**TALLER SOBRE INTEGRIDAD DE PASAPORTES**

**Secretaría de Relaciones Exteriores**

**Ciudad de México, México**

**17-18 de julio, 2017**

**RELATORÍA DÍA 1**

**17 de julio de 2017**

**Sesión Inaugural**

UNODC, en sus palabras de bienvenida, nos hizo una reseña histórica sobre los orígenes del pasaporte, remontándonos a épocas bíblicas y medievales, así como las características de los primeros pasaportes. De manera progresiva, los pasaportes fueron foliados, se insertó la fotografía y papel de seguridad.

El Señor Felipe De La Torre comentó cómo el mercado negro se beneficia de la falsificación de pasaportes. La expedición de documentos apócrifos es un delito, del cual se aprovechan las redes de trata y tráfico. UNODC, a través de su campaña #NegocioMortal hace conciencia en la relación de los delitos de tráfico con el uso de pasaportes fraudulentos.

Estados Unidos, a través del Ministro Consejero Ian Brownlee, enfatizó en que los gobiernos de la región debemos trabajar de forma conjunta para combatir los delitos de trata y tráfico.

Jason Hollman, de Canadá, enfatizó en el uso de documentos fraudulentos y la migración irregular y la importancia en cómo la incursión de nuevas tecnologías nos ayudan a combatir la criminalidad organizada.

La Viceministra Liduvina Magarín señaló la importancia de mantenernos al día en cuanto a la normativa internacional para la emisión de pasaportes.

La Subsecretaria para América Latina y el Caribe, Socorro Flores, de la Secretaría de Relaciones Exteriores de México, destacó la relevancia de este taller, y los retos que tenemos como región. El intercambio de información es vital para combatir a la criminalidad organizada.

**Sesión 1: Contexto internacional y la seguridad de los viajes**

El Señor Felipe De La Torre hizo el recordatorio que el pasado 4 de abril, UNODC hizo el lanzamiento en la Ciudad de Washington DC la campaña #NegocioMortal, para hacer visibles los vínculos del tráfico ilícito de migrantes con otras manifestaciones de criminalidad organizada, donde no escapa el uso de pasaportes falsos.

El Señor Arnulfo Cristancho, a nombre de Migración Colombia, hizo un recuento de las migraciones extra-regionales en Colombia, con referencia a las nuevas rutas que están tomando los flujos migratorios irregulares. Hizo énfasis a los factores asociados a la migración irregular en Colombia y el impacto del tráfico de migrantes en los países de tránsito, destino y origen. De igual forma, los avances institucionales en materia de tráfico de migrantes, con el apoyo de UNODC.

Migración Colombia cuenta con lectoras de pasaportes, equipos móviles y puertas para migración automática.

Desde el 2010, el pasaporte colombiano cumple con los estándares de la OACI y desde el año 2015 se incorporó el chip.

La OIM compartió unas reflexiones sobre cómo podemos poner en práctica acciones en materia de seguridad de pasaportes.

La OIM nos compartió el riesgo de métodos de cruce ilegal de fronteras, con tres niveles:

Riesgo más bajo: con un pasaporte oficial (robado)

Riesgo medio: Como impostor o haciéndose pasar por otra persona.

Riesgo alto: Pasaporte falso o fraudulento

Muchas veces el uso de pasaportes fraudulentos se da por ignorancia, cuando es utilizado por las personas que son víctimas del tráfico ilícito de migrantes o la trata de personas.

La vulnerabilidad más grande no es pasaporte fraude, sino el proceso de emisión de pasaportes y la carencia de elementos de seguridad en la integridad de pasaportes.

La base es el sistema de gestión de identidad, seguido de la seguridad de los documentos y posteriormente la seguridad en frontera.

OIM compartió importantes reflexiones en cuanto a la necesidad de dar el salto al pasaporte electrónico. Un pasaporte electrónico no tiene mucha utilidad si no es utilizado adecuadamente. Las agencias deben apoyar a los Estados a decidir cuáles son sus necesidades y opciones, a garantizar la calidad (incluyendo el cumplimiento de las normas de la OACI) y apoyar a los Estados a no desperdiciar recursos.

OIM compartió sus prioridades para la asistencia, entre las que destacan el apoyo a los Estados para hacer procedimientos de integridad de pasaportes y fronteras, así como la capacitación de funcionarios en frontera y mecanismos de evaluación.

Entre más se conozca de las necesidades y retos, OIM y OACI pueden traducirlas en proyectos de asistencia técnica.

**Sesión 2: Requisitos, normas y mejores prácticas internacionales**

Presentación sobre Requisitos, normas y mejores prácticas internacionales

Ricardo Delgado, OACI

Al ser parte de Naciones Unidas, OACI debe armonizar sus objetivos a los Objetivos de Desarrollo Sostenible (ODS), incluyendo entre otros, igualdad de género, trabajo decente, reducción de inequidades, protección de la tierra y la vida, la justicia y la paz para reforzar las instituciones de diferentes gobiernos.

Más de la mitad de movimientos internacionales se dan por la vía aérea, razón por la que hay que reforzar la seguridad documental en aeropuertos.

El anexo 9 integra las normas y los métodos recomendados, para el ingreso de aeronaves, pasajeros y equipaje, carga y correo.

Los Estados deben tener las formas de coordinar a lo interno el cumplimiento de las disposiciones, por ejemplo las autoridades de aviación civil con las respectivas policías de control migratorio.

Normas de la OACI van más allá de las recomendaciones, son formas de aplicación necesaria para la regulación aérea internacional. Si bien no dice la palabra “obligatoria”, se reconoce una aplicación uniforme como necesaria y deseable.

Los Estados deben notificar a la OACI cuáles normas o métodos recomendados no pueden cumplir.

Los Estados deberían unirse al Directorio de Claves Públicas (PKD), si emiten documentos de viaje electrónicos, mediante chip, para que la información sea intercambiada por otros países que emiten pasaporte electrónico, para que la información se pueda leer y tener el intercambio real de la información.

Los Estados tienen la obligación de reportar a INTERPOL la pérdida o robo de pasaportes o aquellos pasaportes que han sido removidos de sistema.

También, debe haber una base de datos creada, con una infraestructura pública creada a nivel nacional.

Si bien los documentos de viaje deben ser de lectura mecánica desde el año 2005, en muchos países fueron engañados por los proveedores que venden pasaportes.

El Señor Delgado recalcó la importancia de compartir con los demás países las limitaciones, para evitar que sus documentos de viaje electrónicos sean objeto del mercado negro.

Los Estados también deberían tener un sistema de información anticipada de pasajeros (API), información que debería estar en los datos de la primera página del pasaporte. Los Estados deben buscar mecanismos seguros para la transmisión de la información y no utilizar cuentas de correo como Hotmail o Yahoo ni mucho menos redes sociales.

Actualmente, la emisión de pasaportes electrónicos no es una norma, sin embargo un pasaporte electrónico nos brinda más seguridad que un documento de viaje de lectura mecánica.

Es importante tomar en consideración el control en el resguardo, custodia y almacenamiento de pasaportes, así como la inspección de sistemas y herramientas.

Las autoridades de Aviación Civil son el nexo directo con la OACI. Tienen un contacto inmediato, sin tener que recurrir a los ministerios de Relaciones Exteriores.

OACI enumeró las agencias que deben formar parte del Comité para la implementación del Programa Nacional de Transporte Aéreo, así como la Estrategia Nacional de Autenticidad de la Identidad.

La verificación y control recae en las autoridades de control fronterizo. De ahí la importancia de la coordinación entre las autoridades a cargo de la emisión de documentos de viaje y las autoridades de control fronterizo.

Se tiene que tomar en cuenta la privacidad de la información.

En la sesión de preguntas y comentarios de la sesión 3, se hicieron importantes reflexiones acerca del resguardo de las personas menores de edad.

Se reiteró en la importancia de compartir los problemas que se atraviesan, para ayudar a OACI a resolver los problemas y dar el oportuno seguimiento.

México resaltó el contacto con Migración Colombia, en el marco del diálogo con la Conferencia Suramericana de Migración (CSM), en el seguimiento al Grupo ad hoc sobre migrantes extra-regionales. El tema que compartió Migración Colombia es uno de los temas a abordar en el diálogo entre CRM y CSM.

**Sesión 3: Herramientas de apoyo a la implementación**

La Señora Nicoletta Bouwman, del Ministerio de Inmigración, Refugiados y Ciudadanía de Canadá compartió los estándares y prácticas recomendadas en la guía de la OACI y en el anexo 9.

