SOBRE A

TABLA DE CONTENIDO

DOCUMENTOS DE ACREDITACIÓN

Capacidad y Solvencia

FL-01 Formulario de inscripción y Comprobante de pago

- ✓ Midas Dominicana S.A.
- ✓ Magallanes Media S.A.

FL-02 Formulario de presentación de oferta

✓ Consorcio IDSecure IDS

Acuerdo Consorcial

✓ Consorcio IDSecure IDS

Copia del Registro Nacional del Contribuyente (RNC).

✓ Midas Dominicana, S.A.

Registro Proveedores del Estado y/o Constancia de inscripción

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.
- ✓ Toppan Security, S.A.S.
  (Anteriormente HID Global CID, S.A.S.)

Copia de documento de identidad con poderes otorgados y Gerente Unico del Consorcio

✓ Consorcio IDSECURE IDS

Registro Mercantil.

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.
- ✓ Toppan Security, S.A.S.
  (Anteriormente HID Global CID, S.A.S.)

Documentos Corporativos y Certificados de Good Standing

- ✓ Magallanes Media, S.A.
- ✓ Toppan Security, S.A.S
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.

Cartas de Autorización Periféricos

- ✓ Midas Dominicana SA
  - Escáner
  - Lector de firma
  - Lector de huellas
  - Impresora punto de venta Térmica
  - Lector de huellas digital personal
  - Cámara fotográfica

Carta del fabricante o distribuidor con experiencias similares en materiales requeridos a empresas o instituciones de gobiernos.

- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.

Copia de los Estatutos Sociales

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Toppan Security, S.A.S
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.

Lista de la composición accionaria

✓ Midas Dominicana, S.A.

Estados Financieros de los últimos tres (3) períodos fiscales, Anexo 8, IR-2 o Equivalente

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Toppan Security, S.A.S
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.

Poder de Representación

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Toppan Security, S.A.S
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.

Certificación de pago al día en obligaciones fiscales

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Toppan Security, S.A.S
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L

Certificación de pago al día de la Seguridad Social

- ✓ Midas Dominicana, S.A.
- ✓ Magallanes Media, S.A.
- ✓ Toppan Security, S.A.S
- ✓ Litho Formas, S.A. de C.V.
- ✓ IXLA, S.R.L.

Declaración Jurada no antecedente FL-06

✓ Consorcio IDSECURE IDS

Cartas de referencias bancarias, solvencia y respaldo económico USD$2,000,000.00

- ✓ Midas Dominicana, S.A.
- ✓ Litho Formas, S.A. de C.V.

Declaración Jurada Indice de Solvencia del Consorcio y Análisis Financiero

✓ Consorcio IDSECURE IDS

Declaración Jurada Volumen de venta del Consorcio

✓ Consorcio IDSECURE IDS

Volúmenes de venta Empresa Local

✓ Midas Dominicana, S.A.

Muestras

- ✓ Consorcio IDSecure IDS
  - 10 muestras personalizadas
  - Manual de Muestras
  - Copia de la Norma ISO18745

DOCUMENTO TECNICOS

Resumen Ejecutivo

Presentación del Consorcio y las capacidades específicas de cada empresa

Para el desarrollo de este proyecto, se ha conformado el **Consorcio IDSecure IDS**, una alianza estratégica entre empresas líderes en identificación digital y gestión de documentos de alta seguridad. Cada miembro aporta su experiencia y capacidades específicas para ofrecer una solución integral y escalable.

Integrantes del Consorcio:

1. **MIDAS DOMINICANA S.A.** Somos un grupo empresarial dominicano con **+20 años** de experiencia conformado por empresas especializadas en **Servicios Electrónicos, Seguros, Remesas y Tecnología**, ofreciendo soluciones empresariales en **República Dominicana, Estados Unidos, Haití, Europa y Panamá.**

Desarrolla soluciones tecnológicas y comercialización de transacciones electrónicas con base en República Dominicana con cobertura nacional.

Proveemos tecnología y apoyo comercial a diversos comercios detallistas, empresas de servicio de primera necesidad, telefónicas y gobierno.

Con nuestras plataformas tecnológicas, equipos de operaciones comercial y servicio al cliente, garantizamos la eficiencia y efectividad de integración de nuestros aliados.

Gracias a los **+5,000** colaboradores, los aliados estratégicos, marcas y empresas internacionales que representa, **Midas Dominicana** desarrolla proyectos y servicios con los más altos estándares de calidad, generando valor a su gente, sus aliados y clientes.

Con servicios electrónicos para la recarga de minutos (tiempo aire) y pago de factura en mas de treintaicinco mil puntos de ventas a nivel nacio

nal en la republica dominicana, somo la red mas grande de productos y servicios electrónicos y plataformas del país.

En el sector de remesas gestionamos el cambio de divisas, pago y captación de remesas a destinos como USA, Europa, Haití, Chile, Colombia y Venezuela.

Aseguradora Nacional de riesgos generales con proyectos en el sector privado y público dentro de la república dominicana, baja la marca MIDAS SEGUROS.

Proyectos en alianza con Veridos, Thales y Endtrust, compañías con alta experiencia en temas de seguridad y documentos de identidad para gobiernos, ferrocarriles y defensa. Sistemas de control aéreo, marítimos, fronteras y peajes.

Tecnología y operación para programa de subsidios ADESS con mas de 5000 puntos afiliados.

Misión

Nuestra misión es forjar relaciones sólidas y estratégicas que aporten un valor competitivo excepcional. Nos enfocamos en la innovación, la calidad, la seguridad y la agilidad como pilares fundamentales para impulsar el desarrollo económico y social de nuestros socios, inversionistas, aliados y clientes.

Buscamos fortalecer nuestra conexión con cada uno de estos grupos, asegurándonos de que nuestras acciones y alianzas contribuyan de manera significativa a su crecimiento y éxito sostenible.

VISIÓN

Nuestra visión es convertirnos en un referente, tanto a nivel local como internacional, en el desarrollo de empresas exitosas. Aspiramos a ser reconocidos por nuestra capacidad para garantizar alta rentabilidad a través de la creación de soluciones, productos y servicios de excelencia.

Además, nos comprometemos a mantener los más altos estándares operativos en todos los mercados en los que participamos. Al hacerlo, buscamos no solo cumplir con las expectativas de nuestros clientes, sino también superarlas, estableciendo así un modelo de negocio sostenible y ejemplar que inspire a otras organizaciones en su camino hacia el éxito.

VALORES

- **Innovación**
  - Buscamos constantemente nuevas formas de mejorar y adaptarnos a las necesidades del mercado.
- **Calidad**
  - Nos esforzamos por ofrecer productos y servicios que superen las expectativas y los estándares más altos.
- **Compromiso**
  - Estamos dedicados a cumplir nuestras promesas y a trabajar por el éxito conjunto.
- **Responsabilidad**
  - Actuamos con ética y sostenibilidad, considerando el impacto de nuestras decisiones en la sociedad y el medio ambiente.
- **Servicio**
  - Valoramos cada interacción y nos comprometemos a brindar una atención excepcional a nuestros clientes y colaboradores

2. **LITHO FORMAS S.A. DE C.V.** es una empresa con más de 70 años de experiencia en la fabricación de documentos de alta seguridad, incluyendo pasaportes, tarjetas de identificación y otros documentos oficiales.

Fundada en México en el año 1954 como una compañía pionera de formas impresas, Litho Formas ha logrado un crecimiento consistente gracias a la visión y adaptación a los nuevos mercados.

Somos parte de THOMAS GREG & SONS (TG&S), grupo líder a nivel internacional en el desarrollo, implementación, comercialización, distribución y logística de soluciones integrales de seguridad que consolidan documentos físicos, digitales y servicios que garantizan la funcionalidad de dichos documentos. Con presencia en Colombia, Estados Unidos, México, Perú, Brasil, Panamá, Filipinas, India, Guinea, España y Reino Unido, es a través de TGS que Litho Formas se mantiene vigente con las tendencias y necesidades de diferentes continentes y regiones, para el desarrollo de soluciones de seguridad a la medida.

Litho Formas cuenta con experiencia internacional en proyectos de identidad en países como: México, Estados Unidos, Nicaragua, Colombia, Costa de Marfil, Camerún, entre otros.
Las diferentes certificaciones de Litho Formas la califican como empresa confiable para prestar servicios de seguridad en aplicaciones relacionadas a Identidad, Medios de Pago, Loterías y Sorteos, Procesos Electorales, entre otros. Habiendo obtenido la certificación ante Intergraf de ISO14298 a su nivel más complejo, Nivel Banca Central, Litho Formas está calificada no sólo para la fabricación de credenciales de alta seguridad en policarbonato, sino también para prestar los servicios de Personalización de los documentos oficiales (pasaportes, cédulas de identidad, licencias de conducir, matrículas consulares, etc.), lo que implica el manejo (recepción, resguardo, utilización y eliminación) de información oficial de los ciudadanos de distintos gobiernos.

Somos una empresa especializada en impresión de seguridad, equipada con el conocimiento, la experiencia y la maquinaria necesaria para producir documentos de alta seguridad, utilizamos diversos sustratos (como papel de seguridad, Teslin, PVC, PET, Policarbonato, ABS y compuestos), técnicas de impresión (como offset, serigrafía, flexografía, intaglio, estampados, impresión digital), tintas de seguridad, manejo experto en tecnologías de diseño (como microimpresión, tramas cifradas, errores deliberados, etc) e integración de tecnología en chips (de contacto, sin contacto RFID/NFC y de interfaz dual).

El adecuado manejo de la seguridad de información y conocimiento en tecnologías de Tarjetas Inteligentes permiten que Litho Formas desarrolle soluciones a la medida para las necesidades específicas de sus clientes.

Con sus más de 900 empleados en México, Litho Formas complementa su oferta de documentos valorados con servicios de consultoría, enrolamiento, personalización centralizada y/o descentralizada, trazabilidad, inclusión de códigos QR propietarios, validación biométrica, entre otros.

Proveedor de tecnología de impresión y personalización de tarjetas en policarbonato con altos estándares de calidad.

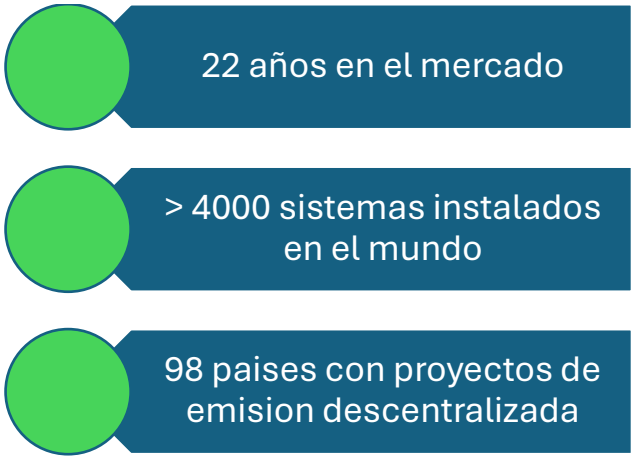
Experiencia en la provisión de documentos de identidad en varios países de América Latina.

---

3. **IXLA S.R.L.** es una empresa italiana, fundada en 2003 y emplea aproximadamente a 45 personas. Cuenta con una certificación ISO 9001-2015. La sede central está en el norte de Italia, en dos sitios industriales, y cuenta con operaciones locales para ventas y soporte técnico en Singapur, South Carolina (EE. UU.) y Buenos Aires (Argentina). El modelo de negocio de IXLA se basa en una dedicación total y enfoque en la entrega de productos de primera clase, colaborando con Integradores de Sistemas para llevarlos al mercado. Desde Noviembre 2024 es parte de HID, con sede en Austin, Texas; HID cuenta con más de 4.500 empleados en todo el mundo y opera oficinas internacionales que brindan soporte a más de 100 países. HID es una marca del Grupo ASSA ABLOY, líder mundial en soluciones de acceso. El Grupo opera en todo el mundo con 61.000 empleados y ventas de 141.000 millones de coronas suecas. El Grupo ocupa una posición de liderazgo en áreas como la apertura eficiente de puertas, las identidades de confianza y la automatización de entradas.

QUIEN SOMOS

IXLA S.R.L., es un fabricante de clase mundial de sistemas de personalización láser y de inyección de tinta para el sector público y financiero, dedicados a la personalización segura de credenciales gubernamentales y comerciales para tarjetas y pasaportes.



MISIÓN DE LA EMPRESA

- Proporcionar sistemas para la personalización de tarjetas y pasaportes a través de tecnología láser y de color.
- Diseñar y desarrollar sistemas altamente eficientes y especializados para el mundo de la identificación.
- Seleccionar partner estratégicos para la realización de proyectos complejos.

SOLUCIONES

- Impresoras de tarjetas de policarbonato para documentos de identidad y licencia de conducir, con codificación del chip con contacto y sin contacto, tecnología laser y tinta.
- Impresora para pasaportes electrónicos, con tecnología láser y tinta y con codificación del chip.
- aplicación software para la integración de la impresora en una plataforma integrada de datos.
- Servicios de instalación, mantenimiento, garantía y soporte técnico. Soporte on line, desde remoto y on site.

PRODUCTOS

Líneas de productos

- Sistemas de escritorio para la personalización de cédulas de identidad electrónicas y permisos de conducir, para la emisión descentralizada (modelos IDX, ID5, ID7, IDC)
- Sistemas de escritorio para la personalización de tarjetas bancarias (ID5X, ID7X)
- Sistemas de escritorio para la personalización de pasaportes electrónicos ((modelos XP24/25, XPRINT)
- Sistemas de emisión de tarjetas centralizada de tamaño mediano. (BOX).

---

4. **TOPPAN SECURITY SAS (ANTIGUA HID GLOBAL)** Como parte del Grupo Toppan, con más de 30 años de experiencia en impresión de seguridad y unos ingresos anuales de aproximadamente 13 mil millones de dólares, **Toppan Security SAS** es un líder mundial de la industria en soluciones de identidad y tecnologías de impresión de seguridad. Nos especializamos en la fabricación y personalización de tarjetas y pasaportes seguros, al mismo tiempo que ofrecemos soluciones tecnológicas de nicho como el registro de población nacional, la emisión de documentos nacionales de identidad y pasaportes, el registro de votantes, el registro de trabajadores civiles, la producción de licencias de conducir, el registro de vehículos motorizados, soluciones de pensiones, pagos en efectivo y soluciones biométricas seguras.

Figure 1: Productos y soluciones de Toppan Security

Toppan Security SAS se destaca como una de las empresas más importantes del mundo en este campo, gracias a nuestra amplia experiencia y su impresionante historial. Aportamos una gran cantidad de propiedad intelectual de proyectos gubernamentales similares, particularmente de implementaciones exitosas recientes de sistemas de personalización biométricos, de tarjetas y pasaportes en varios países.

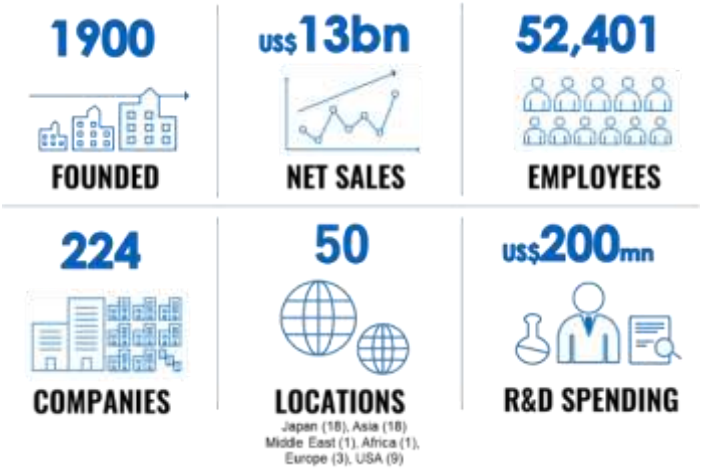
En Toppan Security SAS, comprendemos la importancia de respaldar los imperativos clave de las políticas, los negocios, los aspectos técnicos y operativos. Nuestra propuesta de valor se adapta cuidadosamente para abordar estos aspectos críticos, lo que nos permite ofrecer soluciones que tienen un impacto positivo en la efectividad, la eficiencia y el ahorro de costos de nuestros clientes. Contamos con evidencias concretas que validan los beneficios que nuestras soluciones aportan a las operaciones de nuestros clientes.

Confiamos en que la información proporcionada en este documento demuestre nuestra voluntad, habilidades y capacidad comprobada para proporcionar la tecnología y los servicios requeridos.

GRUPO TOPPAN

Como socio de confianza para gobiernos, bancos centrales e instituciones financieras desde que comenzamos a imprimir certificados de acciones en 1902, **Toppan Group** es un líder mundial en sistemas de emisión de pasaportes e identificaciones gubernamentales, impresión de tarjetas inteligentes, billetes y tecnología antifalsificación con múltiples instalaciones de producción en todo el mundo. Durante los últimos 30 años, nuestros productos y soluciones de seguridad han sido seleccionados por gobiernos de todo el mundo.

Como parte de Toppan Group, Toppan Security SAS es un proveedor de soluciones globales con un enfoque predominante en las industrias de pagos e identidad. Nuestro objetivo es desarrollar la próxima generación de documentos de seguridad virtuales y físicos, y estamos continuamente buscando empresas en las que invertir, para aumentar nuestro alcance tecnológico y geográfico.



TOPPAN y HID-CID

El 31 de enero de 2025, TOPPAN completó oficialmente la adquisición del negocio de Identidad Ciudadana (CID) de HID

Con instalaciones de impresión de seguridad de última generación en ocho países y una presencia global que abarca más de 20 oficinas, esta integración fortalece nuestra capacidad para ofrecer soluciones de identificación gubernamental innovadoras y confiables en todo el

mundo. El equipo de CID, con sus 20 años de experiencia y un historial de entrega de soluciones a más de 50 países, aporta capacidades invaluables que posicionan aún más a TOPPAN Security SAS como líder mundial en soluciones de identidad.

Experiencia

Con nuestra amplia experiencia y gama de productos especializados, Toppan Security SAS está excepcionalmente bien preparado para diseñar e implementar soluciones rentables que se alineen con los resultados exitosos en varios países de todo el mundo. Nuestra impresionante trayectoria no solo demuestra nuestras habilidades y desempeño colectivos en la entrega de soluciones comerciales, sino que también destaca nuestro compromiso de cultivar relaciones duraderas con los clientes que garanticen la operación sostenible y efectiva de las soluciones que brindamos.

En particular, hemos implementado con éxito sistemas de personalización de pasaportes electrónicos en el Ministerio del Interior de Bahréin, Barbados, Kazajstán, Mongolia, entre otros y en los últimos años con experiencias importantes en el desarrollo de identidades móviles para la República de Argentina y Filipinas.

Reconocimiento Internacional

Toppan es reconocida internacionalmente por sus capacidades y la entrega de proyectos exitosos. Así lo avalan los diversos reconocimientos y premios internacionales que ha recibido el Grupo.

Las Soluciones de Identificación para Gobierno

HID ha demostrado ser un socio comprometido a resolver de las principales necesidades de sus clientes de gobierno, en la mejor calidad, tiempo y forma, para lo cual nuestras soluciones incluyen lo siguiente:

- Documentos de identidad de última generación utilizando materiales cuidadosamente seleccionados y técnicas de impresión avanzadas (por ejemplo, identificación nacional, identificación de residente extranjero, licencia de conducir, identificación electoral del votante, registro de vehículos, etc.).
- Componentes de documentos electrónicos, insertos y cubiertas electrónicas, hojas de datos, y pre-laminados utilizados en las libretas de pasaporte e identificaciones electrónicas actuales.
- Patente de prevención de grietas permite prolongar la vida útil de los documentos.
- Soluciones de autenticación biométrica confiables, seguras y convenientes.
- Una línea completa de lectores de documentos oficiales de gobierno.
- Soporte para ofrecer soluciones integrales.

- Innovadora tecnología para la emisión de documentos de identificación digitales y virtuales, HID goID™.
- Solución modular para la emisión y gestión de documentos electrónicos seguros HID Integrale™.
- Sistemas Operativo para Chip (COS) HID SOMA™ de gran seguridad que alimenta los microcontroladores integrados en los documentos electrónico.
- HID Mirage™, la cual es una característica de seguridad basada en la personalización de una ventana transparente a través del grabado con láser en positivo y negativo.
- Sistemas de personalización de documentos de seguridad de alto volumen y gran rendimiento.

---

5. **MAGALLANES MEDIA S.A** , registrada en Argentina con CUIT 30-71037547-6 y con oficinas en Magallanes 1315 Ciudad Autónoma de Buenos Aires 1288, es una empresa dedicada al desarrollo y provisión de soluciones tecnológicas para la industria de medios de comunicación, industria gráfica, y la administración pública. A lo largo de su trayectoria la empresa se ha desempeñado en varios sectores tecnológicos con los más altos estándares de calidad y profesionalismo. Se presenta por medio de la presente a esta contratación en consorcio para suplir los equipos, materiales y servicios para la impresión de la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI) para la Junta Central Electoral en República Dominicana.

   Fundada en el año 2007, Magallanes Media empezó desarrollando los medios digitales de las revistas de la editorial Producciones Publiexpress, principalmente medios de interés general de consumo masivo. Magallanes Media continúa con esta línea de negocio y hoy produce y mantiene tecnológicamente a uno de los 10 medios de contenido digital con mayor tráfico de Argentina, www.pronto.com.ar.

   Del lado de la administración pública, en el año 2019 Magallanes Media se presentó y fue adjudicada una licitación para la provisión de una solución integral de credenciales de identidad digitales portables en dispositivos móviles para el Registro Nacional de las Personas (RENAPER). Junto con el RENAPER, en noviembre de 2019 Magallanes Media lanzó el primer documento nacional de identidad (DNI) digital del mundo y hoy la solución continúa funcionando con más de 6,500,000 de credenciales digitales activas. Magallanes Media es el proveedor del sistema de emisión y gestión del DNI (cédula) digital que se porta dentro de la app Mi Argentina. La credencial digital cuenta con sofisticados sistemas criptográficos y de encriptación que garantizan la seguridad de los datos personales de los ciudadanos. En el año 2023 Magallanes Media se presentó y fue adjudicada la renovación de este contrato; esta vez para la provisión de la misma solución integral de credenciales

de identidad digitales portables en dispositivos móviles para el RENAPER pero esta vez interoperable y basada en el estándar ISO 18013-5. En el año 2023 Magallanes Media se presentó y fue adjudicada una licitación para la renovación de la infraestructura de PKI del RENAPER. Este proyecto fue entregado en 2024 y continúa en funcionamiento. Magallanes Media entregó con éxito nuevas infraestructuras de PKI ICAO 9303 para documentos de viaje, IACA para la cédula digital ISO 18013-5, y firma digital para el DNI electrónico con chip en Argentina. Magallanes Media también brinda el servicio de mantenimiento de dicha infraestructura.

Magallanes Media también se presentó y fue adjudicada en los años 2022 y 2024 licitaciones para la provisión al RENAPER de sistemas de detección de ataques de presentación tanto para rostro como para documentos físicos. Magallanes Media opera estos sistemas desde el 2023, con volúmenes diarios de más de 500,000 transacciones por día. La solución de prueba de vida de rostro, o detección de ataque de presentación (PAD), de Magallanes Media cumple con el estándar ISO 30107-3. A raíz de estos proyectos Magallanes Media se ha posicionado como una empresa líder en materia de identidad digital y biometría. Asimismo, el equipo de trabajo de Magallanes Media también le brinda servicios de consultoría al Renaper y al proveedor de las tapas, (eCover), hoja de policarbonato, y máquinas de personalización del pasaporte argentino.

Magallanes Media también ha logrado integrar servicios de tecnología para la producción de productos gráficos en la industria gráfica, en entre ellos IPESA, una de las líderes del segmento de impresión de revistas y catálogos en rotativas offset y la producción de estuches de cartulina para la industria de la exportación de langostinos.

Magallanes Media cuenta con amplia experiencia en integración y desarrollo de distintas soluciones tecnológicas personalizadas tanto en el ámbito privado como para la administración pública. La empresa está capacitada y cuenta con un equipo de profesionales altamente preparados para llevar a cabo el procedimiento en cuestión y brindar una alta calidad de servicios a la Junta Central Electoral de República Dominicana.

Conclusión

Esta estructura de colaboración garantiza una solución robusta, con capacidades especializadas en cada etapa del proyecto.

El **Consorcio IDSecure IDS** presenta una propuesta integral, cumpliendo con los estándares más exigentes de seguridad, interoperabilidad y eficiencia en la emisión de documentos de identidad. La combinación de tecnologías avanzadas, experiencia internacional y compromiso

con la innovación posiciona esta solución como la mejor alternativa para la modernización del sistema de identificación en la República Dominicana. Con este documento introductorio se establecen las bases para el desarrollo de los siguientes capítulos que profundizarán en cada aspecto de la solución propuesta.

Visión del proyecto sugerencias y recomendaciones.

El proyecto para la emisión de la nueva Cédula de Identidad y Electoral (CIE) y la Cédula de Identidad (CI) de la República Dominicana busca modernizar y fortalecer el sistema de identificación ciudadana. La propuesta del consorcio integra tecnologías avanzadas de grabado láser, autenticación digital y seguridad criptográfica, garantizando documentos seguros, confiables y adaptados a los estándares internacionales establecidos por la OACI y las normas ISO.

La visión del proyecto se enfoca en ofrecer una emisión ágil y segura de los documentos de identidad, garantizando su interoperabilidad tanto a nivel nacional como internacional. El uso de equipos de impresión de alto rendimiento y materiales de alta resistencia permitirá garantizar la integridad, autenticidad y durabilidad de cada documento emitido, cumpliendo con las especificaciones técnicas y los requisitos operativos establecidos en el pliego de condiciones.

Sugerencias para el Éxito del Proyecto

1. **Optimización del Flujo de Trabajo**
    - Implementar procesos automatizados para la personalización y control de calidad de las tarjetas, garantizando un rendimiento óptimo y una alta precisión en el grabado láser.
    - Aprovechar la capacidad de los equipos de impresión y los sistemas de alimentación de tarjetas para reducir los tiempos de producción y minimizar las interrupciones.
2. **Fortalecimiento de la Seguridad Documental**
    - Mantener el uso de elementos de seguridad avanzados, como ventanas transparentes, microtextos, tintas ópticamente variables (OVI) y elementos holográficos, para garantizar la protección contra intentos de falsificación.
    - Asegurar que los chips sin contacto cumplan con los protocolos ISO 14443 y las especificaciones de la ICAO, permitiendo una autenticación electrónica segura y eficiente.
3. **Garantía de la Calidad y la Trazabilidad**

- Integrar sistemas de verificación óptica y cámaras de alta resolución para garantizar la alineación precisa de los datos impresos y codificados.
- Capturar imágenes de cada tarjeta para su registro en el sistema de auditoría y trazabilidad, cumpliendo con los estándares de seguridad de la JCE.

4. **Integración Tecnológica y Conectividad**
   - Garantizar la integración de los sistemas de impresión con la infraestructura tecnológica de la JCE mediante el uso de APIs y plataformas de gestión centralizada.
   - Asegurar la compatibilidad de los equipos con los sistemas de validación de identidad móvil (Mobile ID) y las plataformas de autenticación digital, cumpliendo con los estándares ISO18013-5 y el ICAO DOC 9303.

Recomendaciones para la Implementación y el Mantenimiento

1. **Planificación de la Implementación**
   - Respetar el cronograma de entrega y asegurar la instalación y configuración de los equipos en los centros de impresión nacional y en el exterior, garantizando su funcionamiento óptimo.
   - Realizar las pruebas de concepto obligatorias en Santo Domingo, demostrando la capacidad de personalización física y digital conforme a los requisitos de la JCE.
2. **Mantenimiento Preventivo y Correctivo**
   - Implementar un programa de mantenimiento preventivo para garantizar el funcionamiento continuo de los equipos de impresión y evitar interrupciones en la producción.
   - Asegurar la disponibilidad de repuestos y consumibles esenciales, considerando las condiciones ambientales y la intensidad de uso en cada centro de impresión.
3. **Capacitación y Transferencia de Conocimientos**
   - Ofrecer programas de formación para los operadores de los equipos de impresión, técnicos de soporte y personal administrativo, asegurando el correcto uso y mantenimiento del sistema.
   - Proporcionar manuales de usuario detallados y acceso al soporte técnico para resolver incidencias de manera ágil y eficiente.

Curriculum del líder del proyecto con mínimo 5 años de experiencia, proyectos de identificación de tarjetas de policarbonato en instituciones públicas

Curriculum del personal técnico certificado en tecnología de impresión de tarjetas

Curriculum del personal técnico (10) en campo (a nivel nacional) con experiencia en la producción de documentos de identidad, modelo decentralizado.

Requisitos de experiencia (OBLIGATORIOS)

Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo el suministro de impresoras de documentos de identidad de policarbonato electrónicos, incluyendo la instalación y el mantenimiento, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública.

Al menos una (1) experiencia en un proyecto, en el cual el oferente haya llevado a cabo un suministro de tarjetas de identidad electrónicas de policarbonato, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta y a nivel de institución pública

Al menos una (1) experiencia, en el cual el oferente haya implementado un proyecto de transición de documentos de identificación mecánicos (sin electrónica) a documentos de identificación electrónicos, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

Al menos una (1) experiencia, en el cual el oferente haya realizado una integración de sistemas, en un proyecto de identificación electrónica, dentro de los últimos 5 años a partir de la fecha de presentación de la propuesta.

Requisitos de experiencia (NO OBLIGATORIOS)

Más de una (1) experiencia, en distintos clientes y países, en cédulas digital o identidades móviles (Mobile ID). Solo proyectos de 100,000 cédulas en total, dentro de los últimos 5. Al menos una de las referencias debe ser ISO 18013-5**.**

Al menos una (1) experiencia de haber operado un proyecto de impresión de soluciones de identificación a nivel de gobierno con el suministro y mantenimiento de al menos doscientas (200) impresoras distribuidas nacional e internacional (fuera del país).

Al menos una (1) experiencia en República Dominicana en proyectos de mantenimiento de tecnología en gobierno con al menos cinco (5) años de experiencia.

PROPUESTA TECNICA Y ANEXOS

La presente propuesta ha sido elaborada en respuesta a la Licitación Pública Internacional JCE-CCC-LPI-2024-0001, convocada por la **Junta Central Electoral (JCE)** de la República Dominicana, para el diseño, suministro y puesta en marcha del sistema de emisión de **la nueva Cédula de Identidad y Electoral (CIE) y Cédula de Identidad (CI)**. La solución planteada por el **Consorcio IDSecure ID**S garantiza el cumplimiento integral de los requerimientos técnicos, operativos y legales establecidos en el Pliego de Condiciones Específicas, así como en las respuestas aclaratorias y enmiendas emitidas durante el proceso.

A lo largo del documento, se detallarán los aspectos clave del proyecto, incluyendo las capacidades del consorcio, las especificaciones de las tarjetas y equipos de impresión, la infraestructura de seguridad PKI, la plataforma digital para cédulas, los kits de periféricos, el plan de mantenimiento y los programas de capacitación, asegurando que cada componente de la solución propuesta se alinea con los estándares internacionales y los objetivos estratégicos de la JCE

Descripción de la Prueba de Concepto

La Prueba de Concepto (PoC, por sus siglas en inglés) que presentará el **Consorcio IDSecure IDS** dará inicio con una presentación donde se detallarán las características de cada uno de los elementos que formarán parte de la prueba. Estos elementos son:

- **Módulo de Enrolamiento y dispositivos involucrados.**
    - Este módulo, desarrollado exclusivamente para la prueba de concepto, está alineado a las necesidades específicas de captura de información en tiempo real.
- **10 Tarjetas blancas de muestra / Propuesta de Tarjetas con diseño.**
    - Se utilizarán 10 tarjetas blancas con ventana y CLI para demostrar las capacidades de personalización solicitadas.
    - Se presentará y explicarán las distintas medidas de seguridad propuestas en un diseño exclusivo para la Cédula de la República Dominicana, utilizando dispositivos de validación que garantizan el cumplimiento de cada elemento.
- **Impresora IXLA IDX DF-01.**
    - Impresora láser con capacidad de grabación de chip.
- **Aplicación de ID Digital.**
    - Esta aplicación demostrará la funcionalidad de creación de una Credencial Digital a partir de un documento físico, así como la validación biométrica con prueba de vida.

Una vez los integrantes de la comisión evaluadora estén familiarizados con los elementos a utilizar durante la demostración, iniciará la prueba dando secuencia a los siguientes procesos:

1. La JCE escogerá una persona del comité evaluador para que, de la mano con el proponente, realicen el llenado de un cuestionario en un sistema habilitado por el consorcio para simular el proceso de enrolamiento que realizaría un ciudadano al momento de solicitar su Cédula de Identidad y Electotal, integrando durante el proceso:
    a. Toma de **fotografía**. Siguiendo los estándares de ICAO para asegurar el tamaño, resolución y posiciones de la imagen, para facilitar la futura impresión y su utilización para validaciones biométricas.
    b. Toma de **datos biográficos** de la persona.

2. Una vez concluido el proceso de toma de datos (fotografía y biográficos), el sistema de enrolamiento genera un registro en formato XML que será puesto a disposición del sistema de personalización.

3. Para presentar el proceso de emisión, el operador de la impresora IXLA IDX DF-01 tomará el registro previamente enrolado en el paso 1 y dará la instrucción de impresión. Durante este proceso, con una duración máxima de 1 minuto, la impresora realizará las siguientes funciones:
    3.1 El alimentador carga una tarjeta en el transporte desde uno de los dos alimentadores.
    3.2 El sistema de transporte mueve la tarjeta a la posición de codificación.
    3.3 Se ejecuta la codificación sin contacto, guardando en una estructura predefinida y cumpliendo los estándares ICAO, los datos biográficos y la fotografía.
    3.4 La tarjeta se mueve a través de la unidad *flipover* a la posición láser.
    3.5 Se ejecuta el grabado láser de la fotografía a escala de grises y datos biográficos al anverso. Al menos uno de los datos será grabado con una configuración especial para generar un efecto táctil.
    3.6 En la misma posición se realiza la impresión del CLI y la fotografía fantasma en la ventana transparente.
    3.7 Para el segundo ciclo de grabado, la tarjeta se mueve a la posición *flipover*, y es volteada, regresando a la estación láser.
    3.8 Se graba el reverso de la tarjeta con láser (similar al punto 6) para la impresión del MRZ.
    3.9 La tarjeta se libera en la bandeja de salida, si algo sale mal, la tarjeta se retrae a la posición *flipover* y se mueve a la bandeja de rechazo debajo del volteo.

4. Una vez la Cédula ha sido personalizada gráfica y eléctricamente, el proceso continuará con la generación del ID Digital. Para este proceso, el consorcio utilizará la Aplicación de ID Digital, realizará lectura del MRZ impreso en el documento y la lectura del Chip personalizado con los datos del ciudadano a través de conexión NFC/RFID. La

Aplicación validará a través de una *Selfie*, por medio de algoritmos de reconocimiento facial, que la persona solicitando la creación del ID Digital (el ciudadano) coincide con la información biométrica contenida en el chip y que se trata de una persona viva (prueba de vida).

5. El consorcio demostrará la posibilidad de autenticar una persona utilizando el ID Digital recientemente creado a través de la validación biométrica facial, poniendo a prueba la solución al intentar validar a una persona errada (demostrando el mensaje de no coincidencia), y finalmente demostrar la validación con la persona correcta (demostrando el mensaje de coincidencia).

NOTA INTRODUCTORIA IMPORTANTE:

La oferta aquí descrita, incluye los siguientes aspectos clave que garantizan el cumplimiento de esta, frente a los requerimientos establecidos en el *Pliego de Condiciones Específicas LPI-01-2024, las respuestas y aclaraciones incluidas*:

1. **Cumplimiento obligatorio solución de PKIs,** Nuestra oferta incluye una **infraestructura de clave pública (PKI) compuesta por tres sistemas diferenciados**, diseñada específicamente para cumplir con las certificaciones y normas de seguridad exigidas en las bases de la licitación y las respuestas a las consultas de los oferentes:

    a. **PKI de Firma Digital:** Permite a los ciudadanos firmar documentos electrónicos y realizar autenticación en aplicaciones de la JCE y de terceros. Cumple con los estándares X.509v3 y RFC 5280, garantizando la validez jurídica de las firmas digitales.

    b. **PKI de Firma de Documentos:** Garantiza la autenticidad, integridad y no repudio de los documentos electrónicos emitidos por la JCE, conforme a las recomendaciones del *Doc 9303 de la OACI* y los protocolos BAC y SAC-PACE.

    c. **PKI de Seguridad para Documentos Electrónicos:** Asegura la protección de los datos biométricos y de identidad almacenados en el chip sin contacto, cumpliendo con el estándar ISO/IEC 14443 y el protocolo EAC para control de acceso extendido.

2. **Tiempo de entrega total inferior al requerido,** logrando agregar a nuestra oferta la implementación en **4.5 meses**, en lugar de las 6 meses establecidas, lo que permitirá a la JCE iniciar la recedulación antes del tiempo previsto.

3. **Carta de autorización de los periféricos propuestos,** requisito indicado en las consultas de los oferentes, garantizando la autenticidad de los equipos y la disponibilidad de soporte postventa.

4. **Capacidad de producción garantizada,** con tecnología de impresión láser de alta precisión que asegura la emisión de más de 100 tarjetas por hora, garantizando la personalización de los documentos en el menor tiempo posible.

5. **GARANTIA:** Nuestra oferta INCLUYE **5 años la garantía de las impresoras**, con el soporte en sitio del mantenimiento de las impresoras y no en la sede central de la JCE, manteniendo los mismos niveles de acuerdo de servicio.

6. **LECTORES RFID:** En cumplimiento con la respuesta 35 sobre el Lector de RFID, CCC-308-24 Respuestas aclaraciones y enmiendas técnicas II, que indica "*Se debe de añadir en costo de los 230 lectores en el FL-05 Presentación de Oferta Económica y se debe de añadir cotización individual en el desglose del Kit de dispositivos*" hemos incluido **230 unidades Lectores RFID (ITEM VIII)** a nuestro formulario FL-05 y dentro del kit de periféricos, el precio unitario del mismo.

7. **UPSs PARA ENERGIA CONTINUA**: según el requerimiento del **Pliego de Condiciones Específicas LPI-01-2024** que indica, *"Cada impresora de personalización debe estar equipada con **una fuente de alimentación ininterrumpida** para cubrir los PC integrados y la producción durante al menos dos minutos."* Y la respuesta/aclaración del documento **CCC-308-24 Respuestas aclaraciones y enmiendas técnicasII**, "*Pregunta: Entendemos que la UPS puede ser externa. ¿Es correcto nuestro entendimiento?, **Si***", hemos incluido en nuestra propuesta, **214 UPSs** con las características requeridas como.

8. **TARJETAS DE MUESTRAS:** Proporcionamos con nuestra propuesta diez (10) muestras de las tarjetas (adicionales a las requeridas para la prueba de concepto). Las muestras son capaces de representar la personalización de las cédulas electrónicas y los detalles de las características que el proveedor propone, y éstas se explican claramente. Junto al informe agregamos un **informe de pruebas independientes** de acuerdo a la norma I**SO 18745**.

9. **RPE DE EMPRESA EXTRANJERA**: El Consorcio IDSecure IDS de resultar adjudicado solicitará el Registro de Proveedores del Estado (RPE) de sus empresas extranjeras y del mismo, en un plazo no mayor de diez (10) días hábiles a partir de la fecha de notificación de adjudicación.

10. **DOCUMENTOS EN ESPAÑOL:** Todos los documentos, como poderes, que hubiese sido otorgado en un idioma que no sea el español; fueron traducidos por un intérprete judicial en la República Dominicana.

11. **PLAZO DE VALIDEZ DE LA OFERTA:** El plazo de validez de muestra oferta es de **150 días** a partir de la fecha límite de presentación de la oferta.

1. ESPECIFICACIONES TÉCNICAS DE LAS MÁQUINAS DE IMPRESIÓN

Nuestra propuesta responde a los requerimientos de la Junta Central Electoral (JCE) de la República Dominicana para la emisión y personalización de cédulas de identidad mediante tecnología de grabado láser de alta seguridad. La solución presentada se basa en el fabricante **IXLA SA**, miembro del consorcio y su tecnología **IXLA IDX**, un sistema compacto de emisión de tarjetas de policarbonato con grabado láser de alta precisión.

IDX Desktop Card Printer

1.1 DESCRIPCIÓN DEL SISTEMA IXLA IDX DF-01

El **IDX DF-01** es un producto único que integra una unidad de láser de fibra de 20W flexible y confiable – la misma utilizada en muchos otros productos de la gama IXLA –, proporcionando un rendimiento óptimo y una alta calidad en el grabado láser de tarjetas, garantizando operaciones estables y silenciosas.

El control del láser es el mismo que se aplica a todos los sistemas IXLA, estando integrado en una única placa altamente integrada con una pantalla gráfica a color para monitorear el estado y las operaciones.

A pesar de su diseño compacto, el **IXLA IDX DF-01** cuenta con un **alimentador doble** con capacidad total para **100 tarjetas**, permitiendo cargar uno o dos tipos de tarjetas. Además, dispone de una bandeja de salida frontal con capacidad para **40 tarjetas o más de 100** y una **bandeja de salida trasera desmontable con capacidad para 200 tarjetas**.

Esta solución permite trabajar con **lotes individuales** o con **dos tipos de tarjetas simultáneamente**, sin necesidad de intervención manual para intercambiarlas.

El **alimentador está protegido por una puerta frontal bloqueable mecánicamente**, que facilita la carga y descarga de tarjetas y es controlada por un sensor.

La **bandeja de salida frontal** para **40 tarjetas** se encuentra en la base del equipo y almacena las tarjetas en **posición vertical**, permitiendo una recogida sencilla de las tarjetas personalizadas. **Opcionalmente, se puede añadir un contenedor metálico** para expandir la capacidad a más de **100 tarjetas**.

La **bandeja de salida trasera** es una **unidad desmontable** con capacidad superior a **200 tarjetas**, utilizada para mejorar el rendimiento al expulsar las tarjetas finalizadas por la parte trasera del sistema, despejando el camino para las tarjetas entrantes y permitiendo una **operación en paralelo** de codificación, grabado láser y verificación de calidad.

Las **tarjetas rechazadas** se almacenan en un contenedor interno, cuyo acceso requiere abrir el sistema con las **llaves de seguridad dedicadas**.

