones de uso intensivo, reduciendo tiempos de inactividad y mejorando la experiencia del cliente.

CARACTERÍSTICAS TÉCNICAS Y BENEFICIOS

- **Alta velocidad de impresión:** Con una capacidad de hasta 250 mm/seg, la impresora permite la emisión de recibos de forma ultrarrápida, ideal para momentos de alta demanda.
- **Resolución de 203 dpi:** La tecnología de impresión térmica directa asegura textos y gráficos nítidos, fundamentales para una legibilidad impecable en ambientes comerciales.
- **Interfaz dual (USB/RS232):** Facilita su integración con diversos sistemas de punto de venta, garantizando compatibilidad con múltiples plataformas operativas.
- **Diseño compacto y de fácil mantenimiento**: Su innovador sistema de "drop-in & print" elimina la necesidad de mecanismos de carga complicados, reduciendo el tiempo de cambio de rollo y aumentando la fiabilidad operativa.
- **Capacidad para rollos de 10 cm de diámetro:** Esta característica permite utilizar hasta un 60% más papel en cada rollo, lo que se traduce en menores costos operativos y menos interrupciones por reposición.
- **Compatibilidad con ESC/POS y suministro completo:** Viene equipada con fuente de poder y es compatible con los estándares de emulación más utilizados en la industria, facilitando su implementación en infraestructuras digitales existentes.

VENTAJAS

• **Incremento en la eficiencia operativa:** La alta velocidad de impresión y la capacidad extendida del rollo reducen los tiempos de espera en el punto de venta.
• **Reducción de costos:** Menor frecuencia en el cambio de papel se traduce en ahorro en insumos y logística.
• **Integración versátil:** La interfaz dual y la compatibilidad con ESC/POS permiten una implementación sencilla en diferentes entornos tecnológicos.
• **Fiabilidad y durabilidad:** Su diseño robusto y fácil mantenimiento garantizan un funcionamiento constante incluso en condiciones de uso intensivo.
• **Mejora en la experiencia del cliente:** Un proceso de emisión de recibos ágil y sin contratiempos contribuye a una atención más fluida y satisfactoria.

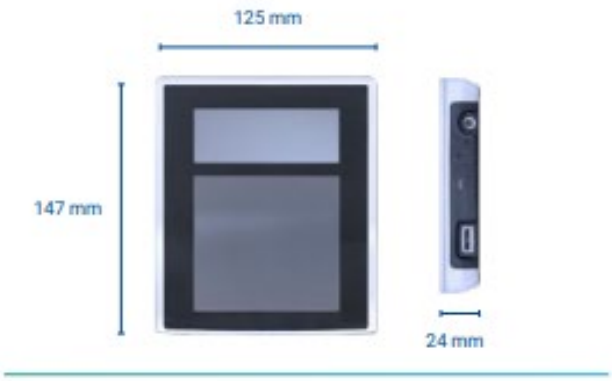
5.5 ESCÁNER DE HUELLAS DIGITALES LIVETOUCH QUATTRO

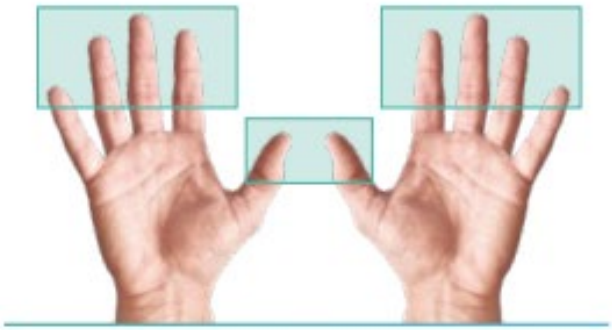
El LIVETOUCH QUATTRO responde a las exigencias de seguridad e interoperabilidad requeridas en los procesos de identificación nacional. Su integración dentro de los centros de emisión de documentos garantiza un registro biométrico confiable, alineado con estándares internacionales.

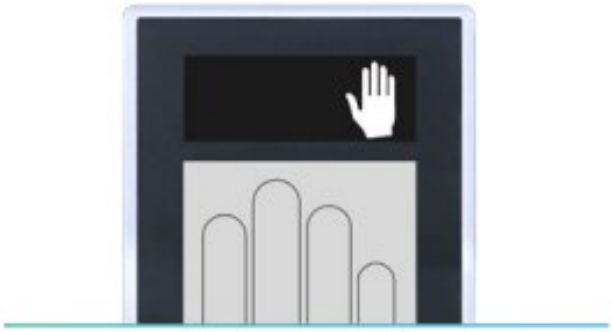
Su capacidad de captura rápida y su sistema de corrección visual reducen significativamente los tiempos de inscripción, permitiendo una experiencia más eficiente tanto para el personal de la JCE como para los ciudadanos.

CARACTERÍSTICAS TÉCNICAS Y BENEFICIOS

- **Captura multifuncional de huellas:** Permite la obtención de huellas planas, rodadas y el método 4-4-2, optimizando el registro de datos biométricos con alta precisión.
- **Pantalla táctil interactiva:** Incluye un sistema de guía visual que facilita el proceso de captura y minimiza errores de inscripción.
- **Alta resolución de imagen:** Sensor con 500 dpi, garantizando una calidad de imagen certificada por el FBI y BSI.
- **Diseño compacto y portátil:** Con dimensiones de 125 mm x 147 mm x 24 mm y un peso de solo 360 g, es ideal para integraciones en infraestructuras existentes.
- Conectividad avanzada: Compatible con USB 3.0 y 2.0, asegurando una transmisión de datos rápida y estable.
- **Protección robusta y durabilidad:** Recubrimiento de vidrio resistente a arañazos y certificación IP54, protegiendo contra polvo y salpicaduras.
- **Captura de firmas digitales:** Funcionalidad integrada que permite la recolección de firmas manuscritas sin necesidad de un dispositivo adicional.







5.6 CÁMARA CANON EOS REBEL T7

En el marco del fortalecimiento de los procesos de identificación, la captura de imágenes de alta calidad es un pilar fundamental para garantizar la precisión y confiabilidad en la documentación oficial. La Canon EOS Rebel T7 ha sido seleccionada como una solución tecnológica clave para la obtención de imágenes que

cumplan con los requerimientos técnicos de identificación, asegurando una captura fiel y detallada de cada ciudadano.

CARACTERÍSTICAS TÉCNICAS Y BENEFICIOS

- **Calidad de imagen excepcional:** Con un sensor CMOS de 24.1 MP, la cámara proporciona imágenes de alta resolución esenciales para la identificación digital y la verificación biométrica.
- **Procesador de Imagen DIGIC 4+**: Optimiza el rendimiento y garantiza una reproducción de color precisa, fundamental para la identificación oficial.
- **Sistema de enfoque automático de 9 puntos:** Facilita la captura de imágenes nítidas en condiciones de alta demanda, asegurando uniformidad y precisión.
- **Pantalla LCD de 3.0 pulgadas:** Permite visualizar y ajustar la toma en tiempo real, facilitando la operatividad en centros de emisión de documentos.
- **Conectividad Wi-Fi y NFC**: Permite la transferencia rápida de imágenes al sistema central de la JCE, agilizando los procesos administrativos.
- **Compatibilidad con infraestructuras digitales:** Integración eficiente con el sistema de captura y almacenamiento de datos de la JCE.

VENTAJAS

- Estandarización en la captura de imágenes para cédulas de identidad.
- Reducción de tiempos de procesamiento mediante transferencia inalámbrica.
- Alta fidelidad en la reproducción de detalles faciales, mejorando la autenticación visual.
- Facilidad de uso y configuración rápida, adaptándose a los entornos operativos de la JCE.
- Durabilidad y resistencia, garantizando un funcionamiento óptimo en condiciones de uso intensivo.

5.7 CONDICIONES DE SUMINISTRO Y AJUSTE DE PRECIOS

El Consorcio Cédula 4.0 RD se compromete a suministrar los periféricos detallados en esta sección en un período de treinta (30) días calendario después de la solicitud formal de la Junta Central Electoral (JCE).

Los precios de los equipos podrán ajustarse anualmente conforme a la inflación, asegurando que las condiciones económicas reflejen las variaciones del mercado.

Además, la JCE tendrá la facultad de decidir la compra o no de estos equipos, de acuerdo con sus requerimientos operativos y disponibilidad presupuestaria.

ÍTEM VI - ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO

6 PLAN DE MANTENIMIENTO PARA IMPRESORAS Y PERIFERICOS

SERVICIO TÉCNICO

- **Localidades:** Las localidades incluyen la Republica Dominicana, EEUU y España.

- **Infraestructura de Soporte:** La infraestructura de Soporte consta de al menos:

- **República Dominicana:**

- Técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Hasta 15 técnicos locales del C4RD disponibles de forma presencial
- Cuatro (4) Regionales existentes en la actualidad desde donde se habilitará el servicio de manera estratégica. Allí, en la localidad, C4RD dispondrá de su estructura de soporte actual incluyendo la inclusión de personal técnico propio del fabricante cuando fuese necesario como la infraestructura de recursos en la localidad, transporte, taller y/o almacenes de repuestos debidamente equipados con las herramientas de trabajo, etc

- **EEUU:**

- 4 técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Hasta 70 técnicos locales del C4RD disponibles de forma presencial
- Regional existente en la actualidad desde donde se habilitará el servicio de manera estratégica, siendo Nueva York el punto de atención focal. Allí C4RD dispondrá de su estructura de soporte actual incluyendo, personal técnico propio del fabricante como la infraestructura de recursos en la localidad, transporte, taller y/o almacén de repuestos debidamente equipados con las herramientas de trabajo, etc.

- **España:**

- 4 técnicos propios del fabricante de impresoras que operaran el servicio de mantenimiento disponibles de forma remota y/o presencial; conformado por un supervisor técnico y tres ingenieros de servicio.
- Se contara con al menos 1 técnico local del C4RD disponibles de forma presencial
- Una (1) Region actualmente existente desde donde se habilitará el servicio de manera estratégica, incluyendo Madrid. Allí C4RD dispondrá de su estructura de soporte actual incluyendo, personal técnico propio del fabricante como la infraestructura de recursos en la localidad, transporte, taller y/o almacén de repuestos debidamente equipados con las herramientas de trabajo, etc

- **Tiempos de Respuesta:**

- Ocho (8) horas de tiempo de respuesta en localidades lejanas; desplazamientos mayores a 2 hrs.
- Cuatro (4) horas en localidades cercanas a los centros de servicios de C4RD; desplazamientos menores a 2 horas.

- **Contingencia:**

- Cada localidad regional de servicios de C4RD contara con al menos un equipo funcional disponible y referido de este lote para sustitución inmediato además de Trick de partes y piezas para reparación.
- Todos los recursos técnicos tienen disponibles medios de comunicación con alcance mundial disponibles, entre sí, con fuentes de información centralizada para consulta técnica; algunas de estas comprenden WhatsApp, llamadas locales y/o llamadas internacionales, etc
- Las fuentes de soporte de asistencia técnica del fabricante, a nivel mundial, están disponibles con respecto al horario laborable del hemisferio occidental, cubriendo entre 8 - 19 hrs diarias entre Domingo y viernes, aprovechando el centro de soporte de Dubái en el medio oriente y el de Bogotá en América Latina.
- 8-9 hrs en ventaja con el horario de apertura de labores con NY, Santo Domingo durante el año.
- 1-2 hrs con el horario de cierre de labores con NY, Santo Domingo durante el año.

- **Registro del Incidentes:**

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.
- Incluir la siguiente información:
- Nombre de la entidad reportante (JCE.RD, JCE.EEUU o JCE.UE).
- Fecha y hora del incidente.
- Identificar como Impresora o Periférico
- Serie del equipo
- Descripción detallada del problema.
- Componentes afectados
- Nivel de urgencia del incidente

- **Protocolos de Escalamiento y Gestión de Incidentes:**

- Definición de niveles de escalamiento con tiempos de respuesta específicos según la criticidad del incidente.
- Disponibilidad de un equipo de soporte de segundo y tercer nivel para atender problemas complejos de hardware y software.

6.1 PLAN DE MANTENIMIENTO PARA PKI

6.1.1 INTRODUCCIÓN

Este documento establece los lineamientos para garantizar la continuidad y estabilidad de la infraestructura PKI-CA suministrada por el consorcio C4RD a la Junta Central Electoral (JCE). La infraestructura PKI es un pilar fundamental para la seguridad digital y la confianza en las transacciones electrónicas, permitiendo la autenticación, el cifrado y la firma digital de documentos.

Garantizar un plan de soporte técnico robusto es esencial para mantener la disponibilidad y la integridad de la plataforma. La implementación de GET Trust, junto con las mejores prácticas de mantenimiento y monitoreo, permite el cumplimiento de normativas internacionales y la continuidad operativa del sistema.

6.1.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA DEL PKI – CA

La JCE depende de la gestión técnica de C4RD para administrar la infraestructura PKI-CA, que abarca la generación y revocación de certificados, el monitoreo de riesgos y el cumplimiento de estándares globales. A través de este esquema, a la JCE se le garantiza la seguridad de sus procesos digitales, mientras que C4RD implementa además medidas para prevenir fallos y responder ante cualquier incidente.

Este programa de soporte y mantenimiento cubre los siguientes aspectos clave:

- **Infraestructura PKI-CA:** responsable de la gestión de claves, la generación y revocación de certificados, así como la administración de la Autoridad de Certificación (CA).
- **Monitoreo y gestión de incidentes:** Se implementan herramientas de auditoría y supervisión que permiten a la JCE detectar y reportar riesgos en tiempo real, mientras que C4RD ejecuta las acciones correctivas necesarias.
- **Seguridad y cumplimiento:** C4RD garantiza la adhesión a los estándares internacionales, como EAL4+, eIDAS y FIPS 140-2, asegurando la protección de la información manejada por la JCE.

El mantenimiento efectivo de la infraestructura PKI-CA es clave para preservar la autenticidad de los procesos digitales. Su robustez depende de una gestión eficiente del ciclo de vida y de la respuesta oportuna ante cualquier incidencia.

6.1.3 MODELOS DE SERVICIO Y SLA

Para garantizar tiempos de respuesta óptimos, la JCE contara con un esquema de soporte técnico proporcionado por C4RD en tres niveles: desde la resolución de consultas básicas hasta la intervención especializada. Los acuerdos de nivel de servicio (SLA) permitirán a la JCE operar sin interrupciones, asegurando que los incidentes sean atendidos según su nivel de criticidad.

Para garantizar la eficiencia y disponibilidad del sistema, C4RD ha definido tres niveles de soporte:

- **Nivel 1 (L1):** Atención inicial y resolución de consultas básicas.

- **Nivel 2 (L2):** Gestión de incidencias técnicas y soporte especializado.
- **Nivel 3 (L3):** Intervención de ingeniería avanzada y escalamiento a proveedores.

6.1.4 SLA Y TIEMPOS DE RESPUESTA

Los tiempos de atención se han definido para minimizar el impacto de las incidencias, en horario 7:00AM a 6:00PM de lunes a viernes y los sábados de 8:00 a 1:00 PM

- **Incidentes críticos (P1):** Respuesta en menos de 2 horas.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- **Incidentes mayores (P2):** Respuesta en menos de 6 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
  -
- **Incidentes mayores (P3):** Respuesta en menos de 8 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
  -
- **Incidentes menores (P4):** Respuesta en menos de 1 día.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

Estos niveles de servicio garantizan la operatividad de la infraestructura y evitan interrupciones en la emisión y validación de certificados digitales.

6.1.5 PROCEDIMIENTO PARA LA APERTURA DE INCIDENTES POR PARTE DE LA JCE

El protocolo de soporte a la JCE requiere el seguir un protocolo estructurado para reportar incidentes a C4RD, incluyendo la clasificación por nivel de urgencia y el envío de información detallada para un diagnóstico preciso. C4RD, a su vez, evalúa cada caso y asigna recursos especializados para su resolución, garantizando una comunicación fluida con la JCE hasta la solución del problema.

Este modelo de soporte robusto gestionado por C4RD, con más de 15 años de experiencia en procesos críticos de negocios del sector privado y público probado ante exigencias de trafico de alta demanda del sector financiero nacional y de servicios públicos opera 24/7 para atenderá cualquier incidencia que afecte la infraestructura PKI-CA.

Este capítulo describe la metodología de categorización y escalamiento de problemas, asegurando que la JCE cuente con un servicio confiable y eficiente en la resolución de inconvenientes técnicos. La metodología implementada por C4RD se basa en un enfoque estructurado de gestión de incidentes, que incluye la identificación, registro, clasificación por niveles de criticidad (P1 a P4), diagnóstico inicial, asignación de recursos especializados, resolución y documentación del incidente.

Además, están establecidos procedimientos de escalamiento para garantizar que, en caso de problemas complejos, los niveles de soporte superiores intervengan de manera oportuna, minimizando el impacto en las operaciones de la JCE.

6.2 CUADRO DE ESCLAMEINTO INCLUYENDO

Matriz de Escalamiento Mesa de Servicios - TIC							
Niveles	**Soporte**	**Tiempo de Respuesta**	**Puesto**	**Nombres**	**Contacto**	**Móvil**	**Correo**
1	L1	De 1 a 30 Minutos	Técnico Especialista 1 - CSI	Mesa de Servicio CSI	809-567-0022 Ext. 282	Técnico de Turno	ServiciosTIC@grupocsi.com.do
2		30 Minutos a 60 Minutos	Técnico Especialista 2 - CSI	Mesa de Servicio CSI	809-567-0022 Ext. 262	(849) 886 2012	jli.infante@grupcsi.com.do
3		60 Minutos (1 Horas) a 120 Minutos (2 Horas)	Gerente de Servicios TIC - CSI	Federico Norberto	809-567-0022 Ext. 281	(809) 443 1502	f.norberto@grupocsi.com.do
4		2 a 3 Horas	VP Comercial - CSI	Ruben Cordero	809-567-0022 Ext. 239	(809) 603 8696	r.cordero@grupocsi.com.do
5		3 a 4 Horas	Presidente - CSI	Manuel Infante	809-567-0022 Ext.222	(809) 430-7242	jm.infante@grupocsi.com.do
6	L2	4 Horas o Mas	Mesa de Servicios GetGroup				soportelatam@getlatamprojects.com

Cuando la JCE identifique un problema en la infraestructura PKI-CA, deberá seguir el siguiente procedimiento para reportarlo a C4RD:

1. Registro del Incidente

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.
- Incluir la siguiente información:

  - Nombre de la entidad reportante (JCE).
  - Fecha y hora del incidente.
  - Descripción detallada del problema.
  - Componentes afectados dentro de la infraestructura PKI-CA.
  - Capturas de pantalla o logs relevantes.
  - Nivel de urgencia del incidente.

2. Clasificación del Incidente

- **Máxima (P1):** El servicio de PKI-CA está completamente inoperativo.
- **Alta (P2):** Falla parcial que afecta la operación de la JCE.
- **Media (P3):** Problemas que afectan el rendimiento sin impacto inmediato.
- **Baja (P4):** Incidentes menores atendidos en la siguiente ventana de mantenimiento.

3. Evaluación y Diagnóstico Inicial

- C4RD realizará un análisis preliminar y solicitará información adicional si es necesario.

4. Resolución y Seguimiento

- C4RD asignará un técnico según la criticidad del incidente.
- Se mantendrá una comunicación constante con la JCE hasta la resolución.
- Se emitirá un informe con causas y medidas correctivas.

6.3 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

La continuidad operativa de la infraestructura PKI-CA de la JCE está respaldada por un plan de mantenimiento estructurado por C4RD. Las tareas preventivas incluyen auditorías de seguridad, actualizaciones de software y revisión de certificados, mientras que el mantenimiento correctivo aborda fallos imprevistos para minimizar el impacto en los servicios digitales de la JCE.

El mantenimiento preventivo, ejecutado por C4RD, incluye:

- Renovación y revocación programada de certificados.
- Verificación de integridad del HSM.
- Simulacros de incidentes y evaluaciones de rendimiento.
- Revisión de certificados y actualización de software.
- Pruebas de penetración y seguridad.

El mantenimiento correctivo responde a fallas imprevistas mediante:

- Atención inmediata de fallos críticos.
- Sustitución de hardware según acuerdos con proveedores.
- Monitoreo de la integridad de certificados emitidos y revocados.

6.4 SEGURIDAD Y CUMPLIMIENTO

Con la JCE, C4RD trabajaremos en conjunto para mantener la infraestructura PKI-CA alineada con estándares internacionales de seguridad, protegiendo la integridad de los datos y la identidad digital. C4RD implementara auditorías periódicas y monitoreo constante para detectar posibles vulnerabilidades, asegurando que la misma cumpla con los requisitos regulatorios en la gestión de certificados digitales.

Para garantizar la seguridad de la infraestructura PKI-CA, C4RD implementa:

- Auditorías internas propias y externas via terceros.
- Monitoreo continuo para prevenir accesos no autorizados.
- Políticas de control de acceso basado en roles.
- Procedimientos de respuesta a incidentes de seguridad.

6.5 KPIS Y MÉTRICAS DE RENDIMIENTO

Para evaluar la efectividad del soporte técnico, la JCE y C4RD dejaran definidos indicadores claves de rendimiento (KPIs) como la disponibilidad del sistema, el tiempo de respuesta ante incidentes y la satisfacción del cliente. El monitoreo constante de estos parámetros permite optimizar los procesos y garantizar la fiabilidad de la infraestructura PKI-CA.

Se emitirán informes mensuales de rendimiento del mes anterior y se ejecutarán conferencias recurrentes de análisis de estos.

Para evaluar la efectividad del soporte, se establecen los siguientes indicadores:

- **Disponibilidad del sistema:** >99.9%.
- **Cumplimiento del SLA:** >95% de los incidentes resueltos dentro del tiempo.
- **Tiempo promedio de resolución:** Optimización de respuestas según la criticidad.
- **Satisfacción del cliente:** Evaluaciones continuas para mejora del servicio.

Este programa garantizara la estabilidad, seguridad y disponibilidad de la infraestructura PKI-CA, reforzando la confianza de la ciudadanía en los servicios de la JCE

6.6 PLAN DE MANTENIMIENTO PARA TARJETA DIGITAL

6.6.1 INTRODUCCIÓN

El presente documento define el **Programa de Soporte y Mantenimiento** para la plataforma de Cédula de Identidad Digital basada en GET Mobile ID, instalada e implementada por GET Group para la JCE. Dado que esta plataforma es crítica para la gestión de identidad nacional, se establece un esquema de soporte robusto y alineado con las mejores prácticas de la industria, garantizando alta disponibilidad (99.95%), seguridad avanzada y continuidad operativa.

Este programa contempla modelos de servicio y SLA, mantenimiento preventivo y correctivo, cumplimiento con regulaciones de seguridad, y métricas de rendimiento que permitan monitorear y optimizar el funcionamiento de la plataforma.

6.6.2 ALCANCE DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA PLATAFORMA

El soporte y mantenimiento de la plataforma GET Mobile ID abarca las siguientes áreas clave:

- **Infraestructura Tecnológica**: Servidores, almacenamiento, red y elementos de seguridad como NG Firewalls y WAF.
- **Software y Aplicaciones**: Mantenimiento de GET Mobile Administrator, GET Mobile ID y GET Mobile Verify.
- **Base de Datos y Firmado Digital**: Gestión del ciclo de vida de los certificados digitales, claves de firma y bases de datos vinculadas al sistema de identidad digital.
- **Monitoreo y Respuesta a Incidentes**: Supervisión proactiva de los servicios para garantizar alta disponibilidad.
- **Gestiones con la Junta Central Electoral (JCE)**: Coordinación para integraciones, actualizaciones y cambios en los procedimientos de identidad digital.

El servicio está diseñado para operar en un modelo **24/7** con distintos niveles de soporte técnico, asegurando la resolución eficiente de incidentes y la actualización continua de la plataforma.

6.6.3 MODELOS DE SERVICIO Y SLA

El servicio de soporte se estructura en distintos niveles, con acuerdos de nivel de servicio (SLA) bien definidos para cada categoría de incidencia en horario 7:00AM a 6:00PM de lunes a viernes y los sábados de 8:00 AM a 1:00 PM:

- **Nivel 1 (Soporte Básico y Atención al Cliente)**: Resolución de consultas, asistencia básica y gestión de usuarios.

- **Nivel 2 (Soporte Técnico Especializado)**: Diagnóstico avanzado de problemas, configuraciones de software y ajustes de red.
- **Nivel 3 (Soporte de Infraestructura y Seguridad)**: Resolución de incidentes críticos, recuperación ante desastres y gestión avanzada de seguridad.

6.6.4 ACUERDOS DE NIVEL DE SERVICIO (SLA):

- **4. Acuerdos de Nivel de Servicio (SLA):**
- **Incidentes críticos (P1):** Respuesta en menos de 2 horas.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- **Incidentes mayores (P2):** Respuesta en menos de 6 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.
- **Incidentes mayores (P3):** Respuesta en menos de 8 hora.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

  Incidentes menores (P4): Respuesta en menos de 1 día.
  - El procedimiento de registro de incidentes incluirá:
  - ▪ Recepción y Registro del incidente.
  - ▪ Análisis y clasificación del incidente.
  - ▪ Investigación y Diagnostico.
  - ▪ Resolución del incidente.
  - ▪ Verificación y cierre.

Cuando la JCE identifique un problema en el servicio de la infraestructura Cedula Digital, deberá seguir el siguiente procedimiento para reportarlo a C4RD:

REGISTRO DEL INCIDENTE

- Contactar a C4RD a través del correo PKICA.C4RD@grupocsi.com.do o mediante el sistema de gestión de incidentes.

- Incluir la siguiente información:
  - Nombre de la entidad reportante (JCE).
  - Fecha y hora del incidente.
  - Descripción detallada del problema.
  - Componentes y/o servicio afectado dentro de la infraestructura Cedula Digital.
  - Capturas de pantalla o logs relevantes.
  - Nivel de urgencia del incidente.

6.6.5 CLASIFICACIÓN DEL INCIDENTE

- **Máxima (P1):** El servicio de Cedula Digital está completamente inoperativo.
- **Alta (P2):** Falla parcial que afecta los servicios o la operación de la JCE.
- **Media (P3):** Problemas que afectan el rendimiento sin impacto inmediato.
- **Baja (P4):** Incidentes menores atendidos en la siguiente ventana de mantenimiento.

5. **Evaluación y Diagnóstico Inicial**
   - C4RD realizará un análisis preliminar y solicitará información adicional si es necesario.
6. **Resolución y Seguimiento**

- C4RD asignará un técnico según la criticidad del incidente.
- Se mantendrá una comunicación constante con la JCE hasta la resolución.
- Se emitirá un informe con causas y medidas correctivas.

6.7 MANTENIMIENTO PREVENTIVO Y CORRECTIVO

Para garantizar el funcionamiento óptimo de la plataforma, se establecen los siguientes tipos de mantenimiento:

6.7.1 ACTIVIDADES PERIÓDICAS

- **Revisión de certificados**: Verificar la validez y vigencia de los certificados emitidos, incluyendo los certificados de la Autoridad de Certificación (CA) raíz y subordinada.
- **Actualización de software y firmware**: Mantener actualizados los sistemas y aplicaciones que utilizan la solución de emisión de credenciales digitales.
- **Revisión de políticas de seguridad**: Verificar que las políticas de seguridad estén actualizadas y sean efectivas para proteger la solución de emisión de credenciales digitales.

- **Realización de copias de seguridad**: Realizar copias de seguridad regulares de la solución de emisión de credenciales digitales, incluyendo los certificados, las claves privadas y los registros de transacciones.
- **Pruebas de penetración y vulnerabilidades**: Realizar pruebas de penetración y vulnerabilidades periódicas para identificar y corregir cualquier debilidad en la solución de emisión de credenciales digitales.

6.7.2 ACTIVIDADES DE MANTENIMIENTO PREVENTIVO

- **Revisión de los registros de transacciones**: Verificar los registros de transacciones para detectar cualquier actividad sospechosa o irregular.
- **Monitoreo de la integridad de los certificados**: Verificar la integridad de los certificados emitidos y revocados.
- **Actualización de la lista de revocación de certificados (CRL)**: Actualizar la lista de revocación de certificados (CRL) para reflejar los certificados revocados.
- **Revisión de la configuración de la solución de emisión de credenciales digitales**: Verificar la configuración de la solución de emisión de credenciales digitales para asegurarse de que esté configurada correctamente y sea segura.

6.7.3 ACTIVIDADES DE RESPUESTA A INCIDENTES

Procedimientos de respuesta a incidentes: Están establecidos procedimientos de respuesta a incidentes para manejar cualquier incidente de seguridad que afecte la solución de emisión de credenciales digitales.

- **Notificación de incidentes**: Notificar a las partes interesadas relevantes en caso de un incidente de seguridad.
- **Análisis de incidentes**: Realizar un análisis detallado de cualquier incidente de seguridad para identificar la causa raíz y tomar medidas correctivas.
- **Recuperación de la solución de emisión de credenciales digitales**: Recuperar la solución de emisión de credenciales digitales después de un incidente de seguridad, incluyendo la restauración de los certificados y las claves privadas.

6.7.4 MANTENIMIENTO CORRECTIVO

- **Solución de Errores Críticos:** Reparación inmediata ante caídas del sistema.
- **Reemplazo de Componentes:** Sustitución de módulos afectados por fallos.
- **Corrección de Brechas de Seguridad:** Ajustes urgentes en respuesta a ataques o vulnerabilidades detectadas.

6.8 SEGURIDAD Y CUMPLIMIENTO

Dado que GET Mobile ID maneja información altamente sensible, el programa de mantenimiento prioriza la seguridad mediante:

- **Cifrado y Protección de Datos**: Uso de criptografía RSA y curvas elípticas.
- **Autenticación Multifactor (MFA)**: Para el acceso administrativo y operación segura se implementarán mecanismos de autenticación y autorización seguros para garantizar que solo los usuarios autorizados puedan acceder a la solución de emisión de credenciales digitales.
- **Firewall de Nueva Generación (NGFW) y WAF**: Control avanzado contra ataques cibernéticos.
- **Cumplimiento Normativo**: Asegurar que la solución de emisión de credenciales digitales cumpla con los requisitos de seguridad establecidos en la norma ISO 18013-5, ISO 27001 y regulaciones nacionales de protección de datos.
- **Monitoreo de Amenazas**: Detección temprana de intrusiones y análisis de comportamiento.
- **Gestión de claves:** Implementación de una gestión de claves segura y eficiente para proteger las claves privadas y los certificados.
- **Registros de auditoría:** Mantener registros de auditoría detallados y precisos para permitir la trazabilidad y la responsabilidad de las acciones realizadas en la solución de emisión de credenciales digitales.

6.9 KPIS Y MÉTRICAS DE RENDIMIENTO

Para evaluar la eficiencia del soporte y mantenimiento, se definen indicadores clave:

- **Disponibilidad del Sistema**: Tiempo efectivo de operación (meta: 99.95%).
- **Tiempo Medio de Resolución (MTTR)**: Promedio de tiempo para resolver incidentes.
- **Tiempo Medio entre Fallas (MTBF)**: Periodo promedio entre fallas críticas.
- **Tasa de Resolución en Primera Llamada (FCR): %** de incidencias resueltas sin escalamiento.
- **Cumplimiento de SLA: % de incidentes resueltos dentro de los tiempos acordados.**
- **Incidentes de Seguridad:** Número de alertas de seguridad atendidas y resueltas.
- **Uso de Recursos:** Análisis de carga en servidores y almacenamiento.

Estos KPIs se revisarán periódicamente, cada trimestre, para identificar oportunidades de mejora y garantizar que la plataforma opere de manera segura y eficiente.

6.10 INVENTARIO

Para garantizar la continuidad operativa y evitar interrupciones en la personalización de documentos de identidad, el Consorcio Identidad 4.0 RD mantendrá un stock de inventario equivalente a un mínimo del 3% Este inventario permitirá una respuesta inmediata en caso de fallas técnicas o necesidades de reposición, asegurando el cumplimiento ininterrumpido del servicio.

ÍTEM VII - CAPACITACIÓN

7. PLAN DE CAPACITACIÓN PARA IMPRESORAS

7.1 ENTRENAMIENTOS

El consorcio Cedula 4.0 RD ha diseñado un plan de entrenamiento sin costo que inicia durante la fase de implementación con un entrenamiento general de todas las funciones de la solución de impresión y acompañamiento directo del fabricante durante el proceso. El entrenamiento será divido en 2 fases un entrenamiento básico de operación para el personal que replicará esta capacitación en los centros de atención que incluye:

- Guía básica de operación de la solución
- mantenimiento preventivo
- validación de calidad de impresión
- resolución de incidencias básicas

Adicional a esto se entregará una guía de referencia rápida para uso básico de la solución y un video interactivo con material que apoya y guía al usuario en como operar la solución esta guía se recomienda que sea realizado en conjunto con la JCE con la solución final aprobada.

De igual forma se realizará un *entrenamiento* más especializado para el *personal técnico de la JCE a* fin de asegurar su conocimiento sobre las *características* técnicas de los equipos, *configuraciones*, y demás aspectos técnicos y operativos de la solución instalada. Dicho entrenamiento será realizado en las mismas instalaciones de la JCE por el personal directo del fabricante del hardware.

7.2 TÓPICOS DE ENTRENAMIENTO:

PREPARACIÓN DEL EQUIPO Y CONFIGURACIÓN INICIAL

Instalación del software: Asegúrate de tener instalado el software adecuado para el modelo de impresora láser. Verifica que los controladores sean los más recientes.

Calibración de la impresora: calibración inicial para asegurarse de que el láser y los componentes mecánicos estén correctamente alineados.

Configuración de la calidad de impresión: Ajusta los parámetros de resolución, velocidad de impresión, y otros aspectos técnicos a las necesidades del proyecto.

PREPARACIÓN DE LAS TARJETAS DE POLICARBONATO

Selección de tarjetas: Asegúrate de que las tarjetas sean del tamaño adecuado y estén libres de imperfecciones. Las tarjetas de policarbonato deben estar diseñadas específicamente para ser impresas con láser.

Limpieza: Es importante limpiar las tarjetas de cualquier polvo o suciedad para evitar manchas o fallas de impresión.

7.4 ENTRENAMIENTO DE LA IMPRESORA (PRUEBAS DE IMPRESIÓN)

Prueba inicial de impresión: Imprime una tarjeta de prueba para evaluar la calidad de la impresión. Revisa la nitidez de las imágenes y la correcta alineación del diseño.

Ajustes: Si los resultados no son satisfactorios, ajusta la configuración si las condiciones del área de impresión esta fuera del requerimiento mínimo de operación.

7.5 ALIMENTACIÓN DE PLATICOS DE POLICARBONATO

Las tarjetas de policarbonato CIE / CI

7.6 VERIFICACIÓN DE LA CALIDAD DE LA IMPRESIÓN

Inspección visual: Verifica la precisión del color, la nitidez del texto y los gráficos, y la consistencia de la impresión.

7.4 MANTENIMIENTO REGULAR

Limpieza del equipo: Mantén el equipo limpio, especialmente los mecanismos láser y de alimentación de tarjetas, para evitar fallos durante la impresión.

Rutina de mantenimiento preventivo para operadores

Rutina de mantenimiento personal técnico JCE.

7.4 RESOLUCIÓN DE INCIDENCIAS

Se realizará un entrenamiento practico con el personal técnico que incluye un manual de servicio para resolución de problemas para fines de consulta.

7.10 CANALES DE ATENCIÓN.

- **Página web para registro de incidencias:** https://www.grupocsi.com.do/soporte-tecnico-hardware/
- **Centro de atención para recepción de reportes telefónicos con horario:** lunes a jueves de 7:00 am a 6:00 pm viernes de 8:00 am a 5:00 pm sábado de 8:00 am a 1:00 pm.

7.11PLAN DE CAPACITACION PARA PKI

7.11.1 CONTENIDO

Los cursos que se describen a continuación ofrecidos y organizados por nuestros formadores para la solución de PKI, GET Trust.

- PKI Basics: formación sobre conceptos básicos de PKI e introducción
- CMS: formación sobre el Sistema de Gestión de Credenciales (CMS): En conjunto con ID PKI
- ID PKI: formación sobre software de ID PKI, incluyendo ID CA
- ID CA: formación sobre software de ID CA
- Instalación de ID PKI: formación sobre instalación de software de ID PKI, incluyendo instalación de ID CA
- Instalación de ID CA: formación sobre instalación de software de ID CA
- ID RA para Operadores: Introducción a PKI + uso de ID RA y EE para operadores. Gestión del ciclo de vida de los certificados
- BAC: formación sobre el módulo BAC
- Firmado electrónico: formación sobre el software de firma electrónica IDnomic Sign

Además de estas formaciones estándar, se puede establecer un programa específico con el cliente para cubrir necesidades específicas, como una formación en profundidad para un grupo especifico de usuarios.

7.11.2 METODOLOGÍA

Nuestros formadores son profesionales de la formación, especializados en nuestro campo de especialización. Ponemos énfasis en los intercambios interactivos y el desarrollo de habilidades a través de la implementación operativa de nuestras soluciones. Como tal, cada sesión incluye conferencias, sesiones de preguntas y respuestas y trabajos prácticos para poner en práctica los conceptos presentados.

7.11.3 DESCRIPCIÓN

Referencia	PKI Basics
Objetivo	• Descubra los certificados y su ciclo de vida • Comprenda las tecnologías y las normas criptográficas • Comprenda la organización de PKI
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Este curso de capacitación proporciona los conocimientos mínimos necesarios para comprender completamente los demás módulos de capacitación impartidos.
Prerequisitos	Formación universitaria básica o ingeniero informático o equivalente mediante experiencia.
Plan	- Fundamentos de criptografía - Implementación de la criptografía

	- Introducción a los conceptos de PKI - PKI y organización - La estructura de la PKI - Jerarquía de autoridad - Autoridad de certificación - Marco legal y regulatorio
Duración	4 horas

Referencia	Sistema de Gestión de Credenciales (CMS)
Objetivo	- Comprender los certificados y las tarjetas inteligentes. - Cómo utilizar tarjetas inteligentes en una infraestructura de gestión de certificados. - Implementar el CMS y sus módulos - Configurar y administrar el CMS - Comprender los componentes clave para utilizar el CMS con todos los demás componentes de PKI.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - - Curso TRN.BASICS
Plan	**Día 1:** - Introducción al CMS y sus componentes - Instalación e inicialización del software CMS - 1ª conexión en modo "Bootstrap" - Inicialización de la configuración - Inicialización de la seguridad (firma de certificados internos de módulos) - Configuración - Protección de datos, claves de almacenamiento (creación e implementación) - Conexión a directorios, creación de fuentes de datos, definición de perfiles de autenticación, aplicaciones (autenticación, firma de correo electrónico y cifrado) - Medios: políticas de PIN, personalización gráfica, fabricantes, gestión de secretos, creación de perfiles para tokens de entrenamiento - Tarjetas inteligentes: arquitectura y concepto, gestión de secretos - Creación de perfiles para tokens de entrenamiento - Presentación del cliente CMS - Generación de archivos XPI - Instalación del cliente CMS - Configuración del navegador para tokens

	- Creación de un perfil de gestión de tarjetas "SelfEnroll" para administradores, gestión de números de serie de confianza - Definición y uso de procesos / flujos de trabajo: - Solicitud de certificado de administrador designado - Control de acceso (zonas, grupos, gestión de derechos de zona y módulo) - Inicio de sesión con certificado de administrador designado - Preparar un Configuración de usuario final - Creación de perfil de Badge Office - Fuente de datos interna, creación y aprovisionamiento **Día 2:** - Creación de un perfil de gestión de tarjetas - Emisión por lotes, envío de correo - Creación de perfil, adición de derechos, creación de tokens, revocación, desbloqueo, seguimiento, desbloqueo de medios sin conexión... - Copia de seguridad/restauración - Administración funcional de CMS, gestión de registros
Duración	14 horas (2 días)

Referencia	Instalación
Objetivo	- Instalar manualmente el software de ID CA. - Conocer los componentes que conforman el producto, las arquitecturas típicas a implementar y las diferentes etapas de una instalación. - Identificar los prerrequisitos para la instalación. - Poner en marcha la solución y acceder a las interfaces de administración.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución PKI (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Introducción a ID PKI y sus componentes técnicos - Arquitectura técnica de la solución - Requisitos previos - Instalación de ID CA - Ejercicios prácticos: - Verificar los requisitos previos - Instalar ID CA - Verificar la instalación correcta - Iniciar servicios y arrancar PKI - Analizar
Duración	7 horas

Referencia	HSM Proteccio Training
Objetivo	- Presentación, preparación e integración de Proteccio HSM en el contexto de un proyecto PKI - Introducción a una ceremonia de entrega de llaves
Audiencia	Cualquier persona involucrada en la implementación de una solución PKI, incluido un HSM de Proteccio (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes), especialmente futuros administradores de PKI o gerentes de soluciones PKI involucrados en la Ceremonia de entrega de claves.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Descripción general de Proteccio HSM, arquitectura de hardware y funciones; - Presentación de los diferentes roles y funciones disponibles para cada uno; - Instalación de equipos y creación de tarjetas maestras SO y maestras de auditoría; - Configuración de red y TLS; - Administración local de equipos; - Instalación de la herramienta de administración en una estación de trabajo Windows y en una estación de trabajo Linux - Actualizaciones de software; - Creación de decks de instalación Shamir; - Creación, configuración y personalización de HSM virtuales; - Gestión de objetos de HSM virtuales; - Gestión de HSM virtuales; - Migraciones de tarjetas inteligentes; - Implementación del modo de balanceo de carga; - Guía de resolución de problemas, mantenimiento de rutina de Proteccio HSM; - Preguntas varias. - Ceremonia de llave con Keyseed - Objetivos de un KC - Procedimiento de KC - Procedimientos y herramientas - • Cierre de un KC
Duración	7 horas

Referencia	BAC Training
Objetivo	- Entender el pasaporte electrónico - Conocer los procesos de solicitud de certificados y su ciclo de vida. - Cómo utilizar tecnologías y estándares criptográficos - Cómo implementar/operar la solución BAC

Audiencia	Cualquier persona involucrada en la implementación técnica de una solución PKI para pasaportes incluyendo el componente BAC (Gerentes de Seguridad, CISOs, Gerentes de Proyecto, Arquitectos, Administradores de Sistemas y Redes), y más particularmente futuros administradores de PKI o referentes de soluciones PKI.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	**Día 1:** - Introducción a la criptografía y PKI - Historia y evolución del pasaporte - Descripción del pasaporte electrónico - Presentación del producto BAC - Descripción general del producto CSCA - Configuración de CSCA - Ejercicios prácticos: - Creación de particiones - Creación de almacén de claves - Creación de CA - Gestión de CA de confianza - Creación y gestión de perfiles de certificados - Gestión de CRL - Renovación de CSCA - Día 2: - Configuración del producto DS - Ejercicios prácticos: - Creación de un área de clientes - Creación de administradores DS - Declaración de usuario de cliente DS - Gestión de claves - Creación de DS - Firma de certificados por DS - o Gestión de estadísticas
Duración	14 horas (2 días)

Referencia	Firmado Digital
Objetivo	- Entender las firmas electrónicas - Conocer el proceso de verificación de firmas mediante certificados - Conocer los diferentes tipos de firma electrónica - Cómo utilizar tecnologías y estándares criptográficos - • Implementar y operar la solución.
Audiencia	Cualquier persona involucrada en la implementación técnica de una solución PKI para pasaportes incluyendo el componente BAC (Gerentes de Seguridad, CISOs, Gerentes de Proyecto, Arquitectos, Administradores de Sistemas y Redes), y más

	particularmente futuros administradores de PKI o referentes de soluciones (integradores) PKI.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso TRN.BASICS
Plan	- Descripción general del producto - Configuración - Ejercicios prácticos: - Parte de configuración - Conexión de HSM - Creación de clave maestra - Conexión a PKI - Configuración de CA de confianza - Configuración de importación y exportación - Configuración de la sección de gestión - Creación de usuarios - Creación de políticas de firma - Creación de claves y perfiles de firma - Configuración de firmas - Creación de visuales - Configuración de preferencias de firma - Gestión de auditorías
Duración	7 horas

7.12 PLAN DE CAPACITACION PARA TARJETA DIGITAL

7.12.1 CONTENIDO

Los cursos que se describen a continuación ofrecidos y organizados por nuestros formadores para la solución de tarjeta digital, GET mID.

- ISO 18013-5 Basics: formación sobre conceptos básicos de ISO 18013-5
- Formación de emisión de credenciales digitales ISO 18013-5.
- Instalación y Configuración de GET Mobile Administrator.
- Aplicación Móvil GET Mobile ID.
- Aplicación Móvil GET Mobile Verifier.

7.12.2 METODOLOGÍA

Nuestros formadores son profesionales de la formación, especializados en nuestro campo de especialización. Ponemos énfasis en los intercambios interactivos y el desarrollo de habilidades a través de la implementación operativa de nuestras soluciones. Como tal, cada sesión incluye conferencias, sesiones de preguntas y respuestas y trabajos prácticos para poner en práctica los conceptos presentados.

7.12.3 DESCRIPCIÓN

Referencia	ISO 18013-5 Basics
Objetivo	Descubra los conceptos básicos de ISO 18013-5 y como su implementación impacta la innovación digital y su ecosistema.
Audiencia	- Cualquier persona involucrada o interesada en implementar una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes, áreas funcionales de emisión de documentos, Planificación e innovación). - Este curso de capacitación proporciona los conocimientos mínimos necesarios para comprender completamente los demás módulos de capacitación impartidos.
Prerequisitos	Formación universitaria básica o ingeniero informático o equivalente mediante experiencia.
Plan	- Resumen ISO 18013-5 - Alcance del ISO 18013-5 - Avances innovadores en el mundo - Relación de la PKI con el ISO 18013-5 - Usos e innovaciones - Marco legal y regulatorio
Duración	4 horas

Referencia	Formación de emisión de credenciales digitales ISO 18013-5.

Objetivo	- Comprender los sistemas y procedimientos involucrados en la emisión de una credencial digital. - Cumplimiento del estándar ISO 18013-5 en su implementación.
Audiencia	Cualquier persona involucrada o interesada en implementar una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de sistemas y redes). Especialmente los futuros administradores de GET Mobile ID o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Conocimientos generales de sistemas Android/iOS e infraestructura API o contenidos formativos. - Curso ISO 18013-5 Basics
Plan	- Flujo de emisión de credenciales. - Componentes e integraciones con sistemas CMS. - Integraciones e interacciones.
Duración	4 horas

Referencia	Instalación y Configuración de GET Mobile Administrator.
Objetivo	- Comprender el modelo de instalación, sus ubicaciones y demás configuraciones aplicadas al proyecto. - Operación de la solución. - Modelo de datos. - Integraciones disponibles.
Audiencia	Futuros administradores de CMS o aquellos responsables de la solución.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Curso ISO 18013-5 Basics - Formación de emisión de credenciales digitales ISO 18013-5.
Plan	- Arquitectura técnica de la solución - Requisitos previos - Instalación de los componentes en el proyecto. - Integraciones disponibles:
Duración	4 horas

Referencia	Aplicaciones Moviles GET
Objetivo	Aplicación de los conceptos adquiridos para el uso de las aplicaciones móviles finales.
Audiencia	Cualquier persona involucrada en la implementación de una solución ISO 18013-5 (gerentes de seguridad, CISO, gerentes de proyectos, arquitectos, administradores de

	sistemas y redes), especialmente futuros administradores de CMS o gerentes de soluciones CMS.
Prerequisitos	- Titulación universitaria o Ingeniero en Informática o equivalente según experiencia. - Conocimientos generales de sistemas Linux/Unix/Windows e infraestructura PKI o contenidos formativos. - Conocimientos generales de sistemas Android/iOS e infraestructura API o contenidos formativos. - Curso ISO 18013-5 Basics
Plan	- Descripción general de las aplicaciones móviles. - Despliegue de soluciones móviles. - Funcionalidades posibles. - Taller Practico.
Duración	3 horas

VIII- OTROS REQUERIMIENTOS

8. PLAN DE CONTINUIDAD DEL NEGOCIO (BCP)

8.1 OBJETIVO DEL PLAN

Este plan es presentado a la Junta Central Electoral con el propósito de garantizar la operación ininterrumpida en la producción y personalización de las Cédulas de Identidad y Electoral. Una de las empresas locales que conforman el Consorcio Identidad 4.0 RD, con 21 años de operación ininterrumpida, ha desarrollado estrategias efectivas para mitigar cualquier riesgo que pueda comprometer la entrega de estos documentos esenciales. Además, esta misma empresa ha sido proveedor de la cédula durante 10 años, lo que refuerza el compromiso y la capacidad de ejecución del presente proyecto, basándose en su experiencia comprobada en la producción e implementación del documento de identidad nacional

8.2 2. ALCANCE

Este plan cubre todas las actividades relacionadas con la producción, personalización, impresión, almacenamiento y distribución de las cédulas, incluyendo:

- Operaciones en los centros de producción.
- Infraestructura tecnológica y seguridad de datos.
- Suministro de materiales e insumos.
- Procesos de impresión y personalización de documentos.
- Coordinación entre seis sucursales estratégicamente ubicadas a nivel nacional, con la sede principal en el Distrito Nacional, que ha operado de manera ininterrumpida durante 21 años, asegurando estabilidad y continuidad en los procesos.

8.3 ANÁLISIS DE RIESGOS

Se han identificado los siguientes riesgos clave para la Junta Central Electoral (JCE):

- **Fallas técnicas:** Posibles disrupciones en los equipos de impresión y en el sistema de personalización de cédulas, lo que podría comprometer la emisión oportuna de los documentos de identidad.
- **Eventos de fuerza mayor:** Desastres naturales como terremotos, incendios o inundaciones que podrían afectar las instalaciones de la JCE y los centros de producción.
- **Ciberamenazas:** Riesgo de ataques cibernéticos que puedan comprometer la integridad de los registros ciudadanos, generar accesos no autorizados o alterar la base de datos de identidad.
- **Disrupciones en la cadena de suministro:** Retrasos en la provisión de materiales esenciales, como tarjetas en blanco, tintas de seguridad y componentes tecnológicos críticos para la emisión de cédula

8.4 ESTRATEGIAS DE CONTINUIDAD

Para garantizar la operatividad ininterrumpida de la JCE, se implementarán las siguientes estrategias:

8.4.1 INFRAESTRUCTURA DE RESPALDO:

- Implementación de servidores redundantes y almacenamiento en la nube para asegurar la integridad y disponibilidad de los datos.
- Establecimiento de centros de producción secundarios para asegurar la continuidad del servicio en caso de fallas críticas.
- Activación de seis sucursales estratégicamente ubicadas como puntos de contingencia operativa.
- Para garantizar la continuidad operativa, se dispone de una fábrica adicional plenamente equipada para asumir la producción en caso de contingencias, en cumplimiento con los requisitos del Pliego de Condiciones.