La guía comprende buenas prácticas sobre la emisión segura de documentos de viaje y una guía para la evaluación.

La Señora Bouwman comentó la importancia de concentrarse en el proceso de emisión.

La guía sirve para que las autoridades puedan evaluar su sistema de emisión por sí mismas y que los evaluadores calificados puedan evaluar el sistema de emisión de otro país. La guía no es un examen, es una herramienta para mejorar el proceso.

El Señor Omar Lemus Loarca, de Guatemala compartió su experiencia en el proceso de custodia y emisión de pasaportes, en sus tres fases: 1) compra de libretas, 2) recepción y resguardo y 3) procedimiento de emisión y entrega de pasaportes.

**Sesión 4: Puntos de contacto sobre integridad y principales retos**

El Señor Malcolm Eales, Director de la División de Integración de Riesgos de Integridad de Canadá compartió temas clave en cuanto a la integridad de pasaportes, desde la perspectiva canadiense. Canadá destacó tres componentes clave en la integridad del pasaporte: emitir un documento seguro, garantizar un sólido proceso de expedición y la gestión de pasaportes en circulación.

Un reto es cómo asegurar integridad cuando tenemos procesos de solicitud en línea. La respuesta está en la misma tecnología. Asimismo, los retos en cuanto a documentos perdidos y robados (tema del día 2), fraude integrado y las mitigaciones que debemos asumir en frontera.

La Señora Martha Martínez Mendoza hizo una presentación sobre la experiencia de México en el proceso de emisión de pasaportes. Es importante encontrar el equilibrio entre los procesos de seguridad y el resguardo constante de la información. El pasaporte mexicano se ha construido con base en lo que constantemente han sido ataques a su integridad. México ha implementado mejores prácticas para prevenir el fraude, entre las que destacan acreditar identidad y nacionalidad, con la presencia del solicitante, así como la captura de datos biométricos. Cuando un usuario solicita su pasaporte de manera recurrente, se contacta a la INTERPOL y se emite una alerta.

**Sesión 5: Gestión de las instalaciones**

El Señor Jeff Cooley, Jefe de la División de Control Interno del Departamento de Estado compartió la experiencia de Estados Unidos en cuanto a los controles y protocolos que emplean en las instalaciones donde se emiten los pasaportes. El Señor Cooley hizo referencia a las cifras, demanda, número de empleados, agencias, puntos de captura y proyecciones de demanda para el 2017, 2018 y 2019 en los servicios de pasaporte.

En cuanto a seguridad de las instalaciones, se emplean múltiples protocolos, por ejemplo: ingreso de personal de limpieza, ingreso de invitados, planes de seguridad, ingreso de dispositivos electrónicos, lóckers para resguardo de pertenencias, manejo de desechos, sistemas de cómputo, etc.

Utilizan sistemas de autoevaluación y Score Cards para identificar logros y desempeño.

**CONCLUSIONES DÍA 1:**

* Intercambio de experiencias país y aprendizaje en todo el proceso de emisión de documentos de viaje, en cuanto a normativa, retos, lecciones aprendidas y buenas prácticas.

Algunos puntos a tomar en cuenta por parte de los Estados son los siguientes:

* Considerar el incremento sustantivo en el flujo de migrantes extra-regionales en los países de la CRM y seguir promoviendo en foros regionales y subregionales en los que participamos, las campañas para combatir los delitos de trata y tráfico, así como su relación con el uso del pasaporte fraudulento.
* Las agencias de Naciones Unidas participantes en este taller, OIM, OACI, UNODC, están comprometidos en apoyar a los Estados miembros de la CRM en la toma de decisión respecto de las necesidades y opciones para garantizar la integridad en la emisión de documentos de viaje (incluyendo el cumplimiento de las normas de la OACI) y apoyar e impulsar a los países a concentrar recursos.
* A sugerencia de la INTERPOL, los países miembros de la CRM deben tener las formas de coordinar a lo interno el cumplimiento de las disposiciones, por ejemplo las autoridades de aviación civil con las respectivas policías de control migratorio.
* A pesar de que las recomendaciones de la OACI no son vinculantes, los Estados miembros de la CRM deben notificar a esta organización cuáles normas o métodos recomendados no son compatibles con su normativa o capacidades instaladas.
* Los países deberían unirse al Directorio de Claves Públicas (PKD), si emiten documentos de viaje electrónicos.
* Los países tienen la obligación de reportar a INTERPOL la pérdida, robo o pasaportes revocados o aquellos pasaportes que han sido retirados de sistema (expirados, cancelados o dañados). También, debe haber una base de datos creada, con una infraestructura pública a nivel nacional.
* Los países también deberían tener un sistema de información anticipada de pasajeros (API), información que debería estar en los datos de la primera página del pasaporte. Los países deben buscar mecanismos seguros para la transmisión de la información y no utilizar cuentas de correo como Hotmail o Yahoo ni mucho menos redes sociales.
* Se exhortó a los países miembros de la CRM a utilizar herramientas prácticas, como la guía de la OACI para la emisión de pasaportes.
* A partir de la experiencia de Colombia, Canadá, Guatemala, México, Costa Rica y Estados Unidos a reconocer las fases comunes de los países para emitir un documento seguro y garantizar un sólido proceso de expedición y la gestión de pasaportes.