1.2 CARACTERÍSTICAS DEL IXLA IDX DF-01

Las características técnicas más relevantes del sistema **IDX DF-01** son las siguientes:

IDX DF-01	Descripción
Personalización	Grabado láser (Clase 1), codificación de chip
Unidad láser	Láser de fibra de 20W refrigerado por aire, con duración de pulso fija o variable, industrial de alta resistencia
Control del láser	Electrónica de control del láser integrada y aplicación de software dedicada (basada en **Win PC, integrada**)
Personalización láser	Grabado en escala de grises de alta resolución y negro total para fotos, firmas, logotipos, texto, microtexto, códigos de barras 1D/2D y grabado táctil
Grabado láser de seguridad	Grabado inclinado MLI/CLI por desviación óptica (espejos), ventanas transparentes y de óxido, funciones patentadas (TruLock® , Mirage®)
Área de trabajo	Mayor que el área ID1/CR80, con un borde de 1.5 mm
Estación de codificación de chip (opcional)	ISO 14443 sin contacto Parte I a IV, tipo A/B, CL & Mifare (opcional), PC/SC
Estación de contacto	Lectura y codificación conforme a ISO/IEC 7816, PC/SC
Segunda estación opcional	Para verificación de integridad de datos
Garantía de calidad	Cámara de alta resolución (5Mpix, estándar) para auto-posicionamiento del grabado láser, con opciones de iluminación estándar o específicas del proyecto
Opciones adicionales de calidad	Software de verificación OCR y lectura de códigos de barras disponibles
Captura de imágenes	Para registro de producción, integridad de datos y verificación de legibilidad

Cámara opcional secundaria	Para verificación de tarjetas entrantes (tipo y orientación)
Alimentador de entrada de tarjetas	Alimentador de 100+ tarjetas para un solo tipo o dos tipos de tarjetas (60/40)
Manejo de tarjetas	Transporte sin rayaduras, modular, con unidad de volteo multifuncional integrada (verificación de tarjeta de entrada, alimentación de la estación de codificación, volteo de tarjeta para grabado en ambas caras)
Bandeja de salida de tarjetas	Apilador frontal estándar para 50 tarjetas; adaptador metálico opcional para aumentar la capacidad a 100 tarjetas
Bandeja de salida trasera opcional	Unidad desmontable con capacidad para 250 tarjetas
Rendimiento (cph)	Hasta 100 tarjetas por hora, dependiendo del diseño, construcción, materiales utilizados, tiempo de codificación y ciclos de control de calidad
Otras opciones	Configuración mecánica para conexión bajo demanda con módulos de personalización adicionales compatibles (impresión por retransferencia o inyección de tinta, laminado)
Monitor de estado	Pantalla gráfica a color de 128x64 píxeles con pantalla táctil para monitoreo de operaciones y alertas
Indicador LED	Barra LED en la parte superior del sistema para indicar estado operativo
Conectividad	Puerto Ethernet TCP/IP, puerto USB para conexión directa con codificadores/cámaras
Integración de software	Integración de software multiplataforma mediante SDK/API propietario de licencia gratuita
Seguridad operativa	Sistemas de bloqueo para evitar la apertura durante el funcionamiento
Seguridad ambiental	Ventilador de extracción con filtro de carbón activado
Diagnóstico	iCube (Interfaz IXLA), aplicación de monitoreo y configuración basada en la web
Dimensiones y Peso	300 x 300 x 500(h) mm (**0.045 m3**)**; 27 kg**
Fuente de alimentación	**110/220V AC MONOFASICA**, 50/60Hz, 300W

1.2.1 Características Técnicas y de Funcionamiento

El sistema de impresión y personalización de tarjetas cumple con los estándares de seguridad y calidad exigidos por la **Junta Central Electoral (JCE)**, garantizando un proceso de producción eficiente y de alta precisión mediante **tecnología de grabado láser de 20W** y **control óptico avanzado**.

- **Máquina de impresión modular**, con posibilidad de añadir o quitar módulos de personalización en color o elementos de seguridad adicionales.
- **Tecnología de personalización por grabado láser en escala de grises**, asegurando máxima precisión en la fotografía del titular y otros elementos de seguridad.
- **Sistema de producción industrial sólido, capaz de operar 24/7**, con un rendimiento de **hasta 100 tarjetas por hora**.
- **Codificación de tarjetas sin contacto,** compatibles con ISO 14443 Tipo A y B.
- **Control de calidad y alineación óptica previo al grabado láser**, permitiendo un ajuste automático del diseño antes de la impresión.
- Los componentes de inspección son ajustables mediante el uso de una unidad de **iluminación LED múltiple** con diferentes longitudes de onda.
- **Hemos agregado a la solución un equipo para energía ininterrumpida, 1 UPS de 1500 VA por máquina, 214 en total,** marca CyberPower, modelo LX1500GU, como una fuente de alimentación externa ininterrumpida para cubrir los PC integrados y la producción, por un mínimo de 2 minutos.

✅ **Eficiencia y Control de Calidad**

- **Sistema de administración de diagnósticos de impresión**, permitiendo monitoreo en tiempo real del rendimiento, conteo de tarjetas impresas y gestión de calidad.
- **Sistema de control óptico** con verificación en tiempo real, asegurando la alineación precisa de los datos impresos con la estructura de la tarjeta.
- **Rechazo de credenciales defectuosas mediante inspección automatizada**, evitando la emisión de documentos con errores en impresión, grabado, codif. de chip espesor, orientación de la tarjeta y referencia.
- **Captura de imágenes para auditoría y validación**, asegurando trazabilidad y cumplimiento de estándares de calidad.
- **Evaluación del chip antes y después de su personalización**, garantizando la integridad de los datos almacenados.
- **La función de detección de CLI** estará disponible independientemente de los demás procesos de inspección de tarjetas.

✅ **Conectividad e Integración**

- **Interfaz TCP/IP con dirección IP ajustable**, permitiendo la integración en una red centralizada para control y monitoreo remoto.
- **Compatibilidad con estaciones de trabajo Windows y Linux**, asegurando interoperabilidad con los sistemas de la JCE.
- **Control de texto, datos gráficos, MRZ y elementos de seguridad avanzados (microtexto, imágenes fantasmas, códigos de barras 1D y 2D).**

✅ **Lectores de Chip y Seguridad Electrónica**

- **Incluye 230 lectores de chip sin contacto, compatibles con ISO 14443 Tipo A y B, ICAO 9303, PA, AA, BAC, EAC y SAC.**
- **Verificación del correcto** funcionamiento del chip mediante protocolo ATS (Answer To Select).
- **Garantiza la interoperabilidad** con sistemas de control de identidad electrónica y verificación biométrica.

1.3 DISEÑO DE IMPRESORA IDX DF-01

El diseño de la impresora láser **IDX DF-01** prioriza un tamaño compacto sin sacrificar la ergonomía adecuada para esta clase de dispositivos, manteniendo las características clave necesarias para la emisión de tarjetas en **documentos de identificación gubernamentales, control de acceso de alta seguridad o aplicaciones financieras**.

El sistema requiere una superficie aproximada de **300 x 300 mm (12” x 12”)**, con un espacio libre ideal en la parte trasera de **300 mm (< 12”)**. Su diseño con parte superior plana, que ofrece una superficie útil, y sus esquinas redondeadas hacen que el **IDX DF-01 sea una solución de escritorio fácil de integrar**.

La **pantalla de estado y operaciones** está ubicada en la parte superior frontal, lo que la hace **visible y fácilmente accesible**. Está asociada con **barras de luz laterales** en la parte superior, las cuales **cambian de color** según el estado de operación de la máquina.

El **acceso frontal al alimentador doble** es **intuitivo y fácil de usar**, al igual que la **bandeja de salida**, que permite almacenar **un lote de 50 tarjetas personalizadas** antes de su recolección.

La integración interna del **módulo láser** es altamente innovadora:

- En el **tamaño y la forma del recorrido de transporte**, lo que garantiza **nitidez y precisión en el grabado** con una tarjeta estable y permite mantener la **distancia focal requerida para el láser**.
- En el **uso óptimo del espacio**, acomodando el transporte, las posiciones de codificación y el volteo de la tarjeta dentro de un área **muy compacta**.
- En la **disposición de los componentes láser y ópticos**, los cuales están organizados de manera que **reducen el tamaño y volumen total de la unidad**.

Las **barras de luz laterales** en la parte superior del sistema, que muestran **iluminación en verde, rojo y amarillo**, permiten una **comprensión inmediata del estado operativo** del IDX DF-01.

Algunas opciones de configuración del producto permiten **mejorar las funcionalidades y el rendimiento**, asegurando **flexibilidad para aplicaciones personalizadas por el usuario**:

- **Expansor opcional de la bandeja de salida frontal**: Se trata de una **placa metálica** que permite **apilar más de 100 tarjetas**, ideal cuando la emisión de tarjetas requiere **procesamiento en volumen**.
- **Microcámara adicional de alta resolución**: Instalada en el área de volteo, permite **capturar una imagen parcial de la tarjeta** para verificar **su orientación y tipo**, evitando **errores humanos** al cargar el stock de tarjetas en los alimentadores.

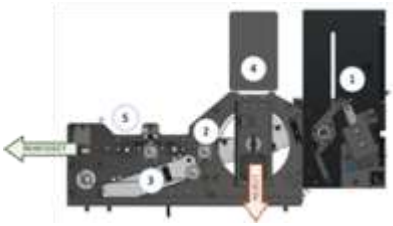
- **Segundo lector de chip**: Instalado debajo de la posición de grabado láser, permite **leer el chip antes de expulsar la tarjeta**, evitando la emisión de **tarjetas con codificación incorrecta**. Junto con la imagen capturada por el sistema de cámara principal, también permite **verificar la integridad de los datos**, asegurando la correspondencia entre los **elementos gráficos y los datos electrónicos**.

- La salida trasera permite la expulsión de tarjetas sin interferir con el procesamiento en paralelo, mejorando el rendimiento en la emisión por lotes y ofreciendo una bandeja de mayor capacidad (> 200 tarjetas).

- La misma bahía de expulsión trasera permite la conexión mecánica de dispositivos adicionales de personalización, como impresión a color o laminado.

1.3.1 Flujo de Trabajo del IDX DF-01

Durante la operación, el **IDX DF-01** permite el **procesamiento paralelo de codificación y grabado láser**, gracias a un diseño que permite la **personalización simultánea de dos tarjetas**.



1. El alimentador (1) carga una tarjeta en el sistema de transporte desde uno de los dos compartimentos, ejecutando al mismo tiempo una **verificación mecánica del grosor de la tarjeta** (de acuerdo con el punto II.1 del Pliego).
2. En la posición (4) se realiza **la verificación sin contacto del ATS** (Answer To Select), para garantizar que el chip funciona correctamente.
3. En la misma posición (4), si **se comprueba que el chip funciona correctamente**, se ejecuta la codificación; la unidad de codificación permite tanto la codificación por contacto como sin contacto.
4. Tras ejecutar la codificación, **se realiza una lectura completa del chip**, almacenando los datos relevantes en un búfer (ChipData).
5. La tarjeta **se desplaza a través de la unidad de volteo** hacia la posición del láser (5).
6. En la estación láser (5), se ejecuta el número necesario de **mediciones de compensación** (IDX DF-01 permite múltiples compensaciones por cada lado), utilizando varios puntos de referencia gracias a la cámara dedicada y la iluminación variable.
7. **El grabado de imágenes y datos** se realiza en la estación láser (5), utilizando las posiciones XY corregidas por las mediciones de compensación del paso 6.
8. Tras completar el grabado, **se captura una imagen completa del anverso** de la tarjeta y se almacena en un búfer (FrontImage).

9. Si se requiere un **segundo ciclo de grabado**, la tarjeta se desplaza a la posición (2), se voltea y vuelve a la posición (5).
10. Se realizan las **mediciones de compensación para el reverso** (igual que en el punto 6) y, a continuación, se procede al grabado láser (igual que en el punto 7).
11. Tras finalizar el grabado, **se captura una imagen completa del reverso de la tarjeta** y se almacena en un búfer (RearImage).
12. **Se ejecuta el control de calidad** (QC) utilizando los datos extraídos mediante OCR/ICR de las imágenes FrontImage y RearImage para garantizar la legibilidad. Los mismos datos leídos mediante OCR se comparan primero con los datos de ChipData para verificar la integridad de los datos entre el chip y las gráficas (los datos deben coincidir en ambas capas de personalización) y luego también con el registro original enviado para la personalización.
13. Si el proceso de control de calidad es positivo, la **tarjeta se expulsa por la parte trasera.** Si ocurre algún problema, la tarjeta se retrae a la posición (2) y se desplaza al compartimento de rechazo situado debajo de la unidad de volteo.

1.4 ENTORNO DE SOFTWARE DE IXLA

Cada sistema suministrado por **IXLA** se entrega con un **paquete de software completo**, común a todos sus productos:

iCube

Para la **interacción directa con los usuarios**, IXLA proporciona una **solución de software basada en la web** que permite el **control del sistema durante las operaciones, diagnóstico y configuración**. La aplicación fue desarrollada por **IXLA** utilizando el **protocolo de comandos para integración** contenido en el **SDK**, el cual está disponible para **todos los clientes y usuarios de IXLA**.

Utilidad de Diagnóstico

La **pantalla principal de la utilidad de diagnóstico** contiene todos los **parámetros de funcionamiento y monitoreo del sistema**, permitiendo al usuario ejecutar **pruebas y enviar comandos directos al hardware**. Debido a la naturaleza técnica de esta herramienta, **su uso está reservado para ingenieros capacitados y su acceso está protegido en el sistema**.

SCAPS SAMLight

La **programación del láser**, que incluye la **preparación de los datos y parámetros de grabado láser** para la personalización de tarjetas, se realiza a través de una **aplicación de terceros estándar en el mercado**: **SAMLight de SCAPS**.

IXLA proporciona con cada sistema una **versión personalizada de SAMLight**.

1.4.1 Entorno SDK de IXLA

IXLA proporciona **de manera gratuita** documentación y código de muestra sobre la **interfaz de programación** de sus productos.

- El **SDK** permite la **integración del sistema de personalización en cualquier aplicación externa** y es un **elemento común a todos los productos IXLA**.
- Funciona como un **protocolo de comandos y datos** que utiliza el **formato de intercambio XML 1.0** sobre una conexión **Telnet**.
- El **protocolo de comandos** no solo ofrece un **conjunto completo y efectivo de instrucciones** que permite el **control total del sistema**, hasta el nivel de **sensores y motores**, sino que también **incluye comandos de alto nivel** para ejecutar tareas ordinarias de personalización.
- Los **integradores de sistemas y desarrolladores de software** pueden **integrar los sistemas IXLA en sus aplicaciones en un plazo de días o semanas**, dependiendo de la complejidad del proyecto.

La solución propuesta, basada en el sistema **IXLA IDX DF-01**, cumple con **todos los requisitos técnicos y operativos** establecidos en el **Pliego de Condiciones Específicas LPI-01-2024**, asegurando una solución de **impresión láser robusta, eficiente y segura** para la emisión de la nueva **Cédula de Identidad y Electoral**. Los equipos contarán con los accesorios, equipos auxiliares y cualquier otro implemento necesario para su operación según las prestaciones especificadas en el presente pliego. Con su tecnología de **grabado láser de 20W**, sistema de **alimentación automática de tarjetas**, módulos de **verificación óptica y codificación de chip**, y su capacidad para trabajar **en paralelo con alto rendimiento (hasta 100 tarjetas por hora)**, garantiza una **producción continua y de alta precisión**. Además, la integración del sistema de **diagnóstico en tiempo real (iCube)** y su arquitectura **modular y escalable** permiten una operación flexible y adaptable a las necesidades de la JCE. Con esta propuesta, la JCE contará con una **solución de vanguardia, totalmente alineada con los más altos estándares internacionales**, garantizando **seguridad, durabilidad y eficiencia en la personalización de documentos de identidad**.

2. ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

Las tarjetas presentadas han sido diseñadas y fabricadas con los más altos estándares de seguridad, durabilidad e interoperabilidad, cumpliendo estrictamente con la normativa OACI Doc. 9303 para documentos de identidad y viaje electrónicos.

Estas tarjetas son fabricadas por **Litho Formas S.A. de C.V.**, empresa integrante del consorcio, y están compuestas por policarbonato de alta resistencia, garantizando una durabilidad mínima de 10 años y una seguridad estructural que evita la manipulación o degradación prematura.

2.2 ESPECIFICACIONES TÉCNICAS DE LAS TARJETAS

2.2.1 Características Generales

Cada tarjeta está equipada con un chip sin contacto (*contactless*) de última generación, que incorpora avanzados mecanismos de autenticación digital y seguridad criptográfica, brindando tres funcionalidades principales:

1. **Documento de Viaje Electrónico (eTravel Document)**
    a. Cumple con los estándares ICAO 9303 para pasaportes electrónicos.
    b. Compatible con sistemas de control fronterizo y validación automatizada de identidad.
    c. Integración con tecnologías de acceso suplementario seguro (SAC), autenticación activa (AA) y control de acceso extendido (EAC).

2. **Firma Electrónica Segura (eSignature)**
    a. Capacidad de generación y almacenamiento de claves criptográficas para la autenticación digital.
    b. Cumplimiento con estándares X.509 y compatibilidad con Infraestructura de Clave Pública (PKI).
    c. Protección mediante PIN/PUK para evitar accesos no autorizados.

3. **Identificación Ciudadana (eID)**
    a. Almacenamiento de datos biométricos y de identidad del titular con acceso seguro.

El diseño y la fabricación de estas tarjetas integran un robusto conjunto de elementos de seguridad física y digital, tales como:

- **Policarbonato multicapa fusionado**, que impide la separación de capas o alteraciones físicas.
- **Protección contra falsificaciones** mediante tecnologías ópticas avanzadas, tales como ventanas transparentes, estructura lenticular, impresión UV y guilloches de alta precisión.
- **Microtextos de alta precisión**, visibles solo con dispositivos de aumento.
- **Tintas ópticamente variables (OVI)**, que cambian de color según el ángulo de observación.
- **Parche difractivo con nanotextos**, generando efectos visuales dinámicos que impiden la falsificación.
- **Sistema de personalización con grabado láser** en profundidad, asegurando permanencia en los datos del titular sin posibilidad de alteración.
- **No presentará ningún riesgo tóxico en su uso normal.**

Funcionalidad de Identificación Ciudadana

El sistema de identificación ciudadana cumple con los estándares internacionales de seguridad y privacidad, garantizando la protección y autenticación segura de los datos del titular.

✅ **Almacenamiento de Datos de Filiación**

- Los **datos de filiación del ciudadano** se almacenarán de manera estructurada en el chip sin contacto, utilizando formatos estandarizados y encriptación avanzada para garantizar su integridad y seguridad.
- El almacenamiento de información sigue los lineamientos de **seguridad de datos biométricos y de identidad**, asegurando su accesibilidad únicamente a través de métodos autorizados.

✅ **Acceso Seguro a la Información**

- El acceso a los datos se realiza bajo **mecanismos seguros de autenticación**, cumpliendo con la normativa **ISO/IEC 14443**, que regula la transmisión de datos mediante tecnología de radiofrecuencia (RFID/NFC).

Además, estas tarjetas han sido diseñadas para operar en entornos extremos, con **resistencia a temperaturas de -35°C a +80°C**, alta humedad relativa y exposición a agentes químicos sin comprometer su integridad o funcionalidad.

La integración de estas características asegura que las tarjetas sean altamente seguras, confiables y compatibles con los sistemas de validación de identidad nacionales e internacionales, proporcionando una solución tecnológica de vanguardia para la identificación y verificación de ciudadanos.

2.3 TIPOS DE TARJETA

El consorcio confirma su capacidad para suministrar y personalizar **dos tipos de tarjetas** destinadas a la identificación ciudadana y electoral, cumpliendo con los estándares de seguridad e interoperabilidad establecidos por las normativas nacionales e internacionales.

Especificaciones de Color y Fondo Preimpreso de las Tarjetas

Las tarjetas destinadas a la **Cédula de Identidad y Electoral (CIE)** y la **Cédula de Identidad (CI)** han sido diseñadas considerando los lineamientos establecidos en la licitación, garantizando su diferenciación visual mediante la **variación de color exclusivamente en el fondo preimpreso**.

Cada tipo de tarjeta se distinguirá por el uso de **dos colores predefinidos en el fondo preimpreso**, lo que facilitará su identificación y evitará confusiones en su uso. Este fondo será impreso con **técnicas avanzadas de seguridad**, incluyendo:

- ✅ **Patrones guilloches de alta precisión**
- ✅ **Microtextos invisibles y visibles.**
- ✅ **Tintas de seguridad con efectos ópticamente variables (OVI).**
- ✅ **Impresión UV para validación con luz ultravioleta**.
- ✅ **Estructura de impresión a registro con laminación de seguridad**.

El proceso de impresión del fondo preimpreso cumple con los estándares internacionales de seguridad documental y garantizará una alta resistencia a la manipulación y a la degradación por factores ambientales o de uso prolongado.
El diseño de la tarjeta ha sido optimizado para asegurar su correcta integración con el proceso de personalización mediante **grabado láser**, permitiendo la emisión segura y eficiente de cada documento de identidad.

1. **Tarjeta para la Cédula de Identidad y Electoral (CIE)**

   - Documento oficial utilizado para la **identificación del ciudadano y su derecho al voto** en procesos electorales.
   - Compatible con sistemas de validación electrónica en **centros de votación, entidades gubernamentales y registros civiles**.
   - Configurada con **funcionalidades avanzadas de autenticación digital y biométrica**, garantizando integridad y no suplantación de identidad.
   - Incluye **certificados electrónicos** para la firma digital y el acceso a servicios de administración electrónica.

2. **Tarjeta para la Cédula de Identidad (CI)**

   - Documento oficial de **identificación nacional** para ciudadanos, residentes y otras categorías autorizadas por la normativa vigente.
   - Permite el acceso a **servicios gubernamentales, financieros y comerciales**, asegurando la autenticación confiable del titular.
   - Compatible con sistemas de control de acceso en **instituciones públicas y privadas**.
   - Configuración específica para su uso en aplicaciones de **identificación móvil (Mobile ID)** mediante interfaz NFC y validación con lectores electrónicos.

Ambas tarjetas están fabricadas con **las mismas características físicas y tecnológicas**, diferenciándose únicamente en:

✅ **Color de la tarjeta (fondos preimpresos)**, facilitando la identificación visual del tipo de documento.

✅ **Personalización del reverso**, adaptada a las necesidades específicas de cada tipo de cédula y sus respectivas funcionalidades.

Estas tarjetas han sido diseñadas para garantizar **seguridad, durabilidad y usabilidad eficiente**, permitiendo su integración con infraestructuras nacionales e internacionales de identificación y control de acceso.

2.4 FORMATO DE DOCUMENTO

Las tarjetas presentadas cumplen con el formato ID-1, conforme a los estándares internacionales establecidos en las normativas ISO/IEC 7816:2019 e ISO/IEC 7810:2019, garantizando su compatibilidad con sistemas de validación y lectura electrónica a nivel global. Se trata de una tarjeta sin contacto, cumpliendo con la normativa ISO/IEC 14443, que regula la transmisión de datos mediante tecnología de radiofrecuencia (RFID/NFC), permitiendo la autenticación segura en sistemas electrónicos de identificación y control de acceso.

Característica	Valor Mínimo	Valor Máximo	Valor de la Muestra
Espesor	0.68 mm	0.84 mm	0.81 mm
Largo	85.47 mm	85.72 mm	85.68 mm
Ancho	53.92 mm	54.03 mm	53.98 mm

Dimensiones de la Tarjeta (Formato ID-1):

Características Claves del Formato:

- Cumplimiento con estándares de documentos de identidad internacionales, facilitando su reconocimiento y compatibilidad con sistemas electrónicos de validación.
- Diseño optimizado para lectura sin contacto, asegurando la interacción fluida con dispositivos NFC y lectores RFID en puntos de control, aeropuertos, bancos y entidades gubernamentales.
- Estructura uniforme y de alta precisión, garantizando un ajuste perfecto en billeteras, dispositivos de impresión y personalización láser.
- Optimización para impresión y grabado láser, permitiendo la personalización de datos variables con tecnología de seguridad avanzada.

Este formato garantiza la interoperabilidad de la tarjeta en sistemas electrónicos de identificación y validación, asegurando su adecuado funcionamiento en entornos nacionales e internacionales.

2.5 MATERIALES

La tarjeta ha sido diseñada con **materiales de alta calidad** que garantizan su resistencia estructural, durabilidad prolongada y una seguridad reforzada contra intentos de falsificación o manipulación.

Está fabricada con **policarbonato de alta resistencia**, compuesto por **7 capas fusionadas** mediante un proceso de **laminación en caliente**, asegurando:

- ✅ **Resistencia a la división o separación de capas**, evitando intentos de alteración o reconstrucción del documento.
- ✅ **Mayor vida útil**, con una durabilidad comprobada de **al menos 10 años** en condiciones normales de uso.
- ✅ **Alta estabilidad térmica y química**, soportando temperaturas extremas de **-35°C a +80°C**, así como exposición a productos químicos sin comprometer su integridad.
- ✅ **Capacidad de grabado láser en profundidad**, permitiendo la personalización permanente de datos con protección contra manipulaciones.

2.5.1 Tintas y Elementos de Seguridad

Para reforzar la seguridad y la autenticidad del documento, la tarjeta incorpora una combinación de **tintas de alta tecnología** y elementos ópticos de validación:

- **Tintas de formulación específica para impresión offset**
  - Desarrolladas para ofrecer **máxima durabilidad y nitidez**, manteniendo la calidad del documento durante toda su vida útil.
  - Especialmente diseñadas para adherirse a la estructura multicapa de policarbonato sin degradación.

- **Tintas de seguridad con pigmento sólido**

  - Altamente resistentes a intentos de eliminación o alteración química.
  - Diseñadas para **evitar la reimpresión o sobreimpresión fraudulenta**.

- **Tintas ópticamente variables (OVI)**

  - Contienen partículas microscópicas que generan un **efecto de variabilidad de color** al cambiar el ángulo de incidencia de la luz.
  - Permiten la validación visual inmediata sin necesidad de instrumentos avanzados.
  - Visibles bajo radiación **infrarroja (IR) y ultravioleta (UV)**, brindando un nivel adicional de autenticación.

- **Elemento Holográfico de Alta Seguridad**

  - Incorporado mediante técnicas de impresión de última generación.

- **Dos elementos holográficos** diseñados con imágenes dinámicas que cambian según el ángulo de visión.
- Contiene **nanotextos y microestructuras ópticas avanzadas**, proporcionando un método de validación visual inmediato y evitando su reproducción fraudulenta.

Este conjunto de materiales y tecnologías de impresión garantiza que la tarjeta cuente con **altos niveles de resistencia, seguridad y autenticidad**, asegurando su fiabilidad en sistemas de validación electrónica y verificación visual.

2.6 CARACTERÍSTICAS ELECTRÓNICAS Y SISTEMA OPERATIVO

Las funcionalidades electrónicas del documento serán operativas únicamente después de realizar una **activación mediante comparación 1:1** al momento de la entrega al ciudadano, asegurando la autenticidad y titularidad del documento.

Una vez entregado, el documento no podrá modificar ni ampliar su funcionalidad, **excepto en lo relativo a los certificados de firma digital**, los cuales cuentan con un ciclo de vida administrado de manera independiente. Para ello, se implementará un sistema robusto de gestión de certificados, asegurando su **generación, actualización y revocación** conforme a las mejores prácticas de seguridad digital.

2.7 CHIP SIN CONTACTO

La tarjeta incorpora un **chip sin contacto (contactless) de alta seguridad de la família P71 de NXP**, diseñado para cumplir con los estándares internacionales de **documentos de viaje electrónicos**, conforme a las especificaciones establecidas por la **Organización de Aviación Civil Internacional (OACI, ICAO Doc 9303)**. Este chip garantiza la autenticidad de la identidad del titular, permitiendo su validación segura en sistemas de control migratorio y plataformas electrónicas de identificación.

Especificaciones del Chip:

- CPU de **16/32-bit**.
- Certificación **CC EAL6+**.
- Criptoprocesador de hardware para operaciones criptográficas. **Unidad funcional criptográfica dedicada** para algoritmos simétricos DES y AES
    - **DES** con longitud de clave de 56 bits, **2DES** de 112 bits, **3DES (Tripe DES)** de 168 bits, en diversas configuraciones.
    - **AES** con longitudes de clave de 128, 192 y 256 bits

- **Acelerador de criptografía asimétrica**, compatible con RSA, ECC y algoritmos relacionados
    - **Criptografía RSA** con longitud de clave arbitraria de hasta 4096 bits.
    - **Criptografía de curvas elípticas (ECC)** con longitud de clave de hasta 571 bits.
- Generador de números aleatorios verdaderos (TRNG), conforme a AIS31
- Soporta hashing de acuerdo con los algoritmos criptográficos: SHA-1, SHA-2
- Protección contra descargas ESD.
- Reloj interno asíncrono (CLK).
- Número de serie único.
- Tecnología de firewall de seguridad entre particiones de memoria.
- Memoria no volátil suficiente para la incorporación de las aplicaciones requeridas, funcionalidades y datos.
- Retención de datos en memoria no volátil de al menos 10 años.
- Al menos 500.000 ciclos de lectura / escritura garantizados
- Soporte de doble interfaz con amplio rango de configuración
    - Interfaz de contacto **ISO/IEC 7816**; velocidades de datos estándar de hasta TA1 = 97h
    - Interfaz sin contacto **ISO/IEC 14443**
    - Interfaz Tipo A para velocidades de datos de hasta 848 kbit/s, con configuraciones de velocidad de datos simétricas y asimétricas
    - Soporte de configuración de **Very High Bit Rate (VHBR**) en la interfaz sin contacto para minimizar el tiempo de transacción (3,4 Mbit/s en la dirección del chip hacia el lector.
- Soporta tecnologías de seguridad avanzadas como **Basic Access Control (BAC), Supplemental Access Control (SAC), Extended Access Control (EAC) y Active Authentication (AA)** protegiendo la información almacenada en el chip contra accesos no autorizados.

Capacidad de Almacenamiento y Protección de Datos Críticos:

- **Almacena datos biométricos del titular**, incluyendo fotografía digital, datos personales y firmas electrónicas.

- **Soporta claves criptográficas X.509 para autenticación digital**, permitiendo su uso en **firmas electrónicas avanzadas y verificación de identidad remota**.
- De acuerdo con la Guía Técnica **TR-03110 del BSI** o similar.

Métodos de Validación del Chip Sin Contacto

- **Validación con Lectores de Documentos de Viaje:**
  - La autenticidad de la tarjeta puede verificarse mediante **lectores RFID/NFC compatibles con ICAO 9303**, presentes en aeropuertos, consulados y puntos de control de identidad.
- **Verificación Biométrica Avanzada:**
  - Los datos biométricos almacenados en el chip pueden ser comparados con los datos en tiempo real capturados por **cámaras de reconocimiento facial y escáneres de huellas dactilares** en sistemas de control migratorio.
- **Autenticación Digital con Firma Electrónica:**
  - La firma electrónica almacenada en el chip permite la validación del documento en sistemas gubernamentales y privados sin necesidad de presentar la tarjeta físicamente.
- **Protección Contra Clonación:**
  - A través de los mecanismos de **autenticación pasiva (PA), activa (AA) y EAC**, se impide la clonación del chip, garantizando que cada documento sea único e imposible de replicar.

4. Beneficios Claves del Chip Sin Contacto

- **Mayor Seguridad y Autenticación Instantánea:**
  - Permite la verificación del documento en **menos de un segundo**, facilitando la validación de identidad en aeropuertos, consulados y puntos de control digital.
- **Compatibilidad con Infraestructura de Identidad Digital:**
  - Puede ser utilizado en soluciones de identidad digital nacional e internacional, facilitando la autenticación en entornos electrónicos.
- **Protección de Datos Personales y Prevención de Falsificaciones:**

- Gracias a su encriptación avanzada y sus protocolos de autenticación, la información contenida en el chip **no puede ser alterada, clonada o leída sin autorización del usuario**.

- **Facilidad de Uso y Mayor Durabilidad:**
  - Su tecnología sin contacto permite su utilización sin desgaste mecánico, aumentando la **vida útil del documento hasta 10 años o más**.

El chip sin contacto incorporado en la tarjeta cumple con los estándares internacionales de seguridad y operatividad, garantizando una autenticación segura, interoperabilidad global y resistencia a intentos de manipulación o falsificación.

2.7.1 Funcionalidad de Firma Electrónica

El sistema de firma electrónica incorporado en la tarjeta cumple con los más altos estándares internacionales de seguridad, permitiendo una autenticación confiable y un uso seguro en entornos gubernamentales, financieros y de identidad digital.

Seguridad y Cifrado Avanzado

- **Acceso protegido mediante PIN / PUK**, asegurando la autenticación segura del usuario.
- **Soporte para algoritmos de firma digital RSA y ECDSA**, cumpliendo con los estándares de la **PKI de Firma Digital** y la **PKI de Firma de Documentos**.
- **Soporte para claves RSA en formato CRT y normal** (exponente privado, exponente público y módulo).
- **Claves RSA con soporte para componentes p y q de longitud variable**, asegurando flexibilidad en la generación de claves criptográficas.
- **Cifrado AES-256 y RSA hasta 4096 bits**, garantizando la protección de los datos almacenados contra intentos de clonación o manipulación.

Infraestructura de Clave Pública (PKI) y Certificación de Seguridad

- Compatible con **Infraestructura de Clave Pública (PKI)** y los estándares **X.509v3 y RFC 5280**.
- **Capacidad de almacenar hasta 4 certificados**, incluyendo claves RSA de 4096 bits y claves de sesión derivadas mediante ECDH.
- Soporte para **curvas elípticas NIST P-256, BrainpoolP256r1**, cumpliendo con los estándares ISO 15946.

- **Certificación CC EAL5+**, garantizando la seguridad en la ejecución de operaciones criptográficas.

Seguridad en la Transmisión de Datos

- **Securización de los mensajes transmitidos entre la tarjeta y el terminal** mediante un canal seguro de acuerdo a **CEN14890 o equivalente**.
- **Confidencialidad de los datos transmitidos mediante Triple DES / AES**, asegurando la integridad de la información.
- **Autenticación mediante MAC ANSI X9.19 y DES**, proporcionando validación criptográfica de la información intercambiada.
- **Protocolo de establecimiento de claves de sesión basado en ISO/IEC 9798-3 Authentication SASL Mechanism**, garantizando un intercambio seguro de claves.

Funcionalidades Claves del Software de Firma Electrónica incluido con el Middleware

- **Estructura interna de ficheros conforme a ISO/IEC 7816-15 (PKCS#15)**, asegurando la organización de los certificados digitales.
- **Drivers de la tarjeta compatibles con PKCS#11, CSP y Card Module**, garantizando su integración con diferentes sistemas operativos.
- **Software de gestión de credenciales digitales**, permitiendo operaciones como:
    - Cambio y desbloqueo de PIN.
    - Borrado y renovación de certificados digitales.
    - Administración de claves y sesión.
- **Compatibilidad con múltiples plataformas (Windows, Linux, MacOS, Android e iOS)**, asegurando interoperabilidad con dispositivos y sistemas gubernamentales.
- **Soporte de librerías y SDKs para aplicaciones móviles**, facilitando el desarrollo de soluciones de identidad digital en Android e iOS.
- **Actualización continua del software**, garantizando compatibilidad con nuevos sistemas operativos, navegadores y estándares de seguridad.

2.7.2 Características del Sistema Operativo del Chip Sin Contacto

El sistema operativo **SOMA c016** para chip sin contacto ha sido diseñado por **TOPPAN Security,** conforme a los estándares internacionales de seguridad y transmisión de datos, garantizando una comunicación eficiente, interoperabilidad global y protección contra

accesos no autorizados, utilizando un sistema operativo nativo, por lo que el mismo **No opera JavaCard, por lo que No aplica** el requisito de bloqueo ante la posibilidad del agregado de nuevas aplicaciones.

Cumplimiento con Estándares de Comunicación y Seguridad

- **SOMA c016** cumple plenamente con los requisitos de **ICAO 9303** para Documentos de Viaje Legibles por Máquina.
- **Protocolo de transmisión basado en ISO/IEC 14443 A/B**, asegurando compatibilidad con sistemas de control de identidad electrónica.
- **Interfaz de comandos conforme a ISO/IEC 7816-4 y PCSC**, permitiendo la interoperabilidad.
- **Generación de identificadores únicos aleatorios (UID/PUPI aleatorio)**, proporcionando mayor seguridad contra ataques de rastreo y clonación.

Seguridad y Tecnología en las Plataformas más Avanzadas

- SOMA c016 se ejecuta sobre la familia P71 de NXP. Dicha combinación garantiza un alto rendimiento en la carga del Sistema Operativo de Chip, la personalización y la lectura de documentos, reduciendo el tiempo de personalización a solo unos pocos segundos. Esto se traduce en la garantía de eficiencia y cumplimiento del volumen de emisión.

Funcionalidad del Documento Electrónico

El sistema operativo **SOMA c016** cumple con los más altos estándares de seguridad para documentos electrónicos, permitiendo la autenticación y validación confiable en sistemas de control fronterizo y plataformas de identidad digital. **SOMA** ha sido certificado según Common Criteria, lo que incluye la auditoría del entorno seguro de desarrollo de TOPPAN Security, así como la evaluación de la calidad del código de SOMA y su resistencia a las pruebas de penetración realizadas por expertos de laboratorio. Los microcontroladores que utilizan **SOMA** cumplen con los requisitos más estrictos de seguridad de datos y comunicaciones, logrando estándares:

BAC: EAL 4+
EAC-SAC-AA: EAL 5+

Soporta los siguientes mecanismos avanzados de protección:

- **Basic Access Control (BAC):** BAC (Control de Acceso Básico) impide que el chip se lea sin acceso físico. El terminal de verificación o dispositivo de inspección utiliza un lector de reconocimiento óptico de caracteres (OCR) para leer la zona legible por máquina y, a partir de esos datos, genera dos claves de cifrado: una clave simétrica para la autenticación mutua y una clave de sesión para cifrar el intercambio de datos con la terminal. Esto protege contra la interceptación de la comunicación entre el chip y el terminal.
- **Supplemental Access Control (SAC):** Al igual que BAC, el Control de Acceso Suplementario (SAC) garantiza que solo se pueda leer cuando hay acceso físico. SAC genera claves de sesión para la comunicación con la terminal de verificación o dispositivo de inspección, pero a diferencia de BAC, SAC emplea criptografía asimétrica más segura.
- **Extended Access Control (EAC):** EAC es un mecanismo adicional que admite y protege los datos biométricos, incluidas las huellas dactilares y los escaneos de iris (cuando se utilizan). Las imágenes faciales, la firma y la información biográfica se siguen recuperando a través de BAC. La OACI (ICAO) recomienda EAC para proteger los datos biométricos, pero no lo ha convertido en un requisito obligatorio para los documentos electrónicos conformes a ICAO. EAC incluye la autenticación del chip y la autenticación del terminal.
- **Active Authentication (AA):** AA protege los datos contra la clonación. Cada chip tiene una clave diversificada (secreta) que es inaccesible para el terminal o dispositivo de inspección. El chip firma el desafío con su clave secreta, que luego se verifica en el terminal o dispositivo de inspección utilizando la clave pública.

Este sistema operativo ha sido elegido para cumplir con los requerimientos de seguridad de la **Junta Central Electoral (JCE), y garantizar su compatibilidad con infraestructuras internacionales de verificación electrónica y control migratorio.**

2.8 CARACTERÍSTICAS DE SEGURIDAD PRINCIPALES

La tarjeta ha sido diseñada con un conjunto de **medidas de seguridad avanzadas** que garantizan su autenticidad, protegen contra falsificaciones y permiten una validación eficiente tanto visual como electrónica. Estas características están distribuidas en múltiples niveles de seguridad, asegurando que el documento sea **altamente confiable y resistente a intentos de manipulación**.

2.8.1 Diseño de Alta Seguridad

La muestra presentada incluye un diseño exclusivo con elementos gráficos de seguridad integrados:

✅ **Anverso:** Representación de la **fachada del Alcázar de Colón**, diseñada con **guilloches complejos, microtextos de alta precisión y tramas de seguridad con modulación de espesor**.

✅ **Reverso:** Imagen del **monumento La Fortaleza Ozama**, utilizando un sistema de impresión offset con patrones de seguridad altamente detallados.

✅ **Software de diseño de seguridad especializado**, que impide la reproducción no autorizada y permite la validación óptica avanzada del documento.

Nota Importante: El Consorcio entregara los diseños de seguridad del documento a la JCE en ficheros vectoriales de formato electrónico.

ANVERSO

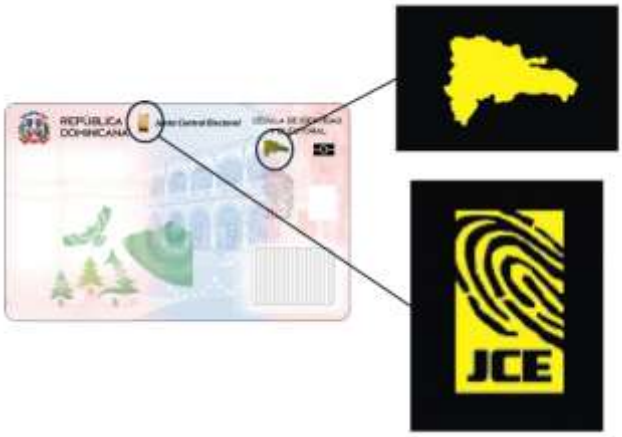
REVERSO

Esta composición gráfica no solo representa **símbolos icónicos de la República Dominicana**, sino que también está diseñada para **prevenir intentos de falsificación** mediante técnicas de impresión especializadas.

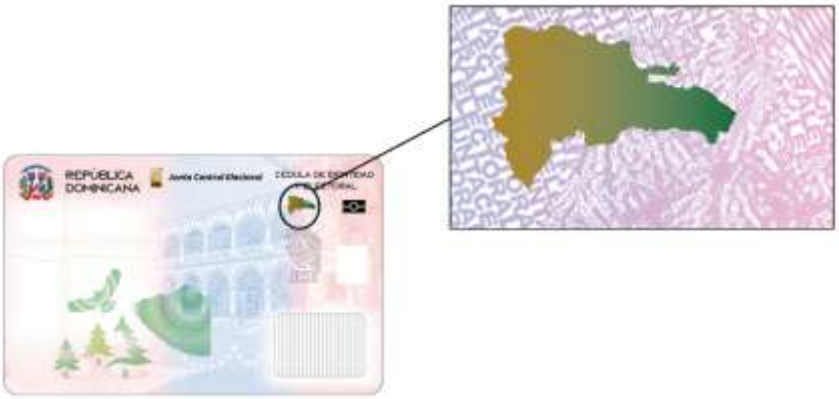
2.8.2 Seguridad con Tintas Visibles e Invisibles

La tarjeta incorpora **dos motivos impresos con tintas de seguridad visibles e invisibles**, que presentan fluorescencia al ser expuestos a **fuentes de luz ultravioleta (UV)**.

- **Validación mediante luz UV:**
  - Al colocar la tarjeta bajo una lámpara de **luz ultravioleta (dispositivo de verificación No. 2)**, los elementos de seguridad impresos mostrarán una **fluorescencia amarilla**, facilitando la autenticación visual rápida y efectiva.



- **Elemento de seguridad del contorno del mapa de la República Dominicana:**



  - Contiene una combinación de **tinta visible e invisible**, además de un **taggant de alta seguridad**, un componente químico especial que solo se vuelve visible cuando es expuesto a un **dispositivo láser**.

- **Validación:** Al dirigir un **láser** sobre este elemento, se proyectará una **luz verde**, confirmando la autenticidad del documento.

Esta combinación de tintas visibles, invisibles y elementos ópticos avanzados dificulta la falsificación y facilita la detección de documentos alterados.

2.8.3 Embozado Superficial en Relieve mediante Laminación a Registro

La tarjeta incorpora un **elemento de embozado superficial en relieve** aplicado mediante un **proceso de laminación a registro**, diseñado para proporcionar una medida de seguridad tanto **visual como táctil**, garantizando la autenticidad del documento y dificultando intentos de falsificación o alteración.

Características del Embozado Superficial en Relieve:

✅ **Autenticidad Visual y Táctil:**

- El relieve se percibe al **tocar la superficie de la tarjeta**, permitiendo una verificación inmediata sin necesidad de herramientas especializadas.
- El diseño del embozado se integra de manera precisa con los elementos gráficos de la tarjeta, asegurando que cualquier alteración resulte en una distorsión perceptible del patrón original.

✅ **Laminación a Registro de Alta Precisión:**

- Utiliza un **proceso de alineación exacta** para garantizar que el embozado coincida perfectamente con los elementos gráficos de la tarjeta.
- Permite una distribución homogénea del relieve, evitando deformaciones o irregularidades que pudieran comprometer la estética y funcionalidad del documento.

✅ **Alta Durabilidad y Resistencia:**

- Diseñado para **soportar el desgaste por fricción**, manteniendo su relieve incluso tras años de uso intensivo.
- No se degrada con la exposición a humedad, temperaturas extremas o agentes químicos, asegurando una **larga vida útil del documento**.

✅ **Protección Contra Falsificación:**

- La aplicación de este embozado en una capa interna de la tarjeta impide su remoción sin dañar la estructura del documento.
- Dado que el relieve está alineado con los gráficos de seguridad y el diseño estructural de la tarjeta, cualquier intento de modificación generaría **inconsistencias visibles y detectables**.

Métodos de Validación del Embozado:

🔹 **Validación Visual:**

- Se inspecciona a simple vista para verificar que el patrón en relieve coincide con el diseño original y no presenta irregularidades.
- Puede comprobarse inclinando la tarjeta bajo una fuente de luz, lo que permite observar sombras y reflejos generados por el relieve.

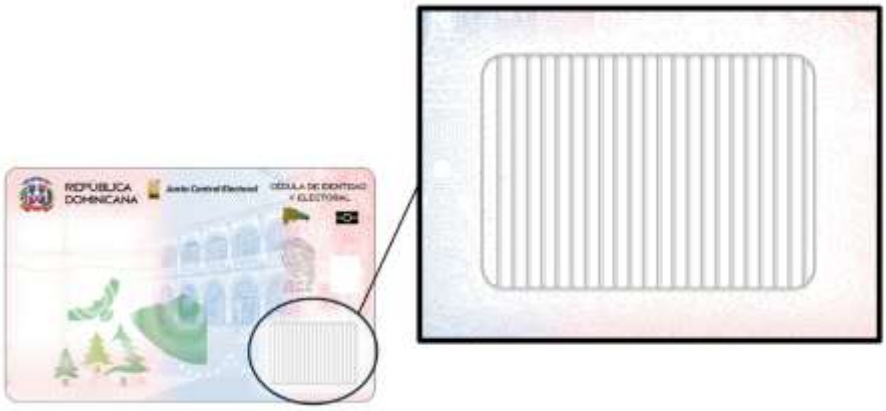
🔹 **Validación Táctil:**

- Se confirma pasando los dedos sobre la superficie del embozado para detectar la textura y la altura del relieve.
- Cualquier alteración en el patrón original o una textura irregular puede indicar intentos de manipulación del documento.

Este embozado proporciona **una barrera efectiva contra la falsificación** y permite que la autenticidad del documento pueda ser verificada rápidamente mediante métodos simples, pero altamente confiables.

2.8.4 Estructura Lenticular para Personalización de CLI o MLI

La tarjeta incorpora una **estructura lenticular de alta seguridad**, diseñada específicamente para la personalización de imágenes con tecnología **CLI (Changeable Laser Image) o MLI (Multiple Laser Image)**. Este mecanismo de seguridad avanzado permite la visualización de **imágenes dinámicas que cambian dependiendo del ángulo de observación**, lo que dificulta su reproducción fraudulenta y mejora la autenticación visual del documento.



Características de la Estructura Lenticular CLI:

✅ **Personalización de Seguridad Visual Dinámica:**

- El sistema **CLI** muestra **una imagen diferente dependiendo del ángulo de visión**, permitiendo la incorporación de datos variables como **fotografía del titular, número de identificación o símbolos de seguridad únicos**, asegurando una **autenticación visual inmediata y efectiva.**

✅ **Integración Directa con la Superficie de la Tarjeta:**

- La estructura lenticular está **incorporada en la tarjeta mediante grabado láser de alta precisión**, fusionándola con la capa superior de policarbonato para evitar alteraciones o intentos de remoción.
- Diseñada para permanecer **inalterable ante intentos de raspado, modificación o falsificación**, garantizando la **protección de la identidad del titular**.

✅ **Alta Resistencia y Durabilidad:**

- Fabricada con materiales que **no se degradan con el tiempo**, manteniendo su integridad visual incluso después de años de uso continuo.

- Soporta **temperaturas extremas, humedad y exposición a agentes químicos**, sin afectar la calidad de la imagen lenticular.

✅ **Dificultad para la Falsificación:**

- La combinación de **CLI con efectos ópticos avanzados** impide la reproducción mediante métodos convencionales de impresión o escaneo.
- Esta tecnología solo puede ser implementada con **láseres de personalización de alta precisión**, restringiendo su duplicación a fabricantes certificados.

Métodos de Validación de la Estructura Lenticular:

🔹 **Validación Visual:**

- La autenticidad del documento se verifica inclinando la tarjeta para observar los cambios en la imagen lenticular.
- Se pueden distinguir entre **dos o más imágenes o elementos de seguridad dinámicos** dependiendo del ángulo de observación.

🔹 **Validación Táctil:**

- La superficie de la estructura lenticular presenta **una ligera variación de textura**, perceptible al tacto, lo que permite detectar su presencia incluso sin luz adecuada.
- Cualquier alteración o irregularidad en la textura puede indicar intentos de manipulación del documento.

Beneficios Claves de la Estructura Lenticular CLI/MLI:

🔹 **Seguridad Visual Dinámica:** Garantiza una verificación rápida sin necesidad de dispositivos especializados.

🔹 **Prevención de Falsificación:** Su complejidad técnica impide la reproducción con técnicas de impresión o fotocopiado.

🔹 **Autenticación Rápida y Efectiva:** Permite la validación en segundos en aeropuertos, bancos, y controles fronterizos.

🔹 **Durabilidad Extrema:** Resiste el desgaste mecánico y la exposición a condiciones ambientales adversas.

2.8.5 Ventana Transparente para Personalización de Seguridad

La tarjeta incorpora una **ventana transparente de alta seguridad**, diseñada específicamente para la personalización de datos críticos, como la **fotografía del titular y la fecha de caducidad del documento**. Esta tecnología avanzada refuerza la autenticidad de la tarjeta, permitiendo una validación visual rápida y efectiva, al tiempo que dificulta los intentos de falsificación o manipulación.

Características de la Ventana Transparente:

✅ **Integración Directa en la Estructura de la Tarjeta:**

- La ventana transparente es **parte del material de policarbonato multicapa**, lo que impide su alteración sin dañar la estructura del documento.
- Fusionada mediante **laminación en caliente**, asegurando su resistencia mecánica y evitando que pueda ser extraída o modificada sin dejar evidencia visible.

✅ **Personalización de Datos Críticos:**

- Diseñada para alojar **fotografía del titular y una impresión tramada de tinta invisible fluorescente,** garantizando la identificación visual del documento.
- **Protección contra intentos de reemplazo:** Cualquier intento de alteración o sustitución de la imagen impresa resultará en una deformación evidente de la ventana.

✅ **Incorporación de Elementos de Seguridad Adicionales:**

- Puede contener **microtextos, imágenes grabadas con láser o tintas de seguridad invisibles** que se activan bajo luz UV o IR.
- Opción de incluir **elementos ópticamente variables (OVI)** dentro de la ventana, ofreciendo validación adicional basada en el ángulo de observación.

✅ **Alta Durabilidad y Resistencia:**

- Fabricada con materiales que garantizan la **transparencia y estabilidad óptica a lo largo del tiempo**.
- No se degrada con la exposición a temperaturas extremas, humedad o agentes químicos.

Métodos de Validación de la Ventana Transparente:

🔹 **Validación Visual:**

- Se inspecciona a simple vista para confirmar la presencia de la imagen del titular y la información impresa en la ventana.
- La autenticidad se verifica mediante **efectos ópticos** incorporados dentro de la ventana transparente.

🔹 **Validación con Luz UV/IR:**

- Puede incluir elementos de seguridad que solo sean visibles bajo **luz ultravioleta o infrarroja**, proporcionando una **autenticación avanzada en entornos de alta seguridad**.

🔹 **Validación Física:**

- Al tacto, la ventana debe sentirse completamente integrada en la tarjeta, sin bordes irregulares ni signos de alteración.

Beneficios Claves de la Ventana Transparente:

🔹 **Dificultad de falsificación:** Su integración con el material de policarbonato la hace imposible de replicar con impresoras convencionales.

🔹 **Autenticación Rápida:** Permite la verificación instantánea en puntos de control, reduciendo el riesgo de fraude.

🔹 **Protección de Datos Claves:** Salvaguarda la fotografía y la información sensible del titular con tecnología de seguridad avanzada.

🔹 **Interoperabilidad Internacional:** Cumple con estándares de identificación utilizados en sistemas de control fronterizo y validación electrónica.

2.9 SISTEMA DE PERSONALIZACIÓN DE DATOS VARIABLES

La tarjeta incorpora un **sistema de personalización avanzada mediante grabado láser**, permitiendo la impresión de datos variables con alta precisión y seguridad. Este método garantiza que la información del titular sea **inalterable y resistente a manipulaciones**, reforzando la autenticidad del documento.

Tomando en cuenta la Personalización de los datos (según punto II.2.1 del pliego, mas abajo ejemplo de la personalización sugerida.

1. Personalización Mediante Grabado Láser

✅ **Alta Precisión y Definición de Imagen:**

- La personalización se realiza mediante **grabado láser de alta resolución**, lo que permite imprimir la fotografía del titular en **escala de grises** con gran nivel de detalle.
- La nitidez del grabado láser mejora la autenticación visual y dificulta la falsificación, ya que cualquier intento de alteración dejaría rastros visibles en la estructura de la tarjeta.

✅ **Datos Variables Grabados Permanentemente:**

- Se graban datos críticos como **nombre completo, número de identificación, fecha de emisión y fecha de expiración**, asegurando su permanencia en la estructura del policarbonato.
- La tecnología de grabado láser evita el uso de tintas o impresiones térmicas convencionales, reduciendo la posibilidad de desgaste o manipulación fraudulenta.

✅ **Escala de Grises para Fotografía de Alta Seguridad:**

- La fotografía se graba directamente sobre una capa interna de la tarjeta, **eliminando el riesgo de alteración o sustitución**.

- Permite la integración con sistemas de reconocimiento facial mediante la conservación de detalles faciales en niveles de contraste óptimos.

2. Estructura de la Tarjeta y Sensibilidad al Grabado Láser

✅ **Capas Múltiples Sensibles al Láser:**

- La tarjeta está formada por **varias capas de policarbonato**, algunas de las cuales poseen **sensibilidad al grabado láser**.
- Esta capa reacciona a la luz del láser, permitiendo una personalización de alta precisión sin afectar la integridad del material.
- Se pueden grabar elementos con diferentes intensidades, generando efectos visuales o texturas táctiles en los datos grabados.

✅ **Personalización de Elementos Sensibles al Tacto:**

- Algunos elementos del grabado láser pueden presentar **relieve perceptible al tacto**, lo que agrega una capa adicional de seguridad y facilita la autenticación del documento sin necesidad de dispositivos electrónicos.
- La textura en el grabado puede integrarse con otros elementos de seguridad, como microtextos en bajo relieve o marcas de identificación táctiles.

3. Validación y Autenticación del Grabado Láser

🔹 **Validación Visual:**

- La fotografía y los datos grabados pueden ser verificados a simple vista, asegurando su legibilidad y autenticidad.
- Se puede inclinar la tarjeta para observar reflejos y contrastes en la imagen grabada, detectando cualquier intento de alteración.

🔹 **Validación Táctil:**

- Los elementos en relieve pueden ser percibidos al tacto, permitiendo la verificación manual sin dispositivos electrónicos.
- Cualquier irregularidad en el grabado podría ser indicio de manipulación fraudulenta.

🔹 **Validación con Luz Ultravioleta e Infrarroja:**

- Dependiendo de la configuración de seguridad, el grabado láser puede contener **marcas invisibles o microtextos ocultos**, detectables solo con luz **UV o IR**.
- Esto agrega un nivel adicional de autenticación en procesos de verificación de alta seguridad.

- **Validación con Dispositivos Electrónicos:**
  - Algunos datos grabados pueden ser verificados mediante lectores especializados que detectan patrones de grabado únicos, mejorando la seguridad en sistemas de control de identidad digital.

4. Beneficios Claves del Sistema de Personalización Láser

- **Seguridad Permanente:**
  - El grabado láser es **inalterable**, evitando que los datos puedan ser modificados o reimpresos fraudulentamente.
- **Durabilidad Extrema:**
  - La información grabada no se degrada con el tiempo, la fricción o la exposición a factores ambientales como humedad, luz UV o productos químicos.
- **Dificultad para la Falsificación:**
  - A diferencia de métodos de impresión convencionales, el grabado láser requiere **equipos altamente especializados**, lo que reduce el riesgo de falsificación.
- **Compatibilidad con Sistemas de Verificación Digital:**
  - La calidad del grabado permite su integración con sistemas de reconocimiento facial y verificación automatizada en aeropuertos, bancos y entidades gubernamentales.
- **Personalización Adaptada a Necesidades de Seguridad:**
  - Se pueden integrar elementos adicionales como **microtextos, marcas táctiles y códigos de autenticación láser**, fortaleciendo la protección del documento.

2.10 CARACTERÍSTICAS DE SEGURIDAD DE LA TARJETA

Las medidas de seguridad implementadas en la tarjeta cumplen con **estándares internacionales de documentos de identidad y viaje**, asegurando **protección contra intentos de falsificación, manipulación o alteración**.

Cada característica de seguridad ha sido cuidadosamente diseñada para proporcionar una autenticación rápida y confiable en diferentes escenarios, desde inspección visual hasta validación en sistemas electrónicos de control de identidad.

2.10.1 Nivel 1 - Características de Seguridad Detectables por Inspección Visual

Las medidas de seguridad de **Nivel 1** pueden ser verificadas a simple vista sin necesidad de dispositivos especializados. Estas características facilitan la autenticación del documento de identidad en **controles fronterizos, bancos, instituciones gubernamentales y cualquier punto de verificación manual**.

2.10.1.1 Impresión en Iris con Cambio de Color

✅ **Tecnología de Impresión de Seguridad**

- La tarjeta incorpora un **patrón de impresión en iris**, compuesto por líneas finas que cambian de color gradualmente a lo largo de su trayectoria sin interrupción del trazo.
- Este **efecto de transición de color** impide que el patrón pueda ser reproducido con técnicas convencionales de impresión o fotocopiado.

✅ **Cambio de Color Gradual (Azul-Rojo)**

- En el diseño de seguridad de la muestra, el patrón de iris **pasa de azul a rojo de manera progresiva**, creando un efecto visual difícil de replicar con impresión digital convencional.
- La autenticidad del documento se puede verificar inclinando la tarjeta bajo distintas condiciones de iluminación para observar el cambio de color.

✅ **Dificultad de Falsificación**

- Debido a su complejidad técnica, la impresión en iris **requiere equipos de seguridad especializados para su producción**, impidiendo su reproducción con métodos comerciales.

- Cualquier intento de alteración del documento resultará en **disrupciones visibles en la continuidad del trazo**, facilitando la detección de intentos de falsificación.

2.10.1.1.1 Métodos de Validación de la Impresión en Iris

- **Validación Visual:**
  - Se verifica el **cambio de color gradual en los trazos**, asegurando que no haya interrupciones o variaciones en el diseño original.
  - Se puede inclinar la tarjeta bajo distintas fuentes de luz para observar la transición de colores en los patrones de seguridad.
- **Validación con Dispositivos de Inspección:**
  - En entornos de alta seguridad, se pueden utilizar **lupas de aumento o escáneres de seguridad óptica** para examinar la precisión del patrón de iris.
  - Dispositivos avanzados pueden analizar la continuidad y la modulación de las líneas de color, identificando cualquier inconsistencia.
- **Validación en Comparación con el Diseño Original:**
  - Los patrones de seguridad deben coincidir **exactamente con los modelos de referencia almacenados en bases de datos gubernamentales o institucionales**, asegurando que la tarjeta no haya sido alterada.

2.10.1.1.2 Beneficios Claves de la Impresión en Iris como Medida de Seguridad

- **Verificación Inmediata:** La autenticidad del documento puede ser confirmada a simple vista en **cuestión de segundos**.
- **Prevención de Falsificación:** Debido a su **dificultad de reproducción**, este elemento se convierte en una barrera contra la manipulación fraudulenta.
- **Facilidad de Validación:** No requiere el uso de equipos avanzados, lo que permite su aplicación en cualquier entorno de inspección.
- **Compatibilidad con Otros Elementos de Seguridad:** Puede combinarse con **tintas ópticamente variables, estructuras lenticulares y microtextos** para reforzar la autenticación del documento.

2.10.1.2 Guilloches: Diseños de Seguridad Avanzados

Los **guilloches** son patrones de seguridad avanzados formados por **movimientos lineales ornamentales** que crean curvas entrecruzadas extremadamente complejas. Estos diseños son generados mediante **software de seguridad especializado**, asegurando que cada patrón sea único e imposible de replicar con métodos de impresión convencionales.

Se trata de una medida de seguridad **altamente efectiva contra falsificaciones**, ya que cualquier intento de reproducción con sistemas de impresión digital o escáneres generará **distorsiones visibles** en los patrones originales.

1. Características de los Guilloches

✅ **Estructura Compleja y Única:**

- Los patrones están compuestos por **curvas entrecruzadas**, elaboradas de manera simultánea y alineadas con precisión micrométrica.
- **Cada tarjeta presenta un patrón de guilloches único**, lo que dificulta la copia exacta del diseño.

✅ **Generación mediante Software de Seguridad Especializado:**

- A diferencia de los patrones decorativos comunes, los guilloches de la tarjeta han sido creados con **algoritmos de generación aleatoria**, asegurando que no puedan ser replicados por software comercial.
- Solo **equipos de impresión de seguridad certificados** pueden reproducir estos patrones con la exactitud necesaria.

✅ **Ubicación Estratégica en la Tarjeta:**

- En el **anverso de la tarjeta**, los guilloches están integrados en el diseño de seguridad y pueden ser identificados con una inspección detallada.
- Se encuentran impresos en zonas clave del documento para dificultar intentos de alteración sin afectar la estructura del patrón.

✅ **Dificultad de Falsificación:**

- La intersección de líneas y la variación en la modulación del trazo hacen que cualquier intento de reproducción con impresoras digitales resulte en **líneas borrosas o inexactas**.
- No pueden ser clonados con escáneres ni reproducidos con técnicas de impresión convencionales debido a su **complejidad matemática y precisión gráfica**.

2. Métodos de Validación de los Guilloches

🔹 **Validación Visual a Simple Vista:**

- Los guilloches pueden ser inspeccionados directamente bajo luz normal, verificando la **claridad del patrón y su integración con el diseño de la tarjeta**.

🔹 **Validación con Lupa de Aumento:**

- Mediante el uso de una **lupa de 10x o superior**, es posible observar con detalle las **curvas entrecruzadas y la modulación del trazo**.
- Cualquier irregularidad o falta de alineación en el patrón puede ser señal de una falsificación.

🔹 **Validación con Dispositivos Electrónicos:**

- Algunos sistemas avanzados de control de identidad pueden realizar un **análisis óptico del patrón de guilloches**, comparándolo con la base de datos del diseño original.
- La verificación electrónica permite detectar **desviaciones en el trazo o inconsistencias en la estructura geométrica** del patrón.

3. Beneficios Claves del Uso de Guilloches en la Tarjeta

🔹 **Dificultad Extrema para su Reproducción:** Solo pueden ser generados por software especializado y replicados mediante impresoras de seguridad certificadas.

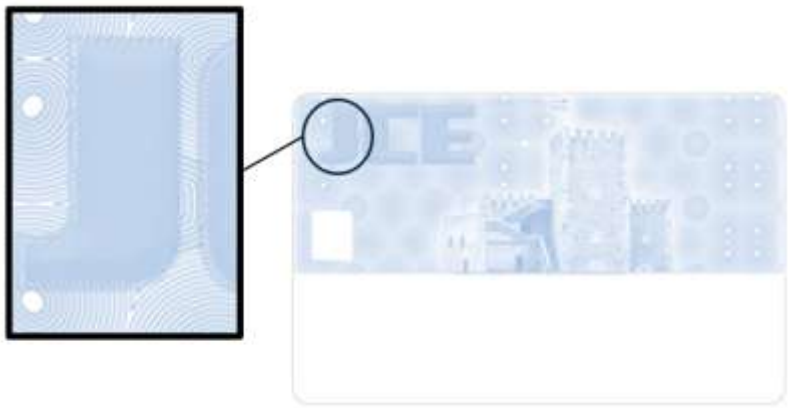
🔹 **Verificación Manual Sencilla:** Pueden ser autenticados con el uso de una lupa, sin necesidad de equipos sofisticados.

🔹 **Protección Contra Alteraciones:** Intentos de modificación o manipulación de los datos de la tarjeta distorsionarían el patrón original, evidenciando cualquier fraude.

🔹 **Compatible con Otros Elementos de Seguridad:** Puede integrarse con microtextos, tintas ópticamente variables y fondos de seguridad, reforzando la autenticidad del documento.

2.10.1.3 Elemento Numismático: Seguridad Óptica con Relieve Visual

Los elementos **numismáticos** son una medida de seguridad avanzada basada en un conjunto de **líneas finas y precisas que, a lo largo de su trayectoria, sufren deformaciones** cuidadosamente diseñadas para generar una **sensación de relieve o volumen tridimensional**.



Esta característica proporciona un efecto visual único que **no puede ser reproducido con impresoras convencionales o escáneres digitales**, ya que la disposición de las líneas es **altamente precisa y depende de técnicas de impresión de seguridad especializadas**.

1. Características del Elemento Numismático

✅ **Estructura Óptica Compleja y Única:**

- Compuesto por **líneas finas de alta precisión**, distribuidas en patrones específicos que generan un efecto visual tridimensional.
- El **relieve aparente** es creado mediante una combinación de **contraste, variaciones en el grosor del trazo y la alineación de líneas**.

✅ **Ubicación Estratégica en la Tarjeta:**

- En el **reverso de la tarjeta**, los elementos numismáticos están integrados en el diseño de seguridad, donde la **deformación de líneas crea un efecto de volumen visible en las letras "JCE"**.
- Ubicados en zonas de alto reconocimiento visual, asegurando que puedan ser verificados con facilidad.

✅ **Dificultad de Reproducción y Protección contra Falsificaciones:**

- La disposición irregular de las líneas y la modulación de su espesor dificultan su reproducción con **impresoras comerciales, escáneres o software de diseño gráfico**.
- Cualquier intento de copia con impresión digital **distorsiona el efecto óptico**, haciendo evidente la falsificación.

✅ **Resistencia a la Manipulación o Alteración:**

- Si el diseño es alterado o modificado de alguna manera, el **patrón de líneas perderá su coherencia óptica y dejará de generar el efecto de relieve**.
- **Cualquier intento de alteración manual o digital es fácilmente detectable**, ya que afectará la continuidad del patrón numismático.

2. Métodos de Validación del Elemento Numismático

🔹 **Validación Visual a Simple Vista:**

- Al observar la tarjeta bajo luz normal, se puede notar la **sensación de relieve en las letras JCE**, generada por la deformación de las líneas.
- Es posible inclinar la tarjeta ligeramente para **ver cómo las líneas cambian su percepción de volumen**.

🔹 **Validación con Lupa de Aumento:**

- Mediante el uso de una **lupa de 10x o superior**, se pueden examinar los detalles del patrón y verificar que las líneas presentan una **deformación progresiva y no artificial**.
- Cualquier intento de falsificación resultará en **líneas discontinuas, sin la fluidez característica del diseño original**.

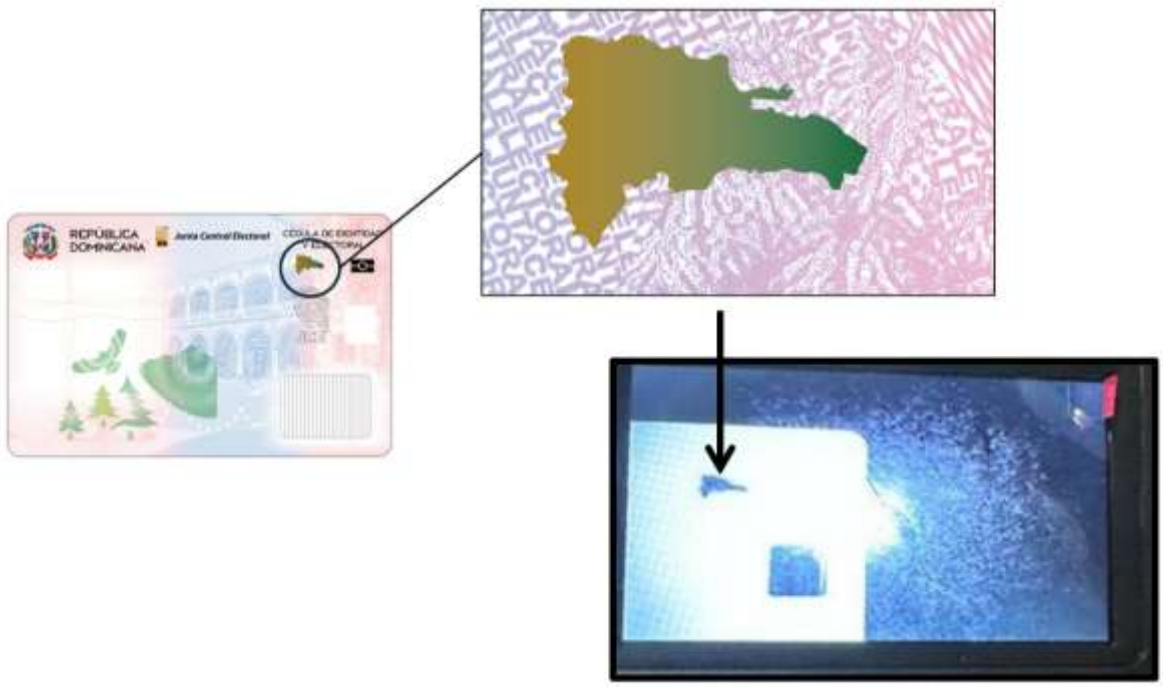
🔹 **Validación con Dispositivos Electrónicos:**

- Algunos escáneres de seguridad pueden **analizar el diseño numismático y compararlo con la base de datos del documento original**, asegurando que la tarjeta no ha sido alterada.
- La verificación electrónica permite detectar **irregularidades en la disposición de las líneas y la estructura del patrón visual**.

3. Beneficios Claves del Uso de Elementos Numismáticos en la Tarjeta

- **Autenticación Inmediata:** Puede verificarse fácilmente con una inspección visual rápida, sin necesidad de herramientas especializadas.
- **Dificultad Extrema para su Reproducción:** Solo puede generarse con equipos de impresión de seguridad especializados.
- **Protección Contra Falsificación:** Si el patrón es copiado o impreso digitalmente, **pierde su efecto de relieve**, facilitando su detección.
- **Complemento con Otras Medidas de Seguridad:** Puede combinarse con **microtextos, tintas ópticamente variables y estructuras lenticulares** para reforzar la autenticidad del documento.

2.10.1.4 Tinta Ópticamente Variable (OVI): Seguridad Visual Avanzada



La **tinta ópticamente variable (OVI - Optically Variable Ink)** es una de las medidas de seguridad más avanzadas utilizadas en documentos de identidad y billetes de alta seguridad. Su característica principal es que **cambia de color dependiendo del ángulo de incidencia de la luz y el ángulo de observación**, lo que la hace extremadamente difícil de falsificar mediante métodos de impresión convencionales.

1. Características de la Tinta Ópticamente Variable (OVI)

✅ **Efecto de Variabilidad de Color Según el Ángulo de Observación:**

- La tinta OVI contiene **finas partículas de interferencia óptica** que reflejan y refractan la luz de manera diferente según el ángulo de visión.
- En la muestra presentada, la tinta está aplicada en el **contorno del mapa de la República Dominicana**, generando un **cambio de color de Verde a Rosa** cuando se observa desde distintos ángulos.
- Este cambio de color es **inmediato y perceptible a simple vista**, lo que permite una validación rápida del documento.

✅ **Protección Contra Falsificación:**

- No puede reproducirse con **impresoras de inyección de tinta, tóner láser o fotocopiadoras**.
- Su aplicación requiere **equipos de impresión especializados y técnicas de deposición de tinta de alta seguridad**, imposibles de replicar con medios convencionales.
- **Cualquier intento de imitación resultará en colores estáticos que no presentan variación con el ángulo de observación**.

✅ **Resistencia y Durabilidad:**

- La tinta ópticamente variable está formulada para **resistir el desgaste por fricción, exposición a luz UV y agentes químicos**, garantizando su integridad a lo largo de la vida útil del documento.
- No se degrada con el tiempo y permanece funcional incluso tras años de uso intensivo.

✅ **Compatibilidad con Tecnología de Validación Infrarroja (IR):**

- Además del efecto de cambio de color visible, esta tinta tiene propiedades que la hacen **detectable bajo luz infrarroja (IR)**.
- En el caso de esta muestra, el **contorno del mapa de la República Dominicana permanece visible a la radiación IR**, lo que añade una capa adicional de seguridad para verificación en entornos de alta seguridad.

2. Métodos de Validación de la Tinta Ópticamente Variable

- **Validación Visual a Simple Vista:**
  - **Inclinando la tarjeta en diferentes ángulos**, se debe observar el cambio de color de **Verde a Rosa**, lo que confirma la autenticidad del documento.
  - La transición de color debe ser **suave y gradual**, sin interrupciones ni cambios abruptos en el tono.
- **Validación con Luz Infrarroja (IR):**
  - Mediante el uso de un **dispositivo de verificación IR (Dispositivo No. 4)**, se coloca la tarjeta debajo de una pantalla con luz infrarroja.
  - En la imagen proyectada, el **contorno del mapa de la República Dominicana permanecerá visible**, lo que confirma la presencia de la tinta OVI con propiedades IR.
- **Validación con Equipos de Control de Documentos de Seguridad:**
  - En entornos de alta seguridad, como aeropuertos y bancos, se utilizan **espectrofotómetros y escáneres de documentos de alta resolución** para analizar la respuesta óptica de la tinta y verificar su autenticidad.
  - Estos equipos pueden medir la longitud de onda exacta de los cambios de color y compararla con los valores de referencia del documento original.

3. Beneficios Claves de la Tinta Ópticamente Variable en la Tarjeta

- **Prevención de Falsificación:** Su producción es altamente especializada y no puede ser replicada con impresoras convencionales.
- **Verificación Rápida y Efectiva:** Puede validarse fácilmente con una inspección visual o con luz IR sin necesidad de herramientas costosas.
- **Alta Durabilidad:** No se desgasta con el tiempo ni con el uso frecuente, asegurando la integridad de la tarjeta.
- **Compatibilidad con Otras Tecnologías de Seguridad:** Puede combinarse con **estructuras lenticulares, microtextos y guilloches**, reforzando la autenticidad del documento.
- **Uso en Entornos de Alta Seguridad:** Cumple con estándares utilizados en pasaportes electrónicos, billetes de banco y documentos de identidad oficiales.

2.10.1.5 Elemento Difractivo Ópticamente Variable: Seguridad Avanzada Integrada en la Fotografía del Titular

El **elemento difractivo ópticamente variable (DOV - Diffractive Optically Variable Element)** es una tecnología de seguridad avanzada diseñada para impedir la falsificación y la manipulación del documento. Este elemento se encuentra **situado en el interior de la tarjeta**, integrándose parcialmente en la **zona de la fotografía del titular y en los textos**, lo que garantiza su protección contra intentos de alteración o sustitución de imagen.

El **uso de elementos difractivos en documentos de identidad** ha sido adoptado a nivel internacional en pasaportes electrónicos, tarjetas de identificación y billetes de banco debido a su capacidad para proporcionar **verificación visual inmediata**, sin necesidad de dispositivos electrónicos adicionales.

¿Cómo Funciona el Elemento Difractivo?

Este elemento de seguridad está compuesto por **microestructuras ópticas grabadas con precisión en el material de la tarjeta**, que generan efectos de **interferencia y dispersión de la luz**. Dependiendo del ángulo de observación y la iluminación, el usuario puede ver:

- **Cambios de color dinámicos**, que varían con la inclinación del documento.
- **Patrones en movimiento o desplazamiento óptico**, imposibles de replicar con impresoras convencionales.
- **Textos o imágenes ocultas**, visibles solo bajo determinadas condiciones de luz.
- **Efectos holográficos en la zona de la fotografía**, asegurando que la imagen no pueda ser removida o reemplazada sin evidentes signos de manipulación.

Este sistema es una medida de **doble protección**, ya que no solo resguarda la identidad del titular evitando la alteración de la foto, sino que también permite **una validación rápida por parte de las autoridades**.

Ubicación y Aplicación en la Tarjeta

El elemento difractivo **se encuentra en el anverso de la tarjeta**, ocupando **parcialmente la zona de la fotografía del titular**. Esta ubicación estratégica permite:

- **Evitar intentos de sustitución de la foto**, ya que cualquier intento de remoción dañaría la estructura del difractivo.
- **Facilitar la verificación manual y electrónica**, ya que el efecto óptico puede ser detectado a simple vista o con equipos de inspección avanzados.
- **Complementar otras medidas de seguridad de la tarjeta**, como microtextos, guilloches y estructuras lenticulares, reforzando la autenticidad del documento.

Niveles de Seguridad Integrados en el Elemento Difractivo

Este **elemento de seguridad opera en dos niveles diferentes**, proporcionando una doble capa de autenticación:

- **Nivel 2 - Validación con Instrumentos Simples (Luz UV, Lupas, Inclinación Visual)**
  - **Efectos de cambio de color** visibles a simple vista al inclinar la tarjeta.
  - **Textos o imágenes ocultas** que solo se revelan con la iluminación adecuada.
  - **Interacción con otras medidas de seguridad de la fotografía**, como tintas ópticamente variables o microtextos.
- **Nivel 3 - Seguridad Forense y Validación en Laboratorio**
  - **Estructuras de nanotextos y micrograbados**, visibles solo con microscopios de alta resolución.
  - **Elementos de validación por láser**, que emiten respuestas ópticas específicas al ser expuestos a ciertos dispositivos de seguridad.
  - **Propiedades de dispersión de la luz bajo espectros infrarrojos y ultravioletas**, permitiendo su autenticación en entornos de alta seguridad.

Beneficios Claves del Elemento Difractivo Ópticamente Variable

- ✓ **Verificación Inmediata:** Su efecto visual permite confirmar la autenticidad de la tarjeta en cuestión de segundos, sin necesidad de equipos especializados.
- ✓ **Protección de la Fotografía del Titular:** Su integración parcial con la imagen impide intentos de alteración, falsificación o reemplazo de la fotografía.
- ✓ **Alta Resistencia a Manipulación:** Al estar fusionado en la estructura de la tarjeta, no puede ser removido ni modificado sin dejar evidencia visible de manipulación.
- ✓ **Dificultad de Falsificación:** Solo puede ser producido mediante **tecnologías ópticas especializadas**, lo que impide su replicación con medios comerciales.
- ✓ **Compatibilidad con Verificación Electrónica:** Puede ser analizado por lectores de identidad y equipos de inspección óptica en aeropuertos, bancos y sistemas de control fronterizo.

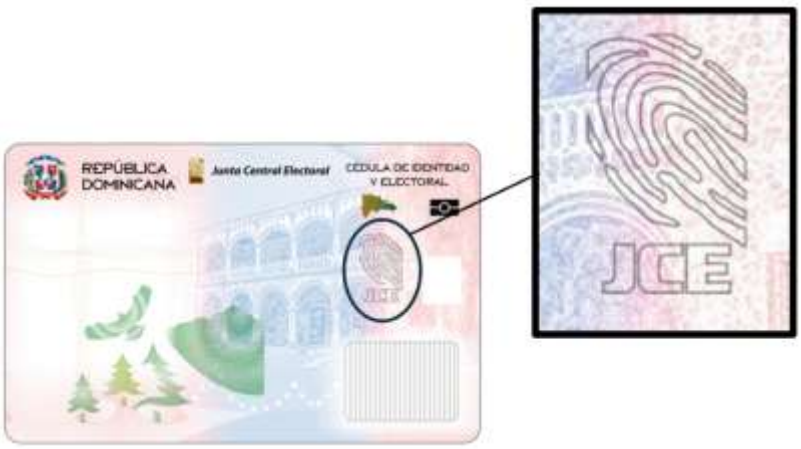
Importancia del Elemento Difractivo en la Seguridad del Documento

El **uso de tecnología difractiva en documentos de identidad** se ha convertido en un estándar internacional, presente en pasaportes electrónicos y sistemas de identidad digital avanzada. **Su incorporación en la zona de la fotografía del titular es una estrategia efectiva para evitar la manipulación del documento**, garantizando que cualquier intento de modificación resulte en la destrucción del diseño de seguridad.

Este tipo de tecnología **permite la autenticación inmediata de la tarjeta, incluso en entornos de control rápido, como aeropuertos o puntos de inspección migratoria**, donde los oficiales pueden verificar visualmente su validez en segundos.

Numeración de la Tarjeta: La tarjeta se identifica individualmente con un número de serie de tarjeta pre personalizado en grabado láser.

2.10.1.6 Elementos Táctiles en Alto o Bajo Relieve y Acabado Mate



Los **elementos táctiles en alto o bajo relieve**, junto con los acabados mate, representan una de las medidas de seguridad más efectivas en la validación de documentos de identidad, permitiendo **una autenticación rápida y sin necesidad de dispositivos electrónicos**. Estos elementos están diseñados para ser **percibidos al tacto**, lo que facilita la detección de intentos de manipulación o falsificación.

En la tarjeta, los elementos táctiles se encuentran estratégicamente **integrados en el anverso del documento**, proporcionando una experiencia de verificación **tanto visual como táctil**. Además, la tarjeta está fabricada con **capas sensibles al láser**, lo que permite que, durante el proceso de personalización, el grabado genere **relieves perceptibles al tacto**, reforzando aún más la seguridad del documento.

1. Características de los Elementos Táctiles y Relieves Personalizados

✅ **Presencia de Relieves en la Superficie de la Tarjeta**

- Elementos en **alto y bajo relieve**, perceptibles al pasar los dedos sobre la superficie del documento.
- Aplicados en zonas estratégicas para garantizar una autenticación manual rápida.

✅ **Personalización en Relieve con Grabado Láser**

- Durante el proceso de emisión de la tarjeta, la personalización mediante **láser de alta precisión** permite que **el nombre del titular y el número de la tarjeta sean grabados con relieve perceptible al tacto**.

- Este método impide la modificación o reimpresión fraudulenta de la información, ya que cualquier alteración sería visible y detectable.

✅ **Acabado Mate y Diferenciación de Texturas**

- Algunas zonas de la tarjeta presentan **un acabado mate**, contrastando con otras áreas brillantes o en relieve, lo que proporciona una capa adicional de seguridad.
- La combinación de diferentes texturas hace que cualquier intento de falsificación sea **altamente visible**, ya que los patrones mate-relieve no pueden ser replicados con impresoras comerciales.

✅ **Integración con la Estructura Multicapa de la Tarjeta**

- Los elementos táctiles no son simples impresiones, sino que están **integrados en la estructura de policarbonato** de la tarjeta.
- Al estar fusionados mediante **laminación en caliente**, **no pueden ser removidos o alterados sin destruir el documento**.

✅ **Alta Durabilidad y Resistencia**

- Diseñados para **resistir el desgaste** por uso continuo, garantizando que los elementos táctiles permanezcan intactos durante la vida útil de la tarjeta.
- No se degradan con la fricción, la humedad ni la exposición a productos químicos.

2. Métodos de Verificación de los Elementos Táctiles y Relieves

- **Validación Táctil Manual:**
  - **Pasando los dedos sobre la tarjeta**, se pueden identificar las diferencias de relieve y textura, asegurando que los datos grabados sean genuinos.
  - En el caso de los nombres y números en relieve, se puede sentir **el grabado profundo generado por láser**.
- **Validación Visual a Simple Vista:**
  - Se puede observar cómo las áreas en relieve generan **sombras y reflejos diferentes** dependiendo del ángulo de iluminación.
  - El contraste entre los acabados mate y los relieves permite detectar intentos de alteración.
- **Validación con Luz Rasante:**
  - Al colocar una fuente de luz en un **ángulo bajo**, los relieves proyectan sombras que permiten ver su profundidad y estructura.
  - Este método es útil en controles fronterizos y entidades bancarias para verificar la autenticidad del documento.
- **Validación con Equipos de Seguridad Avanzados:**
  - Algunos dispositivos de verificación biométrica pueden escanear la superficie de la tarjeta y detectar la presencia de relieves personalizados.
  - Sistemas de detección óptica pueden comparar los patrones de relieve con la base de datos del documento original.

3. Beneficios Claves de los Elementos Táctiles y Relieves Personalizados

- **Autenticación Rápida y Sin Equipos Especiales:** Puede ser verificada de forma **manual e inmediata**, sin necesidad de dispositivos electrónicos.
- **Dificultad de Falsificación:** Su integración en el material de la tarjeta impide que pueda ser **alterada, removida o replicada con impresoras convencionales**.
- **Durabilidad Extrema:** Los elementos táctiles y los grabados en relieve no se desgastan con el uso, manteniendo su integridad durante **toda la vida útil del documento**.
- **Integración con Otras Tecnologías de Seguridad:** Puede combinarse con **tintas ópticamente variables, estructuras lenticulares y guilloches**, fortaleciendo aún más la protección de la tarjeta.

- **Protección Contra Modificación de Datos:** Como el nombre y el número de tarjeta están grabados en relieve mediante láser, cualquier intento de alteración **destruiría la estructura del documento**, haciéndolo inservible.

2.10.2 Nivel 2 - Características de Seguridad que Requieren el Uso de Instrumentos Simples para su Detección

Las tarjetas incorporan una serie de **elementos de seguridad avanzados** que no son visibles a simple vista y requieren **instrumentos simples** como **lupas de aumento y lámparas de luz ultravioleta (UV)** para su verificación. Estas medidas están diseñadas para proporcionar una capa adicional de autenticación, permitiendo que las entidades encargadas de la validación del documento puedan detectar intentos de falsificación mediante **métodos de inspección más detallados**.

1. Elementos de Seguridad Detectables con Lupa de Aumento

- **Microtextos de Alta Precisión**
  - Son textos extremadamente pequeños, insertados en áreas estratégicas del diseño de la tarjeta, que solo pueden leerse con una **lupa de aumento de 10x o superior**.
  - Pueden estar presentes en **fondos de seguridad, imágenes del documento o en los bordes de los caracteres principales**.
  - Cualquier intento de falsificación con impresoras convencionales **resulta en textos borrosos o ilegibles**, facilitando la detección de documentos fraudulentos.
- **Impresión Positiva y Negativa**
  - Algunos textos en microimpresión están diseñados en **impresión positiva (tinta sobre fondo claro)** y otros en **impresión negativa (fondo de tinta dejando el texto en blanco)**.
  - Esta variación hace que cualquier intento de reproducción por métodos convencionales **genere inconsistencias en el contraste y legibilidad**.
- **Guilloches y Tramas de Seguridad**
  - Patrones extremadamente complejos, formados por líneas entrecruzadas con variaciones en su espesor y continuidad, diseñadas con software de seguridad.
  - Bajo una lupa, se pueden observar las **curvas de alta precisión**, imposibles de replicar con impresoras comerciales.

- Si se intenta falsificar, las líneas se verán **pixeladas, desalineadas o con bordes irregulares**.

- **Errores Deliberados en el Diseño**
  - Pequeñas alteraciones insertadas intencionalmente en el diseño, visibles solo con lupa, que permiten identificar si el documento es auténtico.
  - Estos errores están integrados en el fondo del documento o dentro de los microtextos, dificultando su reproducción sin conocimiento del diseño original.

2. Elementos de Seguridad Detectables con Lámparas de Luz Ultravioleta (UV)

- **Tintas Fluorescentes Bajo Luz UV**
  - Elementos gráficos impresos con **tintas invisibles a simple vista**, pero que se iluminan al exponerse a **luz ultravioleta (UV)**.
  - En la tarjeta, estos elementos pueden incluir:
    - **Símbolos de seguridad nacionales**.
    - **Sellos o firmas ocultas**.
    - **Microtextos UV** que solo aparecen bajo la iluminación correcta.
  - La presencia de estos elementos garantiza que el documento sea auténtico y no haya sido alterado.

- **Patrones de Seguridad UV en el Fondo de la Tarjeta**
  - Algunas áreas del diseño contienen patrones impresos con **tintas de fluorescencia variable**, que pueden cambiar de color o mostrar efectos dinámicos bajo luz UV.
  - Si el documento es falsificado, estos patrones no estarán presentes o tendrán una apariencia irregular.

- **Tinta Invisible con Propiedades de Seguridad**
  - Algunas zonas de la tarjeta contienen **elementos impresos con tintas que solo pueden verse bajo luz UV**, como números de serie ocultos o códigos de verificación.
  - Estas marcas de seguridad permiten una autenticación en **entornos de alta seguridad**, como aeropuertos, bancos y controles fronterizos.

- **Elementos con Reacción a Diferentes Espectros de Luz**
  - Algunas tintas pueden mostrar un **doble efecto de fluorescencia** cuando se exponen a distintas intensidades de luz ultravioleta.
  - Estos efectos pueden incluir **cambios de color, aparición de nuevas formas o superposición de imágenes ocultas**.

3. Métodos de Validación de las Características de Seguridad

- **Validación con Lupa de Aumento (10x o superior):**
  - Permite detectar **microtextos, guilloches, patrones de seguridad e impresión en positivo y negativo**.
  - Cualquier irregularidad en la alineación o definición del texto puede evidenciar intentos de falsificación.
- **Validación con Lámparas de Luz UV:**
  - Se utiliza para detectar **tintas fluorescentes, patrones ocultos y microtextos invisibles**.
  - La autenticidad del documento se confirma si los elementos de seguridad aparecen de manera clara y uniforme.
- **Comparación con un Documento Original:**
  - En caso de sospecha, se puede comparar con una tarjeta legítima para verificar la presencia y disposición de los elementos de seguridad.
- **Verificación con Equipos de Inspección Electrónica:**
  - Algunos sistemas de seguridad utilizan escáneres UV y microscopios digitales para validar las propiedades ópticas de la tinta y los elementos gráficos del documento.

4. Beneficios Claves de Estas Medidas de Seguridad

✓ **Dificultad de Falsificación:** Todos estos elementos requieren **técnicas de impresión especializadas** que no pueden replicarse con impresoras comerciales o métodos digitales.

✓ **Verificación Rápida y Efectiva:** Permiten la autenticación manual del documento en **cuestión de segundos**.

✓ **Alta Durabilidad:** Estos elementos de seguridad **no se degradan con el tiempo**, garantizando su funcionalidad durante la vida útil del documento.

✓ **Compatibilidad con Sistemas de Control de Identidad:** Pueden ser detectados en **aeropuertos, bancos, y puntos de control migratorio**, facilitando la validación del documento en múltiples entornos.

Las características de seguridad que requieren **lupas de aumento y lámparas UV** para su detección son una **herramienta clave en la prevención de fraudes y falsificaciones**. Al combinar **microtextos, guilloches, tintas invisibles y patrones de seguridad UV**, la tarjeta se convierte en un **documento de identidad prácticamente infalsificable**, protegiendo la información del titular y asegurando su autenticidad en procesos de validación manual y digital.

2.10.2.1 Microtextos: Seguridad Invisible a Simple Vista

Los **microtextos** son una de las medidas de seguridad más eficaces en documentos de alta seguridad, ya que consisten en textos extremadamente pequeños, imposibles de detectar sin el uso de una **lupa de aumento de 10x o superior**. Este tipo de impresión no solo protege contra intentos de falsificación, sino que también permite **una validación precisa** mediante inspección visual con herramientas ópticas simples.

En la tarjeta, los **microtextos en impresión positiva y negativa** están ubicados en el **reverso del documento**, y contienen la leyenda **"JUNTACENTRALELECTORAL"**, grabada con una tipografía de seguridad especial que impide su reproducción con métodos de impresión tradicionales.

¿Cómo Funcionan los Microtextos?

Los microtextos son líneas de texto que se imprimen en un tamaño tan reducido que **a simple vista parecen líneas continuas o patrones decorativos**. Sin embargo, cuando se observan a través de una lupa de aumento, se revelan claramente como caracteres perfectamente formados.

Existen dos tipos principales de microtextos integrados en la tarjeta:

- **Microtexto en Impresión Positiva**
  - Letras en tinta oscura sobre un fondo claro.
  - Se observa como un texto normal, pero en tamaño extremadamente reducido.
  - Su dificultad de reproducción radica en la **precisión de los trazos y la alineación exacta de cada carácter**.
- **Microtexto en Impresión Negativa**
  - Letras en blanco sobre un fondo impreso.
  - Más difícil de falsificar, ya que el fondo debe mantenerse uniforme sin interrupciones en los espacios negativos.
  - Cualquier error en la impresión crea irregularidades visibles al observarlo con lupa.

Ubicación y Métodos de Validación

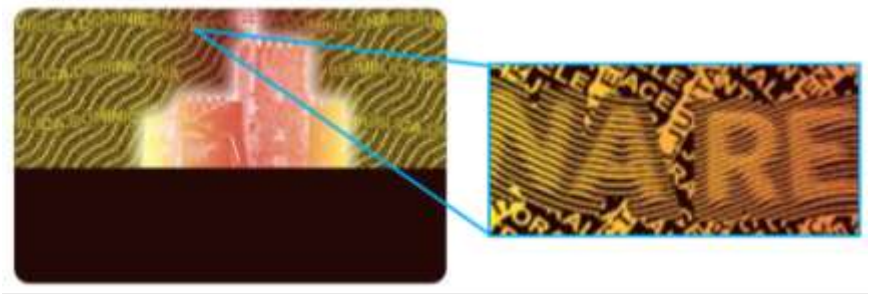
📌 **Ubicación en la Tarjeta:**

- Los microtextos en positivo y negativo están impresos en el **reverso de la tarjeta**.
- Se encuentran en zonas estratégicas que facilitan su inspección con lupa, sin alterar la estética general del documento.

🔍 **Método de Validación con Lupa:**

- **Colocar la lupa de aumento sobre la tarjeta.**
- **Buscar las áreas donde se han impreso los microtextos.**
- **Observar la leyenda "JUNTACENTRALELECTORAL" y verificar que los caracteres sean claros y definidos.**
- **Confirmar la presencia de microtextos en positivo y negativo, verificando que no haya distorsiones o interrupciones en el patrón.**

UV Malla de fondo en microtextos: En el reverso de la tarjeta se cuenta con un tramado con microtextos de fondo.



2.10.2.2 Microtextos con Tintas Fluorescentes: Seguridad Bajo Luz UV

Algunos microtextos pueden estar impresos con **tintas de fluorescencia invisible**, lo que significa que **solo pueden verse bajo luz ultravioleta (UV)**. Esta característica añade una **capa extra de protección**, permitiendo la autenticación del documento en controles de seguridad de alto nivel.

💡 **Validación con Lámpara UV:**

- **Exponer la tarjeta a una fuente de luz ultravioleta.**
- **Observar la aparición de microtextos fluorescentes ocultos en áreas estratégicas del diseño.**
- **Verificar que los caracteres sean uniformes y sin alteraciones, asegurando la autenticidad del documento.**

¿Por Qué los Microtextos Son Difíciles de Falsificar?

✓ **Requieren impresión de alta precisión:** Solo pueden producirse con **prensas de impresión especializadas**, imposibles de replicar con impresoras láser o de inyección de tinta.

✓ **Invisibles a simple vista:** Sin una lupa o un microscopio digital, los microtextos parecen líneas continuas, lo que evita su identificación por falsificadores.

✓ **Cualquier alteración genera distorsiones visibles:** Si alguien intenta copiar o modificar la tarjeta, los caracteres del microtexto se vuelven borrosos o desalineados, facilitando la detección de un documento fraudulento.

Importancia de los Microtextos en la Seguridad del Documento

- **Validación Rápida y Accesible:** No se necesitan equipos costosos para verificar su autenticidad, solo una **lupa de aumento**.
- **Dificultad de Copia:** Su complejidad técnica impide que sean replicados con métodos de impresión estándar.
- **Resistencia a Manipulación:** Si la tarjeta es alterada, los microtextos pierden su alineación y claridad, dejando evidencia de falsificación.

- **Protección contra Copias Digitales:** No pueden reproducirse con escáneres, cámaras o impresoras convencionales.

Los **microtextos en impresión positiva, negativa y fluorescente** son una de las medidas de seguridad más efectivas en la lucha contra la falsificación de documentos. Su integración en la tarjeta permite una **verificación rápida, precisa y accesible** mediante una simple lupa de aumento o luz ultravioleta.

Errores Deliberados en el Documento: Medida de Seguridad Invisible

Los **errores deliberados** son una de las medidas de seguridad más sofisticadas utilizadas en documentos de alta seguridad. Se trata de **pequeñas alteraciones intencionales en el diseño del documento**, colocadas estratégicamente en áreas específicas que solo el **emisor del documento conoce**.

Estos errores no pueden ser detectados a simple vista y requieren **una lupa de aumento** para ser identificados correctamente. Su propósito es proporcionar un método de autenticación exclusivo para entidades emisoras y autoridades de validación, impidiendo la reproducción precisa del documento por parte de falsificadores.

¿Cómo Funcionan los Errores Deliberados?

- **Ubicación Estratégica y Conocimiento Exclusivo del Emisor**
  - Estos errores están ocultos en **zonas específicas del documento** que no interfieren con el diseño general.
  - **No son visibles a simple vista**, por lo que solo pueden ser detectados con herramientas ópticas.
  - **Solo el organismo emisor del documento conoce su ubicación exacta**, lo que permite una validación rápida sin revelar su existencia al público general.
- **Errores Mínimos Pero Deliberados**
  - En la tarjeta, uno de los errores deliberados es una **letra "T" invertida**, que puede visualizarse solo con lupa y **ubicándola en la posición correcta** indicada en el diseño de seguridad.
  - Otros errores pueden incluir **ligeras modificaciones en patrones de guilloches, microtextos, símbolos o numeraciones**, haciendo que cualquier falsificación sea fácilmente identificable.
- **Imposibilidad de Reproducción Exacta**

- Dado que estos errores **no siguen un patrón público ni estandarizado**, un falsificador no puede replicarlos con precisión.
- Si alguien intenta copiar la tarjeta sin conocer la ubicación de estos errores, la falsificación no pasará una verificación detallada con lupa.

Método de Validación de los Errores Deliberados

📌 **Ubicación en la Tarjeta:**

- Los errores están **colocados en áreas estratégicas del diseño**, invisibles a simple vista.
- Solo pueden ser detectados si se **conoce su posición exacta y se utiliza una lupa de aumento**.

🔍 **Proceso de Verificación con Lupa de Aumento:**

- **Colocar la lupa de aumento sobre la zona específica indicada en el documento.**
- **Observar atentamente hasta identificar la letra "T" invertida u otro error deliberado.**
- **Comparar con un documento original para verificar que el error se encuentra en el mismo lugar.**
- **Si el error está ausente o mal replicado, el documento es fraudulento.**

Beneficios Claves de los Errores Deliberados en el Documento

✓ **Autenticación Exclusiva:** Solo las autoridades emisoras y de validación conocen su ubicación exacta, lo que dificulta su detección por falsificadores.

✓ **Imposible de Replicar:** Dado que no se publica su existencia ni ubicación en documentos oficiales, una copia falsa nunca podrá replicarlos con exactitud.

✓ **Verificación Rápida y Segura:** No requiere tecnología avanzada; una simple lupa es suficiente para autenticar la tarjeta en cuestión de segundos.

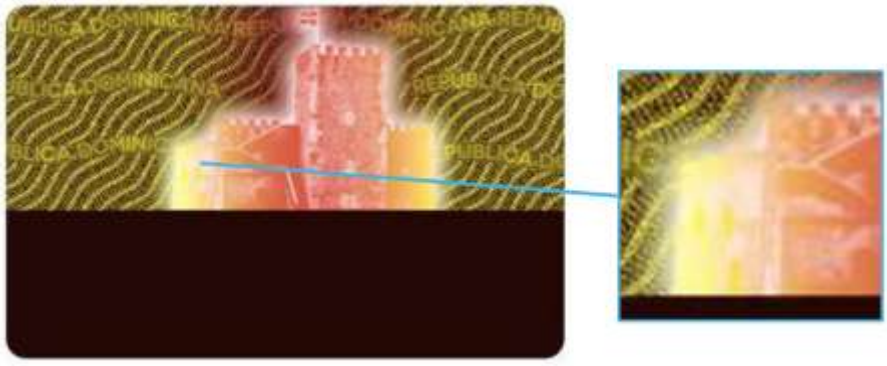
✓ **Dificultad de Manipulación:** Si alguien intenta modificar el documento, la eliminación o alteración de estos errores será **altamente visible**.

✓ **Complemento a Otras Medidas de Seguridad:** Se integra con **microtextos, guilloches y patrones de impresión especializada**, reforzando la protección del documento.

Los **errores deliberados en el documento** son una **capa de seguridad invisible pero extremadamente efectiva**. Al ser **imperceptibles a simple vista** y estar ubicados en

posiciones desconocidas para el público, se convierten en una barrera infranqueable para falsificadores.

2.10.2.3 Tinta Invisible con Fluorescencia UV e Impresión Arcoíris



La tarjeta incorpora una combinación de **tinta invisible fluorescente bajo luz ultravioleta (UV) y técnicas avanzadas de impresión arcoíris**, lo que proporciona una **doble capa de seguridad visual**. Estas características permiten una **autenticación rápida y confiable** mediante inspección visual y el uso de dispositivos UV, dificultando significativamente cualquier intento de falsificación.

Este sistema de seguridad combina tres tecnologías clave:

- **Tinta Invisible Fluorescente**
- **Impresión Arcoíris Visible (Offset Multicolor)**
- **Impresión Arcoíris Invisible (Detectable Solo con Luz UV)**

1. Tinta Invisible con Fluorescencia UV

- **Protección Invisible a Simple Vista**
  - La tinta fluorescente es **invisible bajo luz normal**, pero al exponer la tarjeta a **luz ultravioleta (UV)**, los elementos de seguridad impresos se hacen visibles de inmediato.
  - Permite la **inclusión de códigos de verificación ocultos, sellos de autenticidad y patrones de seguridad únicos**.
- **Dificultad de Falsificación**

- No puede ser reproducida con **impresoras convencionales, fotocopias o técnicas de escaneo digital**.
- Si una tarjeta es falsificada, los elementos en tinta invisible **no estarán presentes o no responderán correctamente a la luz UV**.

◆ **Ubicación en la Tarjeta**

- La muestra contiene **impresión arcoíris invisible en el reverso**, la cual solo es visible al exponerla a luz UV.
- Bajo luz UV, **el color de la impresión cambia de amarillo a rojo y viceversa**, proporcionando una autenticación instantánea.

2. Impresión Arcoíris Visible (Offset Multicolor)

◆ **Cambio Gradual de Color a Simple Vista**

- En el **anverso de la tarjeta**, la impresión arcoíris es visible a simple vista y **cambia de color de rojo a azul y viceversa** al inclinar el documento.
- Utiliza una **combinación de tintas de seguridad y técnicas de impresión offset en capas**, lo que genera una transición de colores suave y sin interrupciones.

◆ **Propiedades de Seguridad Contra Falsificación**

- No puede ser reproducida con **impresoras láser, inyección de tinta o fotocopias**, ya que requiere **equipos de impresión especializados** con alineación milimétrica de las tintas.
- Si se intenta copiar con métodos digitales, la transición de colores será **inconsistente y presentará saltos bruscos entre tonalidades**.

3. Impresión Arcoíris Invisible (Detectable Solo con Luz UV)

◆ **Segunda Capa de Protección con Validación UV**

- A diferencia de la impresión arcoíris visible, la impresión arcoíris invisible **no puede verse bajo luz normal**.
- Solo se activa al exponer la tarjeta a **luz UV con la lámpara identificada con el número 2**.

◆ **Cambio de Color Bajo Luz UV**

- En el reverso de la tarjeta, la impresión arcoíris invisible **cambia de amarillo a rojo y viceversa** bajo luz UV.

- Esta propiedad permite una **autenticación rápida** en controles de seguridad sin la necesidad de equipos costosos.

🔹 **Ubicación Estratégica**

- Se encuentra en zonas clave del reverso de la tarjeta, protegidas contra intentos de alteración o eliminación.
- Si la impresión ha sido manipulada, el efecto arcoíris UV no funcionará correctamente, alertando sobre posibles fraudes.

4. Métodos de Validación de la Tinta Invisible y la Impresión Arcoíris

📌 **Validación Visual de la Impresión Arcoíris Visible:**

✅ Inclinar la tarjeta y verificar el **cambio de color de rojo a azul** en el anverso.

✅ Confirmar que la transición sea **suave y sin saltos abruptos de color**.

💡 **Validación con Luz UV para la Impresión Arcoíris Invisible:**

✅ Colocar la tarjeta bajo una **lámpara de luz UV**.

✅ Observar la impresión en el reverso y verificar que **cambie de amarillo a rojo y viceversa**.

✅ Si la impresión no responde a la luz UV, la tarjeta podría ser fraudulenta.

5. Beneficios Claves de la Tinta Invisible y la Impresión Arcoíris

✓ **Dificultad Extrema de Falsificación:** Ambas tecnologías requieren **impresión offset de seguridad**, inaccesible para falsificadores.

✓ **Verificación Rápida y Confiable:** Puede autenticarse fácilmente con **inspección visual y lámparas UV**.

✓ **Protección Doble:** La combinación de **impresión visible y tinta invisible UV** crea un nivel de seguridad adicional.

✓ **Resistencia al Desgaste:** La impresión no se degrada con el tiempo ni con el uso frecuente.

✓ **Compatible con Otros Métodos de Seguridad:** Se complementa con **microtextos, guilloches y tintas ópticamente variables** para reforzar la autenticidad del documento.

La combinación de **tinta invisible fluorescente, impresión arcoíris visible e impresión arcoíris invisible** es una de las tecnologías más avanzadas de protección contra falsificaciones. Estas características **permiten verificar rápidamente la autenticidad de la tarjeta**, ya sea a simple vista o con luz UV, dificultando su reproducción ilegal.

2.10.2.4 Fondos de Seguridad Visibles e Invisibles en la Zona de la Fotografía

Los **fondos de seguridad visibles e invisibles en la zona de la fotografía** representan una de las medidas de protección más avanzadas en documentos de identidad. Su propósito principal es **detectar cualquier intento de manipulación o sustitución de la imagen del titular**, garantizando que la fotografía original no pueda ser alterada sin dejar evidencia visible.

Este sistema combina **dos niveles de seguridad**:

- **Fondo de seguridad visible, integrado con microtextos y patrones de líneas continuas.**
- **Fondo de seguridad invisible, solo visible bajo luz ultravioleta (UV).**

Estos elementos están diseñados para proporcionar una autenticación confiable y de fácil verificación, permitiendo a las autoridades validar la autenticidad del documento en cuestión de segundos.

1. Fondo de Seguridad Visible en la Zona de la Fotografía

- **Integración con Microtextos de Alta Precisión**
  - En la zona de la fotografía se encuentra un **fondo de seguridad visible**, compuesto por una red de **microtextos**.
  - Este patrón de seguridad incluye la leyenda **"CEDULADEIDENTIDADYELECTORAL"**, impresa con un tamaño tan reducido que solo puede leerse con **una lupa de aumento (dispositivo identificado con el número 1).**
  - Además, el fondo está complementado con un **patrón de líneas continuas con diseño de seguridad**, lo que impide su reproducción con impresoras convencionales.
- **Dificultad de Manipulación**
  - Si alguien intenta **reemplazar la fotografía del titular**, el fondo de seguridad se dañará o desaparecerá, haciendo evidente la alteración.
  - Los microtextos y el patrón de líneas están impresos con técnicas de **registro preciso**, por lo que cualquier intento de replicación con métodos digitales generará **desenfoques, distorsiones o pérdidas de detalle**.
- **Método de Validación con Lupa**

  📌 **Ubicación en la Tarjeta:**
  - Se encuentra en la zona de la fotografía, rodeando la imagen del titular.

  🔍 **Proceso de Verificación:**
  - **Colocar una lupa de aumento sobre la fotografía.**
  - **Buscar la leyenda "CEDULADEIDENTIDADYELECTORAL" e inspeccionar su claridad y continuidad.**
  - **Verificar que el patrón de líneas no tenga irregularidades o interrupciones.**
  - **Si los microtextos no son legibles o presentan alteraciones, el documento podría ser fraudulento.**

2. Fondo de Seguridad Invisible (Detectable con Luz UV)

- **Elemento de Seguridad Oculto en la Zona de la Fotografía**
  - Junto con el fondo visible, la tarjeta cuenta con un **fondo de seguridad invisible**, que **no puede detectarse a simple vista**.

- Para su autenticación, es necesario utilizar una **lámpara de luz ultravioleta (UV), identificada con el número 2**.

🔹 **Patrones de Seguridad Bajo Luz UV**

- Al exponer la tarjeta a luz UV, se revelará un **diseño de microtextos en color amarillo**.
- Además, se visualizarán las siglas **"JCE"**, proporcionando una autenticación inmediata del documento.

🔹 **Dificultad de Copia y Manipulación**

- La tinta utilizada para este fondo de seguridad **no puede ser reproducida con métodos de impresión digital o fotocopias**.
- Si la fotografía del titular ha sido manipulada, el fondo invisible **no coincidirá con su posición original o no aparecerá correctamente bajo luz UV**.

🔹 **Método de Validación con Luz UV**

📌 **Ubicación en la Tarjeta:**

- Directamente sobre la fotografía del titular.

💡 **Proceso de Verificación:**

- **Exponer la tarjeta a una fuente de luz UV.**
- **Observar la aparición de los microtextos ocultos en color amarillo.**
- **Verificar que las siglas "JCE" sean visibles y estén alineadas con el diseño original.**
- **Si el fondo de seguridad no se revela o se observa distorsionado, el documento podría haber sido alterado.**

3. Beneficios Claves de los Fondos de Seguridad en la Zona de la Fotografía

✓ **Protección Contra Manipulación de la Imagen del Titular:** Si la fotografía es removida o alterada, los fondos de seguridad se verán afectados inmediatamente.

✓ **Autenticación Rápida y Confiable:** Puede verificarse con **lupa o luz UV**, sin necesidad de equipos avanzados.

✓ **Dificultad de Reproducción:** No puede ser copiado con impresoras láser, inyección de tinta ni escáneres digitales.

✓ **Alta Durabilidad:** Resistente a la fricción, humedad y exposición a factores ambientales sin perder su funcionalidad.

✓ **Compatibilidad con Otras Medidas de Seguridad:** Puede integrarse con **hologramas, tintas ópticamente variables y estructuras lenticulares**, fortaleciendo la autenticidad del documento.

Los **fondos de seguridad visibles e invisibles en la zona de la fotografía** proporcionan una de las **protecciones más efectivas** contra la manipulación del documento. La combinación de **microtextos visibles, patrones de líneas de seguridad y elementos ocultos bajo luz UV** garantiza que cualquier intento de alteración **sea fácilmente identificable** mediante una inspección visual detallada.

2.10.2.5 Tipo de Fuente No Estándar para Elementos de Texto Impresos

Como parte de las medidas de seguridad avanzadas implementadas en la tarjeta, se ha desarrollado una **fuente tipográfica exclusiva**, diseñada específicamente para la **Cédula de Identidad y Electoral**. Esta fuente única **no está disponible en sistemas de diseño convencionales ni en bases de datos de fuentes comerciales**, lo que impide su reproducción con herramientas de edición digital estándar.

El uso de una tipografía de seguridad personalizada proporciona una **capa adicional de protección** contra intentos de falsificación y facilita la autenticación del documento por parte de las autoridades.

1. Características de la Fuente No Estándar

- **Diseño Exclusivo y No Reproducible**
  - La fuente utilizada en la cédula ha sido diseñada exclusivamente para este documento, asegurando que **no pueda ser replicada con tipografías comerciales o software de edición convencional**.
  - Su diseño incorpora **elementos de seguridad ocultos**, como variaciones mínimas en el grosor de los caracteres y formas irregulares deliberadas que no son perceptibles a simple vista, pero que impiden su reproducción exacta.
- **Ubicación Estratégica en el Documento**

- Esta fuente única puede observarse en el **anverso de la tarjeta**, específicamente en las inscripciones:
    - **"REPÚBLICA DOMINICANA"**
    - **"CÉDULA DE IDENTIDAD Y ELECTORAL"**
- Al estar en posiciones clave, facilita la identificación del documento y su verificación inmediata.

🔹 **Estructura de Seguridad Oculta**

- Algunos caracteres pueden incluir **microvariaciones** en la alineación y en la curvatura de ciertas letras, haciendo que cualquier intento de falsificación con fuentes similares sea fácilmente detectable.
- Al comparar un documento legítimo con uno falsificado, las diferencias en la tipografía se harán evidentes al observar detalles específicos de la forma de las letras.

🔹 **Protección Contra Falsificación Digital**

- No puede ser replicada con **impresoras de uso general, software de diseño gráfico o escáneres de alta resolución**, ya que la fuente ha sido desarrollada para que cualquier intento de copia genere **errores en la alineación y espaciado de los caracteres**.
- Si un falsificador intenta recrear la cédula con otra fuente similar, las diferencias pueden ser detectadas por un experto con un análisis detallado del documento.

2. Métodos de Validación de la Fuente No Estándar

📌 **Validación Visual a Simple Vista:**

✅ Comparar la fuente utilizada en las palabras **"REPÚBLICA DOMINICANA"** y **"CÉDULA DE IDENTIDAD Y ELECTORAL"** con otros documentos conocidos o con la base de datos oficial del emisor.

✅ Observar la consistencia de los caracteres, asegurando que no haya irregularidades en la forma o el espaciado de las letras.

🔍 **Validación con Lupa de Aumento:**

✅ Utilizar una **lupa de 10x o superior** para inspeccionar detalles de la tipografía, como las **microvariaciones en el grosor y curvatura de las letras**.

✅ Comparar la alineación y la estructura de los caracteres para detectar posibles diferencias con fuentes comerciales.

💡 **Validación con Software de Análisis Tipográfico:**

✅ En controles de alta seguridad, se pueden utilizar herramientas de reconocimiento óptico para **comparar la fuente impresa con la versión digital original**, detectando cualquier alteración en el diseño de los caracteres.

3. Beneficios Claves del Uso de una Fuente No Estándar

✓ **Dificultad Extrema de Reproducción:** Al no estar disponible en bases de datos comerciales, no puede ser utilizada en impresoras convencionales o programas de diseño.

✓ **Verificación Manual y Digital:** Puede ser autenticada tanto a simple vista como con herramientas especializadas, facilitando su inspección en entornos de alta seguridad.

✓ **Protección Contra Alteraciones del Documento:** Si se intenta modificar el documento con otra tipografía, cualquier diferencia será detectable.

✓ **Complemento con Otras Medidas de Seguridad:** Puede integrarse con **microtextos, guilloches y tintas ópticamente variables** para reforzar la autenticidad del documento.

El uso de una **fuente tipográfica exclusiva** en la Cédula de Identidad y Electoral es una de las medidas de seguridad más efectivas para impedir la falsificación del documento. Al ser un diseño **no disponible en bases de datos comerciales ni en software de diseño convencional**, su replicación es prácticamente imposible sin acceso a los archivos originales del emisor.

2.11 Tarjeta Multicapa: Seguridad Forense de Alta Resistencia

La **Cédula de Identidad y Electoral** ha sido diseñada con una estructura de **múltiples capas de policarbonato fusionadas**, lo que garantiza una seguridad avanzada, alta resistencia y protección contra intentos de manipulación.

Si bien el estándar de seguridad establece un mínimo de **5 capas**, la muestra presentada ha sido fabricada con **7 capas**, lo que **supera los requisitos de seguridad** y refuerza su durabilidad estructural y sus capacidades de protección contra falsificación.

Esta característica de seguridad **pertenece al Nivel 3**, lo que significa que su validación requiere **equipos de laboratorio especializados** para analizar su composición, estructura y reacción ante pruebas de autenticidad.

1. ¿Cómo Funciona la Seguridad de la Tarjeta Multicapa?

- **Estructura en Capas de Policarbonato Fusionadas**
  - Cada una de las **7 capas de la tarjeta** ha sido fusionada mediante **un proceso de laminación en caliente**, evitando que las capas puedan separarse sin destruir completamente el documento.
  - Este diseño impide **intentos de alteración, duplicación o reemplazo de datos**, ya que cualquier intento de modificar la tarjeta afectaría su integridad estructural.
- **Composición de Capas con Funcionalidad Diferenciada**

Cada capa cumple una función específica en la protección del documento:

1. **Capa Exterior Protectora:** Resistente a rayaduras, humedad, luz UV y desgaste mecánico.

2. **Capa Sensible al Grabado Láser con holograma embebido:** Permite la personalización de datos variables, como la fotografía del titular y el número de identificación, asegurando que no pueda modificarse sin evidencia visible. Además, esta capa porta el holograma, dejándolo atrapado en el interior de la construcción.

3. **Capa de Seguridad Impresa:** Contiene **elementos ópticos de seguridad, guilloches y tintas de seguridad**.

4. **Capa del Chip Sin Contacto:** Incorpora la **tecnología NFC para identificación digital** con almacenamiento seguro de datos. Esta capa refuerza la rigidez de la tarjeta y asegura la estabilidad del documento en condiciones extremas, al conjugar la atenga de cobre y el chip.

5. **Capa de Seguridad Impresa:** Contiene **elementos ópticos de seguridad, guilloches y tintas de seguridad** con la impresión del diseño del reverso de la credencial.

6. **Capa Sensible al Grabado Láser:** Permite la personalización de datos variables, como los códigos de barras, MRZ, y numeración, asegurando que no pueda modificarse sin evidencia visible.

7. **Capa Exterior Protectora:** Resistente a rayaduras, humedad, luz UV y desgaste mecánico.

🔹 **Alta Resistencia Física y Química**

- Las capas fusionadas garantizan que la tarjeta **resista temperaturas extremas, exposición a agentes químicos y condiciones de alta humedad** sin comprometer su integridad.
- Su diseño multicapa hace que **no pueda ser doblada sin fracturarse**, lo que previene intentos de manipulación o alteración física del documento.

2. Métodos de Validación de la Tarjeta Multicapa

📌 **Validación Visual y Física:**

✅ **Inspección visual:** Bajo luz intensa, se pueden notar las diferentes capas en el borde de la tarjeta.

✅ **Prueba de flexión:** Al aplicar presión en los extremos, la tarjeta **mantiene su rigidez y no se deforma** fácilmente.

🔍 **Validación en Laboratorio:**

✅ **Pruebas de microscopía óptica:** Permiten analizar la **composición exacta y la estructura interna de las capas**.

✅ **Análisis de separación de capas:** Técnicas de disolución química y pruebas de resistencia para determinar **la autenticidad y la adhesión de las capas**.

✅ **Exposición a calor extremo:** Pruebas en entornos controlados para evaluar **la reacción de los materiales a temperaturas elevadas**.

💡 **Verificación con Dispositivos de Control de Seguridad:**

✅ **Escáneres de Identificación Electrónica:** Permiten analizar **la presencia de la capa del chip y su integración con el sistema multicapa**.

✅ **Luz infrarroja y ultravioleta:** Algunas capas pueden reaccionar de manera diferente ante estas fuentes de luz, permitiendo verificar la estructura del documento.

3. Beneficios Claves de la Tarjeta Multicapa

✓ **Prevención de Manipulación:** Si un falsificador intenta separar las capas para modificar los datos, el documento se destruirá automáticamente.

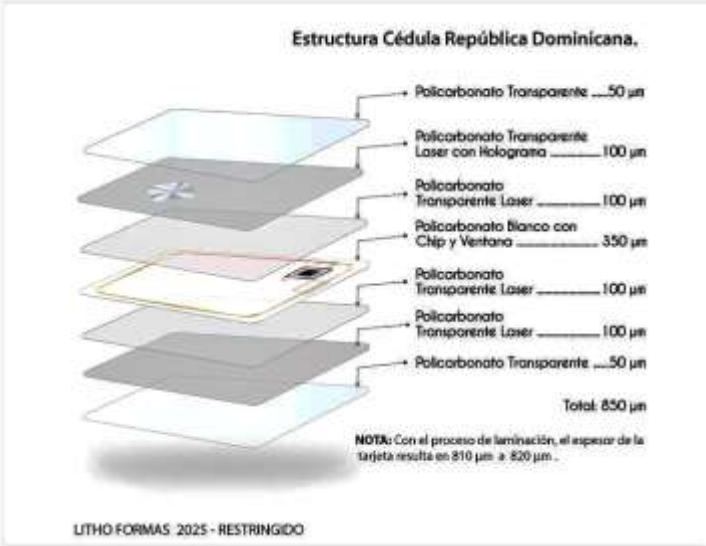
✓ **Resistencia Extrema:** No se deteriora con el tiempo, garantizando una **vida útil superior a 10 años**.

✓ **Protección Contra Falsificación:** No puede ser copiada con impresoras comerciales ni modificada sin dejar evidencia visible.

✓ **Soporte de Tecnologías de Identificación Digital:** Su estructura permite la **incorporación segura del chip sin contacto** y su antena NFC sin afectar la resistencia mecánica de la tarjeta.

✓ **Interoperabilidad con Sistemas de Seguridad Global:** Cumple con los estándares de documentos de identidad **ICAO 9303**, asegurando su compatibilidad con controles de seguridad internacionales.

El uso de **7 capas de policarbonato fusionadas** convierte a la Cédula de Identidad y Electoral en un **documento altamente resistente, seguro e infalsificable**. Su diseño **impide la manipulación de los datos del titular y refuerza la autenticidad del documento** en cualquier entorno de verificación.



2.12 Tintas Invisibles en el Infrarrojo: Seguridad Avanzada en la Impresión del Fondo

Las **tintas invisibles en el infrarrojo** representan una de las medidas de seguridad forense más avanzadas implementadas en la **Cédula de Identidad y Electoral**. Estas tintas están integradas en la impresión del **fondo de seguridad** y son completamente invisibles cuando se observa la tarjeta bajo luz normal, pero se hacen evidentes o desaparecen cuando son sometidas a pruebas con dispositivos de detección en el espectro infrarrojo.

Esta tecnología es ampliamente utilizada en **documentos de alta seguridad, billetes de banco y pasaportes electrónicos**, ya que **impide su falsificación con impresoras convencionales y técnicas de escaneo digital**.

1. ¿Cómo Funcionan las Tintas Invisibles en el Infrarrojo?

🔹 **Propiedades Ópticas Especiales**

- Estas tintas están formuladas con **pigmentos sensibles al espectro infrarrojo (IR)**, los cuales son **completamente invisibles a simple vista**.
- Cuando la tarjeta se examina con **un dispositivo de detección infrarroja (identificado con el número 4)**, los elementos impresos con estas tintas **desaparecen o se muestran con variaciones de intensidad** dependiendo de su composición.

🔹 **Validación con Equipos de Inspección Infrarroja**

- Al colocar el documento bajo un **escáner de infrarrojos**, el fondo de seguridad impreso con estas tintas **no será visible en la pantalla del dispositivo**.
- Este método permite que los agentes de control de identidad y seguridad puedan **confirmar la autenticidad del documento en cuestión de segundos**.

🔹 **Dificultad de Reproducción y Protección Contra Falsificación**

- No pueden ser copiadas con **escáneres, cámaras digitales o impresoras de inyección de tinta y láser**.
- Cualquier intento de falsificación **fallará al momento de ser verificado con luz infrarroja**, ya que una copia fraudulenta no contará con la respuesta óptica correcta.

2. Métodos de Validación de las Tintas Invisibles en el Infrarrojo

📌 **Ubicación en la Tarjeta:**

- Aplicadas en **el fondo de seguridad** de la tarjeta, asegurando que cualquier intento de alteración se haga evidente al momento de la inspección.

🔍 **Verificación con Dispositivo Infrarrojo (Identificado con el Número 4):**

✅ **Encender el dispositivo de verificación infrarroja.**

✅ **Colocar la tarjeta en la zona de detección del escáner.**

✅ **Observar el fondo de seguridad en la pantalla del detector.**

✅ **Confirmar que las áreas impresas con tintas invisibles no sean visibles en el espectro infrarrojo.**

3. Beneficios Claves de las Tintas Invisibles en el Infrarrojo

✓ **Autenticación Forense de Alta Seguridad:** Solo puede ser verificada con **equipos especializados**, impidiendo falsificaciones convencionales.

✓ **Protección Contra Copias Digitales y Reimpresiones Fraudulentas:** No puede ser replicada con escáneres o impresoras domésticas.

✓ **Validación Rápida y Confiable:** Permite autenticar la tarjeta en **cuestión de segundos** mediante un **lector infrarrojo**.

✓ **Integración con Otras Tecnologías de Seguridad:** Puede combinarse con **microtextos, tintas ópticamente variables y hologramas** para reforzar la protección del documento.

✓ **Resistencia y Durabilidad:** Estas tintas son **químicamente estables y no se degradan con el tiempo**, manteniendo su funcionalidad a lo largo de la vida útil del documento.

4. Importancia de las Tintas Invisibles en el Infrarrojo en la Seguridad del Documento

El uso de **tintas invisibles en el infrarrojo** permite una verificación rápida y efectiva de la autenticidad del documento, evitando fraudes y garantizando la protección de la identidad del titular. Su aplicación en el **fondo de seguridad de la tarjeta** proporciona una capa adicional de protección que **impide su falsificación y facilita su autenticación en puntos de control de identidad en aeropuertos, bancos y entidades gubernamentales**.

Las **tintas invisibles en el infrarrojo** representan una tecnología de **seguridad forense de alto nivel**, utilizada en documentos de identidad oficiales para prevenir falsificaciones y garantizar su autenticidad en controles especializados. La imposibilidad de reproducir estos elementos con impresoras estándar convierte a la tarjeta en un **documento prácticamente infalsificable**, asegurando que solo pueda ser emitida y verificada por **autoridades certificadas**.

2.13 Nanotextos integrados en el elemento difractivo.

Como parte de los elementos de seguridad avanzados en la nueva **Cédula de Identidad y Electoral**, el **Consorcio IDSecure IDS** ha incorporado nanotextos y microtextos estratégicamente ubicados en los elementos gráficos clave del diseño, garantizando un alto nivel de protección contra intentos de falsificación.

Se han integrado dos **elementos difractivos de alta seguridad** en el anverso de la cédula, diseñados para ofrecer un efecto óptico variable (OVD) que refuerza la autenticidad del documento.

- **Imagen 1:** Representación del **mapa de la República Dominicana**, con dimensiones de **26.5 x 17.6 mm**, observado a escala **200%**.

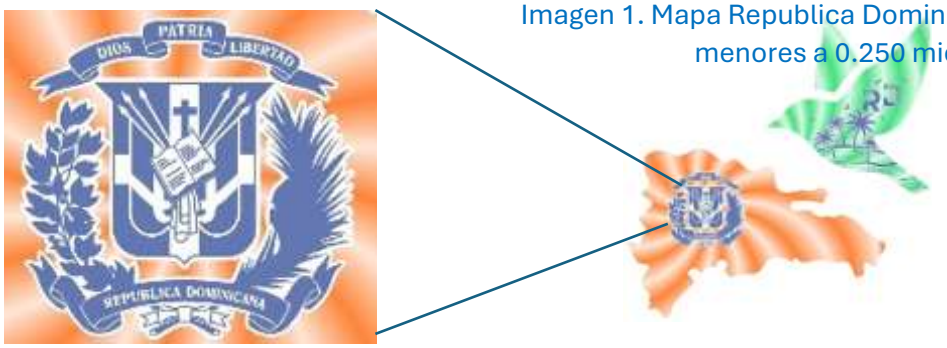


Imagen 1. Mapa Republica Dominicana, nanotextos menores a 0.250 micras

- **Imagen 2:** Representación del **ave nacional, la Cigua Palmera (Dulus dominicus)**, con dimensiones de **16.9 x 18 mm**, también visto a **escala 200%**.

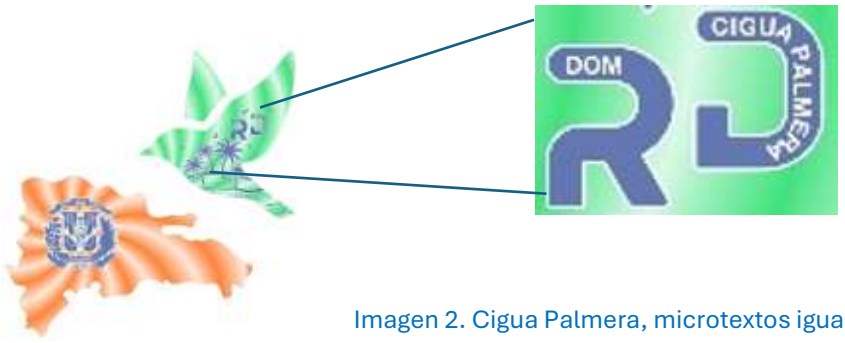


Imagen 2. Cigua Palmera, microtextos igual a 250 micras "DOM" y "CIGUA PALMERA"

Estos elementos están **integrados dentro de las capas de la cédula**, asegurando su permanencia y resistencia a manipulaciones.

Además, los **nanotextos** se encuentran presentes en el **escudo de armas**, mientras que los **microtextos** han sido incorporados dentro del diseño de las letras **R y D**, siglas de **República Dominicana**, formando parte de los efectos reflectantes del documento. Estos textos están impresos con un **color de alta difracción**, lo que permite que **su tonalidad cambie alternativamente con cada rotación del documento**, añadiendo una capa adicional de seguridad visual.

La implementación de estos elementos garantiza que la **cédula de identidad cumpla con los estándares internacionales en seguridad documental**, asegurando su autenticidad y dificultando su reproducción no autorizada.

En conclusión, las tarjetas ofertadas cumplen con todos los requisitos técnicos exigidos por la JCE, asegurando la máxima seguridad y durabilidad en su uso. Gracias a la implementación de múltiples niveles de seguridad, tecnologías de grabado láser y un chip sin contacto de última generación, estas tarjetas ofrecen una solución confiable y moderna para la identificación ciudadana. La integración con estándares internacionales garantiza su interoperabilidad y resistencia a manipulaciones, consolidando así una propuesta robusta y alineada con las necesidades del proyecto.

2.14 Medidas de Seguridad proporcionadas en la personalización

- **Personalización en relieve**. La personalización de los nombres, apellidos y el número de cédula se llevan a cabo con una mayor intensidad en el láser, logrando que los textos ganen relieve sobre la superficie de la muestra.
- **Foto Fantasma en ventana.** En la ventana traslúcida de la muestra se personaliza la fotografía fantasma del ciudadano, lográndose observar por el frente y reverso.
- **Personalización del CLI.** En el área lenticular de la muestra, la láser gira para personalizar en distintos ángulos la fotografía y el fecha de vigencia de la Cédula.
- **Personalización MRZ.** La muestra incluye la personalización del Machine Readable Zone (MRZ por sus siglas en inglés). La Zona de Lectura Mecánica es personalizada en láser al reverso y cumple con los estándares y normas ICAO.

2.15 TRAZABILIDAD

El proceso de fabricación de las Cédulas de Identidad y Electoral, se realiza por medio de lotes de producción controlados por medio de un sistema ERP, utilizando un número único por cada lote.

- Durante todas las etapas del proceso, se cuenta con controles que garantizan la calidad y conformidad de las cédulas. Estos controles incluyen:
- Lotes de materias primas utilizadas – Inspección, pruebas y liberación a producción.
- Procesos de fabricación- Se registran los equipos y personal involucrado en todos los procesos de fabricación de cada lote de producción.

- Control de calidad – Se cuenta con registros de las pruebas de calidad a las que son sometidas las cedulas en cada proceso y su seguimiento.
- Control de volumen por lote- Cantidad de cedulas fabricadas por proceso, incluyendo la merma y el tratamiento de esta hasta su destrucción.
- Todos los controles se encuentran en cumplimiento con el Sistema de Gestión de Calidad y con las normativas aplicables ISO 14298.

2.16 GARANTÍAS

La cédula física está elaborada completamente con láminas de policarbonato, de tamaño ID1. Por su proceso de fabricación donde se funden **siete (7) capas**, por medio de calor y presión, como una única hoja, no es posible separar las capas de material, conservando la funcionalidad. Ofreciendo una durabilidad de **mínimo diez (10) años**.

Permite la inclusión de técnicas de personalización de grabado láser y láser en relieve, mismos que permanecen en la cédula durante la vigencia de esta.

Por lo que resguardando la tarjeta adecuadamente y siguiendo las indicaciones de uso y limpieza, se garantiza que la cédula tendrá una durabilidad de 10 años, conservando las medidas de seguridad.

La deformación causada por el uso normal NO afectará las funcionalidades de la misma al enderezarse con el equipo de lectura.

2.17 RECOMENDACIONES DE USO Y RESGUARDO DE LAS CEDULAS DE POLICARBONATO

Para optimizar la vida útil de las Cédulas de Identidad y Electoral, se emiten las siguientes recomendaciones:

- Almacenamiento en lugar seco y fresco.
- Proteger de la humedad.
- Mantener alejado de materiales oxidantes y de luz solar directa por largos períodos de exposición o llamas.
- No es necesario utilizar productos químicos abrasivos que puedan rayar la superficie, se limpian con un paño suave.
- Evita el uso de objetos punzantes sobre la superficie, ya que pueden causar
- daños permanentes.

3. REQUERIMIENTOS DE PERSONALIZACIÓN DE TARJETAS

El **Consorcio IDSecure IDS**, en su compromiso con la modernización del sistema de identificación de la República Dominicana, ha diseñado una solución integral que combina **tecnología avanzada, interoperabilidad y seguridad digital**. La personalización de las tarjetas se llevará a cabo mediante tecnología de **grabado láser de alta precisión**, utilizando el sistema **IXLA IDX DF-01**, asegurando la durabilidad, seguridad y resistencia de los documentos de identidad. Este proceso permitirá la personalización de datos como nombre, número de identificación, fotografía, firma digital y otros elementos de seguridad esenciales.

Como parte de su estrategia para garantizar un ecosistema de identidad digital seguro y eficiente, el **Consorcio IDSecure IDS** ha integrado una infraestructura **PKI avanzada**, que permitirá la emisión y validación de certificados digitales, asegurando autenticidad e integridad en cada documento emitido. **Magallanes Media**, miembro del consorcio, liderará el desarrollo de la **capa de software del usuario**, proporcionando la interfaz y herramientas necesarias para la interacción segura entre los ciudadanos y la infraestructura de identificación digital.

Esta solución trabajará en **sinergia con la plataforma PKI y la aplicación móvil**, basadas en la tecnología **GoID de TOPPAN SECURITY SAS (antiguo HID Global)**, quienes aportarán su experiencia en seguridad digital. La integración permitirá:

- **Autenticación segura y validación de identidad en entornos físicos y digitales**.
- **Gestión de certificados digitales con una infraestructura confiable y escalable**.
- **Interacción fluida con la aplicación móvil del sistema, asegurando accesibilidad y usabilidad para los ciudadanos**.
- **Firma digital y validación de documentos de identidad con los más altos estándares internacionales**.
- **Desarrollo de herramientas de control y auditoría en tiempo real para la JCE**.

El **Consorcio IDSecure IDS** garantiza que esta infraestructura, combinada con su conocimiento en integración tecnológica, permitirá una **transición eficiente hacia un sistema de identidad digital seguro y moderno**, fortaleciendo la confianza y la seguridad en la identificación de los ciudadanos. La propuesta del consorcio no solo cumple con los requerimientos de la **JCE**, sino que también establece un **nuevo estándar en identidad digital**, asegurando una implementación robusta y sostenible.

3.1 Historia y Evolución de la Personalización de Tarjetas

Desde la implementación de los primeros documentos de identidad, la seguridad y autenticidad han sido prioridades fundamentales. En la actualidad, con el avance de la tecnología digital y la creciente necesidad de identidad segura, las tarjetas personalizadas han evolucionado hasta incluir elementos de alta seguridad como chips electrónicos, grabado láser y medidas antifalsificación avanzadas.

Los documentos de identidad han transitado desde sistemas basados en papel con sellos manuales a tarjetas de policarbonato con múltiples capas de seguridad y chips embebidos. Los gobiernos han invertido en soluciones avanzadas que permiten un control exhaustivo sobre la emisión de credenciales y la verificación digital de identidad.

A nivel global, países como Alemania, Francia y Canadá han adoptado tecnologías similares, utilizando técnicas de personalización avanzadas para evitar fraudes y mejorar la eficiencia en la gestión de documentos de identidad. Nuestra propuesta se inspira en estos modelos internacionales para garantizar un sistema robusto y eficiente.

3.1.1 Objetivos del Proyecto

1. Garantizar un sistema seguro de emisión y personalización de tarjetas.
2. Implementar estándares de seguridad internacional como ISO 9001, ISO 27001 y ISO 14298.
3. Establecer un proceso automatizado y trazable para la personalización de documentos de identidad.
4. Reducir riesgos de falsificación mediante el uso de múltiples niveles de seguridad en las tarjetas.
5. Facilitar la interoperabilidad con sistemas de verificación nacional e internacional.
6. Mejorar la eficiencia operativa y el control sobre la emisión de documentos de identidad.
7. Asegurar la durabilidad de las tarjetas en condiciones adversas.
8. Implementar un sistema escalable que permita futuras integraciones con plataformas digitales.
9. Optimizar los costos operativos mediante la implementación de tecnología avanzada y materiales de larga duración.
10. Garantizar que las tarjetas sean accesibles a través de múltiples medios de autenticación y validación.

3.1.2 Beneficios del Proyecto

- **Seguridad Mejorada:** Implementación de tecnología de punta en la protección de datos y autenticación.
- **Interoperabilidad Internacional:** Cumplimiento con estándares globales para el uso en aeropuertos y trámites consulares.
- **Reducción de Fraudes:** Uso de técnicas avanzadas de grabado y validación biométrica.
- **Eficiencia Operativa:** Automatización de procesos para reducir costos y tiempos de entrega.
- **Compatibilidad con Sistemas Digitales:** Adaptabilidad a plataformas de verificación en línea.
- **Sostenibilidad y Responsabilidad Ambiental:** Uso de materiales reciclables y procesos optimizados para reducir el impacto ecológico.
- **Capacitación y desarrollo del personal técnico:** Implementación de programas de formación para garantizar la correcta manipulación de los equipos y el cumplimiento de los procedimientos.
- **Expansión Modular:** Capacidad de escalabilidad para incluir nuevas tecnologías en el futuro.

3.2 Infraestructura y Seguridad en la Producción

3.2.1 División de Áreas de Seguridad

La planta de producción de LITHO FORMAS está segmentada en cuatro niveles de seguridad, asegurando la integridad del proceso y la protección de la información:

- **Áreas Normales (NA):** Espacios administrativos y de soporte, sin información confidencial ni equipos de producción.
- **Áreas Restringidas (RA):** Control de acceso con tarjetas de proximidad y biometría, almacenamiento de insumos y documentación confidencial.
- **Áreas de Seguridad (SA):** Producción cerrada con monitoreo en tiempo real, medidas de acceso restringido y personal acreditado.
- **Áreas de Alta Seguridad (HSA):** Máximo control de acceso, sistemas de autenticación multifactorial y monitoreo continuo.

Cada una de estas áreas cuenta con barreras físicas y tecnológicas, asegurando un control estricto del flujo de personal y materiales. Se han implementado procedimientos adicionales de auditoría para reforzar la seguridad en cada etapa del proceso de personalización.

3.3 Tecnología de Personalización

3.3.1 Equipos y Procesos

Nuestra solución incorpora el sistema **IDX DF-01** de IXLA con las siguientes características:

- **Personalización por grabado láser de alta resolución (600-1200 DPI).**
- **Impresión en escala de grises y elementos de seguridad visibles e invisibles.**
- **Codificación de chip RFID con tecnología TOPPAN.**
- **Capacidad de producción de hasta 100 tarjetas por hora (60 por hora requeridas).**
- **Personalización de policarbonato con múltiples capas de seguridad.**
- **Integración con bases de datos gubernamentales para validación en tiempo real.**

3.3.2 Personalización de Tarjetas

El sistema de personalización propuesto está diseñado para cumplir con los más altos estándares internacionales de seguridad y precisión, garantizando una emisión de documentos eficiente y confiable mediante **grabado láser en escala de grises de alta resolución (600-1200 DPI)**.

✅ **Tecnología de Personalización y Producción**

- **Personalización mediante grabado láser en escala de grises (mínimo 600 DPI)**, asegurando máxima calidad en la imagen del titular.
- **Manejo automático de tarjetas con alimentador de mínimo 100 tarjetas y bandeja de salida de 100 tarjetas.**
- **Velocidad mínima de personalización de 50 tarjetas por hora**, incluyendo grabado láser, codificación y verificación de calidad.
- **Procesamiento modular y automático de tarjetas**, asegurando que la personalización se realice en una única secuencia sin intervención manual.

✅ **Cumplimiento con Normativas Internacionales**

- **Cumple con la normativa OACI (Doc. 9303)**, asegurando compatibilidad con sistemas de verificación internacional.
- **Codificación de tarjetas inteligentes según ISO 14443 Tipo A y B.**
- **Líneas de lectura mecánica (ZLM) en la zona inferior del reverso de la tarjeta.**

✅ **Elementos de Seguridad y Personalización**

- **Imagen facial en escala de grises** y **elementos de seguridad visual avanzados (imagen fantasma, microtextos, códigos de barras 1D/2D).**
- **Control de calidad con verificación óptica automática**, asegurando alineación precisa del grabado con la estructura de la tarjeta.
- **Verificación del chip antes de la personalización mediante un segundo lector de chip integrado.**

✅ **Integración con la Plataforma de la JCE**

- **Recepción de datos en formato XML** generados por la plataforma de tarjetas de la **JCE**, permitiendo personalización automatizada.
- La solución propuesta podrá **identificar los registros inconsistentes** antes de proceder con la impresión de la tarjeta. Si el registro enviado por la interfaz de integración está incompleto, por la ausencia de alguno de los datos requeridos, el registro será rechazado.
- **Edición de layout para adaptación de tarjetas según perfil del ciudadano** (mayores de edad, menores, naturalizados, extranjeros, etc...).
- **Interfaz TCP/IP con capacidad de asignación y ajuste de dirección IP**, permitiendo su integración con la red central de la JCE.

✅ **Seguridad y Desarrollo de Aplicaciones**

- **Disponibilidad de un SDK (Software Development Kit)** con herramientas de desarrollo, librerías y ejemplos funcionales, facilitando la integración con la infraestructura tecnológica de la **JCE** o terceros.
- **Control de acceso a la máquina mediante credenciales de operador**, con registro de cada sesión de usuario.
- **Eliminación automática y criptográfica de datos temporales**, asegurando que la información no permanezca almacenada después de la personalización, por más de 1 día.
- **Compatibilidad con medidas de seguridad Nivel 1, Nivel 2 y Nivel 3**, asegurando el cumplimiento de todos los requisitos de protección establecidos en la licitación.

✅ **Generación de Reportes y Auditoría**

- **Registro y almacenamiento de información histórica** de producción de tarjetas, **acceso de los operadores,** garantizando trazabilidad durante un periodo de al **menos 4 semanas**.
- **Generación de informes de producción**, a definir por el cliente, permitiendo el monitoreo de estadísticas por máquina, período de tiempo y tipo de documento emitido.

La eficiencia productiva de la solución tecnológica ofrecida ha sido diseñada para lograr más de un **NOVENTA POR CIENTO (90%)** de la misma, calculada según cantidad de tarjetas efectivas producidas por hora / capacidad de máquina por hora informada por el fabricante.

4. INFRAESTRUCTURA PKI Y SEGURIDAD

La Junta Central Electoral (JCE) ha establecido la necesidad de contar con **dos infraestructuras de clave pública (PKI) separadas** para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos y las firmas digitales en el nuevo sistema de cedulación. Estas **infraestructuras** permitirán una **gestión diferenciada** de los certificados utilizados por los ciudadanos y los documentos emitidos por la JCE, asegurando así una separación clara de responsabilidades y funciones dentro del ecosistema digital de identidad.

Las tres infraestructuras son las siguientes:

1. **PKI de FIRMA DE DOCUMENTOS:** Infraestructura dedicada a la autenticación y verificación de documentos oficiales emitidos por la JCE, asegurando que cualquier documento generado por la institución sea inalterable, verificable y confiable.
2. **PKI de FIRMA DIGITAL**: Diseñada para emitir y gestionar certificados digitales destinados a los ciudadanos, permitiéndoles firmar documentos electrónicamente con plena validez legal.
3. **PKI para DOCUMENTOS DIGITALES (IACA):** Infraestructura que actuará como la Autoridad Certificadora de la Autoridad de Emisión ISO 18013-5 (IACA) y será la CA raíz fuera de línea para la PKI utilizada en la emisión de los Documentos de Identidad Digital, **incluida en el CAPITULO DE IDENTIDAD DIGITAL.**

Cada una de estas infraestructuras opera bajo **normativas internacionales de seguridad**, como **X.509v3, RFC 5280, Common Criteria EAL4+ y FIPS 140-2 Nivel 3**, garantizando una gestión segura de claves criptográficas y certificaciones digitales.

4.1 PKI DE FIRMA DE DOCUMENTOS

Para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos dentro del nuevo sistema de cédulas de identidad, el **Consorcio IDSecure IDS** ha seleccionado a **TOPPAN SECURITY SAS (antiguo HID Global)** como proveedor de la Infraestructura de Clave Pública (PKI). TOPPAN SECURITY SAS es una empresa líder en soluciones de seguridad digital y firma electrónica, con una sólida trayectoria en la implementación de PKI para gobiernos e instituciones públicas a nivel global. Su tecnología cumple con los estándares internacionales establecidos por la OACI (Doc 9303), ISO 15408 y eIDAS, asegurando la interoperabilidad, seguridad y confiabilidad del sistema. La solución PKI propuesta garantizará la emisión segura de certificados digitales, la gestión de claves criptográficas y la validación de identidad digital de los ciudadanos.

4.1.1 Características de la PKI

En esencia, la PKI utiliza la criptografía asimétrica, un concepto fundamental en la seguridad de la información moderna basado en un par de claves relacionadas matemáticamente: una clave pública y una clave privada. La clave pública se distribuye libremente y puede ser conocida por cualquier persona, mientras que la clave privada es mantenida de forma segura por el propietario de la clave.

Las soluciones PKI se basan en varios elementos que trabajan en conjunto, por ejemplo, la autoridad de registro, la emisión de certificados, la creación de firmas, la validación de estado y los servicios de revocación. Dado que todos estos servicios se respaldan mutuamente, la seguridad de cada uno es esencial, como los eslabones de una cadena.

La implementación debe diseñarse cuidadosamente, teniendo en cuenta las inevitables amenazas de seguridad. Cada tipo de amenaza debe ser listado y evaluado utilizando una técnica de evaluación de riesgos, donde los riesgos se miden en términos de la probabilidad de ocurrencia y el impacto que podrían causar. Posteriormente, se pueden seleccionar contramedidas para reducir el nivel general de riesgo a un grado aceptable; cabe señalar que es poco probable lograr una seguridad perfecta y siempre se deben tomar decisiones de costo-beneficio al asignar el presupuesto de seguridad.

TOPPAN SECURITY recomienda utilizar una metodología formal, como la ISO 2700x, al diseñar y operar infraestructuras de TI relacionadas con la identidad.

Las mejores prácticas incorporarán:

- **Zonas de seguridad** física concéntricas para proteger activos como servidores, redes y estaciones de trabajo.
- **Módulos de seguridad** de hardware (HSM) para proteger la integridad de las claves secretas y privadas.
- **Técnicas de protección** en internet para sitios web y servicios web.
- **Seguridad procedimental** para proteger al personal administrativo de compromisos.
- **Monitoreo continuo** y revisión de las medidas de seguridad.
- **Actualizaciones regulares** de seguridad del software.
- **Planificación de recuperación** ante desastres y continuidad del negocio.

De acuerdo con el Pliego de Especificaciones, ITEM III - ESPECIFICACIONES TÉCNICAS DE LAS PKI – CA. Nuestra solución es diseñada para cumplir con los requisitos y criterios técnicos, asegurando cumplimiento con el Doc. 9303 de la OACI.

En esta sección, proponemos implementar la infraestructura de criptografía basada en claves públicas (PKI), para emitir y revocar certificados digitales que se utilizarán para firmar electrónicamente las tarjetas electrónicas y para verificar tarjetas electrónicas.
Nuestra propuesta incluye los elementos necesarios la provisión, configuración, integración y puesta en marcha de una Infraestructura de Clave Pública, con finalidad de autenticar la tarjeta electrónica que ofrece acceso de sólo lectura de Chip de Circuito Integrado (IC), que, por su vez, cumple con la norma ISO 15408, y posee certificación CC EAL 4+ en el sistema operativo provisto.
En resumen, proporcionamos componentes y servicios destinados a la emisión segura y eficiente de las tarjetas CI y CIE de próxima generación de República Dominicana.

4.1.2 Componentes de la PKI:

En el caso de ser adjudicados, estaremos coordinando y apoyando la implementación de la CA con las disposiciones legales establecidas en la Ley 126-02 sobre Comercio Electrónico, Documentos y Firma Digital y su reglamento contenido en el Decreto 335-03.

4.1.2.1 Infraestructura PKI - Integrale™ KMS

Integrale™ KMS está diseñado para gestión de las claves para documentos electrónicos seguros y en conformidad con ICAO Documento 9303. Integrale™ KMS proporciona una interfaz gráfica de usuario amigable para la instalación de las CA de ICAO (CSCA y CVCA) o las CA de los documentos digitales (IACA) con la generación y el mantenimiento de claves privadas y el certificado X.509 para la firma y autenticación de documentos.

Garantizando el cumplimiento con las especificaciones:

- El CSCA utiliza algoritmos criptográficos actuales y almacena las claves privadas en un HSM.
- El CSCA trabaja en un entorno sin conexión y será la autoridad encargada de firmar certificados para entidades gubernamentales o documentos de importancia nacional.
- El CSCA generará listas de revocación de certificados (CRL) según ICAO 9303.
- El acceso se da a través de una autenticación multifactorial para el inicio de sesión en la interfaz de administración.
- El CSCA es capaz de emitir los certificados VDS Signer, siendo también responsable de mantener la infraestructura de claves públicas y de gestionar la emisión y revocación de estos certificados

- El CSCA es capaz de emitir certificados de firmante de lista maestra, así asegurando la confianza de todas las entidades.

Infraestructura de Clave Pública (PKI) y Certificación de Seguridad

Nuestra propuesta cumple con los requisitos establecidos en el Pliego de Condiciones, incluyendo la implementación de una **PKI con CA Raíz y CA Subordinada** dentro de las instalaciones de la JCE, asegurando una infraestructura segura y confiable.

1.1 Seguridad y Redundancia

- La infraestructura estará protegida mediante **firewalls avanzados, segmentación de redes y autenticación multifactorial (MFA)**.
- **Redundancia y Alta Disponibilidad (Cluster)**: Se implementará un sistema de **respaldo activo en premisas**, garantizando continuidad operativa, según normas internacionales como la ISO/IEC 270031 o la ISO 22301.
- **HSM Certificado**: Se integrará un **HSM FIPS 140-2 Nivel 3 o superior**, cumpliendo con los estándares internacionales de seguridad.
- **Certificación Common Criteria EAL4+**: Garantizando una evaluación de seguridad robusta.

1.2 Administración del Ciclo de Vida de Certificados

- **Portal Web para la Gestión de Certificados**: Se implementará un sistema que permitirá la emisión, renovación, revocación y auditoría de certificados digitales.
- **Sellos de Tiempo (TSA)**: Integración de una Autoridad de Sellos de Tiempo (Time Stamping Authority) sincronizada con la fuente oficial de la República Dominicana.
- **Cumplimiento Normativo**: Se garantizará la compatibilidad con **X.509, eIDAS CC EAL4+ e ISO 15408**.

1.3 Integración y Compatibilidad

- **Interoperabilidad con sistemas gubernamentales**: Se desarrollarán APIs REST para asegurar la integración con aplicaciones del gobierno y terceros.
- **Soporte para Infraestructura de Clave Pública (PKI)**: Implementación de soluciones criptográficas modernas, incluyendo **RSA 4096, ECDSA y AES-256**.
- **Mecanismos de Autenticación y Control de Acceso**: Se garantizará un modelo de autenticación basado en credenciales digitales con validaciones criptográficas.

Infraestructura PKI: Cumplimiento y Recomendaciones

Nuestra solución de PKI está diseñada para alinearse completamente con los requisitos de la JCE, proporcionando un ecosistema seguro y altamente disponible para la emisión de certificados digitales.

2.1 Refuerzo de Seguridad en la Infraestructura PKI

- **Asegurar la redundancia en la infraestructura de PKI**, especificando claramente la configuración en cluster.
- **Incluir una matriz de cumplimiento**, comparando los requisitos del pliego con las especificaciones de la propuesta.
- **Especificar claramente las certificaciones del HSM**, asegurando que cumple con **FIPS 140-2 Nivel 3 y Common Criteria EAL4+**.
- **Detallar la interoperabilidad de la solución**, asegurando que la PKI puede integrarse con otros sistemas gubernamentales a través de APIs.
- **Ampliar la sección de administración del ciclo de vida de certificados**, incluyendo detalles sobre la capacidad de emisión, revocación y auditoría en el portal web.

4.1.2.2 Firmante de Documentos - Integrale DPS

Integrale™ DPS se propone como el sistema de preparación de datos y firma para documentos electrónicos. Es el módulo específico para la firma de documentos digitales, garantizando su autenticidad e integridad. Integrale ™ DPS se ejecuta en un dispositivo de hardware especializado (HSM). Acepta solicitudes de preparación de datos entrantes de fuentes confiables a través de servicios web de una manera segura y prepara datos con el procesamiento de seguridad.

Para documentos conformes con la ICAO, el DPS ofrece la preparación del formato de Grupos de Datos de la ICAO, así como la ejecución de la operación de firma de documentos con la clave secreta del Firmante de Documentos.

- **Generación del Par de Claves DS**: Los pares de claves DS serán generados por Integrale DPS para la firma de documentos. Una vez generado, el par de claves DS se almacenará de forma segura dentro del HSM y no podrá exportarse. La solicitud de certificado del nuevo par de claves DS se enviará a la CSCA (es decir, KMS) para la emisión del certificado DS.
- **Preparación de Datos ICAO**: Al recuperar la información, el motor integrado agrupará los datos personales de acuerdo con la estructura especificada por los Grupos de

Datos (DG) de la ICAO. Esto incluye la generación de la firma digital, dentro del HSM, con las claves del Firmante de Documentos sobre los DG ya formateados.

Garantizando el cumplimiento con las especificaciones:

- El DS dispondrá de un servicio web SOAP al que llamar para la generación de SOD y creará un SOD conforme a la OACI 9303.
- El DS utiliza algoritmos criptográficos actuales y almacena las claves privadas en un HSM.
- El acceso se da a través de una autenticación multifactorial para el inicio de sesión en la interfaz de administración.

4.1.2.3 Hardware

El hardware cumple a todos los requerimientos para implementar una infraestructura de criptografía basada en claves públicas (PKI). Está incluido en esta propuesta, la provisión, instalación, configuración y puesta en marcha de los dispositivos HSM, certificados como mínimo FIPS 140-2, así como toda la infraestructura adicional para estos dispositivos (racks, cableado de conectividad local). El HSM de nuestra oferta, ofrece característica similares o superiores a las especificaciones proporcionadas.

Categoría	UTIMACO CryptoServer
APIS criptográficos	PKCS #11 Java, Microsoft CNG (evolución de la antigua CAPI),OpenSSL CXI (Utimaco‘s comprehensive Cryptographic eXtended services Interface)
Algoritmos criptográficos asimétricos	RSA, DSA, ECDSA (NIST y Brainpool curves), ECDH (NIST y Brainpool curves), Ed25519, ECC, ECIES. Diffie Hellman (DH) y más.
Algoritmos criptográficos simétricos	AES, AES-GCM, DES, 3DES, CMAC, HMAC, y más.
Condiciones de Operación	Voltaje: 100~220V, Temp: +10°C a +40°C, Humedad (No Condensada): 20% a 90%, supera las MTBF: 150,000 horas a 25ºC.

Certificaciones de seguridad	FIPS 140-2 Nivel 3, Password and Multi-Factor (PED), eIDAS CC EAL4+, EN 419 221-5, UL, IEC/EN 60950-1, IEC/EN 62368-1, CE, FCC
Generación de números aleatorios reales (TNRG)	Cumple
Copia de seguridad de la tarjeta inteligente del material clave	Cumple
Doble conector de red	Cumple
Administración remota (vía red)	Cumple
Administración local	Cumple
Soportar interface gráfica del HSM	Cumple
Opciones múltiples para autentificación y control de acceso	Cumple
Múltiple integración para aplicaciones de PKI, servicios de encriptación	Cumple
Separación de tareas	Cumple
Sistemas operativos soportados: Windows y Linux	Cumple
Rendimiento nominal mínimo (firmas RSA /segundo, 2048 bit, modo Bulk): 25	Cumple
Habilitado para operación en cluster (alta disponibilidad)	Cumple
Debe permitir la importación / exportación de llaves internas a través de un método seguro, desde y hacia otro HSM	Cumple
El HSM deberá proveer mecanismos de detección de apertura llamados "Tamper Evidence" y ser resistentes al forzado, característica denominada "Intrusion Resistant"	Cumple

De acuerdo con los requisitos y siempre que resulte técnicamente beneficioso para el proyecto, se pueden implementar en el HSM Ultimaco algoritmos simétricos y asimétricos que no estén descritos explícitamente en el manual oficial. Este proceso se basa en la utilización del SDK, que permite la integración de algoritmos propietarios (por ejemplo, ECIES, ARIA, SEED, RC2, RC4, RC5 y CAST) y la personalización de derivaciones de claves, previa presentación de las necesidades específicas del cliente durante la ejecución. En todo momento, se mantendrán los estándares de seguridad y rendimiento que caracterizan el proyecto.

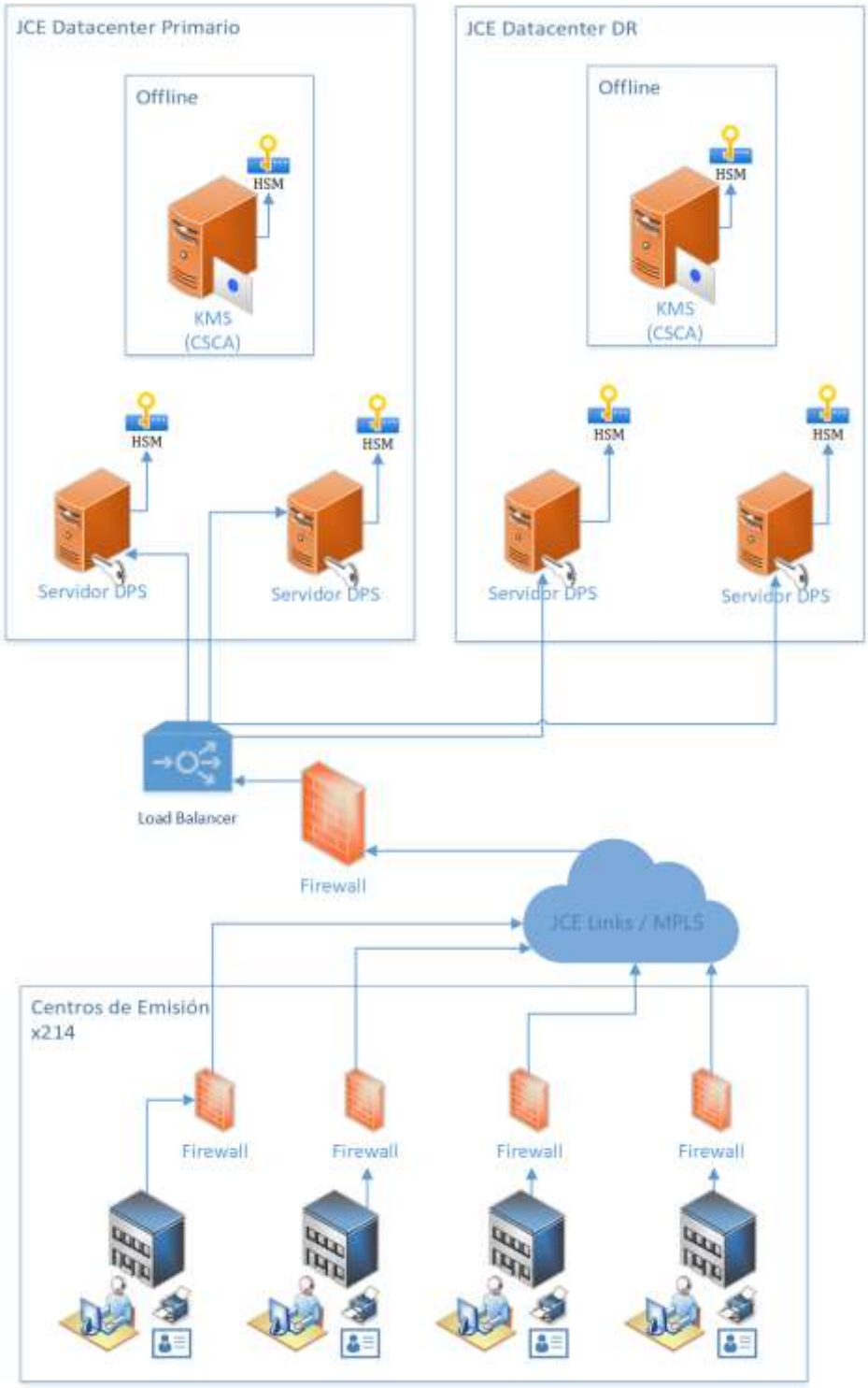
4.1.3 Integración con el sistema documentario del registro nacional

La solución propuesta considera integración de la plataforma de PKI con la solución de personalización con la que cuenta en la actualidad.

4.1.4 Soporte

La solución propuesta considera los niveles de soporte requeridos en el pliego de especificaciones técnicas. Se mantendrá la infraestructura actualizada anualmente y garantizamos su conformidad cuando sea requerida por una puesta al día de las normas y especificaciones contenidas en el Documento 9303, o cuando sea requerido por la JCE.

4.1.5 Arquitectura Propuesta



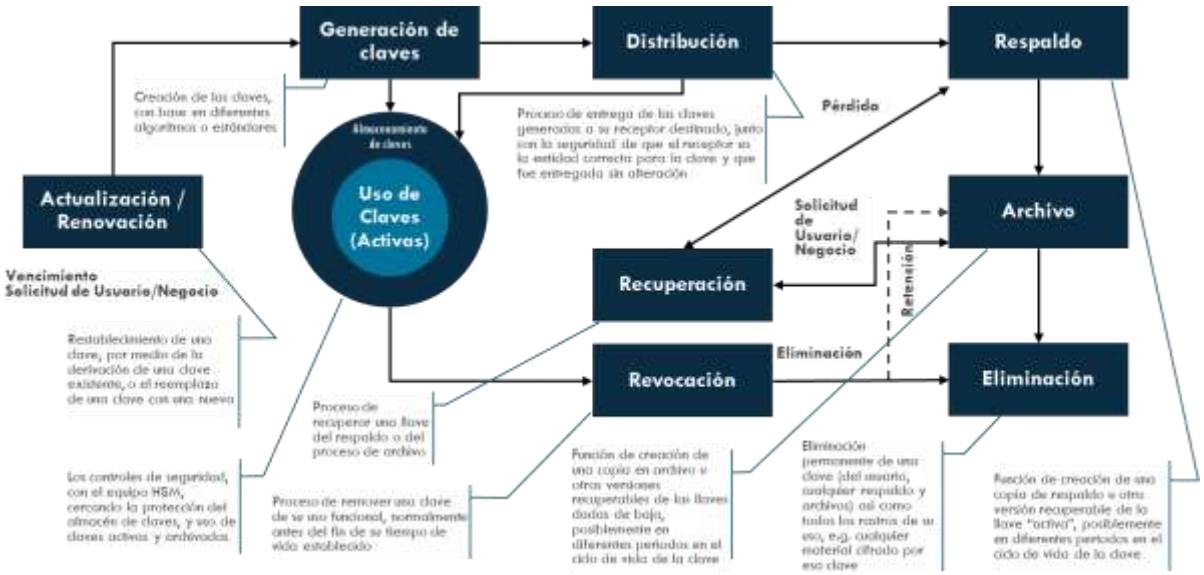
Detalles de los componentes

Gestión de las claves – Integrale™ KMS

Integrale™ KMS está diseñado para la gestión de las claves para documentos electrónicos seguros y en conformidad con ICAO. **Integrale™ KMS** proporciona una interfaz gráfica de usuario amigable para la instalación de la CA, con la generación y el mantenimiento de claves y el certificado X.509 para la firma y autenticación de documentos.

Es muy importante garantizar que el secreto criptográfico para el sistema se genere, almacene y transporte de manera segura. **Integrale™ KMS** se ejecuta en un HSM certificado FIPS-140-2 Nivel 3 (Módulo de seguridad de hardware) para garantizar la calidad de la clave generada, así como el almacenamiento seguro de claves. **Integrale™ KMS**, además, proporciona un mecanismo seguro de transporte de clave, de modo que la clave de autenticación maestra se puede exportar desde **Integrale ™ KMS** de manera segura.

Gestión del ciclo de vida clave en Integrale™ KMS



4.1.6 Operaciones Para Documentos electrónicos

Autoridad de Certificación de Firma de País (CSCA)

Esto incluye la generación de la CSCA, Firmante de Documentos (DS), el par de claves criptográficas y los certificados digitales correspondientes, exportación de los certificados auto-firmados de la CSCA y la generación de la Lista de Revocación de Certificados (CRL).
Autoridad de Certificación de Verificación de País (CVCA)

Esto incluye la generación del par de claves criptográficas Root CVCA y los correspondientes Certificados de Verificación de Tarjetas (CVC). También es compatible con la generación y emisión de certificados para Verificadores de Documentos (DV) y Sistemas de Inspección (IS) nacionales.

Generación y transporte de claves simétricas y asimétricas.

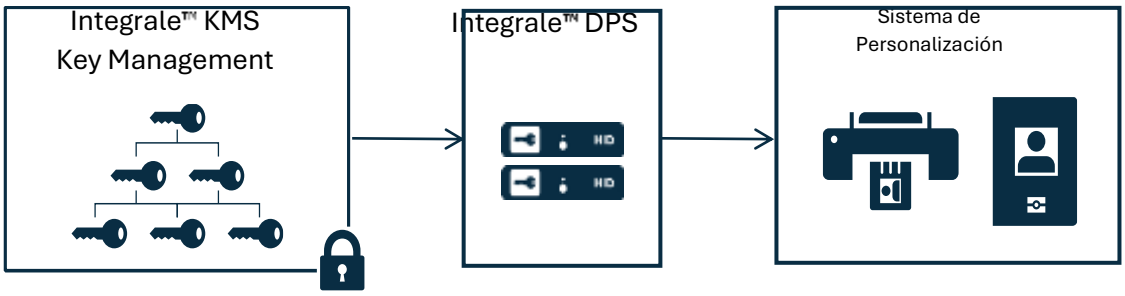
Copia de seguridad y restauración de claves: Se admiten dos modos de copia de seguridad, el formato de 3 componentes y el envoltorio de claves mediante la Clave de Zona Maestra (ZMK).

El formato de 3 componentes consiste en descomponer la llave en 3 piezas separadas para permitir el transporte de la llave en 3 rutas diferentes. La clave original podría reconstruirse solo cuando las 3 piezas se combinen juntas. Este mecanismo proporciona un alto nivel de seguridad y, por lo general, se usará para transportar la Clave de Zona Maestra (ZMK) que se utiliza para transportar otras claves secretas entre los sistemas o el dominio de seguridad. Cuando la ZMK ha sido transportada e importada con éxito, el transporte subsecuente de la llave se puede hacer envolviendo la clave en un formato cifrado por la ZMK.

- **Listado de Claves:** para mostrar todas las claves almacenadas dentro del HSM.
- **Pruebas de Cifrado y Descifrado:** para verificar la integridad de la clave.
- **Auditoría Completa de Rastreo:** en todas las operaciones en **Integrale ™ KMS** para fines de auditoría.

4.1.7 Sistema de Gestión de llaves - Integrale™ KMS

Interacción con la firma de documentos / Sistema de personalización



Integrale™ KMS: Generación de certificado CSCA y Firma de Certificados DS

Integrale™ DPS: Generación de certificados DS, almacenamiento de PMK y certificados DS firmados, preparación y provisión de datos de la aplicación en forma de script de codificación de chip junto con las claves necesarias para el sistema de personalización para la impresión y codificación de las tarjetas.

Sistema de Personalización: actualmente el sistema de personalización de la JCE.

4.1.8 Configuración - Integrale™ KMS

Esta propuesta de configuración de seguridad para el KMS incluye medidas estrictas de control de acceso, operatividad restringida y resiliencia mediante la separación de ubicaciones y administración de claves seguras.

Equipos y Control de Acceso

Infraestructura:

- 2 equipos KMS mantenidos en una habitación segura:
  - 1 x Principal
  - 1 x Respaldo
- 1 equipo KMS adicional para pruebas / desarrollo / capacitación.

Control de Acceso Físico:

- Acceso restringido a personal autorizado.

Operación y Conectividad

Operatividad:

- Operativos únicamente durante la generación y renovación de claves.
- Seguridad adicional: CSCA sin conexión a la red.

Ubicación y Resiliencia

Ubicaciones Separadas:

- Los dos equipos KMS (principal y respaldo) deben mantenerse en ubicaciones separadas para asegurar la resiliencia en caso de incidentes.
- Se instalará en las instalaciones de la JCE, los sistemas y equipos necesarios para generar conjuntos de claves para diferentes períodos de tiempo que se utilizarán para computar las Firmas Digitales que se aplicarán para la firma de los Certificados.

Administración y Control

Tarjetas de Administración:

- Operaciones administradas por tarjetas seguras:
  - Tarjetas de Administrador (Admin)
  - Tarjetas de Operador (Op)
- Cada tarjeta viene con sus propias claves / contraseñas.

Asignación de Titulares de Llave

Designación de Altos Directivos:

- Asignación de 5 altos directivos como titulares de la llave/tarjeta.

Requerimientos para Generación de Certificados

Generación Inicial:

- 5 poseedores de claves necesarios para la primera generación de certificados.

Generaciones Posteriores:

- Se requieren al menos 3 titulares de tarjeta / clave Admin / Op para cada ceremonia de generación de clave posterior.

Recuperación en Caso de Falla

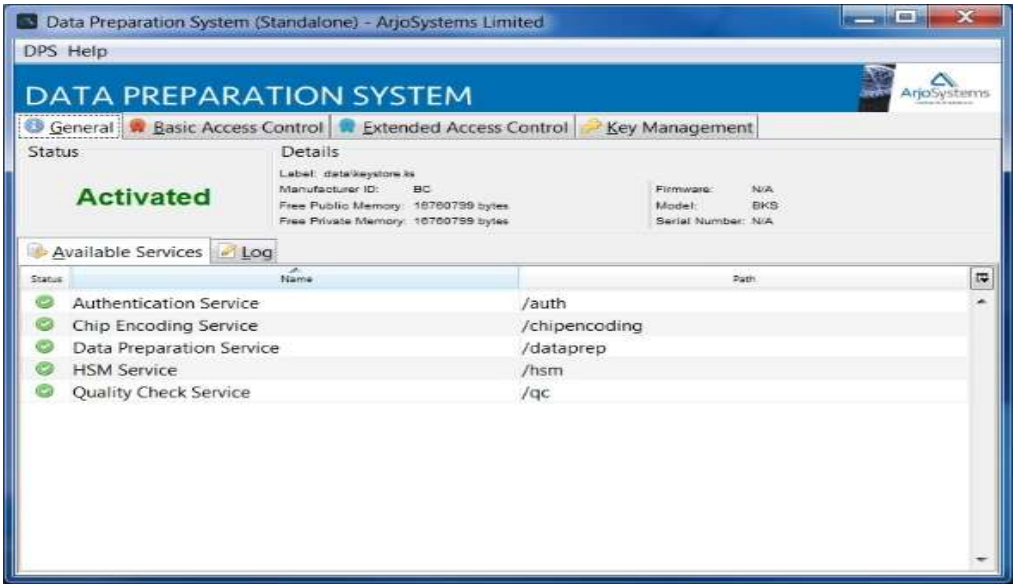
Procedimientos de Recuperación:

- El KMS será recuperable solo con las tarjetas de administración en caso de falla del sistema.

4.1.9 Preparación y Firmante de documentos (DS) – intégrale™ DPS

Integrale ™ DPS se propone como el sistema de preparación de datos para documentos electrónicos.

Integrale ™ DPS se ejecuta en un dispositivo de hardware. Acepta solicitudes de preparación de datos entrantes de fuentes confiables a través de servicios web de una manera segura y prepara datos con el procesamiento de seguridad. Para garantizar la seguridad de datos y los requisitos de privacidad durante la preparación de datos, todos los pasos de procesamiento criptográfico (p. Ej. Generación de **LDS de la OACI**, **firma de documentos** y scripts de codificación) se realizarán en un entorno de hardware seguro **Integrale ™** con un módulo de seguridad de hardware integrado (**HSM**).



A continuación, se muestran las operaciones admitidas por Integrale™ DPS en detalle.

4.1.10 Operaciones relacionadas con la OACI

Para los documentos compatibles con la OACI, Integrale™ DPS realiza la preparación del formato del grupo de datos de la OACI, así como para realizar la operación de firma de documentos con la clave secreta del firmante de documentos.

- **Generación de pares de claves DS**: El **DPS de Integrale™** generará pares de claves DS para habilitar la firma de documentos. El par de claves DS, una vez generado, se almacenará de forma segura dentro del HSM y no se podrá exportar. La solicitud de

certificado del par de claves DS recién generada se enviará al Integrale™ KMS para la emisión de certificados DS.

- **Preparación de datos de la OACI**: Al recibir la información, el motor integrado agrupará la información personal de acuerdo con la estructura de datos especificada por los Grupos de Datos (DG) de la OACI. Esto también incluye la generación de firma digital con las Claves del Firmante de Documentos dentro del HSM sobre los DG formateados.
- **Preparación de datos de chip**: los DGs firmados digitalmente se formatearán en un formato cargable específico para el chip y el sistema operativo de chip utilizado en la tarjeta electrónica. El archivo cargable se devolverá al sistema de llamadas.

4.1.11 Operaciones relacionadas con la Personalización

Clave de transporte de personalización de chip: la clave de transporte para "abrir" el chip para la personalización se transporta de forma segura al cliente final y se almacena en el HSM de Integrale™ DPS. Durante la personalización del chip, se realizará una autenticación mutua exitosa entre el chip y el DPS antes de que se puedan cargar los datos del chip.

Configuración - Integrale™ DPS

Esta propuesta de configuración de seguridad para el DPS asegura que los datos del chip estén protegidos durante la personalización y que el acceso no autorizado sea prevenido mediante el uso de HSM. La operación controlada mediante tarjetas de administrador y operador, así como la necesidad de altos directivos para la configuración inicial y recuperación del almacén de claves, garantiza un entorno seguro y bien administrado para la gestión de personalización de chips.

Equipos y Balanceo de Carga

- 4x DPS y 4 x HSM instalados en servidores de aplicaciones con equilibrio de carga.
- 1 x HSM de repuesto.

Protección y Almacenamiento de Datos

- DPS preparará los datos del chip protegidos por **autenticación pasiva y activa** durante la personalización.
- La **clave de personalización y administración del chip (PMK)** se almacenará en el **HSM** del DPS para evitar el acceso no autorizado.

Activación y Operación del DPS

- DPS debe activarse con la **tarjeta de operación** configurada para admitir la personalización del chip.

- Si el servidor de aplicaciones se reinicia, el operador debe **iniciar sesión** en el servidor y **reactivar el DPS** antes de cualquier personalización del chip.

Asignación de Titulares de Llave

Designación de Altos Directivos:

- Asignación de **5 altos directivos** como titulares de la llave/tarjeta.
- Estos directivos tendrán **tarjetas de administrador y operador**.

Requerimientos para la Configuración Inicial

Configuración Inicial:

- Se necesitarán los **5 altos directivos** para la configuración inicial.

Recuperación de Claves:

- El almacén de claves en el **DPS HSM** solo será recuperable con la **tarjeta de administrador configurada** cuando estén presentes al menos **3 titulares de claves/tarjetas**.

Operación y Activación del DPS

Se asignará **1 administrador** para **operar / activar** el DPS durante la **ceremonia de generación de claves** o después del **reinicio del servidor**.

4.2 PKI DE FIRMA DIGITAL

La PKI de Firma Digital se utiliza para garantizar la autenticidad, integridad y no repudio de documentos electrónicos. Se utiliza para firmar electrónicamente documentos como contratos, formularios, transacciones financieras, entre otros. El objetivo es proporcionar una forma segura de verificar la identidad del firmante y asegurar que el documento no haya sido alterado después de ser firmado.

Este sistema es fundamental para asegurar que **las cédulas de identidad electrónicas (CIE), certificados de nacimiento, documentos de identificación y otros registros oficiales** sean confiables y resistentes a falsificaciones.

Sera un sistema y solución integral que habilitará a los ciudadanos y demás organismos del país a gozar de los principales beneficios de la criptografía. El objetivo principal es proporcionar a los ciudadanos un medio para generar firmas digitales seguras a través de su tarjeta de identidad, garantizando validez legal y seguridad. Esto implica la generación de certificados digitales de firma avanzada.

La PKI de Firma Digital emitirá **certificados digitales** de firma que estarán destinados a ser alojados dentro de las nuevas CI y CIE, con chip sin contacto (contactless) con funcionalidad de firma electrónica. Además de la emisión de certificados digitales de firma avanzada, el Sistema de PKI de Firma Digital dispone la posibilidad de integrar servicios de validación de certificados en línea, sellados de tiempo, portales de gestión del ciclo de vida de los certificados digitales para la JCE, portales de firma de documentos y demás servicios de validación para ciudadanos y otros organismos.

En este contexto, **MAGALLANES MEDIA**, como especialista en identidad digital, infraestructura de clave pública y autenticación remota dentro del consorcio, desempeñará un papel clave en el desarrollo y gestión de esta infraestructura, asegurando su integración con plataformas de validación en línea, sistemas gubernamentales y aplicaciones móviles. La experiencia de **MAGALLANES** en la interoperabilidad de credenciales electrónicas e infraestructura de clave pública fortalecerá la **PKI de Firma Digital**, garantizando su cumplimiento con los estándares internacionales y optimizando su operatividad en entornos digitales y físicos.

4.2.1 Características generales de la PKI de Firma Digital

El sistema de PKI de Firma Digital contempla tanto un Servicio de Autoridad de Certificación (CA) como un Servicio de Protocolo de Estado de Certificados en Línea (OCSP), que pueden ser implementados por la JCE para satisfacer una variedad de casos de uso en negocios digitales, incluida la generación de certificados digitales de firma avanzada. La PKI propuesta proporciona una Autoridad de Certificación (CA) y una Autoridad de Validación OCSP de alto rendimiento, robusta y confiable, que cumple con los estándares RFC 5280, RFC 6960 y RFC 5019. El sistema de PKI de Firma Digital cuenta con la certificación Common Criteria EAL 4 y cumple con los requisitos del Perfil de Protección Aprobado por el Gobierno para Autoridades de Certificación v.2.1 (2017) de la National Information Assurance Partnership. Esto significa que el Servidor PKI está certificado según el perfil de protección más reciente para CA y con un alto nivel de seguridad.

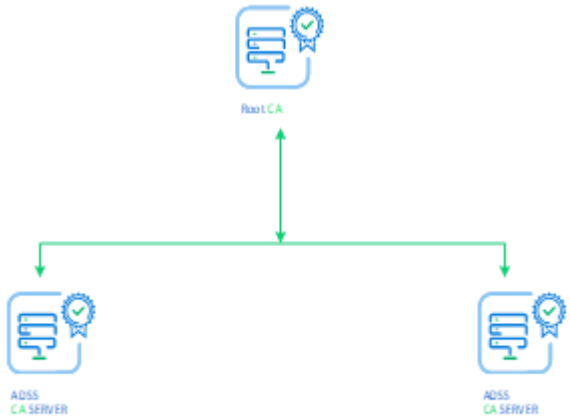
El Servicio de Certificación, la Autoridad de Certificación (CA), permite que las aplicaciones cliente soliciten la generación de claves y la emisión de certificados en nombre de los usuarios finales. En esta oportunidad específica, las claves de firma se generarán directamente en las nuevas CI y CIE, con chip sin contacto (*contactless*), y el Servicio de Certificación solo recibirá una solicitud de firma de certificado (CSR).

4.2.1.1 Generación de certificados digitales de firma avanzada x.509. CA dedicada de firma digital

La Autoridad de Certificación (CA), permite que las aplicaciones cliente soliciten la generación de claves y la emisión de certificados en nombre de los usuarios finales o clientes.

En esta oportunidad específica, las claves de firma se generarán directamente en la nueva tarjeta CI y CIE, y el Servicio de Certificación solo recibirá una solicitud de firma de certificado (CSR) de la Autoridad de Registro.

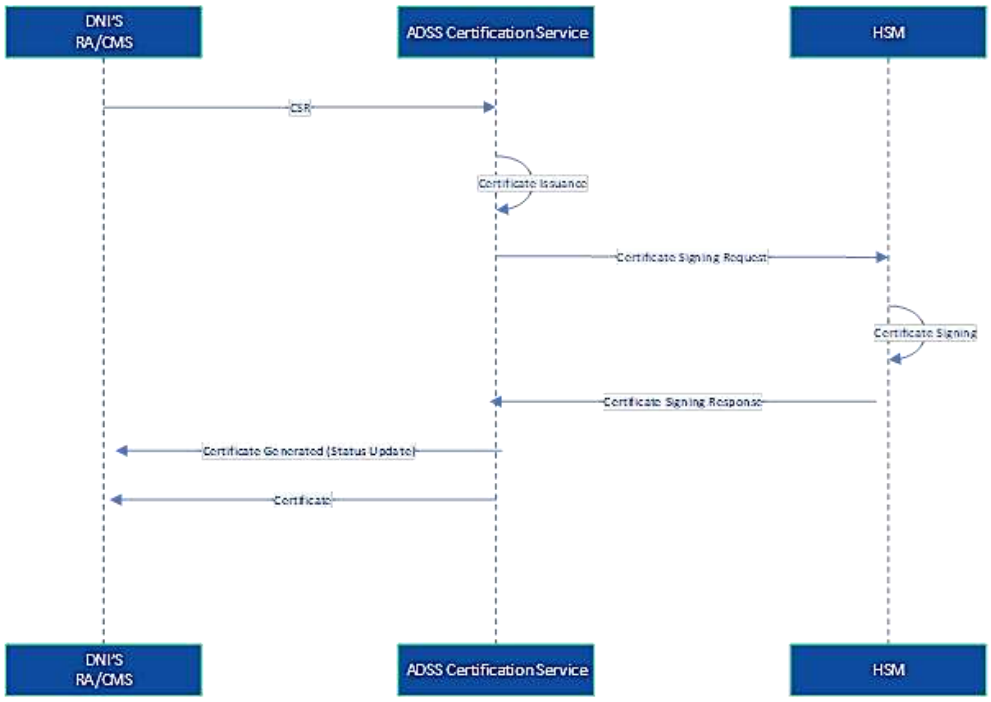
Estamos proponiendo, al menos, una estructura de PKI de dos niveles, que consta de una Autoridad de Certificación raíz (CA) y CAs subordinadas emisoras en alta disponibilidad, como se muestra en la siguiente figura.



De esta manera, La **PKI** establecerá un dominio y cadena de confianza compuesto por los siguientes elementos:

- **Autoridad de Certificación Raíz (Root CA):** También llamada **CA Raíz**, esta CA estará fuera de línea y actúa como el ancla de confianza para la PKI de Firma Digital. Firma los certificados de su autoridad de certificación subordinada y las listas de revocación de autoridad asociadas (**CRLs**).
- Dispondrá de un HSM para almacenar de manera segura las llaves de la CA raíz.
- **CA Emisora:** Una CA en línea y de alta disponibilidad con dos nodos, responsable de firmar y crear los certificados x.509 de los usuarios finales y las listas de revocación de certificados (**CRLs**) asociadas.
- Según las necesidades de la JCE y la demanda de certificados es posible escalar el sistema y comisionar nodos y Cas emisoras adicionales.
- Cada nodo y CA emisora contará con su propio HSM dedicado.

A la hora de la generación de los certificados de firma x.509, el siguiente diagrama secuencial ilustra la interacción a alto nivel entre los diversos componentes involucrados en el caso de uso de generación de certificados.



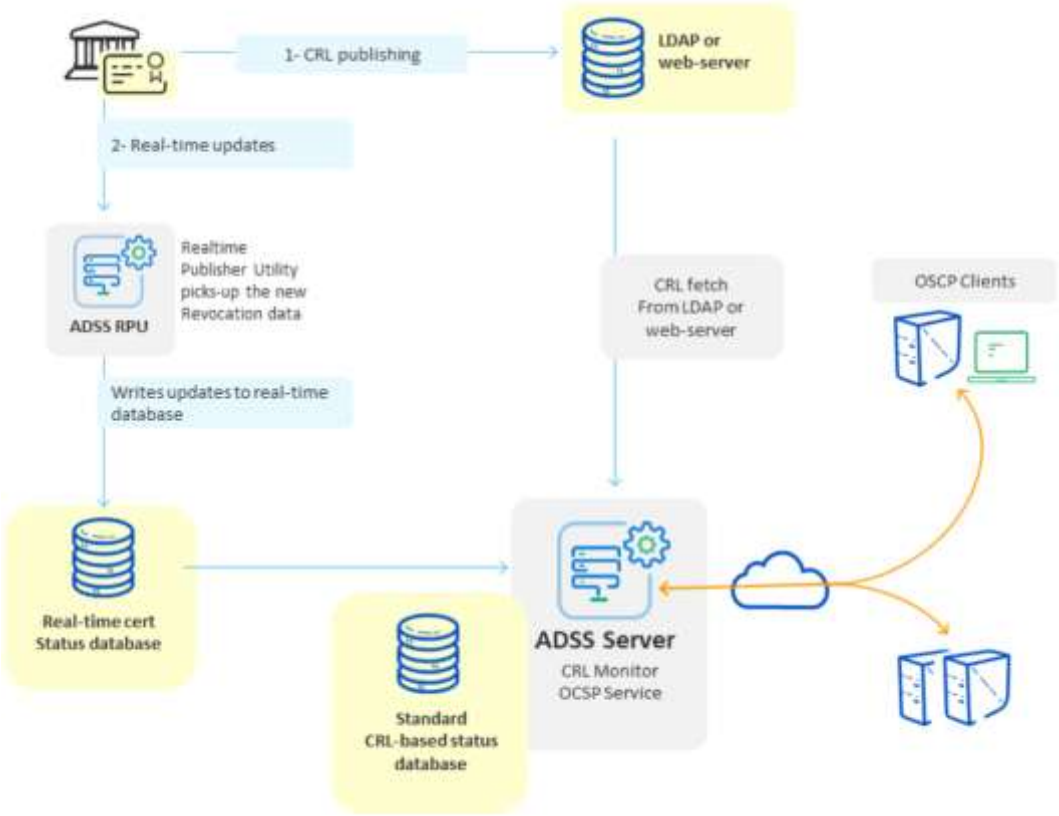
4.2.2 Servicio de validación de certificados (OCSP)

El servicio de protocolo de Estado de Certificados en Línea (OCSP) ayudará a las partes confiables a verificar el estado de un certificado y determinar si es válido o ha sido revocado, basándose principalmente en la lista de revocación de certificados (CRL) de la CA correspondiente.

A continuación, se describe el mecanismo clásico de funcionamiento del Servicio OCSP:

- Un usuario final firma utilizando su clave de firma almacenada en su tarjeta inteligente.
- La aplicación de la parte confiable desea delegar la complejidad de la verificación del estado del certificado al *backend* de la PKI de Firma Digital, por lo que realiza una solicitud OCSP al Servicio OCSP e incluye el identificador del certificado digital en la solicitud.
- El Servicio OCSP realiza todas las verificaciones estándar del estado del certificado y devuelve la respuesta OCSP a la aplicación cliente.

Dependiendo de las necesidades y restricciones del DNI, el servidor OCSP debe implementarse de manera que revele el estado del certificado en tiempo real. Para ello, se puede proponer fortalecer el servicio OCSP con Real-Time Publishing Utility (RPU).



Con respecto a la Lista de Revocación de Certificados (CRL), el DNI tiene varias opciones para su almacenamiento, incluyendo LDAP, un servidor web o una base de datos. La elección específica del método de almacenamiento dependerá de los requisitos de infraestructura y accesibilidad de la JCE y los organismos que precisen realizar este tipo de consultas.

Además, los detalles de implementación tanto del OCSP (Protocolo de Estado de Certificados en Línea) como de la CRL serán discutidos y finalizados en las etapas posteriores del proyecto para garantizar un sistema sólido y seguro de verificación del estado de los certificados.

De todas maneras todos los sistemas necesarios para realizar OCSP, generar y publicar listas de revocación de certificados están incluidos dentro del alcance de esta propuesta.

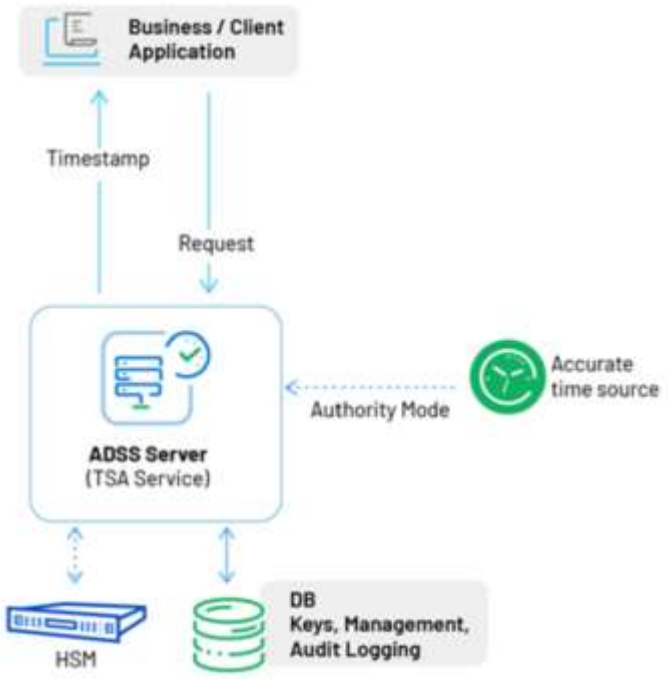
4.2.2.1 Servicio de autoridad de sellos de tiempo, TIME STAMPING AUTHORITY (TSA).

El módulo de servicio TSA producirá principalmente tokens de marca de tiempo para documentos firmados, para demostrar la existencia de los datos de origen de entrada o el hash seguro de los datos en un momento y fecha específicos.

El módulo TSA produce tokens de marca de tiempo RFC 3161 y RFC 5816 para cualquier dato electrónico, para demostrar la existencia de los datos de origen de entrada (o el hash seguro de los datos) en un momento y fecha específicos. El servidor TSA cumple con los requisitos ETSI EN 319 422 y EN 319 421 para servicios TSA.

Existen dos formas diferentes en las que se puede utilizar el servicio TSA para producir tokens de marca de tiempo:

- TSA local: Utilizar el servicio TSA local y las claves locales de firma de marca de tiempo; o
- TSA externa: Enviar la solicitud de marca de tiempo a otro TSA externo. En este caso, el servicio TSA actúa como un concentrador de solicitudes de marca de tiempo, las cuales son atendidas por uno o más TSAs en el backend.



El TSA se utiliza para sellar temporalmente documentos, firmas digitales y mensajes de respuesta de verificación / OCSP para confirmar su validez en un momento específico.

Fortalecer la PKI de Firma Digital con un TSA le permitirá asegurar lo siguiente:

- **Emisión de marcas de tiempo:** El TSA utiliza su certificado confiable para crear un token de marca de tiempo que registra de manera segura el momento exacto en que se creó el documento o la firma digital.
- **No repudio:** La marca de tiempo asegura que la firma no pueda ser fechada de forma retroactiva ni adelantada, evitando cualquier reclamo de que el documento fue firmado en un momento diferente.
- **Validación a largo plazo:** Los TSAs son cruciales para la validación a largo plazo de las firmas, ya que permiten verificar la validez de un documento mucho después de que haya caducado o sido revocado el certificado utilizado para firmarlo.

El módulo de servicio TSA podrá ser sincronizado con la hora oficial de la República Dominicana y las llaves del servicio podrán estar almacenadas en software o hardware. Asimismo, las timestamps podrán ser parta de los elementos que tiene cada firma electrónica.

4.2.3 Portal de gestión del ciclo de vida de los certificados digitales de firma avanzada.

Gestionar certificados digitales de manera efectiva es un requisito clave para cualquier equipo de seguridad informática. El portal de gestión del ciclo de vida de certificados lo hace de manera rápida, simple y segura. Los administradores de seguridad autorizados de la JCE pueden monitorear, revisar y aprobar solicitudes de emisión de certificados, renovar certificados antes de que caduquen y revocar certificados desde una interfaz intuitiva y segura en un navegador web. El portal de gestión del ciclo de vida proporciona notificaciones automáticas de estos eventos críticos en tiempo.

El portal es una aplicación de autoridad de registro de interfaz frontal que aprovecha el poder de la CA de la PKI de Firma Digital para emitir y gestionar directamente el ciclo de vida de los certificados. El portal ofrece una experiencia de usuario intuitiva tanto para administradores como para usuarios finales. Los administradores pueden crear fácilmente flujos de trabajo de inscripción para la obtención de certificados de usuario final o la inscripción de certificados de servidor basados en solicitudes de firma de certificados PKCS#10.

El portal y sistema global de gestión de ciclo del vida de los certificados digitales de firma avanzada permite a desarrolladores integrar la emisión de certificados de manera programática al exponer una API Rest, lo que facilita la integración de la gestión del ciclo de vida de certificados en otras aplicaciones. Este sistema también proporciona protocolos de inscripción estándar de la industria, lo que habilita integraciones de dispositivos y aplicaciones. Las organizaciones pueden emitir y gestionar certificados sin problemas utilizando protocolos estándar del mercado como SCEP.

Para acceder al portal cada usuario autorizado por la JCE deberá tener un certificado de autenticación.

4.2.4 Portal de firma de documentos

Dentro del alcance de esta propuesta estamos incluyendo el uso y acceso a un portal de firma de documentos con el estándar ISO 32000-1 y más avanzado para documentos portátiles PDF.

El portal de firma es un portal web que permite la aprobación en línea rápida y eficiente de cualquier documento empresarial, acuerdo, informe, solicitud o paquete. En este caso será configurado para poder utilizar el certificado digital de firma avanzada x.509 que emitirá el sistema de PKI de Firma Digital y se alojará en la nueva cédula física. Además el portal de firma es compatible con otros productos y servicios de terceros.

El portal web permite firmas electrónicas básicas, firmas electrónicas avanzadas y firmas electrónicas cualificadas del estándar de la Unión Europea. La mejor manera de demostrar que un documento no ha cambiado desde su firma es mediante firmas digitales criptográficas.

El portal web de firma se enfoca en el mercado de alta confianza, permitiendo el uso de esquemas PKI, así como otros certificados de alta confianza, incluidos aquellos reconocidos por Adobe Reader y Word para la seguridad persistente de documentos.

La interfaz web facilita la firma para cualquier usuario. Los documentos pueden compartirse, visualizarse y firmarse en cualquier dispositivo, en cualquier lugar y en cualquier momento, adaptándose a cualquier proceso de aprobación. Se admiten más de 20 idiomas, y otros pueden agregarse o personalizarse fácilmente. Utiliza firmas de larga duración estándar PDF PAdES y Word XAdES. Esto significa que los documentos firmados pueden verificarse de forma independiente, sin necesidad del portal, mediante cualquier lector de documentos compatible, como Adobe Reader, lectores de PDF de terceros, Microsoft Word, Office 365 u otro software compatible.

4.2.5 Otras características del portal de firma:

✓ Compatible con **firmas remotas cualificadas** con **Nivel 2 de Control Exclusivo**.

Compatibilidad con formatos de documentos estándar:

- **PDF**
- **PDF/A-1** (a, b)
- **PDF/A-2** (a, b, u)
- **PDF/A-3** (a, b, u)
- **Documentos de Word**

✓ Todos los documentos están protegidos mediante **cifrado AES-256 bits**.

✓ Ofrece múltiples opciones de autenticación, incluyendo:

- **Microsoft Active Directory**
- **OAuth**
- **SAMLv2**
- **Freja eID**
- **BankID**
- **eID Easy**
- **Office 365**
- **Salesforce**, entre otros.

Evidencia firmada digitalmente:

Todas las operaciones realizadas por los usuarios quedan registradas en un **informe firmado digitalmente**, detallando todas las interacciones con el documento y el flujo de trabajo.

Dentro del alcance estamos incluyendo acceso a este portal para 100 usuarios de la JCE por año para satisfacer los roles de: 1. Administrador, con todos los permisos, esta figura debe poder generar y/o enrolar Agentes Certificadores; 2. Agente Certificador con permisos para enrolar y/o generar certificados para los usuarios finales o firmantes; 3. Firmante, son los usuarios que podrán firmar los documentos.

1. **Características adicionales del sistema PKI de Firma Digital**

- Se contempla una **ceremonia de llaves** y creación de una CA raíz para todo el ecosistema de PKI de Firma Digital.
- **El vencimiento del certificado raíz será configurado a 10-20 años** o a convenir con la JCE.
- **Los vencimientos de los certificados intermedios serán configurados a 5-10** años o a convenir con la JCE.
- **Los vencimientos de los certificados de usuario final y servidor serán configurados a 1-3 años** o a convenir con la JCE.
- Se incluyen los **manuales de operación** de todos los componentes, ceremonia de llaves, procedimientos (CA raíz, renovación de certificados de CA subordinadas, recuperación de desastres)
- Se incluye toda la documentación del sistema de PKI de Firma Digital para definir las **características del certificado digital** de firma electrónica avanzada x.509, la definición de perfiles, sellado de tiempo, protocolos OCSP, y la referencia de todas las APIs para interactuar el sistema e integrarlo con distintas aplicaciones.
- Se incluye el **mantenimiento** de todo el ecosistema de firma digital a dos años.
- Se contempla **la generación, manejo y almacenamiento seguro** de claves criptográficas.
- La oferta incluye toda **la infraestructura física y software necesario** para la implementación, ejecución y mantenimiento de la PKI de Firma Digital, el conjunto de hardware y software en las instalaciones que indique la dirección de informática. El contrato de mantenimiento a cotizar es de dos (2) años. A partir de los dos años, la JCE podrá renovar el mantenimiento con el precio establecido del proveedor de forma anual.
- Se incluye para la solución de la PKI de Firma Digital un ambiente productivo en **alta disponibilidad** con al menos 2 nodos activos en balanceo de carga, un ambiente de DRP en disponibilidad simple (1 nodo) y un ambiente de desarrollo en disponibilidad simple (1 nodo).

- Toda la infraestructura de PKI de Firma Digital utilizará **módulos de seguridad por hardware (HSMs)** certificados (FIPS 140-2 nivel 2 o superior) para la generación y almacenamiento de claves privadas. La PKI de Firma Digital utilizará los mismos módulos HSM que la PKI de Firma de Documentos que cumplen con todos los requisitos de esta licitación y están detallados en la sección de PKI de Firma de Documentos.

- Para el caso del tamaño de llaves de la Autoridad ciudadana, tanto la **Autoridad Raíz como la Autoridad Subordinada** deberán tener un tamaño de llaves de 4096 bits. Para el caso de los certificados de usuario (ciudadanos) será de 2048 bits o a convenir previo al lanzamiento del proyecto.

- Se contempla que **las nuevas cedulas CI y CIE** puedan cambiar o ampliar su funcionalidad una vez se hayan entregado al ciudadano, en particular hablando de los certificados de firma digital que podrán tener un vencimiento diferente al documento físico en cuyo. En este caso se proveerá la administración de todo el ciclo de vida de estos (generación, actualización y revocación) en la electrónica de los documentos.

- La oferta incluye la generación de certificados digitales de firma dentro del **ambiente de pruebas**.

- Se incluye todo el **software y middleware** necesario para que la JCE desarrolle la integración entre la PKI y el Chip *contacless*.

- La oferta incluye la emisión de 1,000 certificados x.509 por año no acumulable y no prorrogable, por los primeros dos años, para permitirle a la JCE integrar y configurar correctamente todo el ecosistema de firma digital.

- Se provee la funcionalidad de **revocación de certificados** y sello de tiempos.

- El sistema propuesto estará bien **protegido** de cualquier acceso externo o no autorizado a través del diseño inherente y las instalaciones de seguridad de hardware y tendrá medidas de seguridad robustas, entre otras:

  - Se incluye la implementación de sistemas avanzados de monitoreo y detección de intrusos (IDS/IPS). El monitoreo incluye de infraestructura, de seguridad y de comunicaciones

  - Autenticación multifactorial (MFA para acceso a la administración). Cifrado avanzado en todas las comunicaciones y datos almacenados, utilizando algoritmos criptográficos robustos y actuales.

- Segmentación de redes que aísle la infraestructura de PKI de otras redes.
- Mantenimiento de todos los sistemas y software de la PKI actualizados con los últimos parches de seguridad.
- Realización de auditorías regulares y evaluaciones de seguridad.
- Capacitación del personal involucrado en la operación y gestión de la PKI sobre las mejores prácticas de seguridad y procedimientos de respuesta a incidentes.

5. PLATAFORMA DIGITAL PARA CÉDULAS

Para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos dentro del nuevo sistema de cédulas de identidad, el **Consorcio IDSecure IDS** ha seleccionado a **TOPPAN SECURITY SAS (antiguo HID Global)** como proveedor de la Infraestructura de Clave Pública (PKI), implementando su solución GoID. GoID es una plataforma avanzada de identidad digital que permite la emisión segura de certificados digitales, la gestión de claves criptográficas y la autenticación de identidad en entornos físicos y digitales. Esta tecnología cumple con los estándares internacionales establecidos por la OACI (Doc 9303), ISO 15408 y eIDAS, asegurando la interoperabilidad, seguridad y confiabilidad del sistema.

5.1 GoID™: Introducción de Identidad Móvil Nacional

La solución de identidad digital **goID** consiste en una **SDK** que facilita la generación de un documento digital de alta seguridad en el dispositivo móvil del usuario, representando una alternativa conveniente, segura e instantánea a los documentos de identificación físicos tradicionales. Utilizando avanzados algoritmos de cifrado de datos y estrictas medidas de seguridad en la comunicación, **goID** reduce significativamente el riesgo de robo de identidad y mejora la privacidad de los ciudadanos.

GoID convierte un dispositivo móvil en un medio confiable para la verificación de identidad, eliminando la necesidad de portar documentos físicos que pueden ser perdidos, robados o falsificados. Esta solución aprovecha la tecnología de vanguardia para garantizar que solo el propietario legítimo del dispositivo pueda acceder a su identidad digital, proporcionando una capa adicional de seguridad.

Los robustos algoritmos de cifrados empleados por **goID** aseguran que los datos de identidad estén protegidos en todo momento, tanto en almacenamiento como en tránsito. Esto significa que cualquier intento de interceptar o manipular los datos será infructuoso, manteniendo la integridad y confidencialidad de la información del usuario.

Además, las medidas de seguridad de comunicación implementadas por **goID** garantizan que cada transacción y verificación de identidad se realice de manera segura. Estas medidas incluyen autenticación de dos factores, biometría y otras tecnologías avanzadas que hacen que la falsificación o el acceso no autorizado sean prácticamente imposibles.

La adopción de **goID** no solo mejora la seguridad, sino que también simplifica el proceso de verificación de identidad, haciendo que sea más rápida y eficiente. Esto es especialmente útil en situaciones donde la verificación rápida de identidad es crucial, como en el acceso a servicios gubernamentales, financieros y de salud.

GoID representa el futuro de la identidad digital, combinando seguridad avanzada, conveniencia y eficiencia para ofrecer una solución robusta que protege la identidad de los ciudadanos y facilita su uso en la vida cotidiana.

5.1.1 Características Generales

De acuerdo con el Pliego de Especificaciones, ITEM VI - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL. Nuestra solución es diseñada para cumplir con los requisitos y criterios técnicos, asegurando cumplimiento con el Doc. 9303 de la OACI.

Es parte el alcance de suministro, software, hardware, licencias y cualquier otro requisito necesario para implementar el servicio de identificación digital en dispositivos móviles y cumplir con los estándares ISO18013-5. Estamos conscientes del "Guiding Core Principles for the Development of Digital Travel Credential (DTC) de octubre de 2020" y nuestra solución es también compatible con la implementación de DTC. La solución implementada será escalable y optimizable para adaptarse a la evolución de la demanda de este tipo de documentos.

Se implementará la solución de identidad digital dentro de un plazo menor al de 4.5 meses, después de la firma del contrato. Esta solución será administrada por la JCE e integrada al sistema nacional de identidad mediante el uso de API's para la identificación y verificación de la identidad de los ciudadanos. La tarjeta digital podrá ofrecer (si las leyes lo permiten) las mismas garantías jurídicas al titular que el CEI o CI.

El Consorcio será responsable del desarrollo y exposición de las APIs necesarias para la integración del sistema de identidad digital con la infraestructura de la JCE, asegurando la interoperabilidad con las bases de datos existentes en SQL Server 2022 y siguiendo el modelo de arquitectura cliente-servidor.

Los datos son entregados firmados electrónicamente por la JCE. Esta firma electrónica certificada permitirá que terceros validen tanto la integridad como la procedencia de los datos presentados por el ciudadano. Tanto la firma de los datos como su validación se realizarán utilizando los certificados electrónicos administrados por la JCE, como Autoridad Certificadora descrita en el apartado de Infraestructura de Clave Pública.

5.1.2 Aspectos de la Tarjeta Digital

De acuerdo con el Pliego de Especificaciones, ITEM VI - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL. La solución de Tarjeta Digital cumple con las siguientes características:

- La solución incluye el sistema de gestión del ciclo de vida de las credenciales digitales, de forma que se registren los eventos de acceso a cada credencial, así como proporcionar las aplicaciones o interfaces necesarias para la implantación de nuevas soluciones.
- La solución incluye un canal de comunicación que utiliza algoritmos de cifrado para conectar los dispositivos y ejecutar el proceso de verificación. Dependiendo del caso de uso y de la disponibilidad del dispositivo, se emplean protocolos NFC (Near Field Communication) y/o BLE (Bluetooth Low Energy), asegurando siempre el cumplimiento de la norma ISO 18013-5.
- La solución tiene las funciones de recepción, almacenamiento y protección segura de credenciales digitales en aplicaciones móviles, así como el uso de notificaciones PUSH para enviar mensajes masivos o personalizados al titular de la credencial digital.
- La solución utilizará durante el proceso de emisión o activación de la identidad digital, el mecanismo de *liveness detection* (prueba de vida), para prevenir ataques de presentación. El mecanismo de *liveness detection* utilizará la plataforma de liveness de Magallanes Media que cuenta la certificación ISO 30107-3. Los documentos que acreditan esta certificación se incluyen en esta propuesta.
- La aplicación móvil proporcionará al titular del documento de identidad digital el desbloqueo de la App mediante autenticación de dos factores (2FA).
- La aplicación móvil propuesta funciona sin conexión con la internet, permitiendo la visualización local de los datos de las credenciales digitales, utilizando un método de verificación de la autenticidad de la identidad digital. También tendrá la capacidad de realizar consultas en línea, en caso de que se requiera llevar a cabo algún tipo de verificación de la información del titular de la identidad digital.
- La aplicación móvil permite que la visualización del documento de identidad digital se diseñe según las especificaciones de la JCE, ofreciendo una vista de pantalla completa con las visualizaciones del anverso y reverso al tocar la credencial, y mostrando los mismos datos que el documento de identidad físico. Sin embargo, para prevenir situaciones potenciales de fraude, como el conocido *Flashpass*, donde el portador del documento digital muestra solo una foto del documento en pantalla para hacerse pasar por verdadero, recomendamos que los datos visualizados en las credenciales digitales sean mínimos para reforzar la verificación a través de la app y garantizar su autenticidad.

- La aplicación móvil tiene la capacidad de compartir únicamente la información que el titular de la identidad digital desee compartir, en el momento de la verificación de la identidad.
- Las aplicaciones móviles informarán al titular cuando su identidad digital ha sido revocada, mediante una alerta al entrar en la App, indicando el cambio en la validez de su documento digital.
- La solución propuesta incluye mecanismos de protección contra ataques que incluyan, entre otros, ingeniería inversa, manipulación de código, detección de rooting/jailbreak/debugging, etc.
- La solución propuesta posee capacidad de incorporar información en las imágenes de los solicitantes como medidas de seguridad complementarias.
- Incluir información en imágenes de solicitantes
- La solución permitirá la incorporación de información visual de seguridad en las imágenes de los solicitantes (por ejemplo, marcas de agua, códigos cifrados, etc.).

5.2 Características Técnicas de la solución propuesta

En complemento a los aspectos mencionados anteriormente, la solución cuenta con las siguientes características técnicas:

- **Certificación:** ISO/IEC 18013 Parte 5. La solución ofrecida contará con la certificación ISO/IEC 18013 Parte 5.
- **Herramientas de Desarrollo:** Se hará disponible la SDK y API para uso del personal técnico de la JCE o terceros.
- **Integración de Servicios:** Integrará con los sistemas de identificación de la JCE.
- **Infraestructura PKI:** La solución utilizará la PKI para emisión de documentos digitales (IACA).
- **Aplicaciones Móviles:** La solución será multiplataforma compatibles con iOS y Android.
- **Seguridad:** La solución incluirá protección contra ingeniería inversa y clonación.
- **Activación Remota:** La solución incluirá un mecanismo para activación remota de identidad digital, considerando el tiempo de validez del enlace (unas horas), el mismo se podrá enviar por correo electrónico, mensaje de texto u otro medio a determinar. Se manejara un doble factor de autenticacion 2FA.
- **Liveness Detection:** La solución utilizará *liveness detection*, como mencionado anteriormente, para el proceso de activación de identidad digital remota para la prevención de suplantación de identidad. El sistema estará de acuerdo con el estándar de referencia ISO 30107-3, y se presentará certificación de cumplimiento de ISO 30107-3.

- **Alta Disponibilidad:** La plataforma contará con un esquema de alta disponibilidad de servicio.
- **Interoperabilidad:** La plataforma permitirá la interoperabilidad y escalabilidad del servicio para la implementación de diferentes mecanismos de control de dispositivos.
- **Intercambio de Datos:** La aplicación de identidad móvil permitirá intercambio de datos personales iniciado por el titular de acuerdo con la norma ISO/IEC 18013-5.
- **Selección de Datos:** La aplicación de identidad móvil permitirá la selección de campos específicos para compartir y las categorías de campos.
- **Administración de Emisiones:** La solución incluirá el sistema para administración de la emisión de identidades digitales para evidenciar el registro de eventos y accesos, incluyendo las interfaces necesarias para nuevas soluciones.
- **Seguridad de Comunicaciones:** Asegurará todas las comunicaciones entre aplicaciones móviles, incluyendo las interacciones en línea y fuera de línea.
- **Canales de Comunicación:** La solución propuesta utiliza algoritmos de encriptación en canales de comunicación, en detalle en la sección de Componentes.
- **Funcionalidades de App:** La solución proveerá las funciones para recibir, guardar y proteger credenciales digitales. Se demostrará el uso de notificaciones PUSH y almacenamiento seguro.
- **Autenticación:** Las aplicaciones móviles permitirán el desbloqueo de la App mediante autenticación de dos factores (2FA), como mínimo PIN y verificación facial.
- **Funcionalidad Online / Offline:** Las aplicaciones móviles permitirán el funcionamiento offline para visualización de datos y también permitirán consultas en línea.
- **Visualización de Documentos:** Permitirán la visualización de documentos de identificación digital en pantalla completa y el cambio de anverso a reverso, conforme especificado por la JCE.
- **Compartir Información:** Tendrán la capacidad de compartir información seleccionada durante la verificación de identidad.
- **Notificaciones de Revocación:** Informarán al titular sobre la revocación de su identidad digital mediante alertas en la App.
- **Capacidad de Servicio:** Al menos 5,000 solicitudes diarias de credenciales digitales. La solución será modular y escalable para adaptarse a la evolución en la demanda de este tipo de documentos.
- **Interfaces de Comunicación:** Utilizarán e integrarán con interfaces de comunicación existentes para el envío de órdenes de emisión por parte de la JCE.
- **Análisis de Interfaces:** Se proporcionará un plan de análisis y pruebas para el ajuste de interfaces de comunicación propuestas por la JCE, incluyendo la definición de escenarios de prueba.

- **Consistencia de Datos:** Mantendrán la consistencia de estados entre soluciones para el proceso de actualización y sincronización al sistema institucional para la identificación de personas.
- **Disponibilidad de Operación:** Garantizamos disponibilidad del 99.95% durante horas de producción, excepto por razones atribuibles a la JCE.
- **La aplicación permitirá generar un código bidimensional** que contendrá los datos del ciudadano y su respectiva firma electrónica certificada. Además, el usuario podrá seleccionar qué datos compartir a través de dicho código bidimensional, garantizando privacidad y seguridad en el intercambio de información

5.3 App Ciudadana

Dentro del alcance de esta propuesta se incluye el desarrollo y mantenimiento a dos años de lo que se denomina la app ciudadana contenedora de la credencial digital.

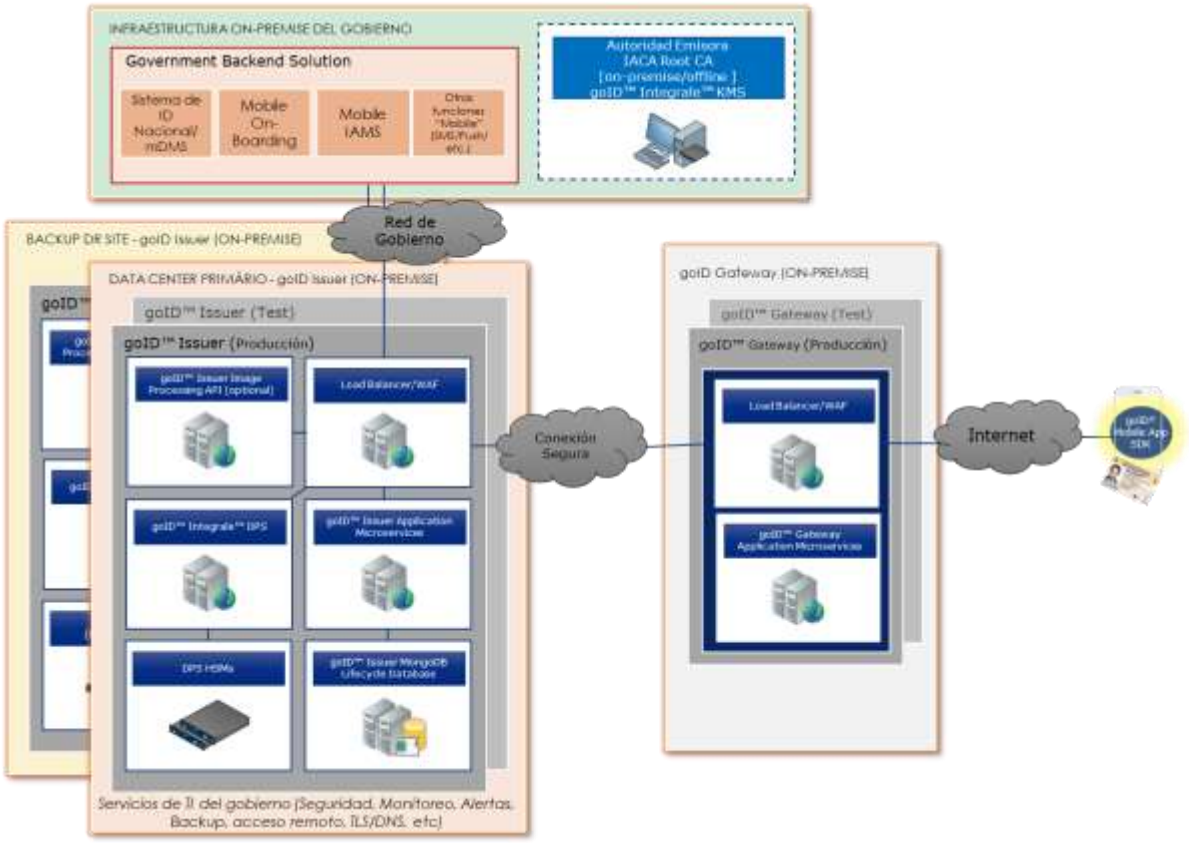
La app tendrá las siguientes funcionalidades y características

- Integración del SDK goID para poder alojar y verificar la cédula digital
- Flujo de verificación de identidad del ciudadano previo a la solicitud y emisión de la cédula digital. El flujo de provisionamiento de la credencial digital será de la siguiente manera. O a convenir entre el consorcio y la JCE.
    - Enrolamiento y onboarding del ciudadano en la app. Creación de usuario
    - Lectura del MRZ de la cédula física mediante OCR y la cámara del dispositivo móvil.
    - Desbloqueo del chip contactless mediante NFC para Basic Access Control (BAC) y levantar los datos biométricos y biográficos del chip.
    - Verificación biométrica con reconocimiento facial y prueba de vida (liveness detection) entre el usuario tenedor de la app y los datos biométricos del chip contactless en la cédula física. La prueba de vida será pasiva con el sistema de Magallanes Media que cumple con **la certificación ISO/IEC 30107-3**.
    - Emisión y descarga de la cédula digital en base a los datos biométricos y biográficos del chip contactless en la cedula física.
- Módulo para compartir datos de la credencial digital con otros dispositivos verificadores
- Capacidad de actuar como verificador de otras cédulas digitales si la JCE lo desea.
- Diseño gráfico y UI a convenir con la JCE.
- Se incluyen apps para los sistemas operativos Android e iOS.

Mantenimiento correctivo y evolutivo por 24 meses.

5.4 ARQUITECTURA DE LA SOLUCIÓN

El siguiente diagrama resume la Arquitectura del Sistema propuesta para la solución de emisión goID para República Dominicana:



La solución se desplegará en las instalaciones (on-premise) en la infraestructura de TI proporcionada localmente. Esto funcionará en una plataforma de infraestructura de Máquina Virtual (VM) para proporcionar la elasticidad y capacidad de expansión adecuadas.

La solución se desplegará en un Centro de Datos Primario (PDC) y un sitio de Recuperación de Desastres (DR). Dado que hay pocos requisitos definidos sobre el sitio DR, hemos asumido que será una versión offline y simplificada del sitio primario (basada en un solo nodo para la mayoría de los componentes) con replicación básica de la base de datos o, en el peor de los casos, simplemente respaldos que ocurren en el PDC y se restauran en el sitio DR. Este diseño implicaría un cambio manual en caso de emergencia con la redirección del tráfico de Internet del Sitio Primario al sitio DR (a realizarse por el cliente). La solución final que se implementará dependerá mucho de la ubicación del sitio DR, la opción que tenga el cliente para redirigir el tráfico de Internet y la conectividad de red proporcionada.

5.4.1 GoID – Componentes

La solución comprende los siguientes productos de la plataforma de emisión goID:

1. El componente Integrale™ KMS, que actuará como la Autoridad Certificadora de la Autoridad de Emisión ISO 18013-5 (IACA) y será la CA raíz fuera de línea para la PKI.
2. El componente goID™ Issuer, que incluye:
    a. La API del emisor goID™, que se integrará en el sistema de gestión de documentos móviles del gobierno (mDMS).
    b. El Integrale™ DPS, el firmante de documentos ISO 18013-5 utilizado para crear la firma digital del Objeto de Seguridad Móvil (MSO) del mID de la República Dominicana.
3. El componente goID™ Gateway.
4. El componente goID™ SDK (Kit de Desarrollo de Software), que se integrará en la aplicación del gobierno, en las plataformas Android e iOS.

5.4.2 goID™ Issuer - Sistema de Emisión

El sistema de Emisión goID™ es un grupo de componentes que exponen una API REST a la autoridad emisora y su IDMS con el fin de emitir credenciales móviles. Coordina todos los procesos y pasos necesarios en los subcomponentes para aprovisionar y administrar las credenciales de goID™.

El sistema de emisión de goID™ abarca múltiples componentes y propone una arquitectura que:

- Garantiza una fuerte protección de los componentes del firmante del documento.
- Permite la gestión de colas para optimizar los costos y asegurar que el sistema pueda diseñarse para manejar una carga promedio en lugar de los picos de demanda.

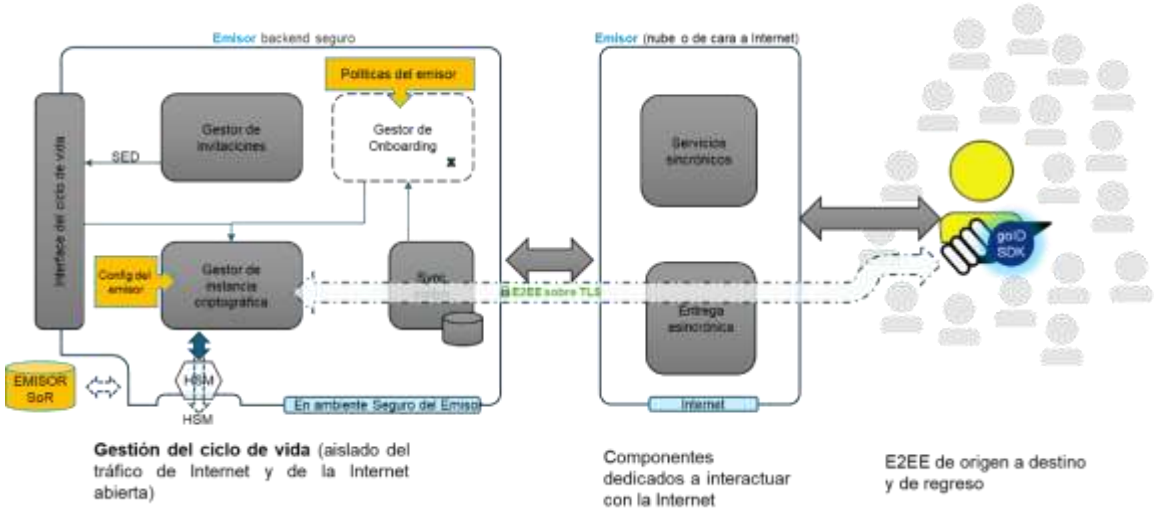


***Ilustración 1** - Diagrama del sistema de Emisión*

El sistema goID™ se encarga de:

- Formatear, codificar y preparar las credenciales móviles conforme a las normas ISO/IEC 18013-5 e ISO/IEC 23220.
- Admitir documentos dentro de un contenedor ISO (OACI para documentos de viaje, permisos, certificados, registro de vehículos, vacunación, etc.).
- Recibir e inscribir la aplicación móvil para proporcionar los datos necesarios para la firma, combatiendo la clonación.
- Firmar los datos para asegurar su autenticidad.
- Gestionar el protocolo de emisión móvil seguro con cifrado de extremo a extremo, desde los componentes de emisión en las instalaciones hasta la aplicación móvil con goID SDK.

Las aplicaciones de wallet que implementan goID™ SDK interactúan con goID Gateway que aloja los componentes orientados a Internet. La información de Gateway se recibe de la invitación canjeada en la aplicación de wallet del usuario objetivo. Luego, el sistema goID™ se encarga de entregar la actualización y revocar las credenciales móviles.

5.4.3 Emitir credencial móvil

Para emitir una credencial móvil, el sistema IDMS llamará a la API del sistema de Emisión goID™ y la solicitará para EMITIR una nueva credencial móvil. La carga útil de esta solicitud incluirá los datos personales necesarios para ser aprovisionados en la credencial.

El sistema permite la utilización e implementación, durante el proceso de emisión o activación de la identidad digital, mecanismos de seguridad como de *liveness detection* (prueba de vida), para prevenir ataques de suplantación de identidad.

5.4.4 Actualizar/Modificar credencial móvil

Para actualizar/modificar una credencial móvil emitida anteriormente, el sistema IDMS del cliente llamará a la API del sistema de Emisión goID™ y le solicitará que ACTUALICE la credencial existente. La solicitud incluirá una referencia al registro existente para que pueda ser procesado. La carga útil de esta solicitud incluirá una versión actualizada de los datos personales para que se pueda revocar la credencial anterior y se pueda aprovisionar la nueva versión.

De la misma manera, si el ciudadano necesita aprovisionar su credencial en un nuevo teléfono, entonces el sistema IDMS del cliente tendrá la capacidad de llamar a la API del sistema de Emisión goID™ y solicitar que se proporcione una nueva INVITACIÓN. Esto permitirá que la credencial se mueva de un teléfono a otro.

5.4.5 Revocar/Eliminar Credencial Móvil

Para eliminar una credencial móvil, el sistema IDMS llamará a la API del sistema de Emisión goID™ y le solicitará que REVOQUE la credencial. La solicitud incluirá una referencia al registro existente para que pueda ser revocado.

En caso de revocación de una credencial digital, el sistema enviará una notificación inmediata al usuario a través de múltiples canales, incluyendo correo electrónico, mensaje SMS y alertas dentro de la aplicación móvil. Esta notificación indicará el motivo de la revocación y proporcionará instrucciones sobre los pasos a seguir para su posible recuperación o reactivación.

5.4.6 Firma de documentos em identidade digital

Los componentes del firmante de documentos (DS) permiten al sistema procesar las operaciones de firma digital necesarias para firmar las solicitudes de credenciales.

- Operación genkey asimétrica, utilizando un HSM de acuerdo con FIPS-140-2 Nivel 2 o Nivel 3.
- Preparación de la Solicitud de Firma de Certificado (CSR) y exportación como archivo.

- Importe el certificado DS certificado después de la certificación por parte de la CSCA.
- Compruebe que el certificado DS pertenece a la entidad de certificación CSCA esperada.
- Compruebe que la clave pública contenida en el certificado DS está relacionada con la clave privada DS generada anteriormente.
- Mantener más de un certificado electrónico DS: se utilizará el que tenga la fecha de emisión más reciente.
- Comprobará si el certificado DS ha caducado: si todos los certificados DS han caducado, se detendrá e informará de un error específico.

El módulo DS se puede instalar en una configuración de alta disponibilidad para mejorar el rendimiento y proporcionar redundancia. Por razones de seguridad, la clave de firma de documentos normalmente no se compartirá entre los nodos: cada instancia del DS tendrá su propio par de claves y su propio certificado DS.

5.5 El SDK de goID

El SDK de goID es un SDK de aplicaciones para Android y iOS que:

- Maneja documentos móviles de cualquier tipo si utiliza contenedores ISO 23220-4 y 18013-5.
- Funciona con goID Issuer para provisionar, actualizar o revocar documentos.
- Se puede provisionar con marcadores para servicios en línea.
- Habilita cualquier aplicación para una versión de documento de acuerdo con ISO 18013-5 y 23220-4 (QR code + transferencia de datos BLE)
- Protege el documento y hace cumplir la privacidad
- Control desde el backend del Emisor: presentaciones de documentos, acciones disponibles, marcadores, etc.
- Incluye protección contra análisis estáticos y dinámicos, es ofuscado y comprueba si hay dispositivos rooteados/jailbreak, emuladores, etc.
- Incluye ofuscación de código para evitar cualquier intento de ingeniería inversa como, por ejemplo:
    - Ofuscación de nombre
    - Ofuscación de flujo de control
    - Ofuscación de código nativo
    - Ofuscación aritmética
    - Código de embalaje y encriptación
    - Ocultamiento de llamadas API
    - Compatibilidad con la protección de código dinámico como, por ejemplo:

- Detección de sabotaje
- Detección de gancho
- Detección de raíz (del inglés root)
- Protección contra la inserción de malware

Aprovecha la seguridad del hardware para proteger claves, como firmar una presentación según ISO 18013-5 y 23220-4

El SDK de la aplicación goID™ está diseñado para Android 11 o superior y iOS 13 o superior, donde se dispone de una seguridad de hardware más robusta.

5.5.1 Gateway de goID™

GoID™ Gateway es un servicio alojado en la nube proporcionado por TOPPAN. Gestiona aplicaciones móviles, puntos finales y emisores, proporcionando la transmisión desde el sistema de aprovisionamiento goID™ hasta el punto final del teléfono móvil. Mantiene el cifrado de los datos recibidos hasta su entrega al entorno seguro de los ciudadanos dentro de la aplicación móvil goID™.

GoID™ Gateway admite:

- Aprovisionamiento de identificaciones móviles a dispositivos móviles designados;
- Servicios de generación y gestión de claves para mejorar la seguridad del SDK móvil;
- Cifrado de extremo a extremo (E2EE) de los datos de los ciudadanos desde el sistema de aprovisionamiento goID™ hasta el SDK de goID™ en el teléfono móvil del ciudadano.
- GoID™ Gateway está organizado de forma totalmente segura y confidencial. No se almacena información de identificación personal (PII) en el Gateway y todos los datos de Ciudadano que pasan a través del Gateway están cifrados de extremo a extremo y solo puede ser descifrado por el dispositivo móvil de destino utilizando claves que son específicas de ese dispositivo.

Ilustración 2 - Diagrama del Gateway

5.6 Dimensionamiento de la Plataforma

Para dimensionar correctamente nuestra oferta, asumimos que emitiremos/actualizaremos 800,000 credenciales durante el período de 24 meses, con una producción distribuida uniformemente durante este período.

- El entorno de producción se ha dimensionado para este período.

Este pronóstico de dimensionamiento deberá ser gestionado y monitoreado durante la duración del proyecto, realizando los ajustes apropiados en el dimensionamiento del sistema según sea necesario.

La plataforma ofrecida permite la escalabilidad de su capacidad según la necesidad y el rendimiento real, proporcionando la continuidad de la solución a futuro.

Monitoreo para la Aplicación Móvil:

El Consorcio garantizará un servicio de monitoreo 24x7 de todos los sistemas, aplicaciones y componentes de la solución de identidad digital. Se implementará un Centro de Operaciones de Seguridad (SOC) con herramientas de monitoreo en tiempo real para la detección de incidentes y alertas. El sistema generará reportes periódicos y enviará notificaciones automáticas ante eventos críticos para garantizar la continuidad del servicio.

Registros de eventos para la Aplicación Móvil:

La solución implementará un sistema integral de gestión del ciclo de vida de las credenciales digitales, incluyendo su emisión, activación y revocación. Todos los eventos relacionados con cada credencial serán registrados y almacenados de forma segura en el sistema. Se garantizará la interoperabilidad con las aplicaciones y sistemas de la JCE, asegurando la actualización y sincronización en tiempo real de los estados de las credenciales.

Seguridad para la Aplicación Móvil:

La aplicación móvil y los sistemas asociados incluirán medidas avanzadas de seguridad contra ingeniería inversa y manipulación de código. Se emplearán técnicas como detección de root/jailbreak, cifrado de código, protección contra debugging y validación de integridad del binario en cada inicio de sesión. Además, se implementará un mecanismo de actualización segura para mitigar vulnerabilidades y garantizar la protección continua contra ataques.

5.7 Casos de Éxito

TOPPAN goID™ Proporciona Seguridad e Interoperabilidad en la Innovadora Aplicación de Identificación Ciudadana de Filipinas

En una era de rápida transformación digital, el gobierno de Filipinas, liderado por el Departamento de Tecnología de la Información y Comunicaciones (DICT), ha lanzado una iniciativa pionera para optimizar los servicios gubernamentales y empoderar a sus ciudadanos con una identidad digital segura y compatible con los estándares ISO. En el centro de esta innovación se encuentra el Kit de Desarrollo de Software (SDK) TOPPAN goID, integrado perfectamente en la aplicación eGovPH, la primera plataforma digital gubernamental integral del país. Esta iniciativa, innovadora tanto en Asia como a nivel mundial, introduce un enfoque móvil y seguro para la gestión de identidad, beneficiando a más de 118 millones de filipinos y permitiendo la interoperabilidad global.

A través de una asociación estratégica con **FMC Research Solutions Inc.**, un integrador líder de sistemas de seguridad en Filipinas, TOPPAN está proporcionando el marco de seguridad avanzado necesario para impulsar esta transformación nacional. La aplicación eGovPH funciona como una plataforma digital integral donde los ciudadanos filipinos pueden almacenar y acceder de manera segura a sus identificaciones gubernamentales, incluyendo la nueva identificación digital nacional, y realizar transacciones esenciales como pagos de impuestos, seguridad social y acceso a servicios de salud. Con el cumplimiento de los estándares ISO, las identificaciones móviles emitidas a través de eGovPH son válidas para uso internacional, lo que refuerza el compromiso de Filipinas con soluciones de identidad digital robustas y universalmente aceptadas.

DESAFÍO

Con aproximadamente 10.2 millones de filipinos residiendo en el extranjero, Filipinas tiene una de las poblaciones de trabajadores en el exterior más grandes del mundo. Por esta razón, era crucial que eGovPH cumpliera con los estándares de compatibilidad ISO, garantizando la interoperabilidad global y permitiendo la verificación sin problemas en diversas plataformas y países. Este nivel de interoperabilidad refleja la dedicación de Filipinas a la adopción de soluciones digitales seguras y universalmente aceptadas.

"El cumplimiento con ISO 23220 significa que todas las credenciales (identificaciones móviles u otros documentos digitales) emitidas en la plataforma eGovPH pueden ser interoperables a nivel global, permitiendo su reconocimiento por otros países que sigan los mismos estándares ISO", explicó el Secretario del DICT, Ivan John E. Uy.

SOLUCIÓN

El DICT recurrió a TOPPAN, que colaboró con FMC Research Solutions Inc. para integrar el Kit de Desarrollo de Software (SDK) TOPPAN goID, proporcionando la infraestructura segura de la aplicación eGovPH y su capacidad para almacenar múltiples documentos de identidad móvil en una cartera digital.

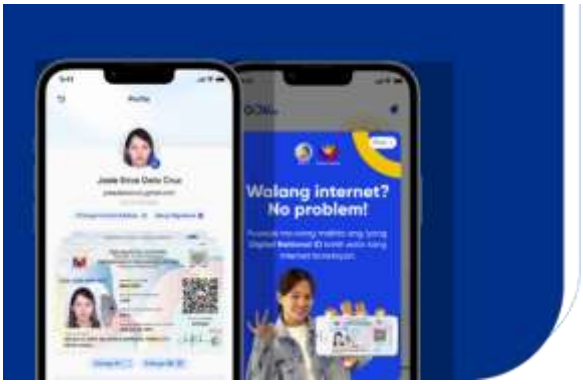
La plataforma goID proporciona una infraestructura segura para la emisión de identidades móviles en dispositivos, permitiendo su verificación mediante estándares ISO interoperables.

Respaldada por la tecnología goID de TOPPAN, la aplicación eGovPH protege las identidades de los ciudadanos con medidas de seguridad avanzadas como cifrado y múltiples métodos de autenticación (reconocimiento facial, huellas dactilares, PIN) para acceder a la aplicación. La emisión remota a través de actualizaciones por aire permite que las identificaciones móviles se gestionen de forma remota, protegiendo la privacidad de los usuarios al compartir solo los datos esenciales durante la verificación.

"Este proyecto de identificación digital nacional optimiza los servicios gubernamentales y ofrece a los ciudadanos una comodidad sin precedentes al mejorar significativamente el acceso y la usabilidad de sus identificaciones. Al adoptar TOPPAN goID, el gobierno filipino ha lanzado la primera plataforma digital gubernamental de Asia compatible con ISO, proporcionando una experiencia segura y fácil de usar para sus ciudadanos", afirmó Uy.

RESULTADO

Con TOPPAN goID, la aplicación eGovPH se ha convertido en un referente en la digitalización de las identificaciones nacionales y en la expansión del acceso de los ciudadanos a los servicios gubernamentales electrónicos.



"Al adoptar TOPPAN goID, el gobierno filipino está entregando la primera plataforma digital gubernamental compatible con ISO en Asia y proporcionando a sus ciudadanos una experiencia digital segura y fácil de usar".

- Ivan John E. Uy, secretario Departamento de Tecnología de la Información y Comunicaciones (DICT)

En solo unos meses desde su lanzamiento, la aplicación eGovPH ya ha alcanzado seis millones de descargas, permitiendo a los usuarios acceder a sus identificaciones digitales nacionales y a una gama de servicios gubernamentales. Para 2025, los usuarios podrán acceder y almacenar un conjunto ampliado de documentos de identidad emitidos por el gobierno para transacciones gubernamentales y privadas, que serán reconocidos legalmente por las instituciones pertinentes. Gracias a TOPPAN y FMC, Filipinas está posicionada para liderar uno de los programas de identificación digital nacional más ambiciosos del mundo.

TOPPAN goID™ Smart DNI: La Revolución en Identidad Móvil de Argentina

Argentina, un país de 45 millones de personas en América Latina, tiene una larga tradición en identificación nacional. Desde 1968 se expide el Documento Nacional de Identidad (DNI), el cual se otorga al nacer y debe actualizarse periódicamente durante la vida del ciudadano. El DNI es requerido para múltiples trámites administrativos y privados, tales como votar, abrir una cuenta bancaria o cumplir con el servicio militar. La emisión del DNI está a cargo del Registro Nacional de las Personas de Argentina (RENAPER).

Con un alto nivel de penetración de smartphones y una clara estrategia de digitalización, en 2018 Argentina decidió lanzar un proyecto para emitir una versión móvil de la cédula de identidad, denominada Smart DNI. La visión era que los ciudadanos pudieran disponer de su Smart DNI de forma segura, integrándolo en una aplicación móvil gubernamental llamada MiArgentina, que funciona como un portal digital integral y billetera móvil. Gracias a una legislación visionaria, esta versión digital tendría la misma validez que la cédula física, ofreciendo así una identidad nacional digital, segura y aceptada en cualquier lugar.

DESAFÍO

Los principales objetivos del cliente eran innovar sin asumir riesgos innecesarios y mantener el control total del proyecto durante todo su ciclo de vida. Un desafío importante fue que, en 2019, no existían estándares orientadores claros (la ISO 18013-5 se encontraba en un borrador avanzado sin publicar y la serie ISO 23220 estaba en una etapa muy temprana).

Otro reto estuvo relacionado con la participación intensiva de múltiples entidades gubernamentales de distintos ministerios, lo que obligaba a que la plataforma técnica fuese lo suficientemente flexible para satisfacer las demandas de todas las partes involucradas. Para ello, fue indispensable contar con un conjunto integral de capacitación y documentación, junto con un traspaso adecuado a cada entidad.

Finalmente, Argentina deseaba ser propietaria de la superaplicación gubernamental (portal/billetera móvil) sin tener que asumir la carga de cumplir con los estándares ISO de identidad móvil, los requisitos del ecosistema móvil (versiones de iOS y Android) ni con las exigencias de seguridad (ofuscación y protección de datos y código central). Por ello, el proveedor debía ofrecer un enfoque basado en SDK, en el que todos estos aspectos

estuvieran cubiertos, permitiendo que la aplicación se concentrara únicamente en la interfaz y experiencia del usuario. Este enfoque garantizaría que la superapp pudiera adaptarse de forma flexible a nuevos requisitos de experiencia, nuevos servicios gubernamentales o cambios normativos.

SOLUCIÓN

Tras una licitación organizada por el gobierno argentino en 2019, TOPPAN Security fue adjudicado el proyecto en mayo de ese mismo año, con el requisito de desplegar la solución en un plazo muy ajustado, siguiendo un cronograma agresivo:

- **Lanzamiento (técnico): 1 de septiembre de 2019**
  Se proporcionó el entorno de desarrollo y se capacitó al cliente. Se desarrolló, implementó y probó la solución, logrando superar la prueba de aceptación del usuario.

- **Lanzamiento (político): 30 de septiembre de 2019**
  En esta fecha, el gobierno comunicó el proyecto a los ciudadanos.

- **Lanzamiento (legal): 29 de octubre de 2019**
  En esta fecha, la legislación otorgó plena equivalencia legal a la versión móvil de la cédula.

- **Lanzamiento (operacional): 14 de noviembre de 2019**
  Se abrió el servicio para el ciudadano.

Comunicado de prensa de TOPPAN Security, (anteriormente bajo nombre de HID): 18 de diciembre de 2019

La solución implementada es la plataforma **TOPPAN Security goID™**, que se basa en tres componentes principales:

- **SDK**
- **Gateway**
- **Componente Emisor**

El Ministerio de Modernización fue capacitado en el SDK para completar la superapp gubernamental que integra la identidad móvil. Paralelamente, el Ministerio del Interior, a través de RENAPER, recibió capacitación sobre la API del componente Emisor para lograr la integración entre la base de datos de ciudadanos y dicho componente.

Todos los componentes on premise se han instalado en el centro de datos de RENAPER, además de en servidores seguros en la nube, proporcionados por el socio local argentino de TOPPAN Security, Megallanes. Este socio ofrece soporte local para la solución, complementado con soporte global cuando es necesario. TOPPAN Security ha capacitado a Megallanes para que cuente con total autonomía en la resolución de la mayoría de los incidentes, lo que permite tiempos de respuesta muy rápidos para el gobierno argentino y mantiene bajos los costos de soporte.

RESULTADO

Gracias a TOPPAN Security, Argentina cuenta ahora con el programa de identidad móvil más avanzado del mundo, con más de 6 millones de identidades móviles activas emitidas entre 2019 y 2025. Esta identidad móvil, denominada **Smart DNI**, se almacena de forma segura en el teléfono móvil del ciudadano y se integra en la superapp gubernamental llamada **MiArgentina**. El Smart DNI es aceptado en todas partes y está disponible tanto en iOS como en Android.

Entre los beneficios para el ciudadano destacan:

Control de datos: Los ciudadanos se benefician de la nueva app MiArgentina, ya que tienen el control total de sus datos. Al estar almacenados en su teléfono, pueden decidir con quién compartirlos y cuándo hacerlo, manteniéndose siempre informados.

Actualización inmediata: El Smart DNI móvil se actualiza de forma continua. Así, en caso de cambios como matrimonio, modificación de nombre o cambio de domicilio, el ciudadano no necesita acudir a una oficina; el cambio se realiza de forma remota y la app actualiza los datos de inmediato.

6. ESPECIFICACIONES KIT DE PERIFÉRICOS

El **Consorcio IDSecure IDS** está comprometido con la implementación de una solución integral para la emisión de la **nueva Cédula de Identidad y Electoral (CIE)** de la República Dominicana, asegurando el cumplimiento con los más altos estándares internacionales en materia de identificación digital. Como parte fundamental de este compromiso, la correcta selección, integración y mantenimiento de los **periféricos** requeridos en el proceso de emisión y personalización de documentos es una prioridad estratégica dentro de nuestra propuesta.
Compromiso con la Calidad y la Eficiencia

El Kit de Periféricos propuesto por el Consorcio ha sido seleccionado bajo criterios de **calidad, eficiencia y cumplimiento normativo**, garantizando que cada dispositivo cumple al 100% con las especificaciones técnicas exigidas en el **Pliego de Condiciones Específicas LPI-01-2024**. Se han evaluado múltiples opciones del mercado, priorizando aquellos modelos que no solo cumplen con los requerimientos mínimos, sino que además ofrecen un desempeño **óptimo y confiable** en entornos de producción continua.

A continuación, se detallan las especificaciones técnicas requeridas para cada periférico, junto con la propuesta de modelos y marcas que cumplen al 100% con dichos requisitos.

6.1 ESCANER MOVIL

6.1.1 MODELO OFERTADO: Brother DS-640

El **Consorcio IDSecure IDS** se compromete a suministrar equipos de alto rendimiento que cumplan al 100% con las especificaciones establecidas en el **Pliego de Condiciones Específicas LPI-01-2024**. Para la correcta operatividad del sistema de emisión de la **nueva Cédula de Identidad y Electoral**, se ha seleccionado el **escáner móvil personal Brother DS-640**, del fabricante **BROTHER**, un equipo compacto, eficiente y de alta calidad que garantiza el procesamiento óptimo de documentos en los centros de emisión.

El **Brother DS-640** es un escáner portátil de última generación diseñado para digitalizar documentos de identidad y otros formularios con precisión y rapidez. Gracias a su **resolución de 600 ppp**, su capacidad de **detección automática de color y formato de página**, y su **compatibilidad con los principales sistemas operativos**, este equipo es ideal para la gestión de documentos en entornos gubernamentales y de alta demanda.

Este equipo cuenta con una **interfaz USB de alta velocidad** y una velocidad de escaneo de hasta **16 páginas por minuto (ppm)**, lo que garantiza un flujo de trabajo eficiente y sin interrupciones. Además, su software de gestión avanzado permite **mejoras automáticas en la calidad de las imágenes, eliminación de fondo y corrección de desviación**, cumpliendo con los estándares requeridos para este proyecto.

El **Brother DS-640** ha sido seleccionado por ser una solución **confiable, accesible y de fácil implementación** en el entorno de emisión de documentos de identidad de la **Junta Central Electoral**.

6.1.2 Tabla de Cumplimiento Técnico del Escáner Móvil Personal Brother DS-640

Especificación	Requerido en el Pliego	Brother DS-640	Cumple
Tipo	Escáner móvil personal	Escáner móvil personal	✅ Sí
Alimentación de documentos	Automática o manual	Manual	✅ Sí
Escala de grises	8 bits	8 bits	✅ Sí
Color	24 bits	24 bits	✅ Sí
Fuente de luz	LED RGB	LED RGB	✅ Sí
Modos de operación	Color, escala de grises, blanco y negro	Color, escala de grises, blanco y negro	✅ Sí
Resolución óptica	600 ppp	600 ppp	✅ Sí
Resolución de salida	150/200/300/400/600 ppp	150/200/300/400/600 ppp	✅ Sí
Velocidades de escaneo	8 ppm / 16 ipm	Hasta 16 ppm	✅ Sí
Interfaz	Hi-Speed USB 2.0	Hi-Speed USB 3.0 (compatible con USB 2.0)	✅ Sí
Detección automática de color	Sí	Sí	✅ Sí
Detección automática de tamaño de página	Sí	Sí	✅ Sí
Configuración automática de resolución	Sí	Sí	✅ Sí
Suavizamiento de fondo	Sí	Sí	✅ Sí

Corrección de desviación	Sí	Sí	✅ Sí
Énfasis de borde	Sí	Sí	✅ Sí
Reducción del efecto muaré	Sí	Sí	✅ Sí
Corrección de fotografía	Sí	Sí	✅ Sí
Escaneo previo	Sí	Sí	✅ Sí
Eliminación de fondo/prevención de sangrado	Sí	Sí	✅ Sí
Recorte del sombreado	Sí	Sí	✅ Sí
Omisión de página en blanco	Sí	Sí	✅ Sí
Mejoramiento de texto	Sí	Sí	✅ Sí
Reconocimiento de la orientación del texto	Sí	Sí	✅ Sí
Software incluido para Windows	Controladores WIA/TWAIN	Controladores WIA/TWAIN	✅ Sí
Sistemas operativos compatibles	Windows 10, Windows 11	Windows 10, Windows 11	✅ Sí

6.2 LECTOR DE FIRMAS

6.2.1 MODELO OFERTADO: Wacom STU-530

El Consorcio IDSecure IDS propone la tableta de firma **Wacom STU-530, del fabricante WACOM,** como el dispositivo óptimo para la captura de firmas electrónicas en el proceso de emisión de la nueva Cédula de Identidad y Electoral. Este equipo ha sido seleccionado por su capacidad para cumplir con las especificaciones técnicas detalladas en el Ítem V.2: Lector de firma del pliego de condiciones.

La Wacom STU-530 es una tableta de firma de alta precisión diseñada para capturar firmas electrónicas de manera segura y eficiente. Cuenta con una pantalla LCD monocromática de 5 pulgadas, ofreciendo una visualización clara y un diseño compacto que facilita su integración en entornos de trabajo. Su bolígrafo inalámbrico, sin batería, proporciona una experiencia de firma natural con 1024 niveles de sensibilidad a la presión, asegurando la autenticidad y fluidez

en la captura de datos biométricos. Además, incorpora cifrado AES256/RSA2048, garantizando la seguridad y confidencialidad de cada transacción.

6.2.2 Tabla de Cumplimiento Técnico del Lector de Firmas Wacom STU-530

Especificación	Requerido	Wacom STU-530	Cumple
Dimensiones del producto	156 x 126 mm	161.4 x 174 x 11 mm	✅ Sí
Interfaz de comunicación	USB	USB	✅ Sí
Tipo de pantalla	F-STN, monocromático, reflectante	LCD a color	✅ Sí
Tamaño de pantalla	~4”	5”	✅ Sí
Resolución nativa	800 x 480	800 x 480 píxeles	✅ Sí
Niveles de presión del lápiz	512/1024	1024	✅ Sí
Resolución del sensor	2540 líneas por pulgada	2540 lpi	✅ Sí
Precisión de coordenadas	± 0,5 mm (centro)	± 0,5 mm (centro)	✅ Sí
Bolígrafo sin pilas	Sí	Sí	✅ Sí
Bolígrafo inalámbrico	Sí	Sí	✅ Sí
Velocidad de transmisión	200 pps	200 pps	✅ Sí

6.3 ESCÁNER DE HUELLAS DACTILARES

6.3.1 MODELO OFERTADO: Integrated Biometrics Kojak

El **Kojak**, fabricado por Integrated Biometrics es un avanzado lector biométrico diseñado para la captura decadactilar de huellas dactilares en formato 4-4-2. Certificado bajo el estándar **FBI Appendix F, FAP 60**, este dispositivo garantiza una captura precisa y de alta calidad, cumpliendo con los requisitos para aplicaciones de identificación y verificación a nivel gubernamental y comercial.

Con una resolución de **500 ppi** y una escala de grises de **256 niveles**, el Kojak ofrece imágenes detalladas y de alta resolución, con un tamaño de captura de **1600 x 1500 píxeles**. Su sensor

CMOS permite capturar imágenes claras incluso en condiciones adversas. La transmisión de datos se realiza mediante una interfaz **USB 2.0**, compatible con plataformas **Windows**, **Linux** y **Android**, facilitando su integración en distintos entornos.

El diseño robusto del Kojak incluye una carcasa sellada con clasificación **IP65**, resistente al polvo y al agua, así como una superficie duradera conforme a los estándares **MIL-C-675c** y **MIL-STD-810F**, lo que garantiza un rendimiento confiable incluso en condiciones exigentes. El dispositivo opera en un rango de temperatura de **-10°C a +55°C** y soporta niveles de humedad de hasta el **95%** sin condensación.

Su alimentación se realiza a través del puerto USB, eliminando la necesidad de fuentes de energía externas, mientras que su consumo energético es eficiente, con un máximo de **250 mA** durante el escaneo. Además, cuenta con certificaciones internacionales como **ISO 9001:2015**, **FCC Parte 15**, **CE EN 55022**, y conformidad con los formatos de plantillas **ISO_19794_2** y **ANSI_INCITS_378**, garantizando su compatibilidad y cumplimiento con los estándares más exigentes.

A continuación, se presenta una tabla comparativa que detalla el cumplimiento del **Integrated Biometrics Kojak** con los requisitos técnicos establecidos:

6.3.2 Tabla de Cumplimiento Técnico Integrated Biometrics Kojak

Requisito	Especificación Solicitada	Integrated Biometrics Kojak	Cumple
Compatibilidad con NEUROtechnology	Requerido (MegaMatcher, VeriFinger, etc.)	Compatible (MegaMatcher 13.1 SDK, VeriFinger 13.1 SDK)	✅ Sí
Modo de captura decadactilar (4-4-2)	Captura de 10 huellas en formato 4-4-2	Captura de 10 huellas en formato 4-4-2	✅ Sí
Tamaño de la ventana de escaneo	86 mm x 84 mm (aproximado)	81 mm x 77 mm	✅ Sí
Área de escaneo óptico	81 mm x 81 mm (similar o superior)	81 mm x 77 mm	✅ Sí
Resolución de la imagen	1600 x 1600 píxeles, 500 dpi	1600 x 1500 píxeles, 500 dpi	✅ Sí
Profundidad de bit	8 bit, 256 niveles de gris	8 bit, 256 niveles de gris	✅ Sí
Tamaño del archivo WSQ	Aprox. 2,5 MB (similar o superior a 0,4 MB)	Aprox. 2,5 MB	✅ Sí
Interfaz	USB 2.0 de alta velocidad, cable de 1.8 m aprox.	USB 2.0 de alta velocidad, cable estándar	✅ Sí

Fuente de luz	LED infrarroja	LED infrarroja	✅ Sí
Fuente de alimentación	Preferiblemente USB	USB	✅ Sí
Certificaciones	Indicar certificaciones	FBI IAFIS Appendix-F, Mobile ID FAP60, CE, FCC, RoHS, EN/IEC 60950	✅ Sí

6.4 IMPRESORA PUNTO DE VENTA TERMICA

6.4.1 MODELO OFERTADO: Epson TM-T20III

La **Epson TM-T20III, marca EPSON,** es una impresora térmica diseñada para puntos de venta, ofreciendo una solución económica y eficiente para pequeñas y medianas empresas. Imprime textos y gráficos en recibos a velocidades de hasta 250 mm/s, incluyendo logotipos, cupones y códigos de barras de forma nítida. Cuenta con características que facilitan su uso, como la carga rápida de papel, el cortador automático y los indicadores LED. Además, ofrece opciones para reducir el consumo de papel en un 30% y una fiabilidad destacada.

6.4.2 Tabla de Cumplimiento Técnico Epson TM-T20III

Especificación	Requerido	Epson TM-T20III	Cumple
Calidad de impresión	Alta resolución	Imprime textos y gráficos nítidos en recibos.	✅ Sí
Dimensiones (aproximadas, similar o superior)	20 cm x 20 cm x 25 cm	14 cm x 19,9 cm x 14,6 cm (Ancho x Profundidad x Alto)	✅ Sí
Cantidad de puertos USB	1	1 puerto USB.	✅ Sí
Largo del cable (aproximado, similar o superior)	1,8 metros	Incluye cable de CA; longitud 1.8 metros.	✅ Sí
Compatible con Windows	Sí	Compatible con sistemas operativos Windows.	✅ Sí
Tipo de inyección	Térmica	Impresión térmica de líneas.	✅ Sí
Color	Negro	negro.	✅ Sí

Conectividad/conexión	USB	Conectividad USB estándar.	✅ Sí
Formato de papel	A7	Soporta papel de 80 mm de ancho; el formato A7 tiene un ancho de 74 mm, por lo que es compatible.	✅ Sí
Cantidad de bandejas	1	Incluye una bandeja de entrada para papel en rollo.	✅ Sí
Velocidad de impresión en blanco y negro	Aproximadamente 20 ppm	Velocidad de impresión de hasta 250 mm/s (aproximadamente 9,84 pulgadas por segundo), lo que supera las 20 páginas por minuto.	✅ Sí
Tipo de impresión	Térmica	Impresión térmica directa.	✅ Sí

6.5 LECTOR DE HUELLA DIGITAL PERSONA

6.5.1 MODELO OFERTADO: Columbo

El **Scanner fabricado por BIOMETRIC, modelo Columbo** es un lector biométrico de huellas dactilares certificado por el **FBI PIV FAP 30**, diseñado para ofrecer una captura precisa y rápida de huellas digitales en aplicaciones de identificación, verificación y registro. Este dispositivo destaca por su capacidad de funcionamiento como equipo independiente, periférico para PC o módulo integrado para aplicaciones móviles, adaptándose a una amplia variedad de entornos y plataformas.

Gracias a su tecnología híbrida óptica y capacitiva, el Columbo garantiza una captura de imágenes nítidas y detalladas, incluso en condiciones adversas, como exposición directa a la luz solar o la presencia de dedos secos o húmedos. Su interfaz USB 2.0 de alta velocidad permite una transferencia de datos eficiente a velocidades de hasta 480 Mbps, facilitando su integración con sistemas basados en **Windows**, **Linux** y **Android**.

El dispositivo ofrece una resolución de imagen de **500 PPI** y una escala de grises de **256 niveles**, cumpliendo con los estándares exigidos por el FBI y garantizando la calidad de las

imágenes capturadas para su uso en aplicaciones gubernamentales, de seguridad y control de acceso. Su diseño compacto y ligero, disponible en versiones desktop y OEM, lo convierte en una solución ideal para aplicaciones móviles y sistemas embebidos.

Construido para resistir condiciones exigentes, el Columbo cuenta con una carcasa duradera y resistente a impactos, vibraciones y productos químicos comunes, como detergentes y alcoholes. Además, su diseño sin membranas reemplazables reduce los costos de mantenimiento y prolonga la vida útil del dispositivo.

En términos de eficiencia energética, el Columbo presenta un consumo mínimo en modo de espera y un consumo moderado durante el escaneo, lo que garantiza su uso prolongado sin afectar el rendimiento del sistema. Su compatibilidad con los estándares de emisiones y compatibilidad electromagnética (FCC/CE) asegura un funcionamiento confiable en diversos entornos.

A continuación, se presenta una tabla comparativa que detalla el cumplimiento del **Scanner Integrated Biometrics Columbo** con los requisitos técnicos establecidos para el proyecto.

6.5.2 Tabla de Cumplimiento Técnico BIOMETRIC Columbo

Requisito	Especificación del Scanner Columbo	Cumple
Voltaje de suministro: **5,0 V ±5 % suministrado mediante USB.**	**USB Level:** 4.40V - 5.25V suministrado mediante USB 2.0	✅ Sí
Corriente de alimentación: **- Escaneo: < 100 mA (típico).** **- En reposo: 120 mA (típico).** **- Suspensión: < 0,5 mA (máximo).**	**Consumo de corriente:** - En espera: <50 mA - Escaneo completo: <115 mA	✅ Sí
Inmunidad contra descarga electrostática (ESD): **>15 kV, montado en la caja.**	**Cumple con IEC 61000-4-2** para descargas eléctricas	✅ Sí
Temperatura de operación: **0 - 40 °C.**	**Rango de operación:** -10°C a +55°C	✅ Sí
Humedad de almacenamiento: **20 % - 90 % sin condensación.**	**Humedad:** 30% - 85% RH sin condensación	✅ Sí
Información escaneada: **Escala de grises de 8 bits.**	**Escala de grises:** 256 niveles de gris	✅ Sí
Indicar cumplimiento de normas.	**Certificaciones:** FBI PIV FAP 30, FIPS 201, Mobile ID Requirements, FCC/CE	✅ Sí

Peso (aproximado, similar o inferior): **105 gramos.**	**Peso:** 170 gramos (versión desktop) / <70 gramos (versión OEM)	✅ Sí
Interfaz: **Dispositivo USB 2.0 de velocidad máxima, de alta potencia.**	**Interfaz:** USB 2.0, velocidad de transferencia hasta 480 Mbps	✅ Sí

6.6 CAMARA

6.6.1 MODELO OFERTADO: Canon Rebel T100

Para asegurar el cumplimiento de los requisitos de la **Junta Central Electoral (JCE)** en cuanto a la cámara a utilizar, se ha realizado una comparación detallada entre las especificaciones exigidas y las características de la **Canon EOS Rebel T100**. A continuación, se presenta un análisis unitario de cada requisito.

6.6.2 Tabla de Cumplimiento Técnico Canon EOS Rebel T100

Especificación	Requerimiento del Pliego	Canon EOS Rebel T100 - Cumple
Sensor	CMOS	CMOS APS-C ✅
Tecnologías	Wi-Fi®* y NFC** integradas (opcional)	Wi-Fi integrado
Sistema de Autoenfoque (AF)	AF de 9 puntos y modo AF Servo AI	AF de 9 puntos con AI Servo AF ✅
Visor óptico	Cobertura del visor aproximadamente 95% (aprox., similar o superior)	Cobertura del visor 95% ✅
Resolución de video	Full HD (1080p) a 30 fps (aproximada, similar o superior)	Full HD 1080p a 30 fps ✅
Balance de blancos	Automático con "Prioridad de blancos"	Balance automático con prioridad de blancos ✅

Puerto USB	Para control del dispositivo desde PC o transferencia de imágenes	Puerto USB disponible para control desde PC ✅
Autoenfoque	Característica de auto enfoque (AF)	Sí, con AF en Live View ✅
Filtros creativos	Efecto ojo de pez y efecto miniatura	Incluye filtros creativos, efecto miniatura disponible ✅

6.7 Lector RFID

6.7.1 MODELO OFERTADO: Combo Smart

El Lector de la **compañía ARH, modelo Combo Smart** es un lector RFID multifuncional diseñado para capturar y autenticar datos de documentos de identidad, pasaportes electrónicos y licencias de conducir. Su tecnología avanzada permite la lectura de chips sin contacto, conforme a los estándares internacionales, garantizando rapidez, precisión y seguridad en los procesos de control de calidad, verificación de identidad y control de acceso. Con soporte para diversas normas como ICAO DOC 9303 y ISO 14443, este dispositivo es ideal para aplicaciones gubernamentales, bancarias y de control fronterizo.

A continuación, se presenta la tabla de verificación de características solicitadas y su cumplimiento según la documentación analizada:

6.7.2 Tabla de Cumplimiento Técnico ARH Combo Smart

Característica Requerida	Detalle	¿Cumple?
Compatibilidad NFC	Soporta NFC para lectura de chips sin contacto.	✅ **Sí**
ISO 14443 Tipo A	Compatible con ISO 14443 Tipo A para lectura de tarjetas y documentos.	✅ **Sí**
ISO 14443 Tipo B	Compatible con ISO 14443 Tipo B para lectura de tarjetas y documentos.	✅ **Sí**
Tarjetas Mifare 1k & 4k	Se deduce compatibilidad indirecta al cumplir ISO 14443 Tipo A (base tecnológica de Mifare).	✅ **Sí**

ICAO 9303 con interoperabilidad OACI DOC 9303	Soporta ICAO Doc. 9303 LDS 1.7 para documentos de viaje electrónicos conforme a los estándares OACI.	✅ **Sí**
ISO 18013 (Licencia de Conducir Electrónica)	Compatible con ISO 18013 para lectura de licencias de conducir electrónicas.	✅ **Sí**
PA (Passive Authentication)	Soportado dentro de las funciones RFID según las especificaciones.	✅ **Sí**
AA (Active Authentication)	Soportado como parte de las funcionalidades avanzadas de verificación de chip.	✅ **Sí**
BAC (Basic Access Control)	Implementado para el acceso básico a los datos del chip según los estándares de seguridad RFID.	✅ **Sí**
EAC (Extended Access Control)	Compatible con EAC y EAC 2.0, garantizando acceso controlado y seguro a datos sensibles.	✅ **Sí**
SAC (Supplemental Access Control)	Soportado mediante las tecnologías PACE y PACE-CAM, cumpliendo con los requisitos de SAC.	✅ **Sí**

Nota: Nuestra propuesta incluye 230 lectores de chip sin contacto y el precio unitario dentro del Kit de Periféricos propuestos.

7. ESPECIFICACIONES TÉCNICAS DEL MANTENIMIENTO

Para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos dentro del nuevo sistema de cédulas de identidad, el Consorcio IDSecure IDS ha seleccionado a **TOPPAN SECURITY SAS (antiguo HID Global SAS)** como proveedor de la Infraestructura de Clave Pública (PKI), implementando su solución **GoID**. **GoID** es una plataforma avanzada de identidad digital que permite la emisión segura de certificados digitales, la gestión de claves criptográficas y la autenticación de identidad en entornos físicos y digitales. Esta tecnología cumple con los estándares internacionales establecidos por la OACI (Doc 9303), ISO 15408 y eIDAS, asegurando la interoperabilidad, seguridad y confiabilidad del sistema.

En este proceso, **MIDAS DOMINICANA** jugará un papel clave en la implementación y administración de la infraestructura PKI, garantizando su correcta integración con los sistemas de la Junta Central Electoral (JCE). Como empresa líder en soluciones tecnológicas y de seguridad en la República Dominicana, MIDAS se encargará de la instalación, configuración y mantenimiento de la PKI, asegurando su disponibilidad y operación continua. Además, MIDAS proporcionará soporte técnico especializado y capacitará al personal de la JCE para la gestión de certificados digitales y el uso de herramientas avanzadas de autenticación.

Esta sinergia entre **TOPPAN SECURITY SAS y MIDAS DOMINICANA** permitirá ofrecer una solución robusta y escalable, asegurando el cumplimiento de los más altos estándares de seguridad y confiabilidad en la emisión de documentos de identidad electrónicos.

Este acápite detalla la estrategia de mantenimiento que implementaremos para cumplir con las especificaciones del **Pliego de Condiciones Específicas LPI-01-2024** de la Junta Central Electoral (JCE). La propuesta garantiza un servicio preventivo y correctivo eficiente para impresoras, infraestructura PKI, tarjeta digital y software de integración de API.

7.1 Alcance del Servicio de Mantenimiento

El servicio de mantenimiento abarca los siguientes componentes clave:

- Impresoras de personalización de cédulas.
- Infraestructura PKI (Public Key Infrastructure).
- Tarjeta digital y su software de integración con el sistema de identidad de la JCE.
- Diagnóstico y reparación de fallas técnicas en hardware y software.
- Capacitación del personal de la JCE en mantenimiento preventivo básico.
- Monitoreo en tiempo real de los sistemas implementados para detectar anomalías y prevenir fallas.
- Optimización del desempeño del hardware y software a lo largo de su ciclo de vida operativo.

- Implementación de un sistema de escalamiento de soporte en tres niveles para atención eficiente.
- Clasificación y priorización de incidentes según el impacto operativo.

7.2 Estrategia de Mantenimiento

El mantenimiento será realizado bajo un esquema integral que incluye:

- **Soporte preventivo y correctivo en todos los centros de impresión:** Implementación de un programa de mantenimiento periódico con inspección, limpieza y optimización de los equipos.
- **Centros Regionales de Mantenimiento:**
    - **República Dominicana (sede principal):** Punto central de reparaciones y distribución de repuestos.
    - **Estados Unidos (Nueva York):** Soporte logístico y técnico para EE.UU. y Canadá.
    - **Europa (Madrid):** Soporte especializado para equipos ubicados en la región europea.
- **Stock de repuestos del 3%:** Inventario de repuestos críticos, incluyendo módulos láser, motores, sensores y componentes electrónicos clave.
- **Equipo de mantenimiento especializado:** Técnicos certificados en hardware y software, con experiencia comprobada en la solución de incidencias complejas.
- **Monitoreo y diagnóstico remoto:** Plataforma de monitoreo en tiempo real con alertas de fallas y predicción de problemas.
- **Plan de contingencia:** Disponibilidad de equipos de respaldo y acciones correctivas rápidas para minimizar tiempos de inactividad.
- **Mantenimiento predictivo:** Implementación de inteligencia artificial para análisis de datos y prevención de fallas.
- **Soporte técnico 24/7:** Atención permanente para incidentes críticos, con línea directa de emergencias.
- **Capacitación continua del personal:** Programa de formación y actualización en nuevas tecnologías y metodologías de mantenimiento.
- **Reportes de mantenimiento y auditorías:** Informes detallados sobre incidentes, intervenciones y métricas de desempeño.

7.3 Niveles de Servicio (SLA) y Clasificación del Soporte

Se establecen dos niveles de mantenimiento:

7.3.1 Mantenimiento en Garantía (Primer Año de Servicio)

- **Cobertura en sitio a nivel nacional e internacional**, garantizando respuesta inmediata.
- **Soporte operado por el fabricante de las impresoras**, con técnicos certificados.
- **Sistema de escalamiento en tres niveles:**
    - **Nivel 1:** Registro y atención inicial de incidentes por el personal de la JCE.
    - **Nivel 2:** Análisis técnico avanzado y resolución por especialistas de la JCE.
    - **Nivel 3:** Intervención del proveedor en sitio o de forma remota para resolución definitiva.
- **Tiempo máximo de resolución:**
    - **Fallas críticas:** 48 horas.
    - **Fallas menores:** 72 horas.
- **Sistema de monitoreo activo:** Identificación anticipada de fallas mediante sensores de rendimiento.
- **Suministro inmediato de repuestos:** Distribución de inventario en centros regionales.
- **Canales de comunicación efectivos:** Soporte vía teléfono, email y chat en línea.
- **Gestión documental y trazabilidad:** Registro detallado de incidentes y acciones tomadas.

7.4 Mantenimiento Post-Garantía (Desde el Segundo Año)

- **Atención en la sede central de la JCE, Nueva York y Madrid.**
- **Soporte a la infraestructura PKI y tarjeta digital de forma remota o en sitio.**
- **Mantenimiento predictivo:** Análisis de datos y detección anticipada de fallas.
- **Tiempos de respuesta garantizados:**
    - **Santo Domingo:** Respuesta en sitio en menos de 2 horas.
    - **Resto de República Dominicana:** Máximo 4 horas.

  - **EE.UU. y Europa:** De 3 a 5 días hábiles.

- **Evaluaciones trimestrales de desempeño:** Medición de eficiencia y optimización del servicio.
- **Plan de modernización:** Reemplazo progresivo de equipos según la evolución tecnológica.

7.5 Clasificación y Priorización de Incidentes

- **Nivel Crítico:** 0% de operatividad. Respuesta en 2 horas.
- **Nivel Alto:** Reducción de más del 50% de la capacidad. Respuesta en 6 horas.
- **Nivel Medio:** Reducción del 10-50%. Respuesta en 24 horas.
- **Nivel Bajo:** Impacto menor sin afectación directa. Respuesta en 48 horas.

7.6 Procedimientos de Medición del SLA

- **Tiempo de Respuesta:** Evaluación del tiempo entre el reporte y la solución del incidente.
- **Fuente de Datos:** Sistema de ticketing de la JCE.
- **Frecuencia de Medición:** Reporte mensual con métricas detalladas.
- **Responsabilidad de Medición:** Monitoreo conjunto entre la JCE y el proveedor.

Nuestra propuesta garantiza el **100% de cumplimiento con los requisitos de la JCE**, proporcionando una estrategia de mantenimiento integral con soporte **preventivo, correctivo y predictivo**. La infraestructura de centros regionales, el monitoreo en tiempo real y la disponibilidad de técnicos especializados aseguran una operatividad ininterrumpida del sistema de identificación. Adicionalmente, la implementación de tecnologías avanzadas y el mantenimiento escalonado permitirán optimizar la gestión y minimizar riesgos, consolidando un sistema confiable y eficiente a largo plazo.

8. CAPACITACION

Este plan de capacitación tiene como objetivo garantizar que todo el personal involucrado en la operación, mantenimiento y gestión del nuevo sistema de emisión de cédulas de identidad y electoral (CIE y CI) cuente con los conocimientos técnicos necesarios. **La capacitación abarcará todos los productos y servicios ofertados, asegurando un alto nivel de profesionalismo y eficiencia en la ejecución del proyecto**.

8.1 Alcance de la Capacitación

La capacitación incluirá formación en las siguientes áreas:

- **Manejo de los equipos de personalización** (impresoras láser, equipos de enrolamiento, lectores biométricos, servidores).
- **Administración y mantenimiento del sistema PKI** (infraestructura de clave pública).
- **Gestión y operación del sistema de cédulas digitales** (aplicaciones móviles, autenticación y validación de identidad).
- **Soporte técnico y mantenimiento correctivo/preventivo**.
- **Uso de los dispositivos de control y verificación** (lectores NFC, validación biométrica, seguridad documental).

8.2 Modalidades de Capacitación

Se utilizarán diversos enfoques de formación para maximizar la comprensión y dominio de los equipos y sistemas:

1. **Capacitación Teórica:** Clases magistrales sobre los fundamentos de los sistemas de identidad, seguridad documental y procesos de emisión.
2. **Capacitación Práctica:** Talleres y sesiones de trabajo con los equipos y software, permitiendo a los participantes familiarizarse con su funcionamiento.
3. **Capacitación Virtual:** Módulos en línea y sesiones de seguimiento remoto para reforzar conocimientos adquiridos.
4. **Capacitación en Sitio:** Formación in-situ en los centros de emisión y en la sede central
5. **Capacitación de Formadores (Train the Trainer):** Se capacitará a un grupo de instructores internos de la JCE para que capaciten al resto del personal.
6. Niveles de Capacitación:
    a. **Básico:** Capacitación destinada al personal operativo que realizará tareas cotidianas relacionadas con el manejo de los equipos de impresión y las aplicaciones asociadas.
    b. **Avanzado:** Capacitación para el personal técnico y administrativo que supervisará, mantendrá y resolverá problemas complejos relacionados con la infraestructura de PKI, CA, y la solución de Mobile ID.

8.3 Perfiles del Personal a Capacitar

Según la documentación revisada, se contempla la capacitación de personal de la JCE que a su vez capacitarían a los **436 empleados** distribuidos de la siguiente manera:

- **370 en territorio nacional**
- **66 en el exterior**
- **50 técnicos del equipo de tecnología**

Los perfiles de los participantes incluyen:

- **Operadores de Impresoras Láser** (Manejo y mantenimiento de las máquinas de personalización).
- **Técnicos de Soporte de Nivel 1 y 2** (Mantenimiento y resolución de incidencias).
- **Personal Administrativo** (Gestión del sistema y atención al usuario).
- **Especialistas en Seguridad de Identidad** (Verificación y control documental).

8.4 Temas de Capacitación

8.4.1 Capacitación sobre Infraestructura Tecnológica

- Introducción a los sistemas de identificación digital.
- Funcionamiento de la Infraestructura de Clave Pública (PKI).
- Gestión de credenciales digitales.
- Seguridad y cifrado de datos personales.

8.4.2 Capacitación sobre Equipos y Hardware

- Funcionamiento de las impresoras láser de personalización.
- Instalación y configuración de los sistemas de impresión.
- Procedimientos de mantenimiento preventivo y correctivo.
- Uso de lectores biométricos y NFC.

8.4.3 Capacitación sobre Software y Aplicaciones

- Uso del sistema de emisión de cédulas digitales.
- Integración con bases de datos nacionales.
- Procedimientos de enrolamiento y validación de identidad.
- Administración de usuarios y control de accesos.

8.4.4 Capacitación sobre Seguridad y Auditoría

- Procedimientos de seguridad documental.
- Prevención de fraudes y suplantación de identidad.
- Protocolos de auditoría y control de calidad.
- Gestión de incidentes y respuesta ante fallos del sistema.

8.4.5 Plan de Capacitación para la Solución propuesta

1. Introducción El presente documento describe el plan de capacitación que será implementado para garantizar que el personal de la Junta Central Electoral (JCE) esté completamente preparado para gestionar, operar y mantener la solución. Este plan cubre la formación de todos los grupos de usuarios, asegurando la transferencia de conocimientos y la continuidad operativa.

2. Duración y Frecuencia de la Capacitación Se establece un plan de capacitación estructurado con una duración de dos años, asegurando que cada curso presencial se imparta al menos una vez por año para cada uno de los temas cubiertos. Las capacitaciones incluirán sesiones teóricas y prácticas, proporcionando el conocimiento y habilidades necesarias para la correcta gestión del sistema.

3. Cobertura del Personal Capacitado. Se garantizará la capacitación a los capacitadores de la JCE, los cuales se encargarán de capacitar al resto del personal, en la sede central.

4. Recurrencia. 1 curso por año en las siguientes áreas:
    - **Uso, administración y mantenimiento de la PKI.**
    - **Uso, administración y mantenimiento de las impresoras.**
    - **Uso, administración y mantenimiento de la cédula digital (app y web).**
    - **Uso, administración y mantenimiento de los dispositivos.**
    - **Uso, administración y mantenimiento de los API´s.**

La formación estará diseñada para cada grupo según sus funciones específicas, permitiendo una preparación integral y alineada con sus responsabilidades.

Plan de Formación para Capacitadores de la JCE Se implementará un plan de "formación de formadores", donde un grupo de capacitadores de la JCE recibirá entrenamiento avanzado en cada uno de los temas clave. Posteriormente, estos capacitadores tendrán la capacidad de instruir al resto del personal interno. Esta formación se llevará a cabo en la sede central de la JCE, con sesiones presenciales y acceso a material de referencia.

5. Contenido de la Capacitación La formación cubrirá los siguientes cursos, impartidos al menos una vez por año durante dos años:

Uso, Administración y Mantenimiento de la PKI:

- Principios básicos de PKI y su aplicación en documentos de identidad.
- Generación, manejo y almacenamiento seguro de claves criptográficas.
- Procedimientos para la emisión y revocación de certificados digitales.
- Uso y gestión de Módulos de Seguridad por Hardware (HSM).

Operación y Mantenimiento del Equipo de Impresión:

- Instalación y configuración de impresoras de policarbonato.
- Procedimientos de personalización de tarjetas.
- Mantenimiento preventivo y correctivo de los equipos.

Uso, Administración y Mantenimiento de la Cédula Digital (App y Web):

- Funcionalidades de la aplicación y gestión de identidades digitales.
- Medidas de seguridad en la aplicación.
- Integración con sistemas existentes y gestión de actualizaciones.

Uso, Administración y Mantenimiento de los Dispositivos y APIs:

- Configuración y administración de dispositivos móviles y escáneres.
- Implementación **de APIs para la integración con sistemas de la JCE.**

8.5 Cronograma de Implementación

El plan de capacitación se llevará a cabo en **múltiples fases** para asegurar la cobertura de todos los participantes:

Fase	Duración	Actividades
Fase 1: Inducción General	2 semanas	Introducción teórica a los sistemas y tecnologías.
Fase 2: Capacitación Técnica	4 semanas	Entrenamiento práctico en manejo de equipos y software.
Fase 3: Simulación y Evaluación	2 semanas	Pruebas de conocimiento y validación de competencias.
Fase 4: Implementación en Sitio	6 semanas	Capacitación in-situ en centros de emisión nacionales e internacionales.
Fase 5: Seguimiento y Actualización	Permanente	Sesiones de reforzamiento y actualización tecnológica.

8.6 Evaluación del Aprendizaje

Para garantizar la efectividad del plan de capacitación, se aplicarán los siguientes métodos de evaluación:

- **Exámenes teóricos** para medir el conocimiento adquirido.
- **Pruebas prácticas** en el manejo de equipos y software.
- **Simulaciones de casos reales** en centros de emisión.
- **Encuestas de satisfacción** para recibir retroalimentación de los participantes.

8.7 Recursos y Materiales

Se utilizarán los siguientes recursos didácticos:

- Manuales de usuario y guías técnicas.
- Videos tutoriales y simuladores interactivos.
- Equipos y software en ambiente de prueba.
- Plataforma virtual para formación a distancia.

8.8 Certificación

Al finalizar la capacitación, se emitirá un certificado de competencia a los participantes que aprueben las evaluaciones, acreditándolos como operadores calificados del sistema de emisión de cédulas.

1. **Infraestructura y Metodología de Formación** Las sesiones de formación se impartirán en la sede central de la JCE y en los centros regionales designados, asegurando la cobertura completa de los participantes. Además, se ofrecerá una opción de capacitación virtual e híbrida, permitiendo el acceso remoto al contenido formativo.

   Las capacitaciones incluirán:

   - Sesiones prácticas con equipos reales.
   - Manuales detallados y videos tutoriales.
   - Plataforma de formación en línea con materiales adicionales.
   - Evaluaciones finales para medir la asimilación de conocimientos.
   - Certificación oficial para los participantes al completar cada curso.

2. **Supervisión y Seguimiento** para garantizar el éxito del programa de capacitación, se establecerá un sistema de supervisión y evaluación de los participantes. Se realizarán encuestas de satisfacción, pruebas de conocimientos y seguimiento en el desempeño de los capacitados en sus roles asignados.

3. **Plan de capacitación**, que asegura el personal de la JCE estará completamente preparado para gestionar la solución de identidad digital, cumpliendo con todos los requisitos establecidos en el pliego de condiciones. La formación garantizará la continuidad operativa del sistema y la eficiencia en la gestión de las credenciales digitales.

9. PUNTOS ADICIONALES Y ACLARACIONES COMPLEMENTARIAS

El presente capítulo tiene como objetivo incluir información adicional y aclaraciones sobre aspectos específicos del proyecto, tomando en cuenta los requisitos establecidos en el **Pliego de Condiciones Específicas JCE-CCC-LPI-2024-0001**, así como las consultas y respuestas emitidas durante el proceso de licitación. Estas precisiones garantizan una alineación total con las expectativas de la Junta Central Electoral (JCE) y refuerzan el compromiso del **Consorcio IDSecure IDS** en la ejecución del proyecto.

9.1 Cumplimiento de la Capacidad de Producción y Entregas

Tarjetas de Identidad

El **Consorcio IDSecure IDS** garantiza la capacidad de producción y suministro de tarjetas de identidad conforme a los siguientes compromisos:

- **Volumen inicial:** 7,200,000 CIEs y 800,000 CIs en los primeros 18 meses.
- **Producción sostenida:** 900,000 CIEs y 100,000 CIs anuales a partir del segundo año de operación, durante los nueve años adicionales.
- **Diferenciación visual:** Ambas tarjetas compartirán las mismas características de seguridad y diseño, diferenciándose únicamente en el color del fondo de policarbonato.

Equipos de Impresión

El consorcio se compromete a:

- **Suministrar 214 máquinas de impresión**, de las cuales 164 serán destinadas a la operación nacional y 50 a las oficinas en el exterior.
- **Cumplir con la instalación y configuración de los equipos** en todos los centros designados por la JCE.
- **Garantizar la integración con el sistema central de la JCE** para la emisión y personalización de tarjetas en tiempo real.

PKI e Infraestructura de Clave Pública

- El adjudicatario asistirá a la JCE en todos los aspectos relativos a la gestión de la **Autoridad Certificadora (CA)**, aunque la obtención de la misma será responsabilidad exclusiva de la JCE, en cumplimiento con la legislación nacional.

Mobile ID y Ecosistema Digital

- Se implementará un **piloto de la Cédula Digital (Mobile ID)** dentro de los primeras 4.5 meses.
- La solución permitirá la interoperabilidad con sistemas gubernamentales y privados a través de **API REST** y el estándar **ISO 18013-5**, asegurando la verificación de identidad mediante credenciales digitales.

- La solución propuesta se integrará a la infraestructura existente de la JCE mediante API REST seguras, permitiendo la verificación y autenticación de ciudadanos en tiempo real. Se asegurará compatibilidad con bases de datos SQL Server 2022 y cumplimiento con estándares de interoperabilidad como ISO 18013-5 y OACI Doc 9303. El sistema estará preparado para integraciones con aplicaciones móviles y sistemas de validación biométrica.

9.2 Etapas del Contrato y Consideraciones Específicas

Con base en el **Pliego de Condiciones**, se detallan aspectos clave de las tres etapas del contrato:

Etapa 1: Implantación y Puesta en Marcha (19 semanas)

- **Entrega del diseño de seguridad** de las tarjetas en 4 semanas.
- **Entrega de 2 impresoras de policarbonato y 2,000 tarjetas para pruebas** en 19 semanas.
- **Implementación de la PKI y ceremonia de llaves** en 16 semanas.
- **Adaptación del SDK de la impresora al sistema de la JCE**.
- **Realización de pruebas piloto de Mobile ID y desarrollo de la app** antes de la semana 19.
- **Entrega de 300,000 tarjetas de policarbonato con certificación de durabilidad** en 19 semanas.
- **Capacitación del personal de la JCE** en la operación y mantenimiento del sistema.

Etapa 2: Operación de la Re-Cedulación Total de la Población (12 meses)

- Se garantizará la entrega de **8,000,000 de tarjetas electrónicas** en un período de 12 meses.
- **Instalación y puesta en marcha de los equipos de impresión en todas las sedes nacionales e internacionales**.
- **Mantenimiento de los equipos en garantía** con técnicos certificados en tecnología de impresión.

Etapa 3: Operación y Mantenimiento (Hasta 10 años)

- **Suministro de tarjetas** en base a la demanda de la JCE (1,000,000 de tarjetas anuales).
- **Mantenimiento de equipos de impresión** en República Dominicana y oficinas en el exterior (Nueva York, Madrid y otros centros estratégicos).

- **Soporte de Nivel 3** para PKI, Mobile ID y sistemas relacionados.

9.3 Aspectos Técnicos y Requisitos Específicos

Impresoras Láser de Personalización
Las impresoras suministradas cumplirán con los requisitos técnicos establecidos en el **Pliego de Condiciones**, incluyendo:

- **Láser de fibra de 20W** para garantizar alta velocidad y calidad en la personalización de tarjetas.
- **Velocidad de producción superior a 50 tarjetas por hora**.
- **Manejo automático de tarjetas con bandejas de entrada y salida** de hasta 250 unidades.
- **Conectividad Ethernet y USB** para integración con el sistema central de la JCE.

Seguridad y Certificaciones de las Tarjetas
Las tarjetas cumplirán con los estándares internacionales:

- **Normativa OACI Doc 9303** para documentos electrónicos de viaje.
- **ISO 14443 (contactless)** y **ISO 7816 (chip de contacto)** para interoperabilidad en sistemas digitales.
- **Durabilidad mínima de 10 años**, garantizada por el uso de policarbonato multicapa y personalización con grabado láser.

9.4 Aclaraciones sobre Requerimientos y Respuestas a Consultas

Tomando en cuenta las respuestas oficiales de la JCE y las consultas presentadas, se destacan los siguientes puntos clave:

1. **Confirmación de volúmenes de tarjetas**: La JCE ha confirmado que los volúmenes anuales de 900,000 CIEs y 100,000 CIs están garantizados por la totalidad de la duración del contrato.
2. **Requisitos de experiencia**: Se confirma y demostramos la experiencia específica en proyectos de personalización de documentos de identidad electrónicos con policarbonato en los últimos cinco años.
3. **Prueba de Concepto (POC)**: Se requiere y confirmamos que realizaremos una prueba funcional en Santo Domingo que incluirá personalización de tarjetas, generación de cédula digital y verificación mediante aplicación móvil.
4. **PKI y Firma Electrónica**: Nuestra propuesta proporciona un portal web para la gestión del ciclo de vida de certificados digitales, permitiendo la emisión, revocación y renovación.

5. **Instalación de equipos en el exterior**: Las impresoras destinadas a oficinas en el extranjero serán distribuidas por El Consorcio, con centros de mantenimiento en **Nueva York y Madrid**.

9.5 Implementación en la propuesta

Nuestra solución asegurará la interoperabilidad a través de los siguientes mecanismos:

A. APIs y Web Services

- Se proporcionarán **APIs RESTful** para la integración con los sistemas de la JCE y terceros.
- Soportará **OAuth 2.0 y OpenID Connect** para autenticación segura.
- Permitirá la validación de firmas electrónicas de documentos emitidos por la JCE en plataformas externas.
- Incluirá un **repositorio central de certificados** accesible mediante servicios web.

B. Soporte para Estándares Internacionales

- La infraestructura de firma digital será compatible con **ISO 32000-1 (PDF Signature) y CAdES/XAdES para documentos electrónicos**.
- Cumplirá con **los estándares de firma electrónica avanzada del Reglamento eIDAS de la Unión Europea**.
- Implementará **validación de certificados X.509 en tiempo real** mediante protocolos OCSP (Online Certificate Status Protocol) y CRL (Certificate Revocation List).

C. Integración con el Sistema Nacional de Identidad

- Permitirá la validación cruzada de identidad con el **Sistema Nacional de Identidad** de la JCE, evitando el uso fraudulento de credenciales.
- Se integrará con la infraestructura de PKI gubernamental para la autenticación de funcionarios autorizados.

El Consorcio IDSecure IDS reafirma su compromiso con la **Junta Central Electoral** en la entrega de una solución tecnológica avanzada, alineada con los más altos estándares de seguridad, calidad y eficiencia.

10. DETALLE ANEXOS

ANEXO 1 Certificaciones y Normas ISO

Certificado ISO 9001:2015

LITHO FORMAS S.A. DE C.V.

Certificado ISO 27001:2013

LITHO FORMAS S.A. DE C.V.

Certificado ISO 14001 – 2015

LITHO FORMAS S.A. DE C.V.

Explicación de presentación y Certificado ISO 14001 – 2015

LITHO FORMAS S.A. DE C.V.

Explicación de presentación y Certificado INTERGRAF ISO 14298:2013 Nivel Banca Central

LITHO FORMAS S.A. DE C.V.

Pruebas de Laboratorio en cumplimiento con la normativa ISO18745

LITHO FORMAS S.A. DE C.V.

Hoja de datos del producto utilizado que evidencia el cumplimiento con la norma ISO/IEC 14443

TOPPAN SECURITY SAS

Conjunto de documentos que incluyen:

Declaración Jurada

Certificación del RENAPER

Orden de Compra

Pliego técnico

Magallanes Media S.A.

Certificados SOMA c016 (Hoja de datos de chip propuesto)

TOPPAN SECURITY SAS

Certificación requerida

Magallanes Media S.A.

Certificado ISO 28001:2007

LITHO FORMAS S.A. DE C.V.

Certificado 2846-1:2017

LITHO FORMAS S.A. DE C.V.

ANEXO 2 Personal Requerido

Líder del proyecto

Consorcio ID Secure IDS

10 hojas de vida del equipo técnico propuesto.

IXLA S.R.L.

Equipo que brindará el mantenimiento a la PKI

Magallanes Media S.A.

Se incluyen dos hojas de vida del equipo junto a sus respectivos certificados

Magallanes Media S.A.

Se incluye hoja de vida acompañada por el certificado de SAFe6 (superior al requisito)

Magallanes Media S.A.

ANEXO 3 Experiencia y Cartas de Referencia

Carta de referencia emitida por el RENAPER en la República de Argentina

(CUMPLIMIENTO: 1 PILOTO O DESARROLLO DE UNA SOLUCION DE CEDULA DIGITAL ISO1803-5)

Magallanes Media S.A.

Declaración Jurada de IXLA S.R.L. donde da fe en la participación en 7 proyectos, incluido mas no limitado al suministro de equipos de Personalización (impresión y su respectivo mantenimiento y soporte)

IXLA S.R.L.

Carta de referencia que acredita el proyecto en el Registro Nacional de Identificación y Estado Civil – RENIEC del Perú.

(CUMPLIMIENTO 1: EXPERIENCIA EN SUMINISTRO DE IMPRESORAS)

IXLA S.R.L.

Carta de referencia para el proyecto de personalización del documento PPT para migrantes de Colombia.

(CUMPLIMIENTO 2: EXPERIENCIA EN SUMINISTRO DE IMPRESORAS)

IXLA S.R.L.

Ordenes de compra en donde el cliente final es la Autoridad de Información y Gobierno – Emiratos Árabes Unidos.

(CUMPLIMIENTO 3: EXPERIENCIA EN SUMINISTRO DE IMPRESORAS)

IXLA S.R.L.

Carta de referencia de Kazajistán donde evidencia la venta de 16 equipos de personalización. Junto a la referencia se evidencia la extensión del proyecto y que el mismo entra dentro de los últimos 5 años.

(CUMPLIMIENTO 4: EXPERIENCIA EN SUMINISTRO DE IMPRESORAS)

TOPPAN Security, S.A.S.

Referencia de Proyecto – secretaria de Hacienda y Crédito Público – Estados Unidos Mexicanos

(CUMPLIMIENTO 1**: EXPERIENCIA EN SUMINISTRO DE DOCUMENTO DE IDENTIDAD ELECTRONICA**)

LITHO FORMAS S.A. DE C.V.

Referencia de proyecto – Ministerio del Interior de la República de Kazajistán. Donde se evidencia la entrega de más de 4 millones de credenciales y sus componentes como parte del proyecto dentro de los últimos 5 años.

*(**CUMPLIMIENTO 2**: EXPERIENCIA EN SUMINISTRO DE DOCUMENTO DE IDENTIDAD ELECTRONICA)*

TOPPAN Security SAS

Carta de referencia conjunta para el proyecto de la República de Nigeria. La referencia está acompañada por facturas como evidencia de las entregas.

(CUMPLIMIENTO 1**: EXPERIENCIA EN PROYECTOS TRANSICION DOCUMENTOS SIN ELECTRONICO A ELECTRONICO**)

IXLA S.R.L.

Carta de Referencia conjunta para el proyecto de la República de Azerbaiyán. La referencia está acompañada por facturas como evidencia de las entregas.

(CUMPLIMIENTO 2**: EXPERIENCIA EN PROYECTOS TRANSICION DOCUMENTOS SIN ELECTRONICO A ELECTRONICO**)

IXLA S.R.L.

Carta de referencia para el proyecto de personalización del documento PPT para migrantes de Colombia. La referencia está acompañada por facturas como evidencia de las entregas.

(CUMPLIMIENTO 3**: EXPERIENCIA EN PROYECTOS TRANSICION DOCUMENTOS SIN ELECTRONICO A ELECTRONICO**)

IXLA S.R.L.

Referencia Con cumplimiento de ISO 18013-5. RENAPER-Argentina

(CUMPLIMIENTO1:** EXPERIENCIA EN PROYECTOS MOBILE ID **con mas de 100 mil credenciales)

Magallanes Media S.A.

Referencia. RENAPER-Argentina

(CUMPLIMIENTO 2 :** EXPERIENCIA EN PROYECTOS MOBILE ID**)

Magallanes Media S.A.

Referencia de Proyecto en Filipinas

(CUMPLIMIENTO 3:** EXPERIENCIA EN PROYECTOS MOBILE ID**)

TOPPAN Security SAS

Referencia de participación conjunta en el proyecto España.

(CUMPLIMIENTO 1:** EXPERIENCIA EN SUMINISTRO EN MAS DE 200 IMPRESORAS DISTRIBUIDAS**)

IXLA S.R.L.

Referencia de EDENORTE, República Dominicana

(CUMPLIMIENTO 1:** EXPERIENCIA EN PROYECTOS MANTENIMEINTO DE TECNOLOGIA EN GOBIERNO**)

Midas Dominicana S.A.

Referencia 1. RENAPER-Argentina

(CUMPLIMIENTO 1:** EXPERIENCIA EN PROYECTOS DE INTEGRACION DE SISTEMAS**)

Magallanes Media S.A.

Referencia 2. RENAPER-Argentina

(CUMPLIMIENTO 2:** EXPERIENCIA EN PROYECTOS DE INTEGRACION DE SISTEMAS**)

Magallanes Media S.A.

ANEXO 4 Declaraciones Juradas

Declaración Jurada de TIEMPO para entrega 4.5 Meses

Consorcio IDSecure IDS

Declaración Jurada - SERVICIOS DE DESARROLLADOR DE PKI

Consorcio IDSecure IDS

Declaración Jurada - PROVEEDORES DE TARJETAS E IMPRESORAS EN EMPRESA CONJUNTA

Consorcio IDSecure IDS

Declaración Jurada - IMPRESORA

(CUMPLIMIENTO 1:** CUMPLMIENTO DE CARACTERISTICAS DE LA IMPRESORA**)

Consorcio IDSecure IDS

Declaración Jurada- PRODUCCIÓN DE LAS TARJETAS

(CUMPLIMIENTO 1:** FABRICA DE TARJETA PRINCPAL Y DE RESPALDO**)

Consorcio IDSecure IDS

Declaración Jurada - CUERPO DE LAS TARJETAS

(CUMPLIMIENTO :** CARACTERITICAS 7 CAPAS DE LA TARJETA Y POLICARBONATO**)

Consorcio IDSecure IDS

Declaración Jurada - PROCESO DE PERSONALIZACIÓN

(CUMPLIMIENTO : CUERPO EN BLANCO Y PROCESO DE PERSONALIZACION NO PATENTADO)

Consorcio IDSecure IDS

Declaración Jurada – EXTENSIÓN DE GARANTÍAS 5 AÑOS (SOPORTE Y MANTENIMIENTO)

Consorcio IDSecure IDS

Declaración Jurada – EXTENSIÓN DE GARANTÍAS 5 ANOS (IMPRESORAS)

IXLA S.L.R.

Declaración Jurada - ELEGIBILIDAD

(CUMPLIMIENTO 2:** EXCLUSIVIDAD DE PARTICIPACION**)

Consorcio IDSecure IDS

Declaración Jurada - MOBILE ID

Consorcio IDSecure IDS

ANEXO 5 Prueba de Durabilidad

Prueba de Laboratorio

(CUMPLIMIENTO:** PRUEBAS DE DURABILIDAD DE LAS TARJETAS**)

LITHO Formas S.A. de C.V.

ANEXO 6 Cronograma

Cronograma Propuesto

Consorcio IDSecure IDS

ANEXO 7 Diseño

Diseño Tarjetas Propuesto

(**CUMPLIMIENTO:** DISEÑO DE TARJETA EN USB)

Consorcio IDSecure IDS

Diseño Tarjetas Propuesto

(**CUMPLIMIENTO:** DISEÑO IMPRESO)

Consorcio IDSecure IDS

ANEXO 8 Hojas de Datos de Productos Periféricos

Hojas de Datos Periféricos

Consorcio IDSecure IDS

- Escáner
- Lector de firma
- Lector de huellas
- Impresora punto de venta Térmica
- Lector de huellas digital personal
- Cámara fotográfica
- Lector RFID (230)

ANEXO 9 Planes de Implementación e Integración

Plan de Implementación de APLICACIONES MOVILES

Consorcio IDSecure IDS

Plan de Integración con los SISTEMAS DE IDENTIFICACION

(**CUMPLIMIENTO:** Integración con el Sistema de Enrolamiento y emisión de cedulas y sus sistemas relacionados)

Consorcio IDSecure IDS

Plan de ANALISIS Y PRUEBA

(**CUMPLIMIENTO:** Ajuste de interfaces de comunicación propuestas por el JCE)

Consorcio IDSecure IDS

Plan de OPERACIÓN Y MANTENIMIENTO

(**CUMPLIMIENTO:** Disponibilidad de 99.95% en horas de producción)

Consorcio IDSecure IDS