  Dirección: 187 Allée des Plagnes, 24300 Mareuil-en-Périgord, Francia

8.4.2 PROTOCOLOS DE RESPALDO DE INFORMACIÓN:

- Respaldo automatizado de bases de datos de identidad con encriptación avanzada para prevenir accesos no autorizados.
- Mecanismos de recuperación rápida de información ante posibles incidentes tecnológicos.

8.4.3 GESTIÓN DE PROVEEDORES ESTRATÉGICOS:

- Acuerdos con múltiples proveedores para diversificar la fuente de insumos críticos y evitar dependencias exclusivas.
- Implementación de un esquema logístico eficiente para la distribución de materiales a los centros de emisión de cédulas.

8.4.4 PLAN DE RECUPERACIÓN ANTE CRISIS:

- Realización de pruebas de recuperación de datos y operatividad para garantizar una respuesta eficiente en situaciones de emergencia.
- Establecimiento de protocolos claros de acción para asegurar la continuidad del servicio de emisión de cédulas.

8.5 PROCEDIMIENTOS DE RESPUESTA Y RECUPERACIÓN

Ante una eventual interrupción del servicio, se activará el siguiente protocolo de actuación:

1. **Activación del Plan:** Identificación inmediata del incidente y notificación a los equipos de respuesta.
2. **Gestión de Contingencias:** Evaluación del impacto en la emisión de documentos y aplicación de medidas correctivas en tiempo real.

3. **Restauración de Operaciones:** Puesta en marcha de procedimientos de recuperación para garantizar la continuidad del servicio.
4. **Tiempo Máximo de Recuperación (RTO):** Restauración completa de operaciones esenciales dentro de un lapso de 24 a 48 horas.
5. **Análisis Post-Incidente:** Evaluación integral del evento, documentación de aprendizajes y aplicación de mejoras en los procedimientos internos.

ROLES Y RESPONSABILIDADES

- **Comité de Seguridad y Continuidad Operativa** Responsable de la coordinación de respuestas estratégicas ante eventos disruptivos.
- **Departamento de Tecnología y Seguridad:** Encargado de la protección y recuperación de los sistemas de información y los datos de la JCE.
- **Unidad de Producción y Logística:** Responsable de garantizar la continuidad en la fabricación y distribución de cédulas en los distintos puntos de emisión.

7. PRUEBAS Y SIMULACROS

- Ejecución de simulaciones periódicas para evaluar la efectividad del plan y su capacidad de respuesta.
- Realización de ensayos de recuperación ante ciber amenazas y fallos técnicos en los sistemas de emisión.
- Auditorías anuales para fortalecer la resiliencia operativa y asegurar el cumplimiento de estándares tecnológicos y de seguridad.

8.6 REQUISITOS DE PRODUCCIÓN Y TIEMPOS DE ENTREGA

INTRODUCCIÓN

El Consorcio Identidad 4.0 RD se compromete a garantizar una producción eficiente, segura y confiable de las Cédulas de Identidad y Electoral (CIE) para la Junta Central Electoral (JCE). Con una infraestructura de producción avanzada, estrictos protocolos de calidad y una logística optimizada, se asegura el cumplimiento de los plazos estipulados en el Pliego de Condiciones, minimizando riesgos y asegurando la disponibilidad ininterrumpida de los documentos.

8.7 INFRAESTRUCTURA DE PRODUCCIÓN Y UBICACIÓN DE LAS FÁBRICAS

El Consorcio Identidad 4.0 RD cuenta con centros de fabricación de alta tecnología, ubicados estratégicamente para optimizar los tiempos de producción y entrega.

UBICACIÓN DE LAS FÁBRICAS Y OFICINAS EN EL EXTERIOR

- **Centro principal de producción:** Angoulême, Rue Louis Pergaud, 16000 Angoulême, Francia.
- **Fábrica de respaldo:** 187 Allée des Plagnes, 24300 Mareuil-en-Périgord, Francia
- **Oficinas regionales y centros de distribución:**
- **Estados Unidos** – Centro logístico para coordinación internacional.
- **Europa** – Oficina para soporte técnico y distribución.
- **República Dominicana –** Sede operativa y de implementación. José Andrés Aybar Castellanos No. 153. La Esperilla

RED DE SUCURSALES DE CSI

- CSI cuenta con seis oficinas operativas en República Dominicana y una en desarrollo en Azua.
- Infraestructura de asistencia técnica presente en el 100% de las provincias del país.

8.8 MEDIDAS DE SEGURIDAD EN LA PRODUCCIÓN

- Control de acceso biométrico y videovigilancia 24/7 en todas las fábricas y centros logísticos.
- Procedimientos de validación digital y trazabilidad para cada documento producido.
- Protocolos de encriptación avanzada en bases de datos para evitar accesos no autorizados
- El Consorcio cuenta con dos plantas de producción estratégicamente ubicadas para garantizar la fabricación segura y eficiente de los documentos de identidad:
- **Planta Principal:** SELP – Angoulême, Rue Louis Pergaud, 16000 Angoulême, Francia.
- **Planta de Respaldo:** SELP – Mareuil-en-Périgord, 187 Allée des Plagnes, 24300 Mareuil-en-Périgord, Francia.

  Ambas plantas cuentan con certificaciones internacionales en seguridad de impresión, control de acceso biométrico y videovigilancia 24/7, garantizando la integridad y trazabilidad del proceso de producción.

8.9 CRONOGRAMA GENERAL DE PRODUCCIÓN Y ENTREGA

Fase de Entrega	Cantidad de Cédulas	Tiempo Máximo
Entrega inicial (prueba)	2,000 tarjetas	Semana 16
Primera producción masiva	300,000 tarjetas	Semana 22
Segunda producción masiva	500,000 tarjetas	Semana 26
Tercera producción masiva	1,200,000 tarjetas	Semana 30
Producción continua	1,000,000 tarjetas cada 4 semanas	Desde Semana 34 hasta la 54

8.10 CRONOGRAMA DE TRABAJO

El cronograma de trabajo establece una planificación general y estratégica para la ejecución del proyecto, asegurando el cumplimiento de los plazos establecidos en el Pliego de Condiciones. Funciona como cronograma madre, ya que proporciona una visión estructurada de las principales fases de producción, implementación y entrega de las Cédulas de Identidad y Electoral (CIE).

Es importante destacar que el cronograma definitivo se elaborará en conjunto con la Junta Central Electoral (JCE), lo que permitirá realizar ajustes y optimizaciones según las necesidades específicas del cliente final. Este proceso garantizará una planificación alineada con las expectativas operativas y los objetivos de la JCE.

Nota: La versión completa del cronograma de trabajo se encuentra en la sección de Anexos, detallando cada actividad clave, sus tiempos de ejecución y los hitos de entrega.