**RELATORÍA DÍA 2**

**18 de julio, 2017**

**Sesión 6: Gestión de la identidad y la seguridad física de los documentos.**

El Señor Ángel Luis Suárez Sanabria, Director General Adjunto Técnico, del Registro Nacional de Población (RENAPO) se enfocó en el acta de nacimiento en línea como herramienta de seguridad de identidad y documentos.

El certificado de nacimiento en línea mejorará el reconocimiento de identidad legal. El manejo de la identidad en México incluye datos biométricos, así como códigos y firma electrónica. El certificado de nacimiento se puede acceder en línea a través de un código QR, en la dirección [www.gob.mx/actas](http://www.gob.mx/actas)

El Sr. Delgado, de la OACI, presentó la gestión de la identidad como un sistema integral, un "ecosistema" que está interconectado entre agencias gubernamentales e intergubernamentales.

La Evidencia de Identidad (EOI) es la información para establecer o verificar una identidad única. Debería haber un equilibrio entre el riesgo y la habilitación o facilitación de los servicios.

En cuanto a la mejora de los documentos de viaje, es mucho más difícil producir documentos de viaje falsos. A medida que se mejora la calidad y la integridad de los documentos de viaje, los objetivos deben centrarse en la debilidad de los documentos.

Necesitamos un alto grado de confianza en los documentos que producimos.

EOI basado en riesgo: El riesgo de identidad está relacionado con el robo de identidad, el terrorismo, el fraude financiero. Estos riesgos afectan la imagen nacional.

Uno de los principios fundamentales es determinar si el solicitante está relacionado con la identidad, para asegurarse de que sólo hay una identidad única.

El solicitante debe tener una identidad válida, robusta, que nos permita la confianza necesaria al renovar un pasaporte.

La verificación se debe hacer con dos o más bases de datos, así como otra información disponible, como los registros de defunción. La biometría, el iris facial y el ojo nos ayudan a garantizar la identidad.

Existe un impacto legislativo sobre el intercambio de información o la protección de la información. No hay "talla única". Hay cuestiones geográficas que deben tomarse en cuenta.

Las matrices de riesgo pueden ser utilizadas por los países como herramientas de su "ecosistema de identidad".

Un alto nivel de confianza requiere un rango de evidencia promedio. Por ejemplo, las preguntas sobre el país de origen son útiles para determinar si la persona está usando una identidad falsa.

Las solicitudes deben ser recibidas y dirigidas a una fuente única.

Puntos claves para la creación de confianza: es muy importante que los Estados establezcan una identidad única en su sistema. Los países miembros reconocieron que si no hay datos biométricos, el desafío es mucho mayor.

Aunque los documentos físicos son útiles, son vulnerables (certificados de bautismo, actas, etc.).

Evolución EOI. A medida que la tecnología y el medio ambiente cambian, los Países Miembros también deben avanzar. Es muy importante que los Países Miembros implementen un sistema de guía de confianza de evidencia de identidad, fortalecimiento de capacidades.

Isaías Antonio Maradiaga, del Ministerio de Relaciones Exteriores de Honduras, compartió su experiencia en sus agencias consulares. Hay varios consulados en América Central y América del Norte donde se producen pasaportes, mientras que otros consulados en América Central, América del Norte, Europa y Asia se concentran en la recolección de datos. Honduras produce tres tipos de pasaportes: pasaportes diplomáticos, oficiales y ordinarios.

La Sra. Claudia Cordero, Investigadora de Fraude Criminal de la Oficina de Seguridad Regional de la Embajada de los Estados Unidos, describió los esfuerzos de coordinación con las autoridades mexicanas en investigaciones de fraude de documentos de viaje. A través de sus actividades de capacitación, mejoran las capacidades de las autoridades en técnicas para identificar el fraude y los pasaportes falsos.

Para identificar el fraude, la entrevista es uno de los primeros filtros, seguido por el reconocimiento facial.

En la sección de preguntas y comentarios de esta sesión, hubo un comentario interesante hecho por México en cuanto a confiar en la buena voluntad de los solicitantes frente a las técnicas de identificación de fraudes.

Los países miembros compartieron la información relativa a los sistemas de consulta de identidad en línea y compartieron los números de identificación con otros documentos, como la licencia de conducir, la tarjeta de identidad y los documentos de viaje.

**Sesión 7: Etapa final del fraude de pasaportes - respuestas y aplicación de la ley.**

Nick Titcombe, Analista de Documentos y Consejero Principal del Centro Nacional de Documentos, de la Dirección General de Operaciones de Canadá, presentó el ciclo de vida de un pasaporte: un modelo emitido por 5 años, tiene validez máxima de 10 años. En el segundo año: empiezan las manifestaciones de fraude.

Canadá proporcionó un análisis sobre las características de seguridad más fuertes.

La impresión intaglio es muy segura, aunque es muy cara.

La impresión de fondo es muy importante también. Es muy fácil de detectar por los oficiales.

Es muy difícil cuando se reproducen patrones sencillos.

A veces las opciones de color están disponibles comercialmente. Se sugiere evitar los colores sencillos como cian y magenta.

Otras medidas son: Micro-impresión, impresión en segundo plano, impresión arco iris y colores verdaderos.

El registro transparente es una característica altamente recomendada.

Después de 15 años de ciclo de vida, los falsificadores tienen tiempo para completar su tarea.

Las características táctiles también pueden ser objeto de fraude.

La tinta ópticamente variable es también una característica costosa.

En un puerto de entrada, los agentes tienen 7 segundos para detectar el fraude.

Si los Países Miembros de la CRM van a usar pasaportes electrónicos, deben ser usados correctamente, y unirse al Directorio de Claves Públicas (PKD).

Aproximadamente 60 de 120 países que tienen pasaporte electrónico, tienen PKD.

Se exhorta a los países miembros de la CRM a producir documentos de viaje con la combinación e integración de características de primer, segundo y tercer nivel.

No hay que confiar únicamente en una característica, sino también en la tecnología y la revisión humana de pasaportes.

Martha Martínez, de la Secretaría de Relaciones Exteriores de México, compartió las acciones en caso de alto fraude visible reportado por las Delegaciones. Hay dos intervenciones de la Dirección General de Delegaciones: acciones preventivas y correctivas.

Entre las acciones correctivas se encuentran la nulidad de pasaportes y, cuando se confirman los casos de fraude, el intercambio de información a través de las alertas migratorias y la notificación a INTERPOL.

Se alienta a los Países Miembros de la RCM a fortalecer las acciones correctivas, tales como el intercambio de datos y la generación de alertas migratorias.

Es importante considerar la buena comunicación entre las agencias gubernamentales

Si la información se maneja electrónicamente, los resultados de la investigación serán más inmediatos, así como la capacidad de responder a los solicitantes.

Ana María Coutu, Oficial de Enlace de la Agencia de Servicios Fronterizos de la Embajada de Canadá en México, compartió los procedimientos para identificar el fraude, el tipo de fraude, las características de seguridad conocidas y la confirmación con la autoridad emisora. Si se confirma el fraude, se notifica a las autoridades de terceros países.

Se exhortó a los Países Miembros de la CRM a intercambiar información y notificar a terceros países los casos confirmados de fraude, cuando sean identificados.

Para fomentar medidas preventivas, se utilizan medidas como la biométrica, el reconocimiento facial y quioscos de atención primaria.

¿Cómo elegir las características correctas al diseñar un nuevo pasaporte?

Lo que necesitamos es un diseño inteligente. No hay nada absolutamente seguro, ni tampoco hay que confiar en el consejo de los vendedores. Es necesario fomentar las tecnologías emergentes, ya que la rotación de oficiales es un desafío. El componente humano es muy valioso, por lo que es muy importante aumentar la formación de acuerdo con las innovaciones tecnológicas. Si tenemos buena tecnología pero los oficiales no están entrenados, no tendremos buenos resultados. Es importante fortalecer la tecnología y la capacitación.

Se instó a los países a identificar las características de seguridad y encontrar un equilibrio.

**Sesión 8: Interconexión entre pasaportes, la frontera y visas.**

El Sr. Erik Slavenas, Especialista en Gestión de Identidad y Biometría de la OIM, compartió consideraciones importantes sobre el control de pasaportes en las fronteras.

¿Cuál es la utilidad en el uso del pasaporte electrónico si en las fronteras se utiliza como un documento de lectura mecánica?

Los laboratorios forenses de alta tecnología no pueden reemplazar las capacidades de examen de pasaportes hechas por oficiales capacitados. El fortalecimiento de las capacidades de los funcionarios fronterizos es muy importante.

"Las fronteras ya no están en las fronteras". Hay un aumento en la dependencia de los datos de viaje y menos en el pasaporte físico. La gestión de fronteras se basa cada vez más en la inteligencia y los riesgos.

El Sr. Slavenas compartió herramientas útiles de la OIM, tales como MIDAS (Sistema de Análisis de Información y Datos de la Migración).

Alejandro Austria De la Vega, Director de Vinculación con el Servicio Exterior del Instituto Nacional de Migración de México, compartió el proceso de expedición de visados autorizado por el Ministerio de Relaciones Exteriores.

La Sra. Gisela Chung, Directora General de la Autoridad Nacional de Pasaportes de Panamá, compartió su experiencia en materia de emisión de pasaportes, así como en el almacenamiento de los documentos de viaje.

Es importante tener procedimientos escritos. A menudo existen procedimientos, pero basados en lo que dice un supervisor de turnos o en prácticas no escritas.

**Sesión 9: Intercambio de información internacional.**

Fabrizio Di Carlo, Oficial Especializado de INTERPOL, destacó que los participantes tienen un buen conocimiento de las actividades de INTERPOL, así como el intercambio de información con esta organización.

INTERPOL compartió dos resoluciones del Consejo de Seguridad de las Naciones Unidas (Resolución 1373, del año 2011 y Resolución 1624, del año 2005), sobre la importancia de combatir el fraude en los documentos de viaje.

Los documentos de viaje robados y perdidos (SLTD) han ido aumentando a lo largo de los años.

Hay una brecha entre el número de pasajeros y el número de casos de SLTD.

SLTD tiene su plan estratégico:

* Aumentar el número de información compartida por los países.
* Reducir el número de “hits” (búsquedas administrativas generadas por documentos).
* Aumentar la calidad de los datos con la meta de una exactitud de datos del 99%.
* Aumentar la búsqueda de datos a nivel mundial.

INTERPOL alienta a los países miembros de la CRM a implementar la tecnología API / PNR / E-VISA, que puede adaptarse a los sistemas de las autoridades.

Asimismo, informar inmediatamente a INTERPOL cuando se identifiquen los pasaportes fraudulentos.

Existen otras bases de datos a las que se puede acceder de forma gratuita, como EDISON TD y el Sistema de Identificación de Documentos para Servicios Civiles (DISCS).

El proyecto Dial-Doc V2 está casi listo y está en proceso de ejecución por parte de INTERPOL.

Es importante aplicar soluciones FIND, con acceso a bases de datos nacionales, regionales e internacionales.

Aplicar WISDM para sincronizar INTERPOL y bases de datos nacionales.

Integrar INTERPOL FIND en los sistemas nacionales de control fronterizo.

Controlar sistemáticamente a cada pasajero.

Malcolm Eales, Director de Integración de Riesgos del Ministerio de Inmigración, Refugiados y Ciudadanía de Canadá destacó que Canadá ha sido un fuerte partidario de SLTD y ha enviado registros actualizados.

Un desafío que se enfrenta es cuando los países introducen errores falsos en el sistema INTERPOL.

La interoperabilidad es clave para obtener mejores resultados en SLTD.

**Sesión 10: Pasaporte Electrónico**

La charla magistral sobre el tema de pasaporte electrónico fue presentada por Michael Holly, Consejero Principal de Asuntos Internacionales del Departamento de Estado, Oficina de Asuntos Consulares, Pasaportes y Servicios, Presidente del Grupo de Trabajo de Nuevas Tecnologías de la OACI.

La emisión del pasaporte electrónico no es un estándar de la OACI. Los países no están obligados a emitir Pasaporte Electrónico. Lo que sí deben emitir los paíes son documentos de viaje de lectura mecánica (MRTD).

La ventaja del pasaporte electrónico es que permite validar en tiempo real.

La infraestructura de clave pública (PKI) permite a una Autoridad Emisora proteger los datos en el chip del pasaporte electrónico.

El intercambio de datos debe cumplir con los estándares legales apropiados.

Una gestión robusta de la identidad es la clave para producir un documento de viaje seguro.

**CONCLUSIONES DÍA 2**

* Integridad, características de seguridad de los documentos de viaje, fraude, interconectividad y E-Passport.

Algunos puntos a tomar en cuenta por los países miembros de la CRM son los siguientes:

* A medida que se mejora la calidad y la integridad de los documentos de viaje, nuestros objetivos deben centrarse en la debilidad de los documentos y los sistemas de apoyo.
* Elementos clave para la generación de confianza: es muy importante que los países establezcan una identidad única en su sistema y la importancia de la seguridad y la integridad de los sistemas de identidad. Los Países Miembros de la CRM reconocieron que si no hay datos biométricos, el reto es mucho mayor.
* Es muy importante que los países miembros de la CRM implementen un sistema de guía de confianza de la evidencia de identidad, así como el fortalecimiento de capacidades.
* Se alienta a los países miembros de la CRM a producir documentos de viaje con la combinación e integración de características de primer, segundo y tercer nivel. Debemos enfocarnos en aquellos elementos de seguridad que son fáciles de verificar y a su vez difíciles de reproducir.
* No confiar solamente en una característica para la validación; sino basarse tanto en la tecnología como en la revisión humana de los pasaportes.
* Se alienta a los Países Miembros de la CRM a fortalecer las acciones correctivas, tales como el intercambio de datos y la generación de alertas migratorias.
* Es importante considerar la buena comunicación entre las agencias gubernamentales.
* Si la información se maneja electrónicamente, los resultados de la investigación serán más inmediatos, así como la capacidad de responder a los solicitantes.
* Se alienta a los Países Miembros de la CRM a que intercambien información y notifiquen a terceros países los casos confirmados de fraude cuando sean identificados.
* Los laboratorios forenses de alta tecnología no pueden reemplazar las capacidades de examen de pasaportes hechas por oficiales entrenados.
* INTERPOL alienta a los países miembros de la CRM a implementar lo siguiente:
	+ La tecnología API / PNR / E-VISA, que pueda adaptarse a los sistemas de las autoridades e integrar dicha tecnología con INTERPOL FIND para una inspección completa de los pasajeros.
	+ Informar inmediatamente a los sistemas INTERPOL (SLTD y / o Dial-Doc) cuando se identifiquen pasaportes fraudulentos (robados, perdidos, revocados, robados en blanco a SLTD, falsos a Dial-Doc).
	+ Aplicar WISDM para sincronizar oportunamente y con exactitud las bases de datos INTERPOL SLTD y nacionales sobre documentos robados / perdidos.
	+ Integrar INTERPOL FIND dentro de los sistemas nacionales existentes de policía y fronteras para los controles sistemáticos contra la base de datos nacional, regional e INTERPOL SLTD.
* Controlar sistemáticamente a cada pasajero, utilizando sistemas, así como el conocimiento y la experiencia de oficiales capacitados.
* Se recomienda el uso de SLTD, tanto por su efectividad como sistema así como por el efecto disuasivo para detectar los pasaportes perdidos y robados.
* También es importante generar conciencia entre las personas sobre la necesidad de proteger sus documentos de viaje y su responsabilidad de informar tanto los documentos de viaje perdidos, robados, así como los documentos encontrados.
* Los pasaportes electrónicos pueden ser una herramienta muy eficaz y están relacionados con el futuro de los pasaportes, pero su eficacia está vinculada al uso pleno de los sistemas PKD.
* Los países miembros de la CRM reconocieron que la gestión robusta de la identidad es la clave para producir un documento de viaje seguro.