COMPENDIO DE PRÁCTICAS RECOMENDADAS DE LAS NACIONES UNIDAS

NACIONES UNIDAS
OFICINA DE LUCHA CONTRA EL TERRORISMO
Centro de la ONU contra el Terrorismo

DIRECCIÓN EJECUTIVA
DEL COMITÉ CONTRA EL TERRORISMO (DECT)
DEL CONSEJO DE SEGURIDAD DE LAS NACIONES UNIDAS

BIOMETRICS INSTITUTE

COMPENDIO DE PRÁCTICAS RECOMENDADAS DE LAS NACIONES UNIDAS

Compilado por DECT y UNOCT en 2018

COMPENDIO DE PRÁCTICAS RECOMENDADAS DE LAS NACIONES UNIDAS

Para el uso responsable y el uso compartido de la biometría en la lucha contra el terrorismo

En asociación con Biometrics Institute

Índice

Resumen ejecutivo

Este compendio brinda una visión general de alto nivel en materia de tecnología biométrica y sistemas operativos en el contexto de la lucha contra el terrorismo. Está dirigido principalmente a los Estados Miembros que tienen poca o ninguna experiencia en aplicaciones biométricas y son susceptibles de enfrentar desafíos de asistencia técnica y desarrollo de capacidades al implementar esta tecnología.

Al final de cada sección se incluyen referencias integrales, de lectura adicional, junto con un resumen de las prácticas recomendadas. A lo largo del compendio se presentan casos de estudio a fin de brindar ejemplos de buenas prácticas y tecnologías emergentes.

La primera sección presenta los elementos principales de la tecnología biométrica y gestión de la identidad, incluyendo el uso extensivo de la biometría en los campos de las ciencias forenses e investigaciones policiales y la complejidad adicional que esto presenta.

La siguiente sección aborda la gestión y los requisitos normativos de la tecnología biométrica desde el punto de vista del derecho internacional, los derechos humanos, las revisiones éticas, los requisitos de protección de la información y el derecho a la privacidad. Luego se presenta una amplia mirada de las potenciales vulnerabilidades de los sistemas biométricos y algunas de las medidas de control que pueden emplearse para mitigar los riesgos. Después se consideran los estándares operativos técnicos y científicos internacionales que cubren la certificación y acreditación de las aplicaciones biométricas así como los sistemas de gestión de la calidad que se emplean en los procesos de ciencias forenses asociados. La última parte de esta sección aborda los requisitos de contratación, mantenimiento y abastecimiento de un sistema o red biométrica de lucha contra el terrorismo y, en particular, las decisiones operativas y financieras clave que deben tomarse al evaluar un posible nuevo sistema o una ampliación.

La sección final brinda una visión general sobre los sistemas y bases de datos biométricos de lucha contra el terrorismo en todo el rango de aplicaciones de cumplimiento normativo, control de fronteras y militares. También considera los beneficios del uso compartido de los datos biométricos a nivel bilateral, multilateral, regional y global y la forma en que los datos biométricos, al utilizarse con otra información de inteligencia, pueden emplearse en forma proactiva para prevenir los actos de terrorismo además de ejercer su función tradicional de herramienta de investigación. Las acciones adoptadas por las autoridades, como resultado de las coincidencias biométricas, se consideran luego en el contexto de los derechos humanos internacionales y de la necesidad de una respuesta proporcionada, legal y plenamente informada. La última parte de la sección aborda la inclusión de la biometría en las estrategias de lucha contra el terrorismo de los Estados Miembros y de las Regiones y el papel esencial de los organismos fronterizos y de cumplimiento normativo en el respaldo activo de estas estrategias.

El compendio es un documento en constante evolución y sus versiones se controlan a fin de:

- de mantenerse actualizadas y responder al rápido avance de la innovación tecnológica y del desarrollo científico en el campo de la biometría y
- adaptarse y ser relevante frente a las amenazas del terrorismo internacionales emergentes y en continua evolución.

Prefacio

La resolución 2322 (2016) del Consejo de Seguridad, al propiciar la cooperación internacional en materia judicial y de cumplimiento de la ley en lo que respecta a los delitos relacionados con el terrorismo, exhorta explícitamente a los Estados Miembros a intercambiar información, incluyendo información biométrica y biográfica, sobre los combatientes terroristas extranjeros y otros terroristas individuales y organizaciones terroristas. En su resolución 2396 (2017), el Consejo decide que los Estados Miembros elaborarán y aplicarán sistemas de recogida de datos biométricos, de conformidad con la legislación local y los derechos humanos internacionales, que podrían incluir la toma de huellas dactilares, la fotografía, el reconocimiento facial y otras formas de recopilación de datos biométricos pertinentes que permitan identificar a las personas, a fin de verificar debidamente y de forma responsable la identidad de los terroristas, incluidos los combatientes terroristas extranjeros. La resolución también alienta a los Estados a que compartan estos datos de forma responsable con otros Estados, así como con la Organización Internacional de Policía Criminal (INTERPOL) y otros organismos internacionales competentes.

El intercambio eficaz de datos biométricos es vital para la investigación de delitos transfronterizos y para la identificación de terroristas. En el contexto de una investigación relacionada con el terrorismo, la biometría y otras técnicas forenses pueden resultar de mucha ayuda para los investigados y fiscales al vincular a una persona con una actividad, evento, lugar o material específico, o a otra persona, entre otras cosas. Por lo tanto, resulta crucial fortalecer la capacidad de los Estados Miembros en esta área.

Este compendio de buenas prácticas y recomendaciones fue desarrollado por el Grupo de Trabajo sobre Gestión de Fronteras y Cumplimiento de la Ley en relación con la Lucha contra el Terrorismo del Equipo Especial de Coordinación Global de la Lucha contra el Terrorismo (CTITF), con el apoyo financiero del Centro de las Naciones Unidas contra el Terrorismo (UNCCT), dentro de la Oficina de Lucha contra el Terrorismo de las Naciones Unidas (UNOCT). El compendio aborda temas fundamentales tales como gobierno, reglamentación, protección de datos, política de privacidad y derechos humanos, así como la gestión de riesgos y las evaluaciones de vulnerabilidad.

Los gobiernos deben abordar las implicancias en materia de derechos humanos que tiene esta tecnología a fin de proteger contra abusos a aquellas personas identificadas por dichos sistemas y garantizar que las acciones tomadas en la etapa de planificación y con posterioridad a la misma se implementen de conformidad con las obligaciones del derecho internacional, tal como se consagran en los instrumentos de derechos humanos internacionales y regionales. Al igual que todas las medidas de seguridad, la biometría presenta vulnerabilidades. Lo que resulta fundamental, es la forma en que se identifican, entienden y minimizan las vulnerabilidades del sistema. Un cuidadoso diseño, un registro preciso de los datos biométricos y la forma en que se configuran los parámetros de compatibilidad son esenciales para su éxito. Existe una cantidad de tecnologías, tanto de software como de hardware, que pueden utilizarse para detectar, combatir y reducir el riesgo de ataques de suplantación de identidad[1].

El Compendio se desarrolló en asociación con el Biometrics Institute, una entidad sin fines de lucro que promueve el uso de la biometría en forma responsable y ética y brinda un foro independiente e imparcial para los usuarios biométricos y otras partes interesadas. El Biometrics Institute trabajó

[1] La 'suplantación' (también denominada ataque de presentación) es la presentación de una biometría falsificada (como una máscara de látex, fotografía, dedo falso o grabación de voz) de un usuario legítimo registrado para obtener acceso no autorizado a un sistema de reconocimiento biométrico.

conjuntamente con la Dirección Ejecutiva del Comité contra el Terrorismo (CTED) para formar un consorcio internacional de expertos con el objeto de dirigir la elaboración del compendio, incluyendo expertos gubernamentales y expertos en biometría con experiencia previa en la lucha contra el terrorismo, cumplimiento de la normativa, control de fronteras, tecnología biométrica, privacidad y protección de los datos.

El Compendio se elaboró dentro del marco de un proyecto a largo plazo tendiente a fortalecer la capacidad de los Estados y de las correspondientes entidades internacionales y regionales para recoger, registrar y compartir información biométrica sobre terroristas, incluyendo combatientes terroristas extranjeros, de conformidad con las resoluciones del Consejo de Seguridad mencionadas más arriba. La implementación de este proyecto de biometría está a cargo de CTED, junto con las entidades del CTITF tales como INTERPOL, la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), la Organización de Aviación Civil Internacional (OACI) y el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR). Los objetivos del proyecto son crear consciencia de las iniciativas regionales e internacionales para promover el uso de la biometría; fortalecer la cooperación y coordinación entre las entidades pertinentes; mejorar el uso y compartir la biometría a nivel global, incluso a través de la promoción de la inclusión sistemática de la información biométrica vinculada a perfiles terroristas en las bases de datos y Notificaciones de INTERPOL; y aumentar la efectividad de la asistencia provista a los Estados Miembros en este área.

Vladimir Voronkov
Secretario General Adjunto
Director Ejecutivo
Oficina de las Naciones Unidas contra el Terrorismo
Centro de las Naciones Unidas contra el Terrorismo

Michèle Coninsx
Subsecretaria General Adjunta
Directora Ejecutiva
Dirección Ejecutiva del Comité contra el Terrorismo

Acerca del Biometrics Institute

Como entidad sin fines de lucro que promueve el uso responsable y ético de la biometría, el Biometrics Institute celebra la oportunidad de apoyar este proyecto. El Biometrics Institute ofrece un foro internacional independiente e imparcial para los usuarios de datos biométricos y otras partes interesadas. Su función es educar e informar a sus miembros, principales interesados y al público acerca de la biometría; respaldar el desarrollo y la concientización respecto de las normas, políticas y mejoras prácticas, y promover la seguridad e integridad de los sistemas y programas biométricos.

El Biometrics Institute se fundó en 2001 y tiene oficinas en Londres y Sídney. Su base de miembros de más de 230 organizaciones de 30 países diferentes cubre una amplia gama de usuarios tales como organismos gubernamentales, fronteras, autoridades de cumplimiento de la ley, bancos y aerolíneas, así como investigadores, proveedores y expertos en privacidad. El Instituto no promueve las tecnologías biométricas sino que enfatiza el uso responsable de los sistemas biométricos, su seguridad e integridad y, sobre todo, la privacidad y protección de los datos. El Instituto reconoce que los sistemas biométricos tienen vulnerabilidades inherentes que deben ser identificadas y mitigadas.

Biometría, privacidad y derechos humanos

La biometría es cada vez más ubicua y, al mismo tiempo, el público ha desarrollado una mayor aceptación de la tecnología, a través del uso de la biometría en los teléfonos móviles, sin ser necesariamente consciente de las implicancias. Esto resalta la necesidad de contar con más educación respecto de los beneficios y riesgos de las aplicaciones biométricas. La biometría es conveniente y puede brindar un mayor nivel de seguridad. Sin embargo, aun presenta desafíos tales como la protección del derecho a la privacidad, la protección de la información y la anti-suplantación. Los datos personales, tales como los datos biométricos, sólo deberían recopilarse y almacenarse cuando sea necesario y proporcionado hacerlo.

La biometría tiene una función cada vez más importante en la lucha contra el terrorismo a nivel mundial, es decir, para combatir el fraude, el robo de identidad y otros delitos penales que los terroristas usan para respaldar sus operaciones. Sin embargo, a fin de desarrollar plenamente el potencial de la biometría, los gobiernos también deben abordar la protección de aquellas personas identificadas mediante dichos sistemas y garantizar que la recopilación, almacenamiento y uso de los datos biométricos se efectúe de conformidad con las leyes en materia de derechos humanos y privacidad, incluyendo el Pacto Internacional de Derechos Civiles y Políticos (ICCPR) y la Declaración Universal de Derechos Humanos de las Naciones Humanas (DUDH).

Se debe proteger a aquellas personas que son víctimas del robo de sus datos biométricos/identidad, o que simplemente se ven involucradas en un error de sistema. Restaurar la identidad de una persona no es tan simple como restablecer una contraseña. Sus datos biométricos lo acompañarán durante toda su vida y por lo tanto se deben tratar con sumo cuidado. Este compendio estipula las cuestiones y posibles soluciones para la difícil tarea de unir estrategias eficaces de lucha contra el terrorismo con el derecho a la privacidad y otros derechos humanos.

Vulnerabilidades y ataques a los sistemas biométricos

Al igual que todas las medidas de seguridad, la biometría tiene vulnerabilidades. Lo fundamental es cómo se minimizan las vulnerabilidades del sistema. Un cuidadoso diseño, un registro preciso de los datos biométricos y la forma en que se configuran los parámetros de compatibilidad son esenciales para su éxito. Si los parámetros se configuran a un nivel muy alto, pueden producirse 'falsos

negativos', denegando el acceso al usuario genuino. Aquellos que no se configuran a un nivel tan alto, pueden producir 'falsos positivos', permitiendo el acceso a usuarios fraudulentos.

El Biometrics Institute empleó un cuidado razonable para garantizar la exactitud del material presentado en este compendio. Debido al contenido y al ingreso de variables durante el proceso de implementación de la tecnología biométrica y con posterioridad al mismo, no se puede considerar responsable al Instituto por los resultados o el cumplimiento. El compendio ha sido preparado únicamente a fines informativos y no pretende brindar asesoramiento en materia legal o de cumplimiento.

Andrew Rice
Presidente y Director
Biometrics Institute

Isabelle Moeller
Gerente Ejecutivo
Biometrics Institute

1. Introducción a los sistemas biométricos e identidad

La Sección 1 presenta los principales elementos de la tecnología biométrica y de la gestión de la identidad, incluyendo el uso extensivo de la biometría en el campo de las ciencias forenses y las investigaciones de cumplimiento de las normas y la complejidad adicional que esto presenta.

Los seres humanos son animales sociales con una capacidad excepcional para reconocer, y por lo tanto distinguir, la gente que les es familiar. Al mismo tiempo los seres humanos tienen un fuerte sentido de identidad, y de su singularidad como personas. Nuestros instintos sociales hacen que nos consideremos a nosotros mismos como personas únicas y que reconozcamos la individualidad de los demás. A nivel biológico, los seres humanos son (a todos los fines prácticos) únicos. Sin embargo, nuestro "motor de reconocimiento humano" no opera biológicamente y de hecho los seres humanos tienen un pobre desempeño para distinguir a la gente que no les es familiar. Los sistemas de identidad empleados por los seres humanos tampoco operan a través del uso de la biología. En cambio, utilizan combinaciones de atributos de identidad y atributos contextuales como marcadores que son representativos de la entidad biológica que describen, pero no son distintivos[2].

Los atributos de identidad incluyen nombres, fecha y lugar de nacimiento, nacionalidad, género e identificadores biométricos[3]. Los atributos contextuales son información transaccional, comúnmente relacionada con lugar y fecha. El uso de los atributos contextuales mejora la garantía de identidad. Los atributos de identidad pueden ser biográficos o biométricos y pueden, bajo ciertas circunstancias, estar sujetos a cambios. Por ejemplo, la mutabilidad de los atributos de identidad biográfica puede incluir:

- Nombres: están sujetos a transliteración, es decir puede haber múltiples formas de escribir el mismo nombre
- Fecha de nacimiento: sujeto a inscripción tardía o inconsistencias en los registros oficiales
- Lugar de nacimiento: puede estar representado de múltiples maneras
- Género: sujeto a la preferencia de la persona, las reasignaciones físicas, etc.
- Ciudadanía: puede ser múltiple y estar sujeta a cambios

Durante el ciclo de vida de la persona los atributos de identidad biométrica pueden estar sujetos a cambio, tal como su tamaño relativo o la claridad y definición de las características extraíbles, a través del proceso de crecimiento y envejecimiento o enfermedad. Algunas personas pueden tener datos biométricos dañados o faltantes. Así, por ejemplo, las huellas dactilares se forman al inicio de la gestación y se mantienen inalteradas durante toda la vida, a menos que se dañen, y pueden conservarse durante un tiempo considerable luego de la muerte, particularmente en ambientes cálidos y secos que causan la disecación de la piel. Si bien la disposición de los surcos de la estructura de la huella dactilar se mantiene constante, el mismo dedo está sujeto a cambios de tamaño a lo largo de la vida y la calidad de las características incluidas en la huella dactilar puede deteriorarse por el abuso ambiental, otros daños y el envejecimiento. Otros datos biométricos pueden estar sujetos a cambios similares. En consecuencia, los algoritmos modernos empleados en las aplicaciones biométricas se diseñan para realizar los ajustes razonables en caso de estos cambios a fin de que se pueda inscribir y mantener la mayor cantidad de gente en un sistema sin importar las variaciones o la edad o el deterioro menor de sus características biométricas.

[2] *Verificación de la identidad: importancia del contexto y continuidad de la identidad*, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

[3] En 1995, el Consorcio de Biometría del Gobierno de los Estados Unidos definió la "biometría" como "…el reconocimiento automático de las personas en base a sus características de comportamiento y biológicas".

Los marcadores biométricos son atributos de identidad y dado que son altamente representativos del ser humano que describen brindan una base sólida para realizar comparaciones digitales. Sin embargo, al igual que los atributos de identidad biográfica, la muestra biométrica, una vez capturada como imagen o convertida en una plantilla o perfil, es diferente de la entidad biológica que describe. La captura y registro de los atributos de identidad, incluyendo los atributos biométricos, es un proceso que siempre es incompleto e imperfecto y por lo tanto puede estar sujeto a error. La coincidencia probabilística inherente a las comparaciones biométricas está sujeta a la variación estadística. La presencia de errores y variaciones estadísticas en los sistemas de reconocimiento humano pueden tornarlos potencialmente vulnerables a una variedad de ataques (Véase la Sección 2.3) a menos que se implementen y actualicen constantemente salvaguardas sólidas como parte de un proceso del Sistema de Gestión de Riesgos.[4] La mitigación de estas vulnerabilidades inherentes de los sistemas de reconocimiento humano es un tema clave en este Compendio.

Los sistemas biométricos están diseñados para reconocer a las personas mediante el uso de sus características biológicas y fisiológicas tales como huellas dactilares, patrones de venas de las manos, iris, rostro, ADN y otros.[5] Cada uno de ellos representa una modalidad biométrica. La elección de la mejor modalidad o modalidades biométricas depende del contexto del caso de uso de la aplicación (Véase la Sección 2.5). En general, las modalidades biométricas comparten características que las hacen, en menor o en mayor grado[6]:

- Universales: pueden encontrarse en todas las personas (excepto en aquellas con características biométricas dañadas o faltantes)
- Únicas: deberían ser capaces de distinguirse entre las personas de la población registrada. Esto puede ser variable respecto de ciertas modalidades, por ejemplo los gemelos compartirán el mismo perfil de ADN pero sus huellas dactilares serán diferentes.
- Permanentes: deberían ser estables y no variar con el tiempo, respecto del algoritmo de coincidencia, teniendo en cuenta las variaciones causadas por el ciclo de vida de la persona
- Mensurables: el sistema debería poder obtenerlas y digitalizarlas fácilmente
- Funcionar eficazmente: deberían ser precisas, veloces y sólidas en los procesos de negocios primarios y de referencia
- Aceptables: deberían satisfacer las normas sociales y las expectativas y ser capaces de ser utilizadas por un gran porcentaje de la población registrada pretendida
- Vulnerables al riesgo de elusión: los impostores pueden potencialmente obtener acceso no autorizado mediante el uso de varios dispositivos y reemplazos a menos que se utilicen rigurosas medidas y se actualicen continuamente

Dado que muchos sistemas biométricos incluyen comparaciones con datos de referencia, un factor clave para elegir la modalidad preferida es la disponibilidad de datos heredados que sean, o puedan

[4] "Los sistemas de reconocimiento humano son inherentemente probabilísticos, y por lo tanto inherentemente falibles. Se puede minimizar la posibilidad de error pero no se puede eliminar. Los diseñadores y operadores de sistemas deberían anticiparse y planificar la aparición de errores, aun cuando los errores resulten infrecuentes". Página 1, *Reconocimiento Biométrico: desafíos y oportunidades, Consejo Nacional de Investigación, Washington (2010), disponible para descarga en:* http://www.nap.edu/openbook.php?record_id=12720&page=1

[5] **Nota:** Este Compendio aborda principalmente aquellos datos de biometría física vinculada a la identidad humana (rostro, huellas dactilares, AND, etc.) y no al comportamiento. Los datos biométricos del comportamiento incluyen modalidades tales como el andar, la escritura en el teclado y las características de uso del 'mouse', las firmas escritas, etc. que miden los patrones de actividad humana.

[6] Listado adaptado de Jain y otros "Biometría: Identificación personal en la sociedad en red", Norwell, Mass.: Kluwer Academic Publisher (1999)

ser, compilados en una base de datos de referencia utilizable y útil para establecer y verificar la identidad. Los sistemas pueden emplear sólo una modalidad (Funcionalidad Monomodal), por ejemplo el reconocimiento facial, o combinar modalidades (Funcionalidad Multi-Modal) tales como huellas dactilares, iris y rostro. Existe una gama de aplicaciones para sistemas biométricos de rápida expansión en los sectores públicos y comerciales que incluyen:

- Registros civiles nacionales para facilitar el acceso a los servicios gubernamentales locales o nacionales
- Licencias de conducir
- Registros de antecedentes penales
- Detección de delitos
- Vigilancia por circuito cerrado de televisión (CCTV)
- Sistemas de seguridad fronteriza/emisión de pasaportes
- Ayuda para refugiados
- Servicios financieros
- Sistemas informáticos
- Acceso seguro a bases de datos
- Acceso a las instalaciones
- Acceso a teléfonos inteligentes
- Gestión de la identidad en servicios de salud
- Control de asistencia en el lugar de trabajo

Las modalidades empleadas en estas aplicaciones pueden identificar a una persona aun cuando presente características falsas o intente hacerse pasar por otra persona. Este es un atributo disponible y puede usarse con gran efectividad para rastrear y encontrar terroristas e interrumpir sus actividades a escala global. Hay una cultura de investigación y desarrollo fuerte y activa en materia de biometría y periódicamente surgen nuevas aplicaciones en el mercado así como también nuevas modalidades.

El modelo operativo estándar de un sistema biométrico básico, como por ejemplo aquél empleado para el control de acceso, comprende las siguientes etapas:

- *Obtención y registro*: consiste en la obtención de una muestra biométrica de una persona (sujeto) mediante el empleo de un dispositivo de captura de datos. El proceso de obtención puede llevarse a cabo mediante el uso de un dispositivo instalado en un lugar fijo y permanente o en un dispositivo móvil que puede cargar los datos desde una ubicación remota. Los datos biométricos pueden obtenerse por contacto con el dispositivo de captura de datos (por ejemplo, las huellas dactilares), por proximidad en el caso de la captura en vivo de imágenes faciales, o remotamente. Sin embargo, el factor de éxito fundamental para cualquier sistema es la calidad de los datos biométricos registrados. Los registros de baja calidad reducirán significativamente el desempeño del sistema, por lo tanto, resulta esencial obtener los datos biométricos bajo un alto estándar a fin de ofrecer una óptima capacidad de coincidencia (Véase la Sección 2.3.3.).
- *Extracción de datos*: consiste en la conversión de la muestra obtenida a una plantilla biométrica, por ejemplo la imagen de una huella dactilar puede transformarse en una matriz digital de números para fines de almacenamiento, búsqueda y comparación. Luego se diseña el proceso de extracción de datos para transformar la imagen cruda o la muestra original en un conjunto de datos digitales utilizables y eficientes que puedan buscarse y compararse en forma precisa con las plantillas de referencia de la base de datos; además esto requiere un

espacio de almacenamiento significativamente menor dentro del sistema en comparación con la imagen/muestra biométrica original.

- *Almacenamiento de datos:* consiste en la retención de los datos registrados en el sistema o base de datos, la que a veces se restringe a sólo una plantilla por persona luego de la finalización de la fase de búsqueda/comparación. Muchos dispositivos de captura de datos cargan la información en un servidor o base de datos central de modo que puedan ser utilizados remotamente sin necesidad de conectarse a otro equipo.
- *Comparación de datos*: consiste en el acceso a la base de datos y en la recuperación de una o más plantillas registradas previamente a fin de su comparación con la plantilla presentada para consulta.
- *Coincidencia de datos:* consiste en el uso de algoritmos de computación para determinar si la plantilla presentada para consulta coincide con la(s) plantilla(s) de la base de datos seleccionada. Las plantillas presentadas para consulta generalmente no son retenidas si han sido comparadas contra una plantilla de referencia de la base de datos.
- *Resultado*: La 'coincidencia' o 'no coincidencia' resultante soportará la función del sistema general, por ejemplo, si el componente biométrico está diseñado para comprobar una declaración de identidad de aquellas personas incluidas en la base de datos que tienen acceso legítimo a un edificio seguro, entonces una 'coincidencia' habilitaría el ingreso, en virtud de la comparación contra la plantilla de la identidad declarada, mientras que una 'no coincidencia' denegaría el acceso.

Sin embargo, no todas las aplicaciones utilizan identidades declaradas ya que existen dos procesos fundamentalmente diferentes que se utilizan en los sistemas biométricos. El primer proceso, que utiliza la identidad declarada, es la:

Verificación (también conocido como comparación uno a uno o 1:1). Este modelo utiliza una identidad declarada para seleccionar sólo una plantilla de la base de datos o documento electrónico para comparación con la plantilla consultada. Es un proceso que compara la plantilla consultada con la plantilla de la base de datos y confirma que las dos plantillas se originan en la misma persona o que no lo hacen.
La verificación pregunta "¿Eres la misma persona que aquella cuya identidad ya ha sido autenticada y registrada en la base de datos?"

El segundo proceso, que es un modelo de búsqueda, es la:

Identificación (también conocido como comparación uno de muchos o 1: n). Esta es una función de búsqueda que no depende de una identidad sugerida y por lo tanto la plantilla de consulta interroga a toda la base de datos para obtener una posible coincidencia. El software de búsqueda y combinación arroja un puntaje de similitud para posibles coincidencias y selecciona en forma automática una coincidencia de alta confianza o presenta una lista de candidatos de coincidencias sugeridas a un operador humano para su comparación con la plantilla de consulta.
La identificación pregunta "¿Estás incluido en la base de datos de referencia y, de ser así, con que registro coincides?"

El valor y el contexto de los resultados de los sistemas de verificación o identificación dependerán del modelo operativo de la aplicación. Por ejemplo, en algunos casos una identificación positiva sería el resultado normal mientras que un resultado negativo sería la excepción (por ejemplo, acceso de personal a un área de seguridad) pero en otros modelos un resultado negativo sería la expectativa normal mientras que un resultado positivo sería la excepción (por ejemplo, una búsqueda de todos

los pasajeros en una lista biométrica de alerta de terroristas). Los sistemas biométricos eficaces integran tareas discretas de verificación e identificación a fin de mejorar el control de la identidad y la confiabilidad de las comparaciones con los conjuntos de datos de referencia.

Muchas aplicaciones biométricas parecen ser completamente automatizadas para el usuario, desde la obtención de los datos hasta el resultado, pero la intervención humana generalmente resulta necesaria en los sistemas más complejos, en varias etapas del proceso, para garantizar que el sistema funcione a la perfección aun cuando esto no resulte evidente para el usuario. Sin embargo, con el crecimiento continuo exponencial del poder de las computadoras y de nuevas tecnologías de procesamiento, el requisito de intervención humana disminuye rápidamente pero mientras puede esperarse que la comparación automatizada de las muestras biométricas se convertirá en la norma, la asociación de las muestras emparejadas con otros atributos de identidad y contextuales probablemente permanecerá, en los casos más complejos, siendo objeto de la decisión humana.

Caso de estudio 1 – Biometría en las fronteras

La autorización de paso de los viajeros en las fronteras mediante la verificación 1:1, informa, y es informada por, evaluaciones de riesgo de viajeros mediante el uso de comparaciones 1:n contra listados de alerta y conjuntos de datos de inteligencia (Véase la Figura 1). Los atributos de identidad registrados en los listados de alertas y conjuntos de datos de inteligencia normalmente están incompletos. Esto se debe a que los objetivos para la inclusión en listados de alerta se identifican a través de un rango de criterios y circunstancias diferentes. No todos los atributos biográficos o biométricos pueden asociarse con cada listado de alerta o listado de inteligencia. Los atributos contextuales son incompletos. Todos los elementos de atributos incluidos en listados de alerta o conjuntos de datos de inteligencia pueden estar sujetos a error.

Figura 1 – adaptada de la *Guía de Gestión de Control de Fronteras de la OACI, Montreal (2018)*
(Con permiso de la OACI)

Comparación	Fuente de los datos de referencia	Base para comparaciones biográficas	Base para comparaciones biométricas	Asociaciones de atributos contextuales
1:1 Verificación	Documentos de viaje	• Nombre • Fecha de nacimiento • Sexo • Nacionalidad	• Facial • Huellas dactilares • Iris	• Hora y lugar • Nacionalidad • Inspección de los documentos de viaje
1:n Identificación	- Listados de alertas - Inteligencia	• Nombre • Fecha de nacimiento • Sexo • Nacionalidad	• Facial • Huellas dactilares • Iris • Voz • ADN	• Hora y lugar • Interpol SLTD • Eventos anteriores • Atributos de asociación (teléfono celular, conexiones al correo electrónico y otros)

Las identidades verificadas contribuyen a una asociación más confiable de atributos biográficos, biométricos y contextuales y por lo tanto a búsquedas más efectivas en los listados de alertas y

bases de datos de inteligencia. En forma crítica, las comparaciones biométricas contribuyen a, pero no determinan exclusivamente, los resultados de comprobación de identidad.[7]

1.1 Desempeño del sistema

El desempeño del sistema biométrico dependerá ampliamente de (1) el alcance y la escala de su uso previsto, (2) la selección de la modalidad o las modalidades más adecuadas para soportar esa aplicación, (3) el procesamiento confiable, consistente y puntual soportado por un requisito de bajo mantenimiento. Las mediciones clave del desempeño de los sistemas biométricos son la precisión, los índices de error[8], la productividad y los volúmenes e índices de gestión de excepciones. En términos generales, la precisión es la medición de la capacidad del sistema para combinar correctamente los atributos de identidad biométricos de la misma persona y, a su vez, evitar la falsa coincidencia de atributos de identidad biométricos de diferentes personas. Los siguientes componentes se utilizan para expresar la precisión de un sistema biométrico, ya sea como un porcentaje o una proporción, y generalmente derivan de pruebas de campo o ensayos de laboratorio.

Tasa de aceptación verdadera (*True Acceptance Rate*, (TAR)) - Representa la medida en que el sistema iguala correctamente los atributos de identidad biométrica de la misma persona.

Tasa de falsa aceptación (*False Acceptance Rate*, (FAR)) – La falsa aceptación se produce cuando el sistema iguala erróneamente la plantilla de consulta biométrica de una persona con la plantilla biométrica de otra persona en la base de datos. La FAR es la cantidad de falsas aceptaciones como una proporción de la cantidad total de consultas biométricas que deberían haberse rechazado, es decir la cantidad de no-coincidencias *generadas y presentadas como coincidencias por el sistema* como una proporción de las no-coincidencias genuinas.

Tasa de rechazo verdadero (*True Rejection Rate*, (TRR)) – La medición de la cantidad de ocasiones en que el atributo de identidad biométrica de una persona *no* se iguala correctamente con los atributos de identidad biométrica de otras personas incluidas en la base de datos, es decir la frecuencia de no-coincidencias correctas.

Tasa de falso rechazo (*False Rejection Rate*, (FRR)) – El falso rechazo se produce cuando la plantilla de consulta biométrica no se iguala con la plantilla de la base de datos correcta aun cuando corresponda a la misma persona. La FRR es la cantidad de falsos rechazos como una proporción de la cantidad total de consultas biométricas que deberían haberse aceptado, es decir la cantidad de coincidencias *generadas y presentadas como no-coincidencias por el sistema* como una proporción de las coincidencias genuinas.

Por lo tanto, es conveniente que al diseñar el sistema se maximicen la TAR y la TRR y se minimicen la FAR y la FRR. En términos simples, por ejemplo, una configuración de exactitud con una TAR de

[7] Para conocer más detalles, remítase a la Guía de Gestión de Control de Fronteras de la OACI, Montreal (2018)

[8] El cálculo de las tasas de error requiere una abstracción, la asunción de un conjunto cerrado, para permitir la posterior realización de una comparación de todo:todo de la base de datos a fin de obtener y calcular las tasas de error. En muchos casos, estos cálculos se realizan mediante simulaciones que utilizan conjuntos de datos estandarizados que pueden ser o no representativos de datos vivos del mundo real. La abstracción de la tasa de error puede ser útil para el diseño del Sistema y para proyectar el desempeño de la verificación 1:1. En el mundo real, con una población mundial de más de 7 mil millones, los reemplazos desde afuera del conjunto son posibles, y en el caso de los listados de alertas y conjuntos de datos inteligentes, se espera que ocurran. Las tasas de error deben usarse con cuidado y aplicarse únicamente a la tarea de verificación. El desempeño de la igualación de los sistemas biométricos en el mundo real puede ser significativamente diferente de aquel pronosticado por las simulaciones de la tasa de error.

70% resultaría en una FAR de 30% mientras que una con una TAR de 97% significaría una FAR de sólo 3%. Cabe aclarar que ningún sistema biométrico opera con una tasa de exactitud del 100%.

Sin embargo, también existe una estrecha relación entre los valores de la FAR y la FRR y el equilibrio deseado entre estas dos tasas de error depende ampliamente del uso comercial del sistema biométrico particular. Por ejemplo, si el acceso de un empleado a las instalaciones de una compañía está vinculado a una aplicación biométrica entonces una alta FRR impediría al personal de la compañía ingresar en forma regular pero a su vez si la FAR fuera demasiado alta entonces el personal no autorizado podría entrar en forma rutinaria. En consecuencia, la aplicación exige un valor Límite ajustable que equilibre la FRR con la FAR a fin de permitir al personal un acceso sin trabas y a su vez impedir el ingreso no autorizado en la *mayoría* de los casos. Si fueran necesarios niveles de seguridad más altos, entonces el límite debería ser realineado a fin de detener el acceso no autorizado disminuyendo la FAR tanto como sea posible, aún a costa de aumentar la FRR, y así afectar el acceso del personal legítimo. Este valor límite es, por lo tanto, generalmente una compensación pragmática entre la FRR y la FAR que optimiza la efectividad del sistema de la aplicación pretendida y sopesa la necesidad de seguridad contra la conveniencia del cliente, la velocidad de procesamiento y los costos generales del sistema. La Tasa de Error Igual (*Equal Error Rate*, (EER))[9] hace referencia a la configuración del límite de algunas modalidades en las que la FRR y la FAR son iguales, es decir la proporción de falsas aceptaciones es igual a la proporción de falsos rechazos.

Existen otros factores que afectan la exactitud tales como la Tasa de Falla de Obtención (*Failure to Acquire Rate*, (FTA)), que, en términos generales, es la proporción de todas las transacciones registradas que no pueden completarse debido a fallas en la presentación (por ejemplo, falta de captura de la imagen), en la extracción de características o en las etapas de control de calidad. Así como la falla del sistema, también incluye casos en los que la persona tiene datos biométricos dañados, lastimados o faltantes. La FTA es una medición importante para determinar la capacidad de operación en vivo de un sistema. Una alta FTA requiere un enfoque alternativo a fin de capturar los datos biométricos de aquellas personas que no pueden registrarse por cualquier motivo. Esto podría incluir el uso de un dato biométrico alternativo similar, como por ejemplo el dedo pulgar izquierdo en lugar del dedo pulgar derecho o incluso agregar una segunda capacidad de reconocimiento biométrico diferente que necesitaría el desarrollo de un sistema multimodal. Si estas alternativas no fueran posibles, entonces podría adoptarse una solución no biométrica, conocida como Gestión de Excepciones. Por ejemplo, este proceso podría requerir que la identidad de aquellas personas que no pueden registrarse biométricamente sea revisada por un operador humano, o la utilización de otros métodos potencialmente menos seguros tales como un código PIN o una firma escrita, todos los cuales pueden reducir la efectividad global del sistema. Las aplicaciones biométricas multimodales generalmente se ven favorecidas por este motivo ya que habitualmente permiten una más alta proporción de registros y a su vez reducen la FTA.

La Tasa de Procesamiento (*Throughput Rate*) determina la cantidad de personas que pueden acceder al sistema dentro de un plazo de tiempo establecido, es decir la capacidad frente a la velocidad. Por ejemplo, un aeropuerto que opera con acceso mediante pasaporte electrónico necesitará calcular los volúmenes reales y pronosticados de pasajeros a fin de instalar la cantidad suficiente de puertas biométricas para facilitar el flujo de pasajeros en forma eficiente durante las horas de mayor demanda. Esto permitiría al sistema biométrico operar dentro de tasas de error predeterminadas, por motivos de seguridad, y a su vez procesar múltiples verificaciones simultáneas en segundos para satisfacer al cliente y a fines de eficiencia comercial.

[9] También denominada Tasa de Error Cruzada (*Crossover Error Rate*)

1.2 El papel de la biometría en las ciencias forenses

En general, la ciencia forense se encarga de la transferencia del material físico o de soportes electrónicos digitales entre personas, objetos y lugares. Este material puede ser visible, tal como la salpicadura de sangre en una pared, invisible, por ejemplo la evidencia de vestigios microscópicos de un disparo o residuos explosivos, o una imagen electrónica como un rostro filmado por una cámara de CCTV. Este material o información puede transferirse antes, durante o después de la comisión de un delito. Alguno de estos materiales también capturan las características *biométricas*, por ejemplo la impresión de una huella dactilar depositada en sudor en un vidrio, una voz grabada durante una conversación telefónica o un perfil de ADN creado con la saliva del borde de una taza. Estos 'datos biométricos forenses'[10] son componentes clave de la ciencia forense y son elementos vitales en las investigaciones de cumplimiento de la ley debido a su potencial capacidad para identificar personas. También son importantísimos para la realización y para el éxito de las operaciones contra el terrorismo ya que:

- Prueban o refutan la participación de una persona en un delito al brindar pruebas incriminatorias o exculpatorias en sí mismas o como parte de otra prueba (Véase el Caso de Estudio 2).
- Ofrecen procesos objetivos y confiables en virtud de la ley que reducen la dependencia en las confesiones sin realizar una investigación penal, particularmente si las mismas se obtienen mediante el uso de torturas u otras acciones coercitivas
- Interpretan la actividad en las escenas del crimen y los hechos asociados
- Vinculan a una persona con una actividad, evento, lugar u otra persona antes, durante o después de un incidente
- Vinculan un evento con otro evento o con múltiples eventos
- Ubican y vinculan datos en diferentes sistemas electrónicos y digitales

Estas prestaciones requieren la colaboración coordinada de otras disciplinas pertinentes de la ciencia forense y de las áreas de especialidad técnica y experiencia en laboratorio. [11] El procesamiento de todo el material criminalístico, en la escena del crimen y en el laboratorio, debería realizarse de conformidad con las normas internacionales y los sistemas de gestión de la calidad vinculados (Véase la Sección 2.4.2.). Las principales disciplinas de la ciencia forense son:

- Evidencia biológica: Ácido Desoxirribonucleico (ADN), fluidos del cuerpo, cabellos, tejidos, etc.
- Marcas: marcas de dedos y palmas, marcas de instrumentos, marcas de calzado, marcas de neumáticos, etc.
- Armas de fuego y balística
- Rastros: pintura, vidrios, fibras, explosivos, etc.
- Prueba digital y electrónica: acceso a dispositivos, descarga de datos, análisis, reconstrucción de daños, etc.
- Drogas: identificación y cuantificación
- Análisis de documentos

[10] Datos biométricos forenses: de dos comunidades a una disciplina. Procedimientos de la Conferencia Internacional del Grupo de Interés Especial sobre Biometría, 6 y 7 de septiembre de 2012; Darmstadt, Alemania.

[11] Muchos de estos se describen en detalle en dos publicaciones disponibles en la Oficina de Naciones Unidas contra la Droga y el Delito (ONUDD): 'Policía: servicios e infraestructura forense' y 'Requisitos de habilidades del personal y recomendaciones de equipos para los laboratorios de ciencias forenses'. (www.unodc.org)

- Análisis de explosivos

El material biométrico forense se utiliza en el trabajo de casos para realizar comparaciones uno a uno (por ejemplo, la comparación de una marca dactilar tomada en la escena del crimen con un conjunto de huellas obtenidas de un sospechoso) y también constituye uno de los tres tipos principales de bases de datos utilizadas por los Científicos Forenses[12]:

1. *Bases de datos de referencia de materiales de trabajo de casos,* por ejemplo, una colección de fibras naturales y artificiales, normalmente obtenida de fabricantes y negocios minoristas, utilizada para identificar, categorizar y comparar con las fibras recogidas en las escenas del crimen
2. *Bases de datos de búsqueda no biométrica,* por ejemplo, armas de fuego y municiones disparadas, huellas de calzado, etc.
3. *Bases de datos de búsqueda biométrica,* colección de materiales y características biológicas humanas, como ADN y huellas dactilares.

Se deben seguir los principios básicos del manejo de la evidencia forense al manipular muestras biométricas dentro del contexto de la ciencia forense y las investigaciones ya que si no los resultados que arroje cualquier sistema de búsqueda biométrica serán inútiles en cualquier proceso judicial posterior. Por lo tanto, los siguientes registros y procedimientos deben emplearse en forma consistente al recuperar cada muestra/artículo de una escena del crimen:

- *Proveniencia*: un registro escrito y fotográfico del lugar de la muestra/artículo
- *Preservación*: la muestra/artículo forense debe recogerse y embalarse de modo tal que la evidencia no se contamine, destruya, altere, pierda o degrade; el embalaje también deberá proteger a la muestra de cualquier daño durante su traslado e impedir que contamine o que se contamine con otros artículos o ambiente; la muestra debería almacenarse a una temperatura adecuada a fin de preservarla y deberá asegurarse que la misma llegue en óptimas condiciones para su análisis en el laboratorio
- *Integridad*: el embalaje deberá ser sólido, intacto y sellarse en forma efectiva a fin de impedir el acceso no autorizado o cualquier interferencia; no debería ser posible agregar o retirar material (incluyendo partículas, gases o líquidos) a través del embalaje
- *Continuidad (cadena de custodia)*: debe llevarse un registro, a partir de la escena del crimen en adelante, de cada persona que toma posesión de la muestra/artículo embalado

Caso de estudio 2 – El Proyecto Inocencia

El Proyecto Inocencia es una organización sin fines de lucro fundada en 1992 por Paul Neufeld y Barry Sheck de la Facultad de Derecho Benjamín N. Cardozo, Nueva York, Estados Unidos. El fin del proyecto era utilizar los perfiles de ADN forenses a fin de exonerar a las personas condenadas erróneamente y reformar el sistema de justicia penal estadounidense para prevenir futuras injusticias. El concepto se basó en el principio de que si la tecnología del ADN podía probar que las personas eran culpables de un delito penal, también podía probar que las personas que habían sido

[12] Las bases de datos de inteligencia forenses en general son administradas y operadas por Científicos Forenses, con base en laboratorios científicos forenses, pero algunas bases de datos biométricos tales como los sistemas de huellas dactilares, ADN, voz y rostro pueden estar a cargo de otro personal perteneciente al entorno del cumplimiento de la ley.

condenadas erróneamente eran inocentes. A la fecha, las pruebas de ADN han dado lugar a 356 exoneraciones y a la identificación de 153 autores potenciales alternativos.

1.2.1 Bases de datos biométricos forenses: categorías de datos

Las bases de datos biométricos forenses, también denominadas Bases de Datos de Inteligencia Forense, son utilizadas habitualmente por los laboratorios de ciencias forenses y las agencias de cumplimiento de la ley. Estas bases de datos han tenido un impacto significativo en las investigaciones penales y, particularmente, en los casos de terrorismo, en muchos países, por más de 100 años. Las modalidades usadas comúnmente son huellas dactilares, ADN, rostro y voz. Cada base de datos comprende dos conjuntos de datos distintos:

Datos de referencia: recogidos bajo condiciones controladas, de aquellas personas arrestadas por un delito o sospechadas de haberlo cometido, por ejemplo, las huellas dactilares de los 10 dedos de la mano tomadas en forma electrónica mediante un escáner o mediante el método tradicional de la tinta y el papel; hisopados bucales extraídos de la cara interna de la mejilla de la persona arrestada o una muestra de cabello o sangre que se procesan para crear un perfil de ADN completo[13]; fotografías digitales del rostro, etc. Los datos de referencia también pueden obtenerse de los oficiales de policía y de aquellas personas que tienen acceso legítimo a las escenas del crimen, antes, durante o después de un delito, a fin de identificar cualquier material forense depositado por ellos y eliminarlo de la investigación.

Datos de la escena del crimen: generados a partir de las muestras y artículos recogidos en las escenas del crimen.[14] La calidad de los datos biométricos de la escena del crimen puede ser altamente variable. El material forense recuperado puede estar dañado, contaminado o carecer de contenido o detalle suficiente por varias razones. Esto arroja un rango de resultados amplio y gradual del proceso de búsqueda y comparación en lugar del habitual resultado binario de 'coincidencia' o 'no-coincidencia' derivado de otros sistemas biométricos 'no forenses' tales como las aplicaciones de control de acceso.

Algunos países también usan grandes sistemas biométricos para llevar a cabo el registro civil de sus ciudadanos, por ejemplo los programas de documentos de identidad. Esto brinda a cada ciudadano una identidad formal y le permite acceder a los servicios gubernamentales y otras prestaciones sociales y comerciales tales como bienestar, vivienda, seguro, servicios bancarios, etc.

Sistemas de registro civil: Las modalidades utilizadas por estos sistemas normalmente son huellas dactilares, rostro o iris o una combinación multi-modal. Estas bases de datos pueden contener millones, decenas o cientos de millones de plantillas biométricas (datos de referencia), dependiendo del tamaño de la población nacional, y están diseñadas principalmente para buscar datos de referencia. Por lo tanto, si el sistema nacional legal y regulatorio permite a las agencias de cumplimiento de la ley realizar búsquedas en estas bases de datos, a los fines de la investigación de un delito, las búsquedas normalmente estarían limitadas únicamente a datos de referencia. Sería

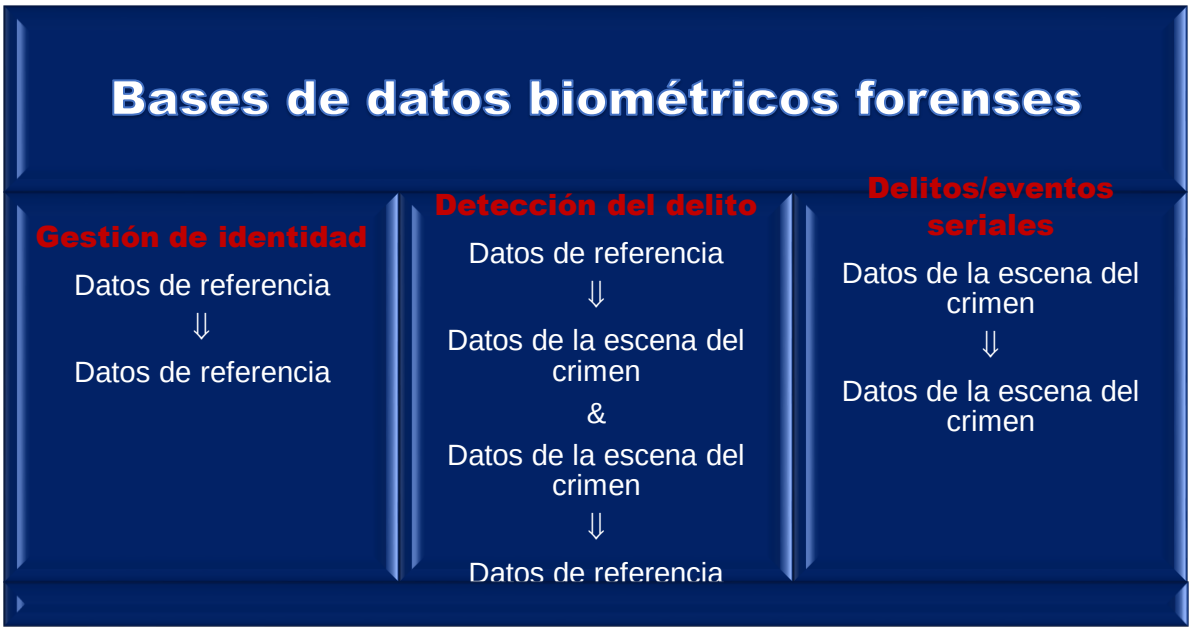
[13] La moderna tecnología del ADN permite realizar un rápido perfil de ADN con los hisopados bucales extraídos de las personas mediante dispositivos totalmente automáticos ya sea en el laboratorio o en las estaciones de policía/ puestos de frontera en poco más de una hora. Esto significa que se pueden realizar búsquedas en las bases de datos de ADN a fin de establecer coincidencias de ADN con las muestras tomadas en la escena del crimen mientras la persona está detenida o bajo custodia.

[14] El término 'escena del crimen' se utiliza aquí en su más amplio contexto, incluyendo lugares físicos, sospechosos, víctimas, testigos y entornos digitales y electrónicos.

posible buscar un conjunto de huellas dactilares o la imagen de un rostro tomada a una persona a fin de determinar si están registradas en el sistema pero la búsqueda de marcas dactilares o de una imagen facial de una escena del crimen probablemente no producirá una coincidencia. Esto se debe a que los algoritmos de coincidencia de un sistema de registro civil normalmente no están diseñados para tratar a los datos de la escena del crimen de la misma manera en que puede hacerlo un sistema de búsqueda forense de un Laboratorio de Ciencias Forenses. Es por este motivo que raramente se emplean las bases de datos biométricos civiles en las investigaciones penales y aun cuando se realice una búsqueda en casos de delitos graves o terrorismo, la tasa de éxito normalmente es extremadamente baja. Sin embargo, las nuevas tecnologías y las fuentes de datos para algunas de estas modalidades, como el rostro, podrán permitir búsquedas más precisas en el futuro. También existe la opción de integrar o adjuntar un software de coincidencia forense a estos sistemas de registro civiles.

1.2.2 Bases de datos biométricos forenses: categorías de búsqueda

Figura 2 – Bases de datos biométricos forenses – Combinaciones de búsqueda



Existen cuatro combinaciones de búsqueda forense básicas empleadas para respaldar el cumplimiento de la ley y las investigaciones penales y estas se realizan a través de las siguientes tres configuraciones de búsqueda (Véase Figura 2):

Búsqueda de gestión de identidad *Combinación 1* – Datos de referencia con datos de referencia

Este tipo de búsqueda determina si un sujeto ya se encuentra registrado en una base de datos mediante la comparación de sus datos de referencia contra todos los datos de referencia archivados en la base de datos. Esta técnica se usa más frecuentemente para establecer si una persona es conocida por la policía y tiene una condena previa y antecedentes penales, particularmente, si ha presentado características falsas. Históricamente, las huellas dactilares se utilizaron a este fin. Se

toma el conjunto de las diez huellas dactilares rodadas[15] ('diez impresiones') de una persona arrestada y se realiza una búsqueda contra la base de datos de las diez impresiones de los delincuentes conocidos. Esto es extremadamente exacto (es decir tiene una TAR muy alta – Véase la Sección 1.1) cuando se realiza con un moderno y eficiente Sistema Automatizado de Identificación de Huellas Dactilares (AFIS) con una base de datos que contiene imágenes de huellas dactilares de alta calidad, es decir se ha asegurado la calidad de toda las huellas dactilares las cuales han sido tomadas bajo condiciones supervisadas por operadores capacitados. Esas búsquedas normalmente se realizan en forma 'autónoma' es decir con muy poca o ninguna intervención humana a menos que se requiera la verificación de una coincidencia. Esto significa que estas búsquedas son extremadamente rápidas de procesar. Los dispositivos móviles modernos de captura de datos permiten a los funcionarios encargados del cumplimiento de la ley tomar las huellas de los dedos o palmas de personas situadas en ubicaciones remotas y en cruces de fronteras y enviar los datos a un servidor central para una búsqueda inmediata. El resultado normalmente se obtiene en segundos o minutos. Algunos dispositivos móviles tienen una base de datos incorporada de modo tal que todas las funciones de búsqueda pueden realizarse a nivel local sin necesidad de transmitir la información a un servidor remoto.

Por supuesto, también es posible realizar una búsqueda de gestión de identidad mediante el uso de otras modalidades biométricas tales como el ADN, rostro, iris, etc. Las búsquedas de gestión de identidad también pueden utilizarse para identificar a personas fallecidas o a personas que sufren de amnesia. El requisito clave, que sustenta todas las búsquedas biométricas, es obtener datos de referencia de alta calidad de un estándar consistente de modo tal que todas las configuraciones de búsqueda operen a su máximo potencial. El material de referencia de baja calidad compromete la eficacia y exactitud de todas las combinaciones de búsqueda.[16]

Una búsqueda de gestión de identidad formula la pregunta "¿Te hemos encontrado antes y quién eres tú?"

Búsqueda de detección de delitos: *Combinación 2* – Datos de referencia con datos de la escena del crimen y *Combinación 3* – Datos de la escena del crimen con datos de referencia

Este protocolo de búsqueda exige una interfaz de doble sentido entre la base de datos de referencia y la base de datos de la escena del crimen que contiene material biométrico forense recogido en las escenas del crimen, por ejemplo las manchas de ADN en la escena del crimen (Muestras Cuestionadas), marcas de dedos y palmas, imágenes faciales, etc. Los datos de referencia recientemente registrados, si aún no se encontraban en la base de datos de referencia, se buscan en

[15] Se debe rolar la punta de cada dígito por la placa del escáner o formulario de huella dactilar desde un borde de la uña hasta el otro borde de la uña a fin de registrar el máximo flujo de crestas y detalles característicos. Las otras impresiones de los dígitos se llaman impresiones 'planas'. Estas se toman en forma simultánea (los dos pulgares juntos y los cuatro dedos de cada mano) presionando el dedo directamente en la placa/formulario. Las impresiones planas se toman como una medida de garantía de calidad para asegurar que las impresiones roladas se hayan registrado en la secuencia correcta.

[16] Es por este motivo que todas las personas arrestadas por delitos relacionados con el terrorismo en el Reino Unido tienen como mínimo tres juegos de impresiones de sus dedos y palmas y este proceso es supervisado por un perito especialista en huellas dactilares. Cada juego incluye el detalle de todas las áreas de las crestas de fricción presentes en la mano, es decir las impresiones estándar roladas y planas, los puntas de los dedos, las impresiones roladas de todas las falanges, toda la superficie de la palma y el canto de la mano en posición cubital, así como también las impresiones plantares (las plantas del pie y los dedos). Este proceso meticuloso produce el mejor conjunto de huellas dactilares de referencia disponibles a los fines de búsqueda y archivo AFIS así como el mayor conjunto de datos de detalles de crestas de fricción disponibles para comparaciones 1:1 con las marcas de dedos/palmas/plantares de la escena del crimen particularmente aquellas realizadas con las puntas o lados de los dedos o cualquier área de la palma.

la base de datos de la escena del crimen y a la inversa, los datos de la escena del crimen recientemente registrados se buscan en la base de datos de referencia. La exactitud de estos tipos de búsqueda puede ser considerablemente menor que la de una búsqueda de gestión de identidad debido a la calidad variable de los datos de la escena del crimen.

Una búsqueda de detección del delito realiza las preguntas "¿Cometiste un delito?" "¿Tienes alguna vinculación con este objeto/lugar?" y "¿Había alguien más contigo?"

Búsqueda de delitos/eventos seriales: *Combinación 4* – Datos de la escena del crimen con datos de la escena del crimen

Este tipo de búsquedas es capaz de vincular escenas del crimen de distintos delitos o aquellas que podrían ocurrir en una única investigación importante mediante la identificación e interconexión de materiales de la escena del crimen de diferentes lugares y brindando una ventaja de inteligencia a los oficiales a cargo de la investigación de esos casos. La identidad de la persona que deposita el material de la escena del crimen se desconoce pero la determinación de que la misma persona ha dejado material biométrico en dos o más delitos o incidentes resulta una ayuda invaluable para los investigados y analistas de inteligencia. El éxito y la exactitud de este tipo de búsqueda dependen en gran medida de la calidad de los datos de la escena del crimen y de la recolección de material compatible en las escenas del crimen. Algunas modalidades resultan mejores que otras para este tipo de búsquedas, por ejemplo el ADN es particularmente eficaz para vincular delitos/eventos en diferentes tipos de investigación tales como terrorismo, homicidio y delitos sexuales.

Una búsqueda de delitos seriales realiza la pregunta "¿Los datos de esta escena del crimen coinciden con aquellos de otros delitos/incidentes?"

Nota: todas las bases de datos descriptas en esta sección tienen diferentes tasas de falsos rechazos dependiendo del tipo y de la calidad de los datos biométricos que contienen. Al igual que todos los sistemas biométricos, una no-coincidencia o resultado negativo (es decir la búsqueda 1:n no dio lugar a una coincidencia) no significa necesariamente que los datos de coincidencia no están en la base de datos si no que puede ser que el sistema no haya logrado encontrarlos por cualquier motivo.

ADN[17] – Categorías de búsqueda adicional

Existen otras técnicas de búsqueda especializadas adicionales que son específicas de las Muestras de ADN Cuestionadas. Los Perfiles de ADN de Referencia se generan en las áreas no codificadas del ADN y se utilizan únicamente a fines de identificación ya que contienen muy poca otra información genética. Las Muestras de ADN Cuestionadas de las escenas del crimen normalmente contienen mucho más material genético y se pueden emplear otras técnicas de extracción y perfilación de ADN para ayudar a los investigadores. Sin embargo, estas técnicas normalmente están sujetas a una estricta supervisión por parte de los responsables del control legal y ético de las ciencias forenses ya que pueden violar las leyes de privacidad y protección de datos sin un sólido marco de gobierno. Algunos ejemplos incluyen:

Evaluación fenotípica: Una técnica que busca rasgos físicos genéticos específicos como por ejemplo cabello rojo o color de ojos en los indicios del crimen. Si bien este proceso actualmente es bastante limitado, los avances de la ciencia en materia del ADN sin duda extenderán el rango de las características fenotípicas en el futuro. Esto permitirá potencialmente a los investigadores obtener

[17] Véase también Revisión y recomendaciones sobre la gestión de la base de datos de ADN, 2017, Grupo de Trabajo sobre ADN de ENSFI, abril de 2017" http://enfsi.eu/wp-content/uploads/2017/09/ADN-databasemanagement-review-and-recommendatations-april-2017.pdf

una 'descripción' más detallada de su sospechoso desconocido a través de los indicios de ADN del crimen.

Búsqueda familiar (parentesco) – El perfil de ADN generado por los indicios del crimen puede no identificarse al realizarse una búsqueda en la base de datos de ADN de referencia. En circunstancias excepcionales, el perfil puede buscarse en la misma base de datos mediante el uso de un software especializado adicional a fin de determinar si el perfil se asemeja al perfil de un familiar sanguíneo cercano que puede estar almacenado en el sistema. Eso puede generar relativamente muy pocas respuestas o miles de respuestas dependiendo de la peculiaridad comparativa de la consulta del perfil de ADN al ser comparado con la totalidad de los perfiles genéticos de la población incluida en la base de datos.

1.2.3 Bases de datos biométricos forenses – Limitaciones y estándares de información

El material forense generalmente se deposita o registra en forma inadvertida durante la preparación o comisión de un delito y puede estar sujeto a un rango de condiciones perjudiciales y restricciones que impiden que se utilicen con la misma eficiencia que los datos de referencia en un sistema de búsqueda biométrica. Algunas de estas condiciones son genéricas pero muchas dependen de la modalidad de la muestra. Algunos de los ejemplos encontrados con frecuencia son:

Rostro – CCTV y otra tecnología de grabación visual externa

- *Compatibilidad del ángulo de la cámara*: las cámaras de CCTV generalmente están ubicadas en una posición elevada mientras que las imágenes habituales del 'prontuario' se toman con la cabeza levantada y a nivel del rostro. Esto dificulta una comparación precisa entre ambos tipos de imagen y, en algunas ocasiones, se torna imposible.
- *Iluminación y exposición:* para producir la mejor imagen los sensores de la cámara dependen de (a) la iluminación general disponible en el ambiente y (b) las configuraciones tales como la velocidad del obturador, diafragma e ISO.
- *Resolución de la cámara*: algunas cámaras tienen baja resolución, es decir sólo registran un número limitado de pixeles y si la cámara se ubica lejos del sujeto la imagen resultante normalmente es granulada y borrosa particularmente si el ambiente tiene poca luz. La imagen resultante contendrá pocos detalles utilizables aun cuando sea agrandada.
- *Compresión:* el componente de registro de datos de la cámara elimina los detalles finos a fin de aumentar la capacidad de almacenamiento de imágenes con una definición más baja
- *Características faciales y cubiertas*: factores como la edad, expresión o características faciales que no son distintivas pueden comprometer la capacidad de identificar rostros al igual que las obstrucciones externas, por ejemplo, anteojos, vello facial, sombreros, cascos, etc. (Véase la Sección 2.3.2.).

Marcas de dedos o palmas (también denominadas impresiones 'latentes'):

- *Suficiencia y área revelada*: sólo una pequeña parte del dedo o la palma entra en contacto con una superficie y por lo tanto sólo se revelan relativamente pocos detalles característicos. Las huellas dactilares de referencia mal tomadas también pueden agravar el problema ya que pueden no revelar la misma área del dedo para su comparación con la marca del dedo.
- *Superposición*: las marcas de dos o más dedos depositadas en el mismo lugar de una superficie que pueden tornar difícil la visualización de una impresión separada de la(s) otra(s).

- *Interferencia*: La interferencia de fondo del sustrato puede oscurecer una parte o la totalidad de la marca del dedo. En general, las marcas de los dedos se encuentran normalmente en la superficie cuando se depositan en un sustrato no poroso o son absorbidas por la superficie en el caso de un sustrato poroso. Por lo tanto, aquellas que están en la superficie pueden estar sujetas a daños o abuso ambiental. La suciedad, los contaminantes u otros artefactos pueden oscurecer o dañar los detalles característicos de la marca.
- *Presión*: el dedo puede estar sujeto a presión vertical o lateral al ponerse en contacto con una superficie lo que puede dar lugar a una marca de dedos distorsionada debido a la elasticidad de la piel.
- *Movimiento*: el dedo puede deslizarse lateralmente durante el contacto con una superficie lo que resulta en una impresión diseminada o en algunos casos en una distorsión o superposición.
- *Limitaciones de la técnica de desarrollo:* la aplicación de polvos de desarrollo de la huella dactilar o de tratamientos químicos podría no revelar la totalidad de la marca en forma clara y puede resultar en una imagen demasiado clara o demasiado oscura con poco contraste.

ADN – material biológico y celular recuperado en las escenas del crimen (también denominado 'indicios del crimen'):

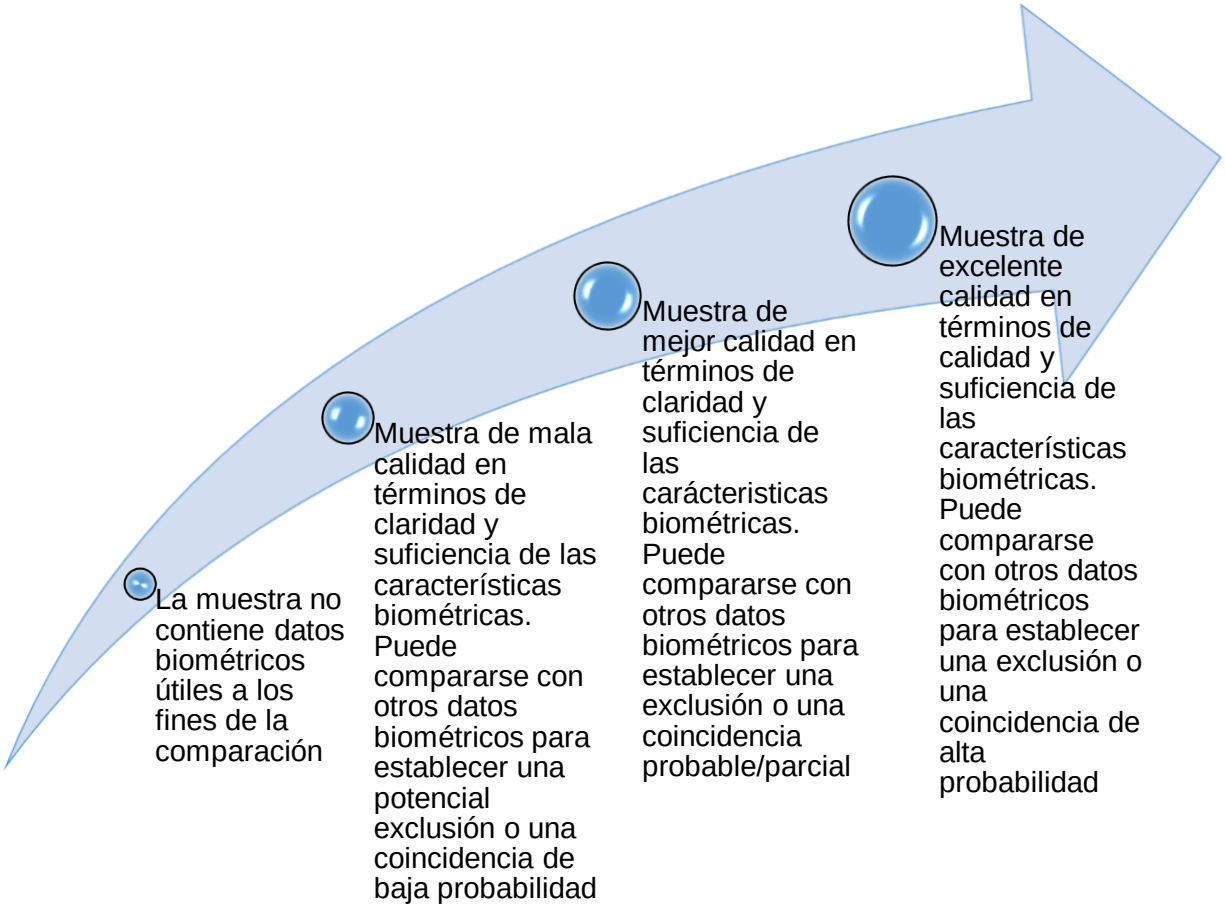
- *Cantidad y calidad*: al igual que con las marcas de los dedos, la cantidad y calidad de ADN depositada en las escenas del crimen es variable y por este motivo algunas coincidencias de ADN se clasifican como 'parciales' en lugar de 'totales'. Esto sucede cuando el ADN disponible es escaso o de mala calidad para producir un perfil de ADN completo. En estas circunstancias la probabilidad de coincidencia o índice de probabilidad se ajusta de modo acorde para reflejar el grado de incertidumbre.
- *Mezclas:* el ADN de más de un donante podrá estar depositado en un lugar y el perfil resultante podrá contener una mezcla de dos o más personas. Los científicos forenses usan el análisis estadístico para interpretar esos resultados y, de ser posible, colaboran a fin de separar y perfilar el ADN de cada donante. Los perfiles individuales en la mezcla también pueden ser de calidad variable.
- *Origen*: las técnicas de laboratorio modernas de ADN generan perfiles de cantidades mínimas de ADN a nivel celular. Sin embargo, dado que los científicos actualmente lidian con esas pequeñas muestras no siempre es posible determinar el origen del ADN hallado en una escena del crimen, por ejemplo un fluido corporal específico.
- *Contaminación*: la consecuencia de esta capacidad de detectar y perfilar las muestras de ADN a tan bajos niveles es que dicho material es de naturaleza fugitiva, es decir es capaz de ser transferido entre las personas, objetos y lugares. Se deben emplear amplias salvaguardas en las escenas del crimen y en los laboratorios para neutralizar la transferencia inadvertida de ADN a través de las acciones de la policía o de los científicos forenses (Véase la Sección 2.3).
- *Abuso ambiental*: el ADN puede destruirse, degradarse o adulterarse como consecuencia de la exposición prolongada a condiciones ambientales adversas tales como temperaturas extremas, humedad y contaminantes.

En consecuencia, la calidad del material biométrico recolectado en la escenas del crimen oscila progresivamente desde sin valor, donde no se pueden extraer características o datos biométricos, hasta de alto valor, donde el material biométrico tiene una cantidad y claridad suficiente de características para permitir la comparación con otros datos biométricos y el potencial para producir una coincidencia de alta probabilidad. La calidad relativa de los otros datos biométricos empleados

en la comparación, ya sea una muestra de referencia o una muestra tomada en una escena del crimen, también es fundamental para el proceso. La capacidad de obtener cualquier grado de coincidencia en el proceso de comparación está directamente relacionada con la calidad de ambas muestras. Este es el motivo por el cual los datos biométricos de referencia, tomados de las personas relacionadas con delitos de terrorismo, deben ser del más alto estándar posible.

La Figura 3 grafica las etapas representativas de esta variación en términos de la calidad de la muestra biométrica y la respectiva progresión desde una baja a una alta probabilidad de coincidencia. Las exclusiones, en donde la comparación muestra que dos muestras biométricas no provienen de la misma persona, normalmente son más fáciles de establecer con material biométrico de mala calidad que las inclusiones (es decir, las coincidencias) pero en el extremo inferior de la progresión de calidad ambos procesos se tornan desafiantes y los resultados de las comparaciones pueden ser inconclusos.

Figura 3 – Datos biométricos de la escena del crimen – Relación entre la calidad de la muestra biométrica y las probabilidades de coincidencia



Criterio de registro de la base de datos: Los datos biométricos de mala calidad generalmente carecen de suficientes características de búsqueda lo cual significa que los datos, al ser archivados en un sistema como por ejemplo AFIS, probablemente respondan con frecuencia en forma desproporcionada a las búsquedas entrantes y esto puede en última instancia comprometer la efectividad del sistema. Esto se debe a que las potenciales coincidencias biométricas son presentadas

por el sistema en la forma de un listado jerárquico de candidatos, que generalmente muestre una cantidad de respuestas pre-configuradas, por ejemplo, las diez primeras coincidencias más probables. Estas son verificadas por un operador humano a fin de determinar si alguna de ellas es una coincidencia real. Cualquier dato de mala calidad archivado en el sistema tiene el potencial de dejar fuera de este listado a las verdaderas coincidencias. Por lo tanto, la decisión de registrar una muestra biométrica tiene que encontrar un equilibrio entre el valor probativo, operativo y de inteligencia de cada muestra contra su calidad técnica o científica (Véase la Sección 2.4.2.). En una red de bases de datos, esos umbrales de registro de datos biométricos de mala calidad deben estar sujetos a estándares colectivos mínimos para garantizar una operación suave y equilibrada a lo largo de la red e impedir que los socios registren datos que podrían alterar una búsqueda eficiente.

Como resultado directo de la progresión de la calidad de los datos biométricos de la escena del crimen, los Científicos Forenses, los Peritos en Huellas Dactilares y otras personas a cargo del procesamiento de material forense han desarrollado varios métodos diferentes para presentar el rango de resultados de sus comparaciones ante los investigadores, analistas de inteligencia o tribunales judiciales. Estos métodos incluyen ampliamente:

- La probabilidad lógica 'bayesiana' y la inferencia estadística para comprobar hipótesis incluyendo las Tasas de Probabilidad que forman la base de las comparaciones de perfiles de ADN. Nota: algunos tribunales y jurisdicciones nacionales no aceptan ciertas variaciones de estos métodos estadísticos [18]
- Escalas de equivalencia verbal, por ejemplo, las comparaciones de huellas dactilares modernas y muchas otras disciplinas de las ciencias forenses
- Conclusiones 'absolutas', por ejemplo, las comparaciones de huellas dactilares tradicionales

Esto significa que el método de comunicación forense *para una misma modalidad* puede variar de país en país o incluso de jurisdicción en jurisdicción de conformidad con los correspondientes requisitos científicos, judiciales, regulatorios y legislativos. Esto, a su vez, puede afectar el criterio de registro de cada base de datos así como el tipo de resultados generados.

Caso de estudio 3 – Normas tradicionales en materia de huellas dactilares

Algunos países aún usan el método 'absoluto' para la identificación de las huellas dactilares que es un sistema tradicional basado en un proceso binario de toma de decisiones, es decir coincidencia o no coincidencia y exige una cantidad mínima predeterminada de características específicas (características biométricas) para confirmar la coincidencia y presentar la evidencia ante el tribunal. Esta norma está escrita en el ordenamiento jurídico de algunas jurisdicciones. Cualquier comparación de una huella dactilar o marca de dedos que presenta un número menor de características específicas que aquel aceptado por la norma no puede ser presentada como evidencia. Obviamente, esto puede presentar dificultades en aquellas jurisdicciones que operan de conformidad con los principios de divulgación plena dentro de sus sistemas judiciales ya que los tribunales pueden requerir que un perito emita una opinión sobre una comparación de una huella dactilar que sea de interés para el tribunal (por ejemplo, puede tener un peso significativo en el caso o tener una relevancia particular en el caso del Demandado) pero que un perito considera por debajo del límite del estándar aceptado para su presentación ante un tribunal. Para superar estas limitaciones, otros países han desarrollado y adoptado en las últimas décadas un enfoque holístico no numérico que no

[18] Como lectura adicional sobre este tema, véase 'Interpreting Evidence: Evaluating Forensic Science in the Courtroom' de Bernard Robertson & G.A. Vignaux (Wiley ISBN 0471 96026 8), 'Introduction to Statistics for Forensic Scientists' de David Lucy (Wiley ISBN 0-470-02200-0) y 'Strengthening Forensic Science in the United States: A Path Forward' del National Research Council of the National Academies (The National Academies Press ISBN-13: 978-0-309-13135-3).

exige una cantidad mínima de características específicas sino que verifica tres niveles distintos de detalle específico de fricción como parte de una evaluación sistemática estrictamente secuencial.[19] Este método puede reportar el resultado de *cualquier* comparación de una huella dactilar en una de cuatro maneras (es decir, identificación, exclusión, detalle insuficiente o inconcluso, o terminología similar) y por lo tanto es capaz de expresar un 'grado de incertidumbre' en línea con otras disciplinas modernas de las ciencias forenses. En consecuencia, en cualquier intercambio internacional de huellas dactilares, se deben hacer concesiones respecto de estas variaciones en los reportes científicos de las mismas modalidades.

Durante la última década se han efectuado considerables análisis e investigaciones sobre este tema ya que varias jurisdicciones preferirían un único método para la presentación de resultados científicos que cubriría las disciplinas convencionales de las ciencias forenses y los exámenes forenses relacionados con tecnologías digitales y electrónicas. Se han presentado varias propuestas pero aún debe acordarse un modelo definitivo y el tema continúa siendo objeto de debate internacional. El terrorismo es una amenaza internacional y por lo tanto es imperativo que aquellas personas que trabajan con datos biométricos y resultados de búsqueda estén plenamente familiarizados con las normas de información de las ciencias forenses de sus socios nacionales e internacionales de intercambio de datos. También es una buena práctica verificar en forma independiente los resultados producidos por los países/jurisdicciones de otros socios sujetando las coincidencias a los protocolos de análisis forense y normas de información del país huésped antes de tomar cualquier acción (Véase la Sección 3.3.3.).

1.2.4 Interpretación científica: identidad y actividad

Existe otro factor significativo que diferencia una aplicación biométrica comercial estándar, por ejemplo un sistema biométrico de acceso a un edificio, de una base de datos biométricos de la ciencia forense. Ambas son capaces de identificar a una persona a través de una búsqueda 1:1 o 1:n pero la aplicación forense tiene una importante característica adicional que es que los datos de la escena del crimen también pueden brindar prueba de la actividad así como de la identidad. Se puede interpretar científicamente que la ubicación, posición, distribución y orientación de la prueba forense brindan información adicional sobre el tiempo y la secuencia de eventos durante un incidente y sobre las actividades de aquellas personas involucradas. Esta prueba contextual extra obviamente aumente el valor probatorio del material de la escena del crimen y debe ser plenamente entendida y tenida en cuenta por aquellos investigadores o analistas que trabajan con los resultados derivados de las bases de datos biométricos forenses (Véase la Sección 3.3.3.).

Nota: los datos biográficos y asociados recogidos durante los procesos de control de fronteras (Véase la Sección 3.1.1.) pueden usarse en una forma similar, junto los datos biométricos, para brindar evidencia de la actividad así como de la identidad. *Esto ilustra la efectividad de usar y compartir los datos biométricos tomados en la escena del crimen y en la frontera a fin de predecir, realizar un seguimiento e interrumpir las actividades terroristas* (Véase la Sección 3.3.2.1.).

[19] Este método se conoce como ACE-V que significa Análisis, Comparación, Evaluación y Verificación.

1.3 Prácticas recomendadas

a) Se alienta a los Estados a adoptar o aumentar su uso de sistemas biométricos para autenticar la identidad de las personas e impedir que las mismas presenten identificaciones falsas o intenten hacerse pasar por otras personas.

b) Los sistemas biométricos están diseñados y se ajustan a las necesidades comerciales específicas en términos de exactitud, seguridad, volúmenes de usuarios, procesamiento y confianza operativa. Por lo tanto, los Estados deberían evaluar cuidadosamente sus propios requisitos de casos de uso antes de invertir en una nueva aplicación biométrica.

c) Los procesos de Gestión de Identidad Biométrica pueden mejorarse a través de su combinación con las bases de datos biométricos de las ciencias forenses a fin de crear un marco de investigación e inteligencia nacional efectivo para combatir el terrorismo y la actividad delictiva relacionada.

d) Existen variaciones entre los estándares y la metodología de información de las ciencias forenses internacionales. En consecuencia, se recomienda capacitar a todo el personal que trabaja con los resultados derivados de las bases de datos biométricos a fin de entender el valor relativo y las potenciales limitaciones de los resultados.

1.3.1 Documentos de referencia

Verificación de la identidad: importancia del contexto y continuidad de la identidad, página 11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

En 1995, el Consorcio de Biometría del Gobierno de los Estados Unidos definió la "biometría" como "…el reconocimiento automático de las personas en base a sus características de comportamiento y biológicas".

Página 1, Reconocimiento Biométrico: desafíos y oportunidades, Consejo Nacional de Investigación, Washington (2010), disponible para descarga en: http://www.nap.edu/openbook.php?record_id=12720&page=1

Jain y otros "Biometría: Identificación personal en la sociedad en red", Norwell, Mass.: Kluwer Academic Publisher (1999)

Guía para entender la biometría (copia de trabajo) – Biometrics Institute www.biometricsinstitute.org

PAS 92:2011 Código de prácticas para la implementación de un sistema biométrico – British Standards Institute www.bsigroup.com

Oficina de Naciones Unidas contra la Droga y el Delito (ONUDD): 'Policía: servicios e infraestructura forense' y 'Requisitos de habilidades del personal y recomendaciones de equipos para los laboratorios de ciencias forenses'. (www.unodc.org)'. www.unodc.org

Informe anual del regulador de ciencias forenses del Reino Unido, noviembre de 2016 – noviembre de 2017 – Dr. Gillian Tully

Revisión y recomendaciones sobre la gestión de la base de datos de ADN, 2017, Grupo de Trabajo sobre ADN de ENSFI, abril de 2017 http://enfsi.eu/wp-content/uploads/2017/09/ADN-base de datosmanagement-review-and-recommendatations-april-2017.pdf

Forensic ADN Typing: Biology, Technology and Genetics of STR Markers – John M. Butler. Publicado por Elsevier Academic Press ISBN-13: 978-0-12-147952-7

Interpreting Evidence: Evaluating Forensic Science in the Courtroom – Bernard Robertson & G.A. Vignaux. Publicado por Wiley ISBN 0471 96026 8

Introduction to Statistics for Forensic Scientists – David Lucy. Publicado por Wiley ISBN 0-470-02200-0

Strengthening Forensic Science in the United States: A Path Forward by the National Research Council of the National Academies. Publicado por The National Academies Press ISBN-13: 978-0-309-13135-3.

2. Gobierno y regulación

A fines de claridad y consistencia, la siguiente sección "Gobierno y regulación" se aplica a todas las secciones de este compendio y debería considerarse aplicable a todas las prácticas, medidas y recomendaciones presentadas y explicadas a lo largo de la presente versión de este compendio.

La Sección 2 aborda el gobierno y los requisitos normativos de la tecnología biométrica desde el punto de vista del derecho internacional, los derechos humanos, las revisiones éticas, los requisitos de protección de la información y el derecho a la privacidad. Luego se presenta una amplia mirada de las potenciales vulnerabilidades de los sistemas biométricos y algunas de las medidas de control que pueden emplearse para mitigar los riesgos. Después se consideran los estándares operativos técnicos y científicos internacionales, que cubren la certificación y acreditación de las aplicaciones biométricas así como los sistemas de gestión de la calidad que se emplean en los procesos de ciencias forenses asociados. La última parte de esta sección aborda los requisitos de contratación, mantenimiento y abastecimiento de un sistema o red biométrica de lucha contra el terrorismo y, en particular, las decisiones operativas y financieras clave que deben tomarse al evaluar un posible nuevo sistema o una extensión.

2.1 Derecho internacional, incluyendo las normas sobre derechos humanos

Los Estados tienen la obligación de proteger a todos aquellos dentro de su jurisdicción contra los ataques terroristas y a llevar ante la justicia a quienes cometan dichos actos y a su vez cumplir con los derechos humanos. El Consejo de Seguridad de las Naciones Unidas y la Asamblea General han resaltado que los Estados deben garantizar que todas las medidas adoptadas para combatir el terrorismo cumplan con todas sus obligaciones en virtud del derecho internacional, particularmente las leyes internacionales en materia de derechos humanos internacionales, refugiados y ayuda humanitaria. El respeto por los derechos humanos y el estado de derecho es complementario de las medidas efectivas contra el terrorismo y esencial para el éxito de los esfuerzos de lucha contra el terrorismo[20].

Es cierto que el alcance de la aplicación de los derechos humanos difiere entre los Estados Miembros. Algunos Estados no son parte de los instrumentos de derechos humanos universales y muchos son parte de los instrumentos de derechos humanos regionales[21] que difieren en ciertos aspectos. Los Estados Miembros también difieren en la incorporación de las normas de derechos humanos internacionales a la legislación nacional. Adicionalmente, algunos Estados han introducido reservas o declaraciones al momento de la ratificación o adhesión, limitando así su compromiso con obligaciones del tratado específicas.

En su resolución 2396 (2017), el Consejo de Seguridad exhorta a los Estados Miembros a que evalúen e investiguen a las personas sospechosas respecto de las cuales tengan motivos suficientes para creer que son terroristas, incluidos los presuntos combatientes terroristas extranjeros y sus familiares acompañantes, incluidos sus cónyuges e hijos, que entren en sus territorios, a que elaboren y lleven a cabo evaluaciones minuciosas del riesgo que plantean esas personas. Al desarrollar sistemas para recopilar datos biométricos, es importante establecer salvaguardas respecto de las normas en

[20] Véase por ejemplo, las resoluciones del Consejo de Seguridad número 1373(2001), 1624 (2005), 2178 (2014) y 2396 (2017); y las resoluciones de la Asamblea General A/RES/68/276 y A/70/L.55

[21] Véase por ejemplo, la publicación de la Agencia de los Derechos Fundamentales de la Unión Europea 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

materia de protección de datos y derechos humanos,[22] prestando particular atención a la necesidad de garantizar que cualquier sistema desarrollado para recolectar y registrar información (incluyendo datos biométricos) respecto de menores deberá sea utilizado y compartido en forma responsable, protegiendo plenamente los derechos humanos de los niños de conformidad con el derecho internacional nacional e internacional, particularmente aquellos incluidos en la Convención de las Naciones Unidas sobre los Derechos de los Niños (CRC) (1989).

Uso de la biometría en cumplimiento de los derechos humanos

Los Estados incorporan cada vez más el uso de la biometría como una importante herramienta para combatir el terrorismo. La identificación de la voz, el escaneo del iris, el reconocimiento facial, las huellas dactilares, el ADN, los escaneos del cuerpo y la forma de caminar son solo algunos ejemplos de las muchas tecnologías digitales que se desarrollan e implementan a fin de combatir el terrorismo. Estas medidas tecnológicas presentan complejos desafíos legales y políticos que son relevantes tanto para los esfuerzos de los Estados tendientes a combatir el terrorismo como para sus obligaciones en materia de derechos humanos. Si bien los sistemas biométricos pueden ser una herramienta legítima para la identificación de los sospechosos de actos terroristas, el alcance técnico expansivo y el rápido desarrollo de esta tecnología merecen mayor atención en lo que se refiere a la protección de los derechos humanos, incluyendo, en forma meramente enunciativa, el derecho a la privacidad. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR) estipula que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; y que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. El Consejo de Derechos Humanos de las Naciones Unidas ha reconocido que "las violaciones o abusos del derecho a la privacidad pueden afectar el goce de otros derechos humanos, incluyendo el derecho a la libertad de expresión y a emitir opiniones sin interferencias, y el derecho a la libertad de reunión y asociación pacífica...."[23] Mientras que el derecho a la privacidad en virtud del derecho internacional no es absoluto, se reconoce que cualquier interferencia con el derecho debe cumplir con los principios de legalidad, proporcionalidad y necesidad. Además, la interferencia de la privacidad autorizada por el Estado sólo puede tener lugar en virtud de la ley, la cual debe cumplir con las disposiciones, propósitos y objetivos del Pacto, y ser razonable en virtud de las circunstancias particulares[24]. Dicha interferencia no deberá constituir una discriminación por motivos de raza, idioma, religión, origen nacional o social, opinión política o de otro tipo, o cualquier otro motivo estipulado en el derecho internacional.[25]

El Relator Especial de las Naciones Unidas sobre el derecho de privacidad ha observado que ciertos países del mundo han identificado un derecho fundamental y general a la dignidad y al desarrollo de la propia personalidad de manera libre y sin trabas, que podría verse afectado negativamente por las violaciones al derecho a la privacidad.[26] La Declaración Universal de Derechos Humanos y el Pacto Internacional sobre Derechos Civiles y Políticos comienzan por establecer que el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana es el fundamento de la libertad, la justicia y la paz en el mundo.[27] Estos derechos podrían ponerse en peligro a través del uso inadecuado de los datos biométricos. El mal uso de dichos datos también podría implicar serios riesgos sobre el derecho a un debido proceso legal, incluyendo el derecho a presumir la inocencia y otros derechos vinculados a los procesos penales.[28] Además, la

[22] S/2015/975, párrafo 8; S/2015/939, Principio 15 (e).
[23] Resolución del Consejo de Derechos Humanos A/HRC/RES/34/7 (2017).
[24] Comentario General N° 16 del Comité de Derechos Humanos: Artículo 17 (Derecho a la privacidad), párrafos 3-4.
[25] ICCPR, Art. 2(1) y 26.
[26] Reporte del Relator Especial sobre el derecho a la privacidad, A/HRC/31/64 (2016).
[27] Declaración Universal de Derechos Humanos y ICCPR, preámbulo.
[28] ICCPR, Artículos 9, 14.

recolección en masa de dichos datos sin cumplir con los principios de necesidad y proporcionalidad podría representar una violación del derecho a la privacidad por sí mismo.[29]

Para impedir el uso indebido de los datos biométricos, los estados deberían considerar revisar sus leyes en materia de protección de datos personales mediante su adecuación a las aplicaciones actuales de las tecnologías biométricas mejoradas. Los estados también deberían revisar su legislación a fin de hacer frente a los desafíos derivados del desarrollo adicional de las tecnologías biométricas. Un enfoque basado en los derechos humanos respecto del uso de la tecnología biométrica debería incluir el uso de salvaguardas procesales y un control efectivo de su aplicación.[30] Esto incluye la creación de organismos de control adecuados e independientes para supervisar las actividades de las agencias del Estado a cargo del suministro de los recursos efectivos en caso de violaciones y la creación de autoridades de supervisión independientes para garantizar el cumplimiento por parte de la agencias de los Estados y el sector privado de las leyes de privacidad y protección de los datos[31].

2.1.1 Ética y biometría

Las tecnologías como la biometría presentan desafíos particulares debido a la brecha creada por la innovación tecnológica y la implementación de leyes que reglamentan dichas tecnologías. En consecuencia, varios Estados han implementado una revisión ética y otros órganos de control para anticipar y considerar esas nuevas tecnologías o aplicaciones y brindar asesoramiento acerca de la legislación, la política gubernamental y la planificación estratégica actual o futura. Estos órganos normalmente están integrados por profesionales experimentados de alto nivel de la sociedad civil, y pueden incluir los sectores públicos y privados, la ciencia y la tecnología, académicos y laicos. Estos grupos de control ético intentan revisar las cuestiones desde una amplia perspectiva, incluyendo el potencial impacto que las tecnologías biométricas pueden tener sobre ciertos grupos de personas o comunidades particularmente respecto de la raza, género, edad, creencias religiosas y orientación sexual.

El siguiente caso de estudio ilustra este enfoque:

[29] ICCPR, Artículo 2(3).
[30] El Comité de Derechos Humanos, en su observación general N° 16 (1988), destacó que los Estados deben adoptar medidas eficaces para garantizar que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y que nunca se la utilice para fines incompatibles con el Pacto Internacional de Derechos Civiles y Políticos. La protección eficaz debería incluir la capacidad de cada persona de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado en archivos de datos automáticos, con el correspondiente derecho a pedir su rectificación o eliminación de datos incorrecto. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Véase:
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en
[31] Resolución de la Asamblea General 45/95 (1990) sobre Principios rectores para la reglamentación de los archivos computarizados de datos personales y el Reglamento General de Protección de Datos de la Unión Europea de 2018, Articulo 51 (Autoridad de Control).

Caso de estudio 4 – Grupo de ética biométrica y forense del Reino Unido[32]

Este grupo surgió del Grupo de Ética sobre ADN Nacional original que se creó para controlar las técnicas y tácticas científicas empleadas en la primera base de datos de ADN del mundo. Su competencia actualmente cubre las ciencias forenses en general así como la tecnología biométrica. El grupo considera cada nueva cuestión contra un amplio marco de consideraciones legales, morales y político sociales. El grupo trabaja en cumplimiento de los siguientes principios rectores:

Principios rectores ***A ser aplicados a los procedimientos biométricos y forenses***	**Principios rectores** ***Implementación de los principios***
▯ los procedimientos deberían usarse para mejorar la seguridad pública y el bien común; ▯ los procedimientos deberían usarse para fomentar la justicia; ▯ los procedimientos deberían respetar los derechos humanos de las personas y grupos; ▯ los procedimientos deberían respetar la dignidad de todas las personas; ▯ los procedimientos deberían, en la medida de lo posible, proteger el derecho de respetar la privacidad y la vida familiar cuando no esto no esté en conflicto con los fines legítimos del sistema de justicia penal de protección del público contra daños; ▯ los desarrollos científicos y tecnológicos deberían aprovecharse para promocionar la pronta exoneración de los inocentes, otorgar protección y resolución para las víctimas y colaborar con el proceso de justicia criminal; ▯ los procedimientos deberían basarse en pruebas sólidas.	▯ imparcialidad – los procedimientos deberían aplicarse sin favoritismo ni discriminación injusta; ▯ proporcionalidad – equilibrio de los derechos individuales y el bien común; ▯ apertura y transparencia; ▯ necesidad de contar con sistemas para identificar errores; ▯ necesidad de control de calidad; ▯ necesidad de responsabilidad pública; ▯ necesidad de control independiente cuando corresponda; ▯ necesidad de brindar información adecuada y cuando corresponda obtener el consentimiento de aquellos de quienes se pretende obtener la información o las muestras.

El grupo también tiene un conjunto de principios respecto de la recolección y el procesamiento de la información:

- ▯ la información debería recogerse, almacenarse y utilizarse únicamente para fines específicos y legales;
- ▯ la recolección, el almacenamiento y el uso de los datos deberán adherirse a los requerimientos legales;

[32] https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group

- deberían tomarse medidas para asegurar la exactitud, seguridad e integridad de la información recogida, almacenada y utilizada;
- los procesos deberían ser sólidos y adaptarse a los estándares internacionales y ser aplicados en forma profesional por personal capacitado;
- la intromisión en las vidas privadas debería minimizarse;
- se deberían tener en cuenta los intereses de los sujetos de datos secundarios (es decir, las personas potencialmente afectadas por la información recogida relativa a otras personas, por ejemplo, familiares).

La amenaza del terrorismo afecta a varios Estados y en consecuencia las agencias de cumplimiento de la ley desarrollan e implementan rápidamente nuevas técnicas dentro de la biometría y las ciencias forenses a fin de brindar protección y mejorar las habilidades de investigación. Los grupos de control ético tienen un papel que jugar en este proceso ya que están en una posición de brindar un comentario informado respecto de la preparación o adopción de una nueva técnica o estrategia. Esto no reemplaza la necesidad de contar con legislación posterior pero puede ayudar a impedir la introducción de nuevos métodos y prácticas que no sean proporcionados o necesarios. Este proceso también alertaría a los legisladores acerca de la urgencia e importancia relativa de la cuestión bajo revisión.

Normas y ejemplos acerca de cómo interactúan la ética y la biometría

En la actualidad, las normas sobre la prestación y el uso en forma ética de la biometría o de la mayoría de las nuevas tecnologías son desiguales a nivel internacional o incluso nacional. La Organización Internacional de Normalización (ISO) ha promulgado sus estándares respecto de las Consideraciones Jurisdiccionales y Sociales y de las Aplicaciones Comerciales, Parte 1 Directrices Generales (ISO/IEC TR 24714: 2008) y su Guía 71:2014 que aborda la ética y, en su Guía 71, los estándares de accesibilidad para grupos tales como tercera edad y discapacitados.

El uso ético de la biometría se extiende al dominio humanitario. Existen muchos programas en los cuales el uso de la biometría ha permitido brindar beneficios. La oficina del Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), por ejemplo, ha utilizado los sistemas biométricos para apoyar sus programas desde 2002 y basa cada vez más el registro en la biometría. La solución de biometría global del ACNUR, el Sistema de Gestión de Identidad Biométrica (BIMS) permite a la organización garantizar la singularidad de cada registro, y verificar que las diversas formas de asistencia que la organización puede brindar (incluyendo alimentos, efectivo, protección o reubicación, entre otras) sean recibidas por los destinatarios correspondientes. Existen otros dos ejemplos en donde el fraude electoral o financiero, dos factores potencialmente desestabilizantes que pueden fomentar la rebelión o el crecimiento del terrorismo, logran minimizarse mediante el uso de identificación biométrica.

El ACNUR también recomienda el registro biométrico de las personas que solicitan asilo como un elemento integral de los sistemas de control de ingreso sensibles a la protección. Esto incluye la implementación de las salvaguardas adecuadas para impedir la posible infiltración de criminales o de aquellos que pertenecen a organizaciones terroristas o extremistas. Las buenas prácticas en este sentido incluyen: (1) el registro adecuado, incluyendo la biometría, por las autoridades fronterizas capacitadas en los aspectos relevantes de la protección en materia de seguridad, refugiados y derechos humanos; y (2) la derivación de aquellos que reclaman protección internacional a los procedimientos de asilo. Como principio general, a fin de no poner en riesgo a los solicitantes de asilo/refugiados, sus datos biométricos y otros datos personales no deberían compartirse con sus

países de origen, a menos que el procedimiento de asilo haya concluido y no se hubiera otorgado la protección. Esto también se aplica a terceros países en circunstancias en donde la protección efectiva del solicitante de asilo o refugiado podría ponerse en peligro.[33]

2.2 Protección de los datos y del derecho a la privacidad

La tecnología biométrica es un activo importante para combatir el terrorismo a escala global. Tiene la capacidad de detectar e interrumpir las acciones terroristas y proteger a la sociedad contra ataques indiscriminados. Sin embargo, la tecnología se basa en la recopilación, almacenamiento y uso de datos personales. Como se analizó anteriormente, estos datos biométricos deben estar protegidos por la ley y deben procesarse sin violar derechos humanos fundamentales, tales como el derecho a la privacidad.

2.2.1 Criterios sobre registro legal y estándares sobre datos

El Consejo de Seguridad de las Naciones Unidas en su resolución 1373 (2001) observó la estrecha conexión que existe entre el terrorismo internacional y la delincuencia organizada transnacional, las drogas ilícitas, el blanqueo de dinero y el tráfico ilícito de armas. En esa misma resolución, el Consejo resolvió que los Estados impidan la circulación de terroristas o de grupos terroristas imponiendo controles eficaces de fronteras y controles en la expedición de documentos de identidad y de viaje, y adoptando medidas para evitar la falsificación, la alteración ilegal y la utilización fraudulenta de documentos de identidad y de viaje.

Para contrarrestar esta relación, es esencial desarrollar una capacidad suficiente y efectiva para combatir el terrorismo en todos los Estados Miembros.[34] El uso de la biometría es una herramienta vital en el desarrollo de esa capacidad.[35] Dado que las tácticas empleadas por los terroristas generalmente incluyen el robo de documentos o identidades, el uso de la biometría brinda una herramienta valiosa para restablecer las identidades de las víctimas de robo de identidad (Véase la Sección 2.3.5.).

A fin de implementar un sistema biométrico que sea eficaz y cumpla con las leyes en materia de protección de datos y defienda el derecho a la privacidad, se deben considerar los siguientes factores:

Garantía de calidad de registro: se deben establecer altos estándares de garantía de calidad de modo tal de poder utilizar el registro y comparación biométrica en forma adecuada en una amplia variedad de entornos como por ejemplo en áreas remotas, en puestos de frontera establecidos o en los aeropuertos que demandan cada vez más un rápido procesamiento de pasajeros mientras que a su vez se deben mantener los niveles de exactitud. En el caso de niños o menores acompañados por sus padres o que viajan solos, se debería tener en cuenta debidamente la posibilidad de que algunos datos biométricos de los niños pueden cambiar a medida que crecen. Además, el Consejo de Seguridad de las Naciones Unidas en su resolución 2396 (2017) destaca que los niños deben ser tratados de manera que se respeten sus derechos y su dignidad, de conformidad con el derecho internacional aplicable.

[33] Véase la Sección E, inciso 17 de ACNUR "Cómo abordar el tema de seguridad sin perjudicar la protección de los refugiados" http://www.refworld.org/docid/5672aed34.html
[34] Véase también las Resoluciones del Consejo de Seguridad 2195 (2014) y 2178 (2014)
[35] Resolución del Consejo de Seguridad de las Naciones Unidas 2396 (2017) y su anterior resolución 2178 (2014)

Legislación sobre privacidad: las autoridades de cumplimiento de la ley pueden limitar el derecho a la privacidad si las medidas adoptadas son necesarias y proporcionadas y cumplen con el derecho internacional en materia de derechos humanos. Por ejemplo, los datos personales de sospechosos y asociados pueden ser usados en emergencias cuando los principios de privacidad clave tales como el consentimiento informado o la recolección de datos personales relacionados pueden dejarse de lado. Sin embargo, estos principios de privacidad tales como el consentimiento informado, la recolección y el uso para fines determinados y el derecho a corregir los registros inexactos o erróneos deberían ser tratados como requisitos predeterminados en la mayoría de los casos. Además, los motivos para apartarse de esos requisitos predeterminados deberían documentarse y registrarse. El acceso del operador a dicho sistemas también debería estar controlado a través de la biometría para garantizar altos estándares de seguridad.

Financiación del terrorismo: para colaborar en la prevención del fraude relacionado con el terrorismo, el robo de identidad y las operaciones financieras, la biometría puede utilizarse como parte de un conjunto de medidas para mitigar dichas amenazas en el sistema financiera. El uso de la biometría para controlar el acceso a las operaciones es por lo tanto una opción efectiva. Un programa nacional para proteger a los consumidores contra el fraude vinculado al terrorismo y el robo de identidad tiene muchos beneficios a nivel de la comunidad y del orden público.[36]

Estándares internacionales sobre datos personales: los estándares sobre datos personales deberían establecerse de conformidad con los estándares internacionales en lugar de utilizar modalidades menos comunes o estándares técnicos que pueden estar basados en factores tales como la presión de industria autóctona o incluso sistemas provistos gratuitamente por donantes de ayuda. Las normas de la Organización Internacional de Estandarización (ISO), la Organización de Aviación Civil Internacional (OACI) y la Organización Mundial de Aduanas deberían ser el criterio inicial en la selección del sistema, respaldadas por las Directrices de Privacidad y el Listado de Verificación del Impacto de Privacidad del Biometrics Institute.[37]

Admisibilidad de la prueba: se debería tener cuidado de garantizar que el uso de todos los datos biométricos y personales se encuentre limitado a los fines autorizados para los cuales se obtuvieron. Esto también garantizará que la información recogida para las bases de datos sea admisible en juicio. Esto debería incluir disposiciones para garantizar la cooperación por parte de la industria informática siempre que se haya establecido una base legal para dicha cooperación.

Interpretación de los resultados biométricos: las agencias de cumplimiento de la ley que detienen o procesan a los terroristas deberían ser conscientes de los riesgos derivados de una mala interpretación de los resultados de las bases de datos biométricos, por ejemplo, entender el valor de una coincidencia parcial de ADN o de una comparación facial inconclusa debido a los problemas ambientales que pueden ocurrir al momento de capturar una imagen facial en un entorno de baja calidad. En esas instancias, el análisis contextual es absolutamente esencial antes de tomar cualquier acción (Véase la Sección 3).

2.2.2 Política de retención o eliminación de datos

Esta es un área en la cual los procedimientos tendientes al cumplimiento de la ley y a combatir el terrorismo deben llevarse a cabo de conformidad con el derecho internacional en materia de

[36] Véase el sitio web del Fondo Monetario Internacional en donde se enuncian instrumentos contra el lavado de dinero y contra el fraude www.imf.org

[37] Véase www.biometricsinstitute.org

derechos humanos, incluido el derecho a la privacidad. Por ejemplo, el derecho a consultar nuestro expediente o a realizar correcciones o solicitar eliminaciones (que en general está garantizado por la legislación en materia de privacidad, como por ejemplo, el *Reglamento General de Protección de Datos* de la Unión Europea)[38] también puede estar calificado por la necesidad de proteger a los testigos o la confidencialidad de las investigaciones en curso.

Las políticas de retención de datos varían ampliamente en todo el mundo, particularmente para aquellos arrestados durante investigaciones de cumplimiento de la ley. Muchas jurisdicciones retienen los datos biométricos de aquellos acusados de un delito durante toda la vida del autor pero no hay un estándar común respecto de aquellos sospechosos y arrestados por un delito pero que posteriormente no fueron condenados.

Una buena práctica es almacenar los datos biométricos en forma separada de sus correspondientes datos biográficos. Las víctimas de robo de identidad (a través de un delito o acto terrorista) podrán requerir el rápido restablecimiento de su identidad luego de que la misma haya sido robada y usada en forma errónea. Al diseñar el sistema, será necesario planificar la reconexión de los datos biométricos y biográficos cuando ello ocurra. Esto puede lograrse a través de la asignación de un solo segmento de metainformación en los registros biométricos en la forma de un único número de referencia. Sin embargo, esa reconexión debería salvaguardarse, a fin de garantizar la integridad del sistema y de los datos en todo momento, y requerirá de un sólido protocolo de seguridad tal como:

- requerir que el funcionario que accede tenga un rango superior dentro de la organización, y
- el uso de sus datos biométricos para acceder al sistema, y
- el registro formal de dicho acceso, y
- el registro formal de los motivos para solicitar dicho acceso

La seguridad se puede mejorar aún más al tener más de una persona dentro de la organización involucrada en la validación de las entradas o el proceso de revocación. Esto permitiría la rotación del personal que realiza estas funciones y crear otra capa de seguridad.

2.2.3 Procesamiento de datos

Una organización responsable por el procesamiento de datos debe designar un controlador de datos que será responsable de administrar todas las actividades de procesamiento de datos, incluida la recopilación, almacenamiento, uso y eliminación de los datos. El controlador de datos retiene la responsabilidad incluso si la función de procesamiento de datos se subcontrata a otras partes.

La ley de privacidad más completa requiere que las autoridades que recopilan datos personales garanticen que no se pueda realizar el procesamiento o almacenamiento en países donde su ley de privacidad sea inferior a la del país de recolección.

Todos los proveedores u operadores externos deben estar sujetos a contratos que requieran un nivel de seguridad muy alto y deben incluir auditorías externas por parte de la agencia encargada y sanciones por el incumplimiento de los requisitos de seguridad y privacidad del contrato.

[38] Reglamento General de Protección de Datos de la Unión Europea 2018, Artículo 7 (Consentimiento), Artículo 17 (Derecho de supresión), Artículo 15 (Derecho de acceso del interesado)

2.2.4 Intercambio de datos

La Organización de Naciones Unidas destacó, en varias declaraciones, la necesidad de cooperación entre los estados en términos de mejoras legislativas para procesar a los terroristas, particularmente los combatientes terroristas extranjeros, protegiendo al mismo tiempo los derechos humanos y la privacidad.[39] El uso compartido en tiempo real de los datos personales como por ejemplo los biométricos tanto dentro de las autoridades del estado y entre los estados también exige cooperación a fin de armonizar la interoperación de las plataformas y formatos.[40]

Cuando se compartan datos personales de terroristas o sospechosos terroristas, será necesario que exista una confianza considerable sobre una serie de cuestiones, como el uso que se dará a los datos compartidos, la precisión y el contexto de los datos y la cantidad y el tipo de datos que se pueden compartir. Los acuerdos de intercambio de datos deben basarse en acuerdos formales celebrados entre todas las partes involucradas.

Hay otros factores que deben tenerse en cuenta en ese proceso de intercambio. Estos incluyen el requisito de que las solicitudes de datos personales se basen en una sospecha genuina de actividad terrorista, detalles de los requisitos de evidencia y el establecimiento de si los datos se obtuvieron en condiciones opresivas, un problema probatorio clave para muchos países.

En general, se aplican los siguientes principios:

1. el intercambio de datos personales, incluidos los datos biométricos, debe ser legalmente aprobado a nivel nacional y estar sujeto a un marco legal claro entre las entidades que envían y reciben los datos, a nivel nacional e internacional
2. el uso de dichos datos debe limitarse a los fines aprobados para los cuales se obtuvieron.
3. los datos solo se pueden compartir con destinatarios de confianza[41]. El principio establecido en la Sección 2.2.3. se extiende al uso compartido de datos y los datos personales no deberían enviarse a las jurisdicciones en las que el nivel de protección de la privacidad es inferior al del país de origen.
4. (de conformidad con la Sección 2.1.) para no poner en riesgo a los solicitantes de asilo o refugiados, sus datos biométricos y otros datos personales no deben compartirse con sus países de origen, a menos que el procedimiento de asilo haya concluido y la protección no haya sido otorgada (Ver también caso de estudio 10).

2.2.5 Prevención del uso erróneo de los datos

Existen al menos dos problemas clave que se relacionan con el uso erróneo de los datos.

[39] Resolución del Consejo de Naciones Unidas 2322 (2016) sobre cooperación internacional y Resolución del Consejo de Naciones Unidas 2396 (2017) Fortalecimiento de medidas para combatir las amenazas causadas por terroristas extranjeros.

[40] Resolución del Consejo de Naciones Unidas 2178 (2014) y la Declaración de Madrid de los Ministros de Asuntos Exteriores en la reunión especial del Comité contra el Terrorismo del Consejo de Seguridad celebrada el 28 de julio de 2015.

[41] Entre los ejemplos de datos compartidos entre destinatarios de confianza se encuentran los acuerdos entre los datos de infracciones registrables de ACRO del Reino Unido con la Oficina Federal de Investigaciones de los EE. UU. u otras autoridades policiales o de inmigración de Unión Europea o el sistema de comunicaciones de policía a policía de INTERPOL I-24/7 respaldado por la base de datos de Documentos de Viaje Robados y Perdidos de INTERPOL y el Sistema de Información de Documentos de Viaje.

El primero es la absoluta necesidad de proteger todos los datos personales, incluidos los datos biométricos, del acceso no autorizado y del uso indebido. Esto incluye amenazas externas y malversación interna por parte de personal autorizado.

El segundo es la necesidad de garantizar que los datos personales proporcionados sean precisos, que se hayan colocado en un contexto relevante y se hayan proporcionado sin malas intenciones. Esto es especialmente importante cuando un gobierno u otra parte pueden tratar de colocar oponentes políticos en los listados de alerta con la intención de afectar sus derechos fundamentales.

2.2.6 Seguridad y validación de los datos

Cada organización debe designar un Controlador de Datos con suficiente antigüedad, capacitación y experiencia, que asumirá la responsabilidad de la recopilación, el uso y el movimiento de todos los datos personales, incluidos los datos biométricos.

Las responsabilidades clave de esta función deberían cubrir la formulación de políticas y los procedimientos operativos estándar. La persona a cargo de esta función también debe decidir, durante la fase de diseño del sistema, qué modalidad o modalidades biométricas serían las más adecuadas para la aplicación.

Todas las políticas y prácticas de privacidad y seguridad efectivas requieren al menos las siguientes decisiones, independientemente de si se ha utilizado o no un dato biométrico:

- ¿Se ha completado una Evaluación de Impacto en la Privacidad[42] antes de la introducción de una nueva práctica comercial o una nueva tecnología?
- ¿Existen programas y procedimientos de capacitación y concientización que mantengan una adecuada privacidad y cultura de derechos humanos, así como un conocimiento práctico de la biometría por todo el personal que opera el sistema?
- ¿Se utilizan técnicas de encriptación o reducción de datos en etapas críticas de la recopilación, almacenamiento, uso y uso compartido de datos personales, incluidos los datos biométricos?
- ¿Existen controles de acceso y registro de acceso rigurosos que requieran que las personas que accedan a archivos de datos personales confidenciales presenten datos biométricos?
- ¿Existen procesos documentados que definan los mecanismos de información y las medidas correctivas requeridas en caso de violaciones de la privacidad y la seguridad?
- ¿Se realizan pruebas y auditorías periódicas para garantizar que se siguen las prácticas de seguridad y privacidad y que son y siguen siendo sólidas y eficaces?
- ¿Existe un proceso formal para documentar y luego abordar problemas que surgen como resultado de la auditoría regular?
- ¿Se realizan verificaciones regulares y aleatorias de la validez e integridad de los datos personales que se conservan en el sistema?

[42] Una Evolución de Impacto en la Privacidad (PIA) forma parte de un enfoque de 'privacidad por diseño' respecto de la gestión de los datos dentro de las organizaciones públicas y comerciales. El proceso PIA garantiza el cumplimiento de los requisitos legales y regulatorios en materia de privacidad mediante la identificación de los riesgos potenciales y el desarrollo de estrategias de mitigación para administrarlos.

Hay una serie de normas y directrices internacionales que brindan asesoramiento a los Controladores de Datos y sus organizaciones.[43]

En términos de la validación de los datos recopilados, incluidos los datos biométricos, es esencial que se siga el debido proceso para proteger los derechos humanos, incluido el derecho a la privacidad, pero también para garantizar que se cumplan plenamente los requisitos judiciales para condenas o, por ejemplo, los procedimientos de extradición. En los procedimientos de extradición, esos requisitos pueden ser más estrictos en algunos países que en otros, especialmente en términos de criterios de prueba e interrogatorio.

Un principio rector clave para las autoridades de cumplimiento de la ley y de control de fronteras debe ser el requisito de contar con equipos de analistas especializados que tengan las habilidades y los recursos para proporcionar resultados procesables y precisos. Esto ayuda al monitoreo terrorista pre y post incidente y a la adquisición de evidencia admisible, incluyendo datos biométricos como ADN, huellas dactilares, rostro y voz. Esta capacidad debe hacer un uso completo de todas las técnicas de búsqueda y captura biométricas.

2.2.7 Supervisión

El uso incorrecto de los datos personales (ya sea con malicia o por error) puede derivar en consecuencias legales adversas y otros daños sobre las personas. Esto se aplica particularmente a los listados de alerta u otros mecanismos de vigilancia.

Se debe tener cuidado al colocar a sospechosos de terrorismo o delincuentes en los listados de alerta. Deben realizarse comprobaciones sólidas y exhaustivas para evaluar los motivos de la inclusión y la validez de todas las solicitudes antes de incluir los datos de una persona en el listado. Los datos contenidos en los listados de alerta deben someterse a revisiones periódicas para garantizar su actualidad y relevancia.

Del mismo modo, de conformidad con la legislación internacional sobre derechos humanos y la legislación sobre privacidad, los sujetos de los datos deben tener derecho de revisión contra su inclusión en cualquier listado. El derecho de revisión y apelación y la existencia de mecanismos de queja deben hacerse públicos por las autoridades de registro.

Durante el proceso de inclusión, las autoridades de cumplimiento de la ley, antiterroristas y fronterizas tienen el deber legal de recopilar, almacenar y analizar los datos de presuntos terroristas y sus asociados y sus patrones de conducta, tales como itinerarios de vuelos, operaciones financieras y cambios de domicilio. Sin embargo, debe garantizarse que la información sobre los sospechosos y sus asociados se mantenga confidencial y dentro de los marcos legales autorizados para que no se produzcan falsos encarcelamientos o persecuciones.

Se debe contar con fuertes garantías contra la recopilación, el almacenamiento y el uso arbitrario de datos personales, incluyendo mecanismos de supervisión por parte de un organismo independiente. Es posible que los estados ya cuenten con organismos de supervisión de la privacidad que puedan llevar a cabo esta función como parte de un mandato existente o ampliado. Sin embargo, si un Estado

[43] Resolución de la Asamblea General 45/95 (1990) sobre Principios rectores para la reglamentación de los archivos computarizados de datos personales y *Directrices de Privacidad sobre Datos Biométricos* del Biometrics Institute diseñadas para uso internacional www.biometricsinstitute.org

no tiene actualmente un organismo de ese tipo, debería establecer uno para cumplir esta función vital.

En particular, es esencial contar con mecanismos de supervisión establecidos en la ley que sean independientes, efectivos e imparciales. Deben tener facultades para monitorear y evaluar la idoneidad de las salvaguardas para los datos biométricos, incluso con respecto al intercambio internacional de dichos datos. Las personas deben poder comunicarse con el mecanismo de supervisión para obtener información sobre sus datos y presentar una queja, si consideran que sus derechos están en peligro. En la medida de lo posible, se debe proporcionar información a los interesados sobre el manejo de sus datos, de forma clara y simple.

Debe haber recursos adecuados previstos en la ley para el caso de violaciones de los derechos humanos en el manejo de datos biométricos, incluidas las violaciones del derecho a la privacidad.

2.3 Gestión de riesgos del sistema

La gestión de riesgos del sistema implica la catalogación de fallas del sistema, ya sea dentro de una parte (como un lector biométrico) o en su totalidad (la configuración del sistema), y determinar si dichas fallas conllevan el riesgo de que el sistema no funcione según lo previsto. Identifica amenazas y riesgos, luego analiza las consecuencias de una amenaza realizada o explotada y, finalmente, implementa mitigaciones cuando es necesario.

Los sistemas biométricos involucrados en las aplicaciones de lucha contra el terrorismo suelen ser complejos, e incluyen múltiples componentes informáticos, interacciones con el entorno de adquisición e interpretación humana. Esto conduce a una situación de riesgo multifacética con muchos puntos de falla potenciales, especialmente dado que los objetivos terroristas están muy motivados y, a menudo, cuentan con recursos suficientes para evitar los controles de seguridad.

La implementación de sistemas de lucha contra el terrorismo, sin la aplicación de una gestión de riesgos adecuada, puede llevar a una confianza irreal en la eficacia del sistema. Las consecuencias podrían incluir la identificación errónea de las personas buscadas, la filtración de información del listado de alerta altamente sensible o la inserción de código malicioso.

Los terroristas conocidos o sospechosos a menudo viajan con identidades falsas o falsificadas. Desde la perspectiva de la gestión de riesgos, por lo tanto, es importante que se hayan implementado correctamente aquellos sistemas de comparación biográfica tradicional (véase Sección 3.1.4.). Las autoridades nacionales de fronteras pueden implementar la verificación biométrica y realizar búsquedas en listados de alerta para ayudar a mitigar este riesgo (véase la Sección 3.3.1.2).

La configuración de un sistema biométrico depende altamente del contexto. Por ejemplo, cada aeropuerto es ambientalmente diferente y también puede variar en cuanto al comportamiento de los pasajeros y la demografía. Esto dará lugar a diferentes tipos de riesgos que requieren estrategias de mitigación. Una estrategia de mitigación vital común para todos, sin embargo, es realizar pruebas de penetración activa regulares por expertos en pruebas para asegurar que se conocen y comprenden los riesgos.

La gestión de riesgos es una actividad especializada y se rige por estándares internacionales y variantes nacionales (consulte las referencias al final de esta sección).

La continuidad del negocio es un factor crucial para cualquier usuario y los protocolos de contingencia deben ser parte integral de los procedimientos operativos estándar para cualquier sistema biométrico. En consecuencia, en el caso de que alguna parte del sistema falle y, por lo tanto, no pueda prestar un servicio normal, es habitual que haya una o más medidas urgentes disponibles para proporcionar cobertura de servicio temporal. Esto puede tomar la forma de una intervención manual por parte de operadores humanos (por ejemplo, los funcionarios fronterizos que asumen la tarea de verificar los pasaportes manualmente cuando las puertas biométricas automáticas fallan) o una reversión a un sistema de respaldo o una matriz de componentes.[44]

2.3.1 Vulnerabilidades y amenazas emergentes

A los fines del análisis, el panorama de amenazas en las aplicaciones biométricas de lucha contra el terrorismo se ha dividido en las siguientes áreas principales:

- *Sistemas informáticos en general:* toda la tecnología de *backend* utilizada para administrar bases de datos, transmitir la información en forma segura, auditar la actividad del usuario y prevenir virus. Esto debería estar cubierto por las mejores prácticas en seguridad informática para sistemas gubernamentales.
- *Sensores y entornos biométricos:* El tipo de tecnología empleada y los riesgos específicos. Por ejemplo, el uso de huellas dactilares falsas, anteojos oscuros o tecnología de cambio de voz.
- *Motores de comparación biométrica:* la configuración de los motores correspondientes, incluida la configuración del umbral, la detección de presentaciones sospechosas y la gestión de los listados de alerta.
- *Supervisión humana:* Todos los sistemas biométricos tendrán cierto nivel de falsas tasas de aceptación y rechazo, y esto es particularmente cierto en el contexto de las búsquedas de detección de delitos, ya que los datos biométricos registrados pueden ser de calidad variable (véase la Sección 1). Estas falsas aceptaciones y rechazos requerirán la investigación y evaluación de operadores debidamente capacitados. El manejo incorrecto puede llevar potencialmente a la detención de los individuos equivocados, prácticas de trabajo ineficaces o, alternativamente, a la pérdida de los objetivos del listado de alerta de alto nivel de amenaza.

Tabla 1

Áreas amenazadas	Responsabilidad	Consecuencias	Ejemplos de medidas de mitigación
Sistemas informáticos en general	Gerentes de seguridad informática	Exposición del listado de alerta, compromiso de la seguridad del sistema, alteración de las	Seguridad de las comunicaciones, antivirus, firewalls (rechazo del servicio), gestión de listados

[44] Un buen ejemplo de esto es la Matriz Redundante de Unidades Independientes (RAID) que se encuentra comúnmente en los Sistemas Automatizados de Identificación de Huellas Dactilares (AFIS). Esta configuración de unidades más pequeñas dentro del servidor se puede combinar para formar una gran matriz que mejora el rendimiento, la seguridad y también proporciona redundancia dentro del conjunto del servidor. La mayoría de los usuarios encargados del cumplimiento de la ley necesitarán sus AFIS para operar las 24 horas los 7 días a la semana los 365 días al año y, por lo tanto, no es una opción cerrar el sistema por un período prolongado de mantenimiento, actualización o reparación. El uso ágil de RAID duplicado por lo tanto permite que el sistema funcione continuamente porque más de un disco puede fallar o ser eliminado de las operaciones en vivo y los datos se conservarán en los discos activos para garantizar la entrega ininterrumpida del servicio al usuario.

		coincidencias. La plantilla biométrica robada puede ser utilizada para la reconstrucción de las características biométricas.	de alerta biográficos, interfaz segura con sistemas externos. Datos biométricos cancelables.
Sensores y entornos biométricos	Proveedor / Integrador del Sistema	Los objetivos del listado de alerta pueden evitar la detección engañando al sensor	Configuración del entorno, detección de la presentación del sospechoso, filtrado de calidad. Algoritmos de redireccionamiento (detección de la presentación del ataque).
Motores de comparación biométrica	Proveedor / Integrador del Sistema / Seguridad informática	Los objetivos del listado de alerta pueden evitar la detección	Afinación del sistema, gestión de calidad del registro, gestión backend adecuada. Uso de datos biométricos multi-modales en lugar de una sola modalidad biométrica.
Supervisión humana	Agencia de seguridad del gobierno / Operadores	Detención de las personas incorrectas, prácticas de trabajo ineficaces, pérdida de objetivos del listado de alerta de alta amenaza.	Educación, capacitación y certificación, auditoría, diseño de interfaz del usuario, terminología adecuada

2.3.2 Amenazas por modalidad

Los sistemas biométricos tienen un complejo panorama de amenazas que aún está evolucionando a medida que la tecnología se implementa más ampliamente. Está fuera del alcance de este documento proporcionar un desglose completo de todas las vulnerabilidades y riesgos en esta área; sin embargo, estos están documentados en la norma ISO / IEC 30107-2_2017 [1] y también en algunos ejemplos específicos para agencias de control de fronteras [2].

Las modalidades biométricas habituales utilizadas para combatir el terrorismo son:

Rostro: el rostro está comúnmente disponible y se adquiere fácilmente mediante sistemas de captura próximos o remotos, pero estos están sujetos a desafíos particulares y limitaciones técnicas que pueden resultar en imágenes faciales de baja calidad. Estas imágenes afectan significativamente la probabilidad de detección correcta (o, a la inversa, el número de falsas aceptaciones generadas por el sistema). La calidad de la foto de registro (la foto utilizada para crear el listado de alerta) y la foto tomada desde una cámara pueden tener un impacto. En el documento de referencia [3] se pueden encontrar ejemplos sobre cómo mejorar el reconocimiento facial. Los atributos de calidad específicos incluyen: iluminación, postura, posición de la cámara, expresión, cubiertas para la cabeza, anteojos, barbas, resolución (píxeles entre los ojos) y edad. Algunas de las vulnerabilidades comunes para el rostro incluyen:

- *Fraude por similitud:* un documento de identidad utilizado por alguien que se parece al sujeto original. Esto permite que la persona incluida en un listado de alerta reclame que no es el objetivo correcto en caso de ser detectada.

- *Máscaras:* cada vez hay mayor disponibilidad de máscaras de látex que son difíciles de detectar por observación casual.
- *Maquillaje:* si la intención es evitar la detección, el uso correcto del maquillaje puede ocultar los rasgos faciales y a su vez parecer naturales para un observador humano.
- *Anteojos:* Los anteojos oscuros o con borde grueso pueden ocultar una parte importante de las características faciales utilizadas para el reconocimiento.
- *Comportamiento:* si los objetivos sospechan que están siendo observados, el uso de un teléfono móvil y mirar hacia el suelo puede dificultar la obtención de una imagen de calidad.
- *Transformaciones:* muestras biométricas (por ejemplo, imágenes faciales) de dos o más donantes que se fusionan para permitir la verificación exitosa de cualquiera de los sujetos donantes contra la identidad transformada.

Huellas dactilares: La biometría de las huellas dactilares se utiliza en todo el mundo para el cumplimiento de la ley, por lo que hay muchas bases de datos y listados de alerta existentes que contienen plantillas de huellas dactilares (véase la Sección 1). Algunas vulnerabilidades comunes de los sistemas biométricos basados en huellas dactilares incluyen:

- *Dedos falsos:* el uso de huellas dactilares falsas hechas de sustancias que imitan las propiedades de la piel. Se pueden usar individualmente en cada dedo o incorporarse como parte de un guante completo para cada mano.
- *Daño premeditado:* cuando un objetivo sospecha que puede estar bajo vigilancia, puede intentar dañarse las huellas dactilares utilizando productos químicos, sustancias abrasivas u otras técnicas.
- *Huellas dactilares post mortem:* los terroristas han utilizado las impresiones de huella dactilar de los fallecidos para crear identidades con el fin de abrir cuentas bancarias y realizar operaciones financieras para financiar sus operaciones.

Iris: El reconocimiento del iris proporciona una modalidad biométrica precisa y confiable. Es estable en el tiempo y difícil de falsificar. Se está llevando a cabo un considerable trabajo de investigación y desarrollo en sistemas de reconocimiento de iris para contrarrestar la falsificación y también presentarlos como una modalidad alternativa / adicional para fines de gestión de fronteras. Las vulnerabilidades incluyen:

- Uso de *lentes de contacto cosméticas* con un patrón de iris impreso.
- Uso de imágenes faciales de alta calidad disponibles en Internet para *impresión de ojos*.
- *Dilatación de la pupila* en la mayor medida posible. De esta manera, es posible que un escáner no reconozca el patrón del iris (el rendimiento del reconocimiento del iris se degrada cuando se aplica un algoritmo de coincidencia al mismo ojo que tiene un tamaño de pupila considerablemente diferente).
- *Lentes de contacto con una matriz de puntos* con un patrón falso directamente en el ojo de la persona. Esto podría hacer que el sistema de escaneo del iris no reconozca un iris en su base de datos.
- *Lentes esclerales con un iris pintado*. Este tipo de lentes cubre toda el área visible del globo ocular, y una persona que la use presentará una apariencia de un patrón de ojos completamente diferente.
- *Implantación quirúrgica de un iris de color* sobre el iris real de una persona. Si bien muchas personas optan por la cirugía simplemente para cambiar su color de ojos, una persona que quiere esconder su identidad también podría usar este procedimiento.

- La coincidencia requiere que las plantillas de referencia se encuentren disponibles durante la autenticación, lo que crea oportunidades para que un atacante robe las plantillas, lo que a su vez permite nuevos ataques.

Voz: La tecnología de identificación de voz se puede usar para monitorear llamadas telefónicas y generar alertas para personas específicas. La identificación de la voz generalmente tiene una precisión marginal para grandes volúmenes de operaciones o grandes bases de datos (particularmente en diferentes canales telefónicos). Sin embargo, la aplicación de esta tecnología puede ser efectiva cuando el número de llamadas a buscar y el número de personas en el listado de alertas es relativamente pequeño y limitado. Algunas vulnerabilidades comunes para la voz incluyen:

- *Modificadores de voz:* Existe una serie de aplicaciones disponibles para teléfonos inteligentes que permiten modificar la voz.
- *Voces sintéticas:* un vector de amenaza emergente es el uso de herramientas que pueden ser entrenadas en una voz de tal manera que la voz sintética puede leer un mensaje escrito a máquina de forma natural.

2.3.3 Calidad del registro

Independientemente de la modalidad, es probable que no valga la pena incluir datos biométricos de muy baja calidad como parte de un listado de alerta. Cuando la calidad es insuficiente, es probable que los datos biométricos pierdan coincidencias genuinas y generen un alto número de aceptaciones falsas. La medición y gestión de la calidad biométrica es un aspecto importante para garantizar un sistema biométrico preciso. Cada modalidad tiene sus propias medidas de calidad, por ejemplo, para el rostro hay cuestiones como la iluminación, la postura y las cubiertas de la cabeza. Cualquier factor que degrade u oculte la biometría durante el proceso de registro afectará la capacidad de búsqueda y comparación del sistema. La definición de las métricas de calidad se incluye en una serie de estándares ISO (véase la Sección 2.4).

2.3.4 Rendimiento y gestión de capacidad

El rendimiento del sistema depende naturalmente de los recursos informáticos disponibles para la comparación y el procesamiento. La igualación biométrica es habitualmente un proceso informático costoso, particularmente en lo que respecta a los grandes listados de alerta. Una de las mayores restricciones en la igualación biométrica son los recursos humanos. Cada coincidencia que necesita ser investigada requiere un operador capacitado para hacer una evaluación. Esto significa, por ejemplo, que incluso si se utiliza un sistema facial con un equilibrio de umbral finamente ajustado, el número de aceptaciones falsas que deben abordarse en un entorno ocupado podría ser considerable. Comprender estos requisitos es una consideración presupuestaria importante, no solo para anticipar los requisitos de construcción inicial, sino también para operaciones futuras.

2.3.5 Robo de identidad

El robo de identidad, en general, es la adquisición no autorizada de los datos personales de una persona, por ejemplo, nombre, fecha de nacimiento, dirección, etc. para cometer un delito y, en particular, fraude, a través del uso de datos robados para realizar solicitudes de préstamos o tarjetas de crédito falsas o comprar productos de alto valor. El robo de identidad que involucra datos

biométricos plantea problemas importantes porque las características biométricas generalmente permanecen con una persona a lo largo de su vida y no se pueden restablecer fácilmente de la misma manera que un código de identificación personal o contraseña. El robo de datos biométricos puede relacionarse con la biometría física real de la persona, por ejemplo, la creación de una réplica de una huella dactilar o máscara facial o puede ser el robo de la plantilla biométrica incluida en una aplicación o base de datos. Se han desarrollado varias medidas de mitigación importantes para combatir estos riesgos y entre las principales se incluyen:

Detección de vitalidad: se incorporan varios sensores en los dispositivos de captura biométrica para observar más allá del sustrato de los datos biométricos que se presentan y diferenciar entre piel viva y un artefacto falso.

Datos biométricos cancelables: Cuando se registra un dato biométrico en el sistema, sus características se distorsionan intencionalmente de manera repetida. Si posteriormente se compromete o se roba la plantilla, se crea una plantilla de reemplazo del mismo dato biométrico utilizando diferentes características de distorsión para que la plantilla robada se vuelva inmediatamente redundante. Por lo tanto, el mismo dato biométrico puede usarse en una variedad de aplicaciones, pero las plantillas serán todas diferentes. Las características biométricas "no distorsionadas" originales nunca se registran, lo que proporciona una mayor protección de la privacidad y seguridad para el usuario.

Se debe tener en cuenta que cuando se utilizan datos biométricos junto con documentos de identidad (como pasaportes), el riesgo de robo de identidad se reduce al mínimo, ya que si un dato biométrico es 'robado' o copiado, el atacante todavía necesita un documento válido que puede, si es necesario, tornarse nulo. Los datos biométricos, como por ejemplo, un rostro, pueden capturarse en forma encubierta o de un recurso en línea por aquellos que desean obtener la imagen. Esto significa que las autoridades que utilizan el rostro como dato biométrico en documentos formales deben asegurarse de que han considerado el riesgo de este tipo de robo y han adoptado las medidas de mitigación adecuadas.

2.4 Normas internacionales

2.4.1 Normas técnicas operativas

Resulta esencial que todo sistema biométrico para combatir el terrorismo sea seguro, confiable y que cubra los requerimientos comerciales específicos del usuario. Estos requerimientos se basan en factores clave tales como:

- Pruebas del sistema para garantizar la conformidad con las especificaciones y mediciones de rendimiento actuales y futuras
- Entorno operativo y red seguros
- Evaluaciones de impacto legal y sobre la privacidad
- Gestión de riesgos para todo el sistema
- Competencia demostrable del operador
- Manejo de datos y garantía de integridad para todas las características del sistema tales como los dispositivos de captura de datos biométricos, el registro de datos y la garantía de las credenciales de identidad, el almacenamiento y la recuperación de los datos, el desempeño de las coincidencias y las tasas de error y cualquier metadato no biométrico
- Confiabilidad del software y del hardware

- Interoperabilidad: transmisión e intercambio de datos con otros sistemas
- Diseño de la interfaz humana: facilidad de uso para (1) la adquisición y el registro de los sujetos de datos y (2) operadores del sistema: conjunto de herramientas, estaciones de trabajo, ergonomía y entorno

Existe una amplia gama de normas internacionales, regionales y nacionales para cubrir estos elementos esenciales y funciones periféricas. Los propietarios, usuarios y clientes de sistemas biométricos confían en estas normas para garantizar que su aplicación funcione de manera efectiva a lo largo de su ciclo de vida y de acuerdo con las especificaciones de desempeño del fabricante. También dependen de normas para garantizar procesos como la adquisición (véase la Sección 2.4), el mantenimiento y la actualización de un sistema biométrico, especialmente si forma parte de una red nacional o internacional más amplia que intercambia datos. Es poco probable que los socios o socios potenciales en dicha red acepten participar si algunos miembros de la red no operaran sus respectivos sistemas biométricos de conformidad con las normas nacionales o internacionales.

La Organización Internacional de Normalización[45] (ISO) desarrolla y publica normas para una amplia gama de industrias, incluyendo la biometría y la ciencia forense. La ISO es una federación mundial de organismos de normalización nacionales, de 162 países, que contribuyen a la producción de normas a través de la membresía de los diversos comités de temas. Otros países pueden unirse como miembros corresponsales o suscriptores para recibir información sobre las normas.

ISO también tiene dos comités conjuntos con la Comisión Electrotécnica Internacional[46] (IEC) que establecen normas y Evaluaciones de Conformidad (CA) para todos los productos eléctricos, electrónicos y relacionados. Una evaluación de conformidad puede asegurar a un posible comprador, que tal vez no entienda completamente las complejidades del sistema o producto, que el mismo cumple con los estándares técnicos y de seguridad requeridos o con otros criterios especificados. Hay tres tipos de evaluaciones de conformidad. La Evaluación de Conformidad de Primera Parte es realizada por el proveedor, la Evaluación de Conformidad de Segunda Parte es realizada por el usuario, pero la Evaluación de Conformidad más sólida es la Evaluación de Conformidad de Terceros, que es realizada por organismos independientes. El proceso se conoce como Certificación porque generalmente se emite un certificado luego de una evaluación exitosa. Su propósito es verificar que un producto o servicio cumple con una determinada especificación o norma ISO/IEC.

Los organismos regionales también pueden establecer normas para armonizar los sistemas y las prácticas de trabajo de un grupo de países. Por ejemplo, el Comité Europeo de Normalización[47] (CEN) reúne a los Organismos Nacionales de Normalización de 34 países europeos y tiene un Grupo de trabajo específico para biometría (WG18) que adapta los estándares de organizaciones internacionales o nacionales para cumplir con los requisitos europeos tales como privacidad y protección de datos.

Algunos estándares son establecidos a nivel nacional por la organización relevante para ese país, por ejemplo, en EE.UU. hay organismos como el *American National Standards Institute* (Instituto Nacional de Normalización Estadounidense (ANSI)) y el *National Institute of Standards and Technology* (Instituto Nacional de Normas y Tecnología (NIST)) que establecen normas que se aplican a la ciencia forense y a las aplicaciones biométricas asociadas. Las normas NIST han sido adoptadas ampliamente por muchos países en áreas clave como la transmisión electrónica de huellas dactilares a través de redes. El NIST también lleva a cabo las pruebas competitivas y la clasificación de los algoritmos de búsqueda y comparación biométricos disponibles comercialmente para otras modalidades

[45] http://www.iso.org
[46] http://www.iec.ch
[47] https://www.cen.eu

biométricas como el rostro y el iris[48]. Esto permite a los posibles compradores de sistemas de concordancia biométrica obtener información objetiva sobre el rendimiento relativo de los algoritmos utilizados por fabricantes rivales en el mercado internacional.

2.4.2 Normas científicas operativas y procedimientos de gestión de la calidad

Además de las normas técnicas y los programas de certificación disponibles para los sistemas biométricos, existen normas ISO para procedimientos de ciencia forense, como ISO/IEC 17025: 2017 "requisitos generales para la competencia de los laboratorios de ensayo y calibración". Esta norma aborda los procedimientos y las competencias necesarias para realizar ensayos y/o calibraciones científicas, incluyendo muestreo. La norma analiza la gestión de los procesos, así como la competencia e imparcialidad de los científicos y la validez de sus métodos. Utiliza auditorías internas y ensayos, realizados por el propio laboratorio, y auditorías externas y pruebas de aptitud, realizadas y supervisadas por organismos de acreditación externos para impulsar la mejora continua y acreditar al laboratorio. Estas inspecciones periódicas independientes determinan si el laboratorio cumple con los estándares requeridos para lograr o mantener la acreditación según ISO17025:2017. La acreditación confirma que los laboratorios cuentan con un Sistema de Gestión de Calidad (QMS) completamente operativo y son competentes para realizar ensayos y calibraciones científicas de manera consistente de acuerdo con la norma.

El QMS analiza regularmente todos los factores que contribuyen al desempeño efectivo del laboratorio y, lo más importante, cualquier instancia de incumplimiento. Los procedimientos de acción correctiva se utilizan para identificar la causa raíz de cualquier incumplimiento y se formulan acciones preventivas para detener una recurrencia. Los análisis de gestión interna evalúan sistemáticamente el desempeño del laboratorio en comparación con una lista de verificación completa de los requisitos de organización, recursos, procesos y gestión que se basan en el Manual de Calidad del laboratorio.

Existen estándares que se pueden aplicar a otras áreas de la ciencia forense, como la investigación de la escena del crimen (por ejemplo, ISO 17020: 2012). Por lo tanto, es posible y muy importante tener un enfoque basado en estándares en las operaciones de lucha contra el terrorismo que cubra todos los procesos de la ciencia forense desde la escena del crimen hasta la sala de audiencias, incluyendo:

- Gestión y examen de la escena del crimen, incluyendo estrategias forenses y biométricas (Véase la Sección 3.3.3.2.), evaluaciones interpretativas, coordinación de recursos, métodos de muestreo, procedimientos anti-contaminación, materiales de embalaje y examen de sospechosos, testigos y víctimas.
- Procesos de laboratorio, incluyendo muestreo, análisis, gestión de bases de datos, competencia del personal y presentación de informes de resultados.
- Pruebas judiciales: protocolos de peritos, imparcialidad y técnicas de presentación de pruebas.

[48] http://www.nist.gov

2.5 Adquisición y gestión de recursos

2.5.1 Adquisición

Los gobiernos nacionales tendrán su propio marco regulatorio y criterios de selección para controlar la adquisición de bienes y servicios. Sin embargo, hay una serie de puntos pertinentes que deben considerarse al evaluar la necesidad de un sistema biométrico y algunos aspectos específicos relacionados con la compra de aplicaciones que se utilizarán para contrarrestar la amenaza del terrorismo:

Requisitos comerciales: las ventajas y las razones para utilizar la biometría en lugar de formas alternativas de reconocimiento y autenticación deben estar claramente articuladas en el plan de negocios. Los beneficios deben sopesarse cuidadosamente frente a las posibles desventajas, como el costo, las vulnerabilidades técnicas, las posibles objeciones y la resistencia del público/clientes, las preocupaciones éticas y otras amenazas identificadas por el proceso de Evaluación de Riesgos. Los volúmenes de usuarios actuales y futuros y los niveles de capacidad de la base de datos deben evaluarse cuidadosamente para garantizar que el sistema pueda hacer frente a los rendimientos esperados, especialmente en los momentos de mayor demanda. (Véase la Sección 2.3.4.).

Privacidad y protección de datos: (véase la Sección 2.2) La capacidad de un sistema biométrico para identificar terroristas conocidos y sospechosos tiene que cumplir con los derechos de las personas a que se respete su privacidad y sus datos personales protegidos de conformidad con las leyes nacionales e internacionales. Los sistemas biométricos pueden cometer errores, ya sea identificando erróneamente o no identificando a las personas, y ambos conllevan riesgos sustanciales para la reputación de los propietarios de los datos. Estos aspectos deben ser considerados cuidadosamente durante la fase de diseño de cualquier aplicación biométrica y se deben implementar procedimientos adecuados para tratar y mitigar tales incidentes cuando ocurren.

Nota: Los recursos necesarios para ampliar la competencia de cualquier organismo de supervisión de la privacidad existente o para crear uno nuevo (véase la Sección 2.2.7) deben incluirse en cualquier política nacional o regional o plan de proyecto que busque desarrollar sistemas biométricos contra el terrorismo.

Seguridad: cualquier parte de un sistema o red biométrica que utilice datos relacionados con terroristas y actos de terrorismo puede convertirse en un objetivo de ataques electrónicos/cibernéticos o físicos externos o interferencia interna o sabotaje por mala conducta del personal. En consecuencia, debe haber altos niveles de seguridad en capas para proteger los entornos operativos, el hardware, el software, la red de comunicaciones y los datos almacenados. También debe considerarse la posibilidad de investigar al personal que opera el sistema y verificar que no son vulnerables a ninguna forma de coerción por parte de terroristas o sus asociados. Deben realizarse auditorías regulares con el objetivo de identificar la corrupción interna y la evidencia de mala práctica. Otras amenazas, como los ataques de presentación (véase la Sección 2.3) también deben abordarse y prevenirse como parte de la estrategia de seguridad general.

Rendimiento: las aplicaciones biométricas que se utilizan para combatir el terrorismo deben operar con los más altos grados de precisión, es decir, tasas de error extremadamente bajas y al mismo tiempo mantener una tasa de rendimiento aceptable. Muchas vidas pueden ponerse en riesgo si el sistema no identifica a un terrorista, por el motivo que sea, en cualquier etapa de una operación. Es probable que la adquisición, el mantenimiento y la actualización periódica de este nivel de

rendimiento biométrico necesiten una financiación significativa durante toda la vida útil del sistema. Este alto riesgo también significa que los procedimientos de gestión de excepciones deben ser completos y exhaustivos para evitar que los terroristas eviten deliberadamente los controles biométricos en favor de sistemas de respaldo potencialmente menos sólidos.

Modalidad biométrica: la decisión de seleccionar una o más modalidades particulares puede depender de factores tales como:

- Accesibilidad y funcionalidad: una decisión de adquisición fundamental es si se debe emplear un solo modo biométrico para la aplicación o utilizar un enfoque multimodal. La modalidad o modalidades seleccionadas deben ser adecuadas para las tareas de comparación de verificación (1: 1) e identificación (1: n) que deben realizar. Los sistemas de un solo modo son normalmente menos costosos de comprar y operar, pero no pueden satisfacer a todos en una población. Puede haber, por ejemplo, un número significativo de personas que no pueden registrarse en un sistema de huellas dactilares debido a que sus manos y dedos están lesionados o mutilados o su piel está dañada por motivos de trabajo, por ejemplo, aquellos que trabajan con productos químicos o ciertos tipos de trabajo manual que pueden ocultar, distorsionar o destruir las crestas de fricción en la superficie de los dedos y las manos. Si la aplicación biométrica necesita registrar a tantas personas como sea posible, es preferible un sistema multimodal (por ejemplo, huellas dactilares e iris), ya que podrá capturar datos biométricos de un porcentaje mucho mayor de la población requerida. Se debe tomar una decisión de compra similar con respecto a la funcionalidad, por ejemplo, ¿es recomendable comprar una aplicación biométrica para una sola función, como un sistema de huella dactilar de antecedentes policiales, o se le podría dar un valor agregado a la inversión mediante la creación de una red multifuncional como los antecedentes penales más la base de datos de delitos combinada con aplicaciones de gestión de fronteras? Incluso es posible ampliar las funciones y las modalidades, si las leyes nacionales lo permiten, para que un país finalmente ejecute solo un sistema biométrico. Algunos países están adoptando este enfoque multimodal y multifuncional a fin de realizar economías de escala, racionalizar la cantidad de personal mediante la combinación de funciones similares y así contar solo con una única estructura de gobierno y gestión para el sistema nacional.
- Compatibilidad de las modalidades y pruebas futuras: un tema clave, al seleccionar la mejor modalidad para una aplicación de terrorismo, será la posibilidad de obtener y compartir dichos datos con socios nacionales o internacionales para identificar posibles terroristas. Por ejemplo, puede haber una red regional de países que comparten datos de huella dactilar de todos los solicitantes de visa que ingresan a través de sus respectivas fronteras. Por lo tanto, cualquier país que desee participar y obtener los beneficios de esta red necesitaría usar huellas dactilares para su sistema biométrico de solicitante de visa, incluso si se recomendara originalmente otra modalidad, por otras razones, en el caso de negocios original. Una extensión de esto sería la consideración de ciertas modalidades, ya que también son elementos biométricos comunes en la escena del crimen y permitirían realizar búsquedas cruzadas con fines de lucha contra el terrorismo. Por ejemplo, las huellas dactilares y el rostro pueden tener preferencia respeto de las modalidades de iris o venas de la mano.
- Captura y registro de datos: por ejemplo, ¿es preferible que la persona esté en contacto o esté cerca del dispositivo de captura o la captura remota resulta ser una mejor opción para el entorno operativo?
- Aceptabilidad y operatividad del rendimiento: algunas modalidades biométricas pueden estar sujetas a preconceptos del cliente, preocupaciones válidas o incluso estigma social, por ejemplo, las huellas dactilares se asocian a menudo con la criminalidad debido a su legado histórico en la labor policial. Se pueden preferir ciertas modalidades porque facilitan la

captura de datos y los procedimientos de registro más rápidos y sencillos, lo que a menudo es una consideración para las aplicaciones que operan un gran volumen de clientes de forma regular, por ejemplo, los puntos de control fronterizos.

2.5.2 Gestión de recursos

La adquisición de una importante aplicación biométrica de gran volumen requiere una considerable inversión de capital para comprar el hardware y el software necesarios y crear entornos operativos adecuados y seguros, como estaciones de registro y captura de datos, salas de servidores, suites de operadores, etc. Además, en el caso de algunas aplicaciones, puede haber costos asociados con la contratación de personal, la capacitación y, si se utiliza un enfoque basado en estándares, la acreditación de forma continua.

Una vez que se haya instalado el sistema y se hayan completado con éxito las pruebas de aceptación, se realizará un trabajo de mantenimiento regular y, ocasionalmente, actualizaciones de seguridad y rendimiento del software para financiar los presupuestos anuales. Esta financiación es adicional al gasto de ingresos anuales básicos para los salarios del personal y al funcionamiento rutinario y efectivo del sistema. Por lo general, se requiere que los sistemas biométricos operen las 24 horas del día durante todo el año y con un tiempo de inactividad mínimo del sistema.

La investigación y el desarrollo comercial mundial moderno en materia de tecnologías biométricas introducen constantemente nuevas iteraciones de software y capacidades actualizadas a un ritmo rápido. Muchos sistemas biométricos funcionan durante veinte años o más y, por lo tanto, requerirán muchas mejoras de rendimiento para evitar ser redundantes. Cualquier aplicación biométrica puede verse seriamente comprometida o fallar por completo si no se mantiene y actualiza regularmente durante su vida útil[49].

Los procedimientos de adquisición y planificación también deben tener en cuenta otros requisitos futuros, como la necesidad de aumentar la capacidad de procesamiento para hacer frente al aumento de la demanda, lo que luego requeriría la ampliación de la capacidad de almacenamiento de la base de datos como resultado directo. También puede haber una necesidad operacional para conectarse y ser interoperable con otros sistemas o bases de datos. Cualquiera de estas mejoras requeriría fondos futuros adicionales que pueden no estar disponibles si los presupuestos se reducen posteriormente o si otras demandas de la competencia tienen prioridad. Por lo tanto, es aconsejable anticipar tales características y requisitos en la etapa de planificación y construir tantos de estos factores como sea posible en los nuevos sistemas. Las aplicaciones deben diseñarse con capacidad de almacenamiento y procesamiento adicional o se debe incluir y acordar el costo de dichas actualizaciones en los contratos de compra. La conectividad y la interoperabilidad con otros sistemas también pueden integrarse en un nuevo sistema si las capacidades de la red se consideran desde el principio. Es considerablemente menos costoso construir interfaces de este tipo en la fase de diseño que presentarlas más adelante, ya que pueden interrumpir el trabajo operativo y probablemente requieran la instalación o reconfiguración de componentes y rutas de conectividad en ambos/todos los sistemas.

[49] Es por estas razones que la OACI exige el uso de imágenes en lugar de plantillas en los pasaportes electrónicos. Esta prueba a futuro asegura que las actualizaciones a algoritmos de coincidencia mejorados sigan siendo una opción para la incorporación en el sistema de inspección de fronteras que se basa en datos biométricos (generalmente imágenes de rostros) leídos de pasaportes electrónicos.

2.6 Prácticas recomendadas

a) Los Estados deberían adoptar un enfoque basado en los derechos humanos para el uso de tecnología biométrica para combatir el terrorismo que incluya el uso de garantías procesales y una supervisión efectiva de su aplicación. Esto incluye establecer o ampliar la competencia de los organismos de supervisión independientes, apropiados y existentes para supervisar la implementación de la legislación de privacidad relevante y la provisión de recursos efectivos en caso de violaciones a este respecto. Esto debería complementarse con un proceso de revisión ética que informe toda la política nacional y la toma de decisiones con respecto al uso de la biometría a los fines de combatir el terrorismo.

b) La aplicación de la tecnología biométrica para combatir el terrorismo internacional y los delitos asociados debe cumplir con los derechos fundamentales de todos los individuos a la privacidad y la protección legal de sus datos personales, incluyendo los datos biométricos.

c) Los sistemas biométricos pueden ser vulnerables a fallas y muchas formas diferentes de ataque deliberado. Por lo tanto, se aconseja a los Estados la realización de evaluaciones periódicas de los riesgos de los procesos de extremo a extremo de sus aplicaciones biométricas para mitigar las amenazas actuales o emergentes.

d) Se recomienda que los Estados operen todos sus sistemas biométricos de conformidad con las normas técnicas internacionales y que obtengan la acreditación formal de sus procesos de ciencia forense y gestión de calidad de acuerdo con las normas científicas internacionales. Esto no solo proporcionará una base sólida para un procesamiento biométrico efectivo, sino que también tranquilizará a los socios internacionales que deseen compartir datos biométricos.

e) La adquisición de sistemas biométricos requiere una planificación estratégica a largo plazo que aborde los requisitos de recursos actuales y futuros, por lo que los Estados deberían considerar:

- Inversión de capital inicial para adquirir y probar el sistema
- Gasto anual sostenible en personal y mantenimiento del sistema más actualizaciones de seguridad y rendimiento
- Presupuestos, capacidad de la base de datos y potencia de procesamiento requerida para la vida útil del sistema
- Conectividad potencial e interoperación con redes nacionales e internacionales y compatibilidad de las modalidades
- Equilibrar los requisitos operativos clave de cualquier sistema biométrico de lucha contra el terrorismo en términos de seguridad, acceso y uso por parte de los clientes, volúmenes de procesamiento y velocidad de procesamiento.

2.6.1 Documentos de referencia

Resoluciones del Consejo de Seguridad de las Naciones Unidas 1373(2001), 1624 (2005), 2178 (2014), 2195 (2014) y 2396 (2017) y Resoluciones de la Asamblea General de las Naciones Unidas A/RES/68/276 y A/70/L.55

Publicación de la Agencia de los Derechos Fundamentales de la Unión Europea 'Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights
http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

S/2015/975, párrafo. 8; S/2015/939, Principio 15 (e).

Resolución del Consejo de Derechos Humanos A/HRC/RES/34/7 (2017).

Comentario General N° 16 del Comité de Derechos Humanos: Artículo 17 (Derecho a la privacidad), párrafos 3-4.

Reporte del Relator Especial sobre el derecho a la privacidad, A/HRC/31/64 (2016).

Declaración Universal de Derechos Humanos y ICCPR, preámbulo. ICCPR, Art. 2(1), 2(3), 9, 14 y 26.

Comité de Derechos Humanos, comentario general N° 16 (1988), Véase: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

Resolución de la Asamblea General 45/95 (1990) sobre Principios rectores para la reglamentación de los archivos computarizados de datos personales y el Reglamento General de Protección de Datos de la Unión Europea de 2018, Articulo 51 (Autoridad de Control).

Reporte del Relator Especial sobre el derecho a la privacidad, A/HRC/31/64 (2016).

Declaración Universal de Derechos Humanos, preámbulo.

Página web de Fondo Monetario Internacional en donde se enuncian los instrumentos contra el lavado de dinero y otros instrumentos para combatir el fraude www.imf.org

Organización Internacional de Normalización http://www.iso.org

Comisión Electrotécnica Internacional http://www.iec.ch

Comité Europeo de Normalización https://www.cen.eu

Instituto Nacional de Normas y Tecnología (EE.UU.) http://www.nist.gov

Reglamento General de Protección de Datos de la Unión Europea 2018, Artículo 7 (Consentimiento), Artículo 17 (Derecho de supresión), Artículo 15 (Derecho de acceso del interesado)

Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos sobre la libertad de expresión.

ACNUR "Cómo abordar el tema de seguridad sin perjudicar la protección de los refugiados" http://www.refworld.org/docid/5672aed34.html

Declaración de Derechos Humanos de las Naciones Unidas, Artículo 9 (Nadie puede ser arbitrariamente detenido ni desterrado) y Artículo 10 (Derecho a ser considerado inocente hasta que se pruebe lo contrario)

Declaración de Madrid de los Ministros de Asuntos Exteriores en la reunión especial del Comité contra el Terrorismo del Consejo de Seguridad celebrada el 28 de julio de 2015.

Grupo de ética sobre biometría y ciencias forenses del Reino Unido *http://www.gov.uk/government/publications/biometrics-and-forensics-etchics-group*

Directrices de Privacidad sobre Datos Biométricos del Biometrics Institute diseñadas para uso internacional *www.biometricsinstitute.org*

ISO/IEC 30107-2_2017: Detección de ataques en la presentación de datos biométricos. Formatos de datos

[2] Frontex, Sistemas de evaluación y prueba de la vulnerabilidad de los controles automatizados de fronteras (Abc) (2017)

[3] Ted Dunstone y Neil Yager, Biometric System and Data Analysis: Design, Evaluation and Data Mining (2008) Springer.

ISO/IEC 27001:2013 Sistemas informáticos – Técnicas de seguridad – Sistemas de gestión de la seguridad informática – Requisitos

ISO 31000:2009 Gestión de riesgos – Principios y directrices

IEC 31010:2009 – Gestión de riesgos – Técnicas de evaluación de riesgos

NIST SP 800-30 Guía para la realización de evaluaciones de riesgo

NIST SP 800-37 Guía para la aplicación del marco de gestión de riesgos a los sistemas informáticos federales: enfoque según el ciclo de vida de la seguridad

ISO/IEC 17025:2017 Requisitos generales de competencia de los laboratorios de ensayo y calibración

3. Sistemas y bases de datos biométricos para combatir el terrorismo

La Sección 3 ofrece una descripción general de los sistemas y bases de datos biométricos vigentes para combatir el terrorismo en todo el espectro de aplicación de la ley, gestión de fronteras y aplicaciones militares. También considera los beneficios de compartir datos biométricos a escala bilateral, multilateral, regional y global y cómo los datos biométricos, cuando se usan con otros datos de inteligencia, se pueden usar de manera proactiva para prevenir actos de terrorismo además de su función tradicional como herramienta de investigación. Las acciones tomadas por las autoridades, como resultado de las comparaciones biométricas, se consideran en el contexto de los derechos humanos internacionales y la necesidad de una respuesta plenamente informada, legal y proporcionada. La parte final de la sección trata sobre la inclusión de datos biométricos en las estrategias de lucha contra el terrorismo de los Estados Miembros y las Regiones y el papel esencial de los organismos encargados de hacer cumplir la ley y las fronteras en cuanto al apoyo activo de estas estrategias.

3.1. Sistemas y bases de datos biométricos vigentes para combatir el terrorismo

3.1.1. Aplicaciones fronterizas

La gestión cada vez más sofisticada de las fronteras[50] desempeña un papel crucial en la lucha contra el terrorismo en general y en la interceptación de combatientes terroristas extranjeros en particular. En gran medida, la modalidad de transporte determina las características y el alcance del funcionamiento de los Puntos de Cruce de Frontera (BCP). Para viajes aéreos internacionales, los BCP están altamente estandarizados. Para los viajes por tierra, agua y mar, generalmente hay dos tipos de BCP, uno para todos los viajeros internacionales y uno reservado para el uso de los nacionales desde cualquier lado del límite. Los viajeros internacionales están obligados a presentarse ante un BCP para ingresar a un estado legalmente. Los BCP para las poblaciones locales están, en general, ubicados en las fronteras terrestres o puertos designados que sirven a dos o más estados próximos. Estos BCP locales a menudo se implementan en conjunto con las Zonas Económicas, donde el límite está en general 25 km tierra adentro en ambos lados y está abierto a nacionales de ambos lados de la frontera. Estos BCP locales no pueden ser utilizados por otros viajeros internacionales.

Los BCP en las fronteras internacionales actúan como un filtro efectivo que puede expandirse o contraerse según el nivel de amenaza. En general, el filtro estará en un nivel "Normal" pero en momentos de mayor amenaza cambiará a Código Naranja o incluso Código Rojo (o alertas equivalentes) y, en algunas situaciones extremas, la frontera se cerrará completamente. En situaciones donde un gran número de personas necesitan ingresar al país rápidamente, como un desastre natural o causado por el hombre en un país vecino, la frontera puede abrirse para permitir

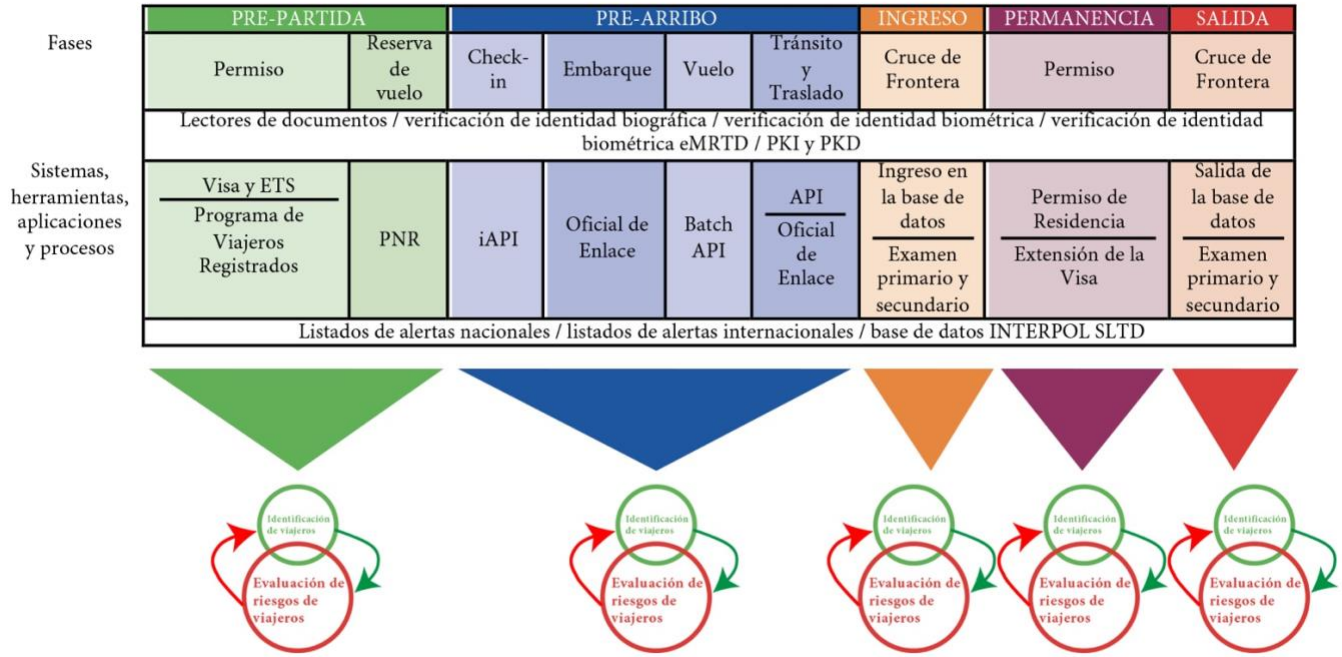
[50] El término "límite" se usa generalmente en referencia a la línea que divide el territorio o el espacio marítimo de dos Estados, mientras que una "frontera" es lo que debe cruzarse para ingresar a un estado. A veces coinciden exactamente, pero es más común que la frontera incluya infraestructura como los puestos de control de inmigración, instalaciones de aduanas, cercas y caminos de patrullaje que se extienden más allá del límite; y, en el caso de los aeropuertos y puertos marítimos internacionales, la frontera puede estar ubicada a cientos de kilómetros del límite. Un límite es esencialmente una línea de definición, mientras que una frontera suele ser una entidad más compleja que comprende varias líneas y/o zonas, cuya función principal es la regulación del movimiento de personas y bienes". *Profesor Martin Pratt de la Universidad de Durham en el Reino Unido.*

un fácil acceso y los controles formales requeridos se realizarán más adelante una vez que las personas hayan llegado a las áreas de seguridad a través de la frontera.

El cruce de fronteras de viajeros y mercaderías es realizado por agencias responsables de inmigración, control de acceso y seguridad, cumplimiento de la ley, aduanas y cuarentena. Las agencias fronterizas requieren un entorno operativo eficiente con personal bien capacitado y motivado, tecnología sofisticada e información actualizada. Un elemento importante de los BCP modernos es la adición de aplicaciones biométricas que ayudan en gran medida a los procesos de gestión de fronteras. Estas forman parte de un enfoque tecnológico más amplio que cubre todos los aspectos de los viajes transfronterizos desde el momento en que se organiza el viaje hasta la llegada y la salida final del visitante. La información recopilada de cada fase de este proceso se recopila de diferentes fuentes y se envía al funcionario de fronteras que la usa, junto con otra información, para decidir si permite que el viajero ingrese al país.

El dominio más desarrollado es el de los viajes aéreos internacionales y este es el que, en el pasado, impulsó la innovación tecnológica basada en estándares que luego se aplicó a las fronteras terrestres y marítimas. Es probable que este patrón de larga data continúe en el uso emergente de la biometría para identificar a los terroristas. La moderna arquitectura del paso de fronteras para viajes aéreos internacionales permite que la identificación del viajero y la evaluación de riesgos se repitan a lo largo del itinerario del viajero a medida que el Estado de destino o de salida tenga información adicional disponible. Las principales fuentes de datos sobre viajeros en el dominio de los viajes aéreos internacionales son las aerolíneas y los gobiernos, y las soluciones emergentes para la aplicación de la biometría mantienen estas mismas dos fuentes de datos.

Figura 4 – Las cinco fases de la continuidad del viaje[51]
(Con permiso de OACI)



Desde la perspectiva de los estados de destino, el proceso de extremo a extremo se divide en cinco etapas (Véase Fig. 4):

1. Pre-partida
2. Pre-arribo
3. Ingreso
4. Permanencia
5. Salida

Considerando que, desde una perspectiva de todo el sistema e internacional, el viaje es una continuidad, porque el proceso de salida del Estado donde comienza el viaje es el proceso de pre-arribo para los Estados de tránsito y destino correspondientes a ese viaje.

Fase 1: Pre-partida

Hoy en día, muchos Estados requieren información previa de todos los viajeros antes de llegar a la frontera. Esta información consiste principalmente en detalles biográficos, documentación y datos de viaje. Cada vez más, los Estados también requieren información biométrica que les permita confirmar la identidad de los extranjeros que ingresan. En el pasado, estos viajeros podían dividirse en dos grupos: los que necesitaban una visa para ingresar al país y los que no. Desde la década de 1990, los datos del sistema de control de salidas de líneas aéreas han estado disponibles para los

[51] Remítase a la Guía sobre Gestión de Control de Fronteras del Programa de Identificación de Viajeros (TRIP) de la OACI, Montreal (2018) para más detalles.

Estados en la forma de Información Anticipada sobre Pasajeros (API) y API interactiva. Hoy en día, los Estados recopilan información de los viajeros antes de viajar a través de una variedad de mecanismos. Los siguientes procesos y sistemas se utilizan actualmente para recopilar la información necesaria previa al arribo:

1.a. Solicitud de Visa 'Clásica': un requisito común en muchos países que se basa en factores históricos, diplomáticos y económicos, así como en las relaciones políticas del Estado. El proceso generalmente implica que el solicitante envíe los atributos de identidad biográfica y biométrica a través de un proceso de solicitud completo que incluye la presentación de documentos de viaje y un arancel a la oficina diplomática o representante del país de destino. Los datos biométricos pueden ser una foto del rostro o un registro, como un conjunto de huellas dactilares. La solicitud será examinada y se emitirá o rechazará una visa. La verificación previa a la emisión puede incluir una búsqueda 1:n en un listado de alerta biométrico para aquellos Estados que han compilado conjuntos de datos para este propósito.

1.b. Solicitud de Visa regional: la colaboración regional entre países es común y cada continente tiene al menos una entidad regional, por ejemplo, el Sudeste Asiático: ASEAN[52], África occidental: ECOWAS[53], Europa: UE, América del Sur: UNASUR[54] y el Caribe: CARICOM[55]. El nivel de cooperación entre estas entidades difiere. Un ejemplo de uno de estos sistemas regionales es la Unión Europea, que ha adoptado un reglamento que requiere que cada estado miembro implemente su propio Sistema de Información de Visas (VIS). Estos sistemas están conectados con el núcleo VIS central, gestionado por la Agencia Europea para la gestión operativa de sistemas informáticos a gran escala (eu-LISA). VIS utiliza controles biométricos en forma de foto del rostro y un conjunto de diez huellas dactilares para verificar la identidad del viajero en la frontera, además de un control biográfico a través del Sistema de Información de Schengen II (SIS-II) [56] y las bases de datos nacionales. La arquitectura de estos sistemas regionales hace posible incorporar la verificación previa a la emisión que incluye una búsqueda 1:n en un listado de alerta biométrico para aquellos Estados y regiones que han compilado conjuntos de datos para este propósito.

1.c. Solicitud tercerizada: Este modelo, que se está volviendo cada vez más popular entre muchos Estados, utiliza proveedores comerciales para recopilar y cotejar toda la documentación e información del solicitante requerida para el proceso de solicitud de visa. El proceso de negocios también puede registrar los datos biométricos del solicitante (imagen facial, imágenes del iris y/o huellas dactilares). La solicitud completa se envía a la oficina diplomática correspondiente para realizar los controles necesarios y decidir si emitir una visa. La verificación previa a la emisión puede incluir la referencia de una imagen o plantilla biométrica al Estado para una búsqueda 1:n en un listado de alerta biométrico para aquellos Estados que han compilado conjuntos de datos para este propósito.

[52] ASEAN Asociación de Naciones del Sudeste Asiático

[53] ECOWAS Comunidad Económica de Estados de África Occidental

[54] UNASUR Unión de Naciones Suramericanas

[55] CARICOM Comunidad del Caribe

[56] eu-SIS-II brinda soporte a la seguridad pública, el control de fronteras y la cooperación policial en Europa entre los Estados firmantes del Tratado de Schengen. La información de las bases de datos de la policía y los listados de alertas fronterizos se comparte entre los Estados. Esta información es accesible tanto en el país como en las fronteras y también se usa para controlar a quienes viajan dentro y fuera de la Unión Europea. El sistema contiene datos sobre personas buscadas y desaparecidas, documentos de identidad/viaje perdidos o robados, datos biométricos, vehículos robados, etc.

1.d. Solicitud en línea/e-Visa: El proceso de solicitud se realiza completamente en línea a través de formularios electrónicos e imágenes escaneadas de la fotografía del solicitante (que cumple con la OACI) y la página biográfica del pasaporte. El proceso de toma de decisiones y cualquier investigación biométrica se lleva a cabo de forma centralizada. Si se emite la visa, el solicitante recibirá una confirmación y se realizará una verificación biométrica de verificación 1:1 en la frontera al comparar el rostro del solicitante con la imagen de la foto presentada para confirmar que el solicitante y el viajero son la misma persona. La verificación previa a la emisión puede incluir una búsqueda 1:n en un listado de alerta biométrico para aquellos Estados que han compilado conjuntos de datos para este propósito.

1.e. Sistemas electrónicos de viaje (ETS): Este proceso recopila datos de identidad básicos de los viajeros, independientemente de los requisitos de la visa. Su funcionamiento es similar al de la Visa en línea/e-Visa, pero los datos biométricos, aparte de la fotografía del rostro, se obtienen en la frontera en lugar de en la etapa previa a la partida.

La otra fuente principal de información sobre viajeros, con anterioridad al inicio del viaje, es aquella recogida por las aerolíneas:[57]

1.f. Sistema de Registro de Nombre del Pasajero (PNR): Una vez que el viajero obtuvo una visa/autorización de viaje, la siguiente etapa es reservar un pasaje aéreo completando la información PNR en línea. Los datos PNR se almacenan en el Sistema informático de reservas (CRS) de la aerolínea para su propio uso comercial y operativo, pero también se ponen a disposición de las agencias fronterizas antes de la partida del viajero. La OMA, junto con la IATA y la OACI, creó y mantuvo normas técnicas (PNRGOV)[58] para el intercambio armonizado de datos PNR entre operadores de líneas aéreas y gobiernos. *Los registros PRN no contienen datos biométricos*. El valor de los datos PNR es que proporciona información contextual importante para mejorar la seguridad de la identidad y para informar sobre los viajeros en función de los riesgos.

Fase 2: Pre-arribo

2.a. La Información Anticipada sobre Pasajeros (API) se crea en los Sistemas de Control de Partida de las líneas aéreas. El API se compila progresivamente en el momento del check-in, pero solo se envía a las agencias gubernamentales de destino después de que todos los viajeros se hayan registrado, abordado el vuelo y se hayan cerrado las puertas de la aeronave. Es importante destacar que la API se complementa en las paradas de tránsito para continuar los vuelos de larga distancia. API utiliza dos fuentes de datos (1) la información de la Zona de Lectura Mecánica (MRZ) del pasaporte del viajero y (2) los detalles del vuelo y la información de facturación, que pueden incluir elementos de datos estándar y adicionales, como el equipaje facturado, número de asientos, número de pasajeros que vuelan, número de vuelo, fecha, hora y lugar de partida y arribo. Esto permite que la agencia receptora realice una verificación previa de todos los pasajeros antes del arribo. El estándar establecido actualmente para la transmisión de datos API *no ha incluido datos biométricos, aunque en el futuro podría ser posible recopilar la foto compatible con la OACI del chip sin contacto del documento de pasaporte/viaje. Esto requeriría la instalación de un lector de pasaportes electrónicos en los mostradores o terminales de facturación y no todos los países cuentan actualmente con esta tecnología.*

[57] Para PNR y API, véase el Anexo 9, 15ta Edición, de la Convención de Chicago, recopilación de normas y prácticas recomendadas, en el Capítulo 9 "Sistema de Intercambio de Datos de Pasajeros". WCO/IATA/ICAO han desarrollado y acordado en forma conjunta en las Pautas sobre PNR (Doc 9944) y API un mensaje electrónico estándar que incluye conjuntos de datos.

[58] Guia de Implementación de Mensajes PNRGOV EDIFACT & XML: www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

2.b. Información Anticipada sobre Pasajeros interactiva (iAPI) Esta es una versión mejorada de API porque envía la información del viajero a la agencia receptora designada en el momento del registro electrónico. Se envía individualmente y no en un lote como en el proceso de API. El proceso iAPI permite completar el listado de alerta y otras comprobaciones antes de que el viajero aborde el avión y, por lo tanto, proporciona un nivel adicional de protección a la aerolínea, a sus pasajeros y al país de destino. *Los elementos biométricos serían similares a API en 2a arriba.*

Caso de estudio 5 – Ingreso sin presentación de un documento de viaje

Se está considerando un esquema para utilizar la próxima generación de puertas de control automatizado de fronteras (ABC) para viajar entre Australia y Nueva Zelanda. Aprovecharía los sistemas iAPI existentes y asociaría las imágenes faciales disponibles en las bases de datos de pasaportes y visas para generar una base de datos de arribos dinámica esperada para cada viajero que arriba. En esta aplicación, el pasaporte electrónico permanece en el bolsillo del viajero y las puertas biométricas ABC comparan la imagen facial del viajero con la imagen de la base de datos de arribos, y solo permiten la entrada si las dos imágenes coinciden. La solución que se está desarrollando es una aplicación de identificación biométrica 1:n a pequeña escala.

Varios Estados complementan su selección previa al arribo con el despliegue de oficiales de enlace, funcionarios gubernamentales de los Estados de destino, que trabajan con las aerolíneas en los aeropuertos de embarque y tránsito para ayudar en la identificación de los viajeros y la evaluación de riesgos.

Fase 3: Ingreso

Un pasajero solo puede viajar cuando todos los protocolos previos al arribo se han completado con éxito. Sin embargo, para la mayoría de las jurisdicciones, la finalización de los procesos de la Fase 1 Pre-partida y de la Fase 2 Pre-arribo no garantiza la entrada al país al producirse el arribo. El funcionario de la frontera toma la decisión final cuando el viajero presenta los documentos y las credenciales necesarios a su llegada. El funcionario de inmigración debe basar su decisión en una serie de factores y los Sistemas Informáticos de Gestión de Fronteras (BMS) han sido desarrollados para ayudar en este proceso. Sin embargo, se debe tener en cuenta que algunos BCP internacionales aún no tienen acceso a la tecnología BMS. La tecnología BMS varía ampliamente en cuanto a la sofisticación de su funcionalidad. En jurisdicciones más sofisticadas, la verificación de identidad biométrica está creciendo. La aplicación de listados de alerta biométrica es mucho menos común. Las principales variantes son:

3.a Sistema informático estándar de gestión de fronteras (BMS): La ley y la legislación nacionales regulan la cantidad y los tipos de controles realizados en la frontera, por ejemplo, ya sea para registrar los detalles de todos los viajeros que ingresan a un país o simplemente realizar búsquedas en listados de alerta o sanciones. Aquellos países que registran todas las llegadas de viajeros requieren algún tipo de BMS. Los datos se pueden registrar manualmente, pero la mayoría de los sistemas modernos usan un lector de pasaportes para cargar datos de la Zona de Lectura Mecánica del documento de viaje y el oficial de fronteras ingresará información adicional sobre la identidad, la duración y el motivo de la visita, la dirección en el país, etc. Luego se buscan los datos en los listados de alerta. *Un BMS estándar no captura datos biométricos para la verificación automatizada*

3.b. Sistema informático electrónico de gestión de fronteras (e-BMS): e-BMS utiliza un lector de pasaporte electrónico para acceder al chip sin contacto incluido en el Documento Electrónico de Viaje

de Lectura Mecánica (eMRTD) [59]. Este chip contiene los datos de MRZ, así como una foto digital del rostro compatible con la OACI y, a menudo, también dos huellas dactilares. En algunos países, solo se puede acceder a estas huellas dactilares para fines de verificación si el e-BMS contiene un certificado digital del país emisor que permite abrir el grupo de datos que contiene las huellas dactilares. Para verificar las identidades de los datos biométricos incorporados en el chip, un e-BMS debe estar conectado a un sistema biométrico y poder capturar los datos biométricos de los viajeros mediante una cámara para el rostro, una cámara de rayos infrarrojos para el iris o un escáner para huellas dactilares para comparar con los datos del chip. Un eBMS es compatible con las verificaciones de identidad biométrica 1:1 mediante el uso de imágenes de características biométricas leídas desde el pasaporte electrónico. Un eBMS puede incluir una búsqueda 1:n en un listado de alerta biométrica para aquellos Estados que han compilado conjuntos de datos para este propósito.

Los terroristas pueden confiar en documentos de viaje fraudulentos para viajar a través de fronteras sin ser detectados. Las tácticas empleadas van desde el uso de una fotografía sustituta o el uso de un pasaporte de alguien con apariencia similar, hasta la creación de una reproducción falsa del documento completo. Un lector de pasaportes electrónicos autónomo, vinculado a un sistema biométrico integrado, es, por lo tanto, una herramienta valiosa para el examen de documentos para contrarrestar el fraude de pasaportes, especialmente en los BCP que tienen recursos limitados para hacer frente a dicho fraude. La instalación de este equipo en instalaciones secundarias puede ayudar en gran medida a los funcionarios fronterizos que investigan a aquellos viajeros cuyos documentos han suscitado sospechas en el BCP.

Caso de estudio 6 – Estructura de datos lógicos versión 2

Un nuevo desarrollo, que puede permitir un acceso más fácil a datos biométricos adicionales almacenados en los pasaportes electrónicos, es la Estructura de Datos Lógicos (LDS), versión 2. La LDS se almacena en el chip sin contacto del pasaporte electrónico o documento de viaje y puede compararse con un 'gabinete' que contiene 16 cajones llamados Grupos de Datos. Parte de la información almacenada es obligatoria, pero la inclusión de otra información es opcional y a discreción de cada país. Los grupos de datos deben cumplir con la estructura OACI - PKI[60]. Esto garantiza que los datos contenidos en la LDS hayan sido emitidos por una autoridad genuina y no hayan sido alterados o revocados. LDS-2 agrega tres elementos más a la estructura LDS que son (1) registros de viaje, sellos de entrada y salida, (2) registros de visa y (3) datos biométricos adicionales. LDS-2 puede almacenarse en el chip sin contacto del pasaporte electrónico a discreción de una autoridad emisora cuando se emiten nuevos pasaportes electrónicos.

Esto significa que las autoridades de control de visas y fronteras ahora pueden escribir información, relacionada con los tres nuevos grupos de datos, en el chip sin contacto de otro país. Los registros de viajes pueden ser almacenados por la agencia de control de fronteras, sellando el pasaporte electrónicamente y los detalles de la visa pueden ingresarse directamente en el Grupo de datos por las autoridades dedicadas y esto podría verificarse electrónicamente al llegar a una frontera. Aquellos viajeros que estén inscritos en programas de viaje registrados podrían tener las plantillas

[59] eMRTD - Un MRTD (pasaporte o tarjeta) que tiene un circuito sin contacto integrado y la capacidad de ser utilizado para la identificación biométrica del titular del MRTD de acuerdo con las normas especificadas en la parte correspondiente del Doc 9303 de la OACI - Documentos de viaje de lectura mecánica.

[60] La OACI define PKI (Infraestructura de Clave Pública) como un conjunto de políticas, procesos y tecnologías que se utilizan para verificar, registrar y certificar a los usuarios de una aplicación de seguridad. Una PKI utiliza criptografía de clave pública y prácticas de certificación de claves para asegurar las comunicaciones.

biométricas relevantes almacenadas en su pasaporte electrónico para su uso en las puertas de ABC en los países participantes.

Nota: La condición legal para escribir nuevos datos en el chip sin contacto será el intercambio de certificados OACI-PKI entre la autoridad emisora de pasaportes electrónicos y el país que desee agregar los datos. LDS-2 no puede utilizarse a menos que se cumpla esta condición legal.

3.c. Sistema informático de gestión electrónica de fronteras y biométrica (e-2BMS)**:** Es similar al e-BMIS, pero no utiliza un lector de pasaportes electrónicos porque los datos biométricos están registrados en la frontera y a través del sistema de visas. La ventaja de este sistema es que todo el proceso biométrico es propiedad del país de destino y permite a los funcionarios controlar la calidad de los registros para obtener el máximo rendimiento del sistema de verificación biométrica 1:1. Por ejemplo, la adopción de esta arquitectura por los Estados Unidos permite la integración de las verificaciones biométricas de los listados de alerta 1:n contra los extensos registros del listado de alerta compilados por el gobierno de los EE.UU. de todos los pasajeros extranjeros que arriban al país.

3.d. Sistema de control automatizado de fronteras (ABC): el aumento exponencial en el número de pasajeros internacionales durante las últimas décadas ha impulsado la innovación tecnológica y la automatización en las fronteras. Desde el primer sistema de control automatizado de fronteras en el aeropuerto de Schiphol en los Países Bajos, los sistemas ABC se han extendido por todo el mundo y ahora se utilizan regularmente en muchos países. Las iteraciones modernas del sistema utilizan sensores de alta velocidad y datos biométricos almacenados en el chip de los documentos electrónicos de viaje como rostro, iris y huellas dactilares para completar la verificación biométrica 1: 1 para facilitar la entrada automática a través de las puertas fronterizas. Esto permite que las nacionalidades o los grupos prioritarios precalificados se muevan rápidamente a través de los BCP en grandes volúmenes con un retraso mínimo y libera a los funcionarios de la frontera para que se concentren en otros viajeros que puedan necesitar una inspección más detallada. Las autoridades nacionales o regionales deciden qué nacionalidades o grupos pueden usar sus puertas ABC, en un momento dado, según las evaluaciones de riesgo actuales y la legislación asociada. Las soluciones ABC pueden incluir una búsqueda 1:n en un listado de alerta biométrica para aquellos Estados que han compilado conjuntos de datos para este propósito.

Fase 4: Permanencia

Cada país tiene la responsabilidad de administrar a los no nacionales que pueden visitar brevemente, quedarse más tiempo o residir dentro de sus fronteras. Esta tarea puede recaer en diferentes autoridades y agencias, según las leyes y regulaciones nacionales, pero las funciones serán similares, por ejemplo, emitir permisos de residencia y de estudiante, procesar reclamos de refugiados y de asilo y solicitudes de naturalización, además de los deberes de cumplimiento de la ley, tales como tratar con personas que permanece por más tiempo en forma ilegal, delitos de tráfico de personas y explotación laboral, etc.

Un buen ejemplo de esto a nivel regional son los sistemas eu-VIS y eu-SIS-II de la Unión Europea que se han descrito más arriba en la Fase 1.b. Estas bases de datos permiten a todas las autoridades competentes de los países de la UE gestionar a los ciudadanos extranjeros dentro de sus respectivas fronteras. Además, existe Eurodac, que es una base de datos centralizada de la UE que recopila y procesa las huellas dactilares digitalizadas de los solicitantes de asilo. Actualmente lo utilizan 28 países de la UE, así como Noruega, Islandia, Suiza y Liechtenstein. Eurodac procesa, almacena y/o compara las huellas dactilares de nacionales de terceros países o apátridas que tienen al menos 14 años y que han (1) solicitado asilo en cualquiera de los países participantes de Eurodac o (2) han sido detenidos en relación con un cruce irregular de una frontera exterior o (3) se ha encontrado que

están ilegalmente en un país Eurodac. Eurodac también desempeña un papel importante en la ejecución del Reglamento de Dublín. Este regula las solicitudes de los solicitantes de asilo y está diseñado para evitar múltiples solicitudes de asilo en diferentes países de la UE. El objetivo principal del reglamento es asignar la responsabilidad de procesar una solicitud de asilo en un solo Estado miembro, con mayor frecuencia al país donde el solicitante de asilo ingresó por primera vez en la UE para su posterior procesamiento. Desde julio de 2015, las autoridades encargadas del cumplimiento de la ley han tenido acceso limitado a Eurodac, en condiciones muy estrictas, para realizar búsquedas específicas de huellas dactilares. Estos deben llevarse a cabo caso por caso y solo en relación con la prevención, detección e investigación de ciertos delitos graves y delitos de terrorismo.

Los datos biométricos recopilados por las agencias fronterizas durante las fases anteriores del viaje pueden, en un contexto apropiado de investigación o recopilación de inteligencia, compartirse con las agencias de seguridad y de aplicación de la ley.

Fase 5: Salida

El proceso de pre-partida es similar a los protocolos de pre-arribo. El viajero debe hacer el check-in en línea o en el aeropuerto y presentar sus documentos antes de abordar el vuelo. Los sistemas ABC se complementan con una serie de programas de viajero frecuente, como el "Programa de viajero registrado". Estos programas requieren que el viajero se inscriba para ser miembro, registre sus datos biométricos y algunos también pueden tener un proceso de investigación. EE.UU., por ejemplo, cuenta con el Programa de Ingreso Global que permite la autorización expedita para los viajeros pre-aprobados y de bajo riesgo cuando se mueven a través de las fronteras de los EE.UU. Los miembros del programa proceden a los quioscos de Ingreso Global designados, presentan su pasaporte legible por máquina o la tarjeta de residente permanente de los EE. UU., colocan sus huellas dactilares en el escáner para la verificación de huella dactilar y completan una declaración de aduanas. El quiosco emite al viajero un recibo de la transacción. Los viajeros deben ser aprobados previamente para el programa de Ingreso Global. Todos los solicitantes deben someterse a una rigurosa verificación de antecedentes y a una entrevista personal antes del registro.

Aunque no todos los países llevan a cabo un control de salida de inmigración en el momento de la partida, muchos todavía verifican a un viajero que abandona el país. Por lo general, esto implicará verificar que el nombre dado en una tarjeta de embarque coincida con el que se muestra en el documento de viaje y realizar una búsqueda en los listados de alerta biográfica, para determinar que los detalles del vuelo coinciden con el horario de ese día y que el viajero no se excedió en su estadía. Además de estos controles, también se evalúa a los viajeros, en búsqueda de envíos de drogas y dinero, tráfico de personas a otros países y especialmente a los combatientes terroristas extranjeros, según su documento de viaje, tarjeta de embarque y otros criterios específicos.

Caso de estudio 7 – Verificación biométrica al momento de la partida

Un modelo emergente en los Estados Unidos es que las aerolíneas, los aeropuertos y el gobierno trabajen en conjunto para invertir en iniciativas de facilitación en las puertas de embarque que brinden un mecanismo alternativo para obtener una verificación biométrica al momento de la partida. A principios de 2018, tanto Lufthansa como British Airways estaban realizando ensayos con reconocimiento facial. Esta es una aplicación adicional de una verificación biométrica 1:n de viajeros conocidos, análoga a los acuerdos que se están desarrollando en las asociaciones entre aerolíneas y gobiernos para viajar entre Australia y Nueva Zelanda (Véase caso de estudio 5).

3.1.2 Aplicaciones de la policía e INTERPOL

Las bases de datos biométricos utilizadas en la vigilancia policial suelen estar integradas por Datos de Referencia de los detenidos (imágenes faciales, huellas dactilares y perfiles de ADN), datos de la escena del crimen y otros datos no identificados, por ejemplo, derivados de consultas de personas desaparecidas o fallecidas o actividades de recopilación de inteligencia. Estos sistemas pueden operar a nivel local, provincial o nacional para cumplir funciones tales como mantener registros de antecedentes penales, investigar delitos o generar productos de inteligencia forense. Los datos biométricos generados a partir de investigaciones sobre terrorismo pueden agregarse a estos sistemas o cargarse en bases de datos exclusivas como una medida de seguridad adicional. Independientemente de la configuración de la base de datos utilizada, habrá una necesidad operativa de buscar en todos los sistemas debido al potencial cruce entre el terrorismo y el delito general, por ejemplo, individuos que cometen fraude o robos de alto valor para financiar específicamente actividades terroristas, etc. *Idealmente, también deberían ser interoperables con las aplicaciones biométricas fronterizas, si así lo permite la legislación nacional.*

A nivel internacional, la policía puede intercambiar datos biométricos a través de acuerdos bilaterales, multilaterales o regionales, pero el único método oficial a nivel mundial es a través de la Organización Internacional de Policía Criminal (OIPC, o más comúnmente conocida como INTERPOL) que facilita la cooperación policial internacional. Cabe señalar que los países que aportan datos a las bases de datos de Interpol:

1. *retienen la titularidad de sus datos* y pueden eliminarlos de las bases de datos en cualquier momento (véase la Sección 3.3.2. Búsquedas unidireccionales).
2. *determinan el alcance de los datos que se buscan* es decir, sus datos de búsqueda y sus datos archivados no se exponen a los datos biométricos de los países designados.

INTERPOL cuenta con tres bases de datos biométricos que pueden ser utilizadas por sus 190 países miembros:

Rostro: Proporciona la siguiente funcionalidad:

- Identificación de fugitivos y personas desaparecidas
- Identificación de personas desconocidas de interés
- Identificación de personas en imágenes de los medios de comunicación
- Verificación de 'fotografías de identificación policial' (imágenes en custodia) recibidas contra una base de datos (1:n).

Huellas dactilares: Sistema AFIS. Este sistema permite a los funcionarios encargados del cumplimiento de la ley autorizados de los países miembros acceder a la base de datos de forma remota y recibir una respuesta automática utilizando la red de comunicaciones global segura de Interpol I-24/7. La base de datos contiene Datos de Referencia (huellas digitales y palmares) y Datos de la Escena del Crimen (marcas digitales y palmares).

ADN*:* Sistema de ADN (que opera en forma similar al Sistema AFIS). INTERPOL ha acordado normas sobre el procesamiento de datos de ADN con todos los países miembros y la base de datos consta de cuatro secciones:

- escenas del crimen sin resolver
- delincuentes conocidos
- personas desaparecidas

- restos humanos no identificados

INTERPOL también ofrece los servicios de Cotejo Bilateral de ADN que brinda una plataforma privada para la búsqueda y comparación de ADN entre dos países. El acuerdo se basa en la confianza compartida, la estrategia policial, la legislación compatible y los criterios de coincidencia mutuamente acordados, por ejemplo, un número mínimo de loci. Cada país selecciona los perfiles de ADN y los envía en forma segura a INTERPOL. Cualquier coincidencia detectada se notifica a ambos socios y los datos se eliminan del sistema. Los países pueden usar esta herramienta para realizar comparaciones puntuales o como parte de sus operaciones regulares de comparación.

Una función importante de las bases de datos biométricos de INTERPOL es recopilar datos biométricos sobre combatientes terroristas extranjeros y otros terroristas para prevenir su movimiento a través de las fronteras. Esto es compatible con el flujo de acción de la estrategia global contra el terrorismo de INTERPOL que prioriza la identificación de miembros de grupos terroristas transnacionales conocidos.

3.1.3 Bases de datos biométricos de INTERPOL: supervisión y regulación

La regulación interna y el funcionamiento de las bases de datos biométricos de INTERPOL están supervisados por la Comisión de Control de Archivos de Interpol (CCF), que es un organismo independiente. Tiene tres funciones:

1. asegurar que el procesamiento de datos personales por parte de INTERPOL cumpla con las regulaciones de la Organización
2. asesorar a INTERPOL sobre cualquier asunto relacionado con el procesamiento de datos personales
3. procesar solicitudes respecto de la información incluida en los archivos de la Organización.

La CCF se convirtió en un organismo oficial de la Organización cuando la 77ma Asamblea General votó en 2008 para fortalecer su estatus mediante la modificación de la Constitución para integrar la CCF a su estructura legal interna. En noviembre de 2016, la Asamblea General de Interpol adoptó un paquete de reformas relacionadas con los mecanismos de supervisión de Interpol. El paquete incluía la adopción del nuevo Estatuto de la CCF que reformó profundamente su composición, estructura y procedimientos. Este nuevo marco legal entró en vigencia el 11 de marzo de 2017 y reforzó las funciones de supervisión y asesoría de la Comisión, al tiempo que fortaleció su capacidad para proporcionar un recurso efectivo a las personas con respecto a los datos que se pueden procesar en los archivos de INTERPOL.

3.1.4 Gestión de los datos biométricos y biográficos incluidos en listados de alerta

Los listados de alerta son una forma de sistema de alerta, basado en varios tipos de datos, que operan a nivel nacional y, a veces, regional. Su objetivo es proporcionar advertencias anticipadas y procedimientos de verificación para ayudar a reconocer e identificar a los delincuentes, terroristas y bienes o materiales sospechosos en los puntos de cruce de frontera. Hay varios tipos de listados de alerta que incluyen:

- *Listados de alerta biográficos:* información sobre personas buscadas o desaparecidas, personas de interés, prohibiciones de no volar, etc.

- *Listados de alerta biométricos:* las modalidades habituales incluyen huellas dactilares, imágenes faciales e iris (actualmente el ADN no se utiliza ampliamente) y tienen una función similar a la de los listados de alerta biográficos, es decir informar sobre personas buscadas o desaparecidas, personas de interés, terroristas conocidos o sospechosos, etc.
- *Listados de alerta que contienen información sobre bienes y documentos:* vehículos robados, documentos de viaje perdidos y robados[61], obras de arte robadas, etc.
- *Listados de alerta que contienen información sobre modus operandi o el reconocimiento de bienes peligrosos:* el método específico utilizado para ejecutar un delito o una serie de delitos, nuevas formas de reconocer moneda falsificada o documentos de viaje, métodos y componentes químicos utilizados en la fabricación de drogas ilícitas, etc.

Los organismos internacionales y regionales encargados de hacer cumplir la ley, tales como INTERPOL[62] y EUROPOL[63], y los organismos que no tienen a su cargo el cumplimiento de la ley también utilizan los listados de alerta para otras aplicaciones que resultan en una amplia y diversa gama de usuarios:

- *Cumplimiento de la ley:*
  - Internacional[64]: INTERPOL[65].
  - Regional: EUROPOL[66] y otros organismos regionales
  - Nacional[67]: policía, inmigración, aduana etc.
- *Organismos internacionales*
  - Naciones Unidas (ONU,[68]) etc.
- *Organismos públicos*,
  - Autoridades emisoras de pasaportes,[69] Autoridades emisoras de licencias de conducir, etc.
- *Organizaciones privadas/comerciales,*
  - Aerolíneas, compañías de seguros, fabricantes de alimentos, etc.

Los organismos que no tienen a su cargo el cumplimiento de la ley emplean los listados de alerta dentro de sus áreas de responsabilidad o negocio a fin de proteger sus productos y procesos y prevenir acciones fraudulentas.

3.2 Limitaciones de los listados de alerta biográficos

La mayoría de los listados de alerta relacionados con el cumplimiento de la ley se basan en la información biográfica de una persona, por ejemplo, nombres, fecha de nacimiento, etc. Esta

[61] Véase: https://www.interpol.int/INTERPOL-expertise/I-Checkit
[62] Véase: https://www.interpol.int/
[63] Véase: https://www.europol.europa.eu/
[64] Véase: Guía sobre Gestión de Control de Fronteras del Programa de Identificación de Viajeros (TRIP) de la OACI, versión 1, capítulo: 5-M
[65] Véase: https://www.interpol.int/INTERPOL-expertise/Bases de datos
[66] Véase: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
[67] Véase: Guía sobre Gestión de Control de Fronteras del Programa de Identificación de Viajeros (TRIP) de la OACI, versión 1, capítulo: 4-E
[68] Véase: https://www.un.org/sc/ctc/
[69] Véase: https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

información puede no ser confiable y estar sujeta a cambios o errores. Algunos ejemplos comunes son:

- error de ortografía o traducción incorrecta de nombres
- uso de un nombre alterado o apodo en lugar del nombre oficial incluido en el documento de viaje
- fecha de nacimiento errónea o secuencia de dígitos incorrecta, por ejemplo, 01-12-1967 en lugar de 12-01-1967
- la persona posee dos nacionalidades
- la persona cambió su nombre y obtuvo una nueva identidad o documento de viaje
- la persona presenta un documento de viaje falsificado, falso u obtenido en forma fraudulenta bajo otro nombre
- la persona presenta un documento de viaje auténtico de otra persona para hacerse pasar por el portador original
- la persona "comparte" un documento de viaje con alguien que usa una fotografía 'transformada', es decir una imagen combinada de dos rostros diferentes (Véase la Sección 2.3.2.)
- mellizos o trillizos cambian documentos de identidad y/o de viaje

Por lo tanto, la identificación positiva de la persona es de suma importancia y esto ha dado lugar a la creación de listados de alerta biométricos.

3.3 Listados de alerta biométricos

Los listados de alerta biométricos desempeñan un papel adicional en los procesos de verificación biométrica 1:1 realizados en las fronteras. La verificación de comparación 1:1 (véase la Sección 3.1) utiliza la información biométrica almacenada en el chip del documento de viaje electrónico para autenticar la identidad de la persona que llega a la frontera. El concepto del listado de alerta va un paso más allá e introduce una capacidad de búsqueda 1:n (uno a muchos) para verificar los datos biométricos del viajero contra una base de datos biométricos de las personas de interés. Se requiere un equipo de registro biométrico similar para ambos procesos, pero la base de datos necesitará un software de búsqueda 1:n, así como un software de comparación 1:1 para que pueda realizar una o ambas tareas según sea necesario. Esto obviamente requerirá una inversión extra. La efectividad de la búsqueda 1:n en el listado de alerta dependerá de:

- la calidad de los datos registrados
- el tipo de datos almacenados en la base de datos
- el rendimiento del sistema (Véase la Sección 1.1)
- la vulnerabilidad del sistema a los ataques de presentación que usan técnicas tales como transformación o suplantación de identidad (Véase la Sección 2.2)

Entre los ejemplos de grandes listados de alertas internacionales y regionales se incluyen:

INTERPOL I-24/7 : Todas las bases de datos de INTERPOL, excepto la Red de Información de Balística de INTERPOL (IBIN), son accesibles en tiempo real a través de la red I-24/7 que conecta todas las Oficinas Centrales Nacionales (BCN) de INTERPOL. Está vinculado al sistema de Avisos de INTERPOL para emitir alertas internacionales para fugitivos, presuntos delincuentes, personas vinculadas o de

interés en investigaciones criminales en curso, personas y entidades sujetas a sanciones del Consejo de Seguridad de la ONU, amenazas potenciales, personas desaparecidas y cadáveres.

Sistema de Información EUROPOL-EIS: Esta base de datos contiene información delictiva y de inteligencia que cubre todas las áreas delictivas obligatorias de Europol, incluido el terrorismo.

Caso de estudio 8 – ETIAS

La Comisión de la Unión Europea propone el establecimiento de un Sistema Europeo de Información y Autorización de Viajes (ETIAS[70], por su sigla en inglés) para reforzar la seguridad de los viajes al área de Schengen bajo acuerdos sin visado. El listado de alerta de ETIAS, que será establecido y administrado por Europol, consistirá en datos relacionados con personas sospechosas de haber cometido o de haber participado en un delito o personas respecto de las cuales existen indicaciones objetivas o motivos razonables para creer que cometerán delitos penales.
El listado de alerta se establecerá sobre la base de:

1) el Listado del Comité de Sanciones de las Naciones Unidas
2) información relativa a delitos terroristas u otros delitos penales graves provista por los Estados Miembros
3) información relativa a delitos terroristas u otros delitos penales graves obtenida mediante cooperación internacional.

3.3.1 Beneficios de las aplicaciones biométricas contra el terrorismo

3.3.1.1 Dentro de las fronteras nacionales

Las bases biométricas de datos han desempeñado un papel cada vez más importante en las investigaciones de delitos desde el desarrollo de la primera clasificación de huellas dactilares y sistemas de búsqueda en la década de 1890. La informatización y los avances científicos y tecnológicos del siglo XX aumentaron en gran medida la eficiencia y el poder de procesamiento de tales sistemas y ampliaron la gama de modalidades disponibles como rostro, ADN, voz, etc. Los sistemas de búsqueda biométricos utilizados por muchas agencias de cumplimiento de la ley hoy en día cuentan con funciones avanzadas y algoritmos complejos que pueden facilitar la búsqueda rápida y precisa de grandes volúmenes de datos. Sin embargo, la gran ventaja que tiene la búsqueda en bases de datos de Detección de Delitos Penales sobre la mayoría de los otros procesos de investigación y recopilación de inteligencia es que proporciona vigilancia continua las 24 horas del día, todos los días del año, siempre que los datos se conserven en la base de datos. Una coincidencia se puede encontrar tan pronto como se registren y busquen los datos, siempre que los datos coincidentes ya estén en la base de datos, o se puedan registrar en el sistema y producir una coincidencia, semanas, meses, años o incluso décadas más tarde. En consecuencia, la búsqueda en las bases de datos de Detección de Delitos Penales se considera uno de los activos más rentables y consistentemente útiles disponibles para el moderno investigador y analista de inteligencia. Las bases de datos también pueden:

[70] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

1. combinarse a escala nacional para brindar cobertura efectiva a un país independientemente de su tamaño físico y su población relativa,
2. operar con los sistemas biométricos de frontera, y
3. vincularse a bases de datos biométricos internacionales u otras bases de datos biométricos relevantes.

Investigación forense en tiempo real

Las agencias de cumplimiento de la ley en muchos países han desarrollado y utilizado esta tecnología biométrica para establecer la identidad de los perpetradores y confirmar sus antecedentes penales, probar o refutar la participación de los sospechosos en delitos y vincular delitos. Estas bases de datos han demostrado ser particularmente valiosas en las investigaciones de terrorismo y su contribución se ha mejorado, en los últimos años, con el advenimiento de la "Investigación Forense en Tiempo Real". Este proceso explota la rápida recuperación y la generación de datos forenses de búsqueda en las escenas del crimen como imágenes faciales recuperadas de dispositivos electrónicos o fotografías, muestras de ADN rápidamente perfiladas o la transmisión electrónica de imágenes digitales de marcas de dedos de la escena del crimen directamente a un AFIS para una búsqueda instantánea. Ahora es posible, y se está volviendo cada vez más rutinario, buscar y comparar material biométrico evidentemente significativo mientras el examen de la escena del crimen aún está en progreso. Esto tiene el potencial de generar inteligencia forense que puede identificar rápidamente a un sospechoso o crear o cambiar líneas dinámicas de investigación para los investigadores en las primeras etapas de una investigación. En las investigaciones sobre terrorismo, esto puede identificar a otros sospechosos o asociados justo después de un incidente y ayudar a prevenir nuevos ataques. Obviamente, esta capacidad se mejora aún más si el conjunto de datos biométricos que se buscan en tiempo real es lo más amplio posible.

Las bases de datos son muy útiles cuando se trata de las consecuencias de los "atentados suicidas" en los que los restos físicos del bombardero pueden mezclarse con los de las víctimas. Es imperativo en estas ocasiones determinar con urgencia tanto la identidad del atacante, avanzar en la investigación y tratar de frustrar nuevos ataques, como la identidad de las víctimas en nombre de sus familias. El ADN, las huellas dactilares y las piezas dentales (odontología forense) son los principales datos biométricos utilizados, ya que son los principales identificadores empleados para la identificación de víctimas de desastres[71].

3.3.1.2 A través de las fronteras nacionales

Como se describió anteriormente, las intervenciones biométricas en las fronteras se dividen en dos categorías:

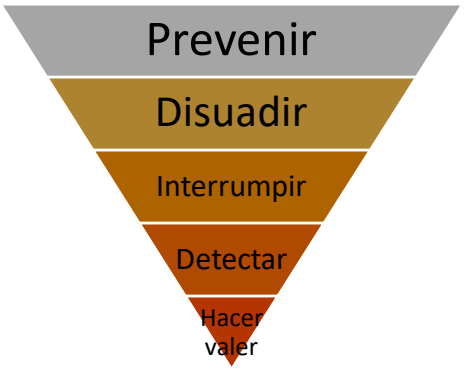
(1) *Verificación de identidad biométrica (1:1)* : la comparación de datos biométricos obtenidos del viajero en la frontera con datos biométricos, por ejemplo, almacenados en el documento de viaje, como un pasaporte electrónico
(2) *Búsqueda en listados de alerta biométricos (1:n)*: la búsqueda de datos biométricos obtenidos del viajero en la frontera o de su solicitud de documentos de viaje o pasaporte electrónico en una listado de alerta que contiene los datos biométricos de las personas de interés, como las

[71] La identificación de víctimas de desastres (DVI, por su sigla en inglés) es un procedimiento reconocido internacionalmente para recuperar e identificar a las víctimas de un incidente de muerte masiva y para apoyar a las personas en duelo durante el proceso. Es realizado por personal de cumplimiento de la ley y los procesos se acuerdan a nivel internacional a través de la membresía de los comités de Interpol DVI. Interpol también puede proporcionar asistencia directa y coordinación en caso de incidentes internacionales grandes y complejos.

buscadas por las autoridades de cumplimiento de la ley, terroristas conocidos o sospechosos, etc.

Cada proceso mejora la evaluación de riesgos de los viajeros a través de la gestión de identidad.[72] La configuración óptima es tener ambos procesos en funcionamiento a través de una frontera. La verificación de identidad de frontera confirmará la identidad del viajero en comparación con los datos biométricos registrados y autenticados, pero una búsqueda en el listado de alerta biométrica puede revelar que la identidad confirmada es un tema de interés. Este enfoque requiere una mayor inversión, pero los niveles adicionales de garantía y seguridad que proporciona normalmente justificarán el gasto adicional.

Figura 5 – Adaptado de la Guía sobre Gestión de Control de Fronteras del Programa de Identificación de Viajeros (TRIP) de la OACI, *Montreal (2018)*
(Con permiso de OACI)



Agencias de frontera	Prevenir, disuadir e interrumpir el viaje	Listados de alerta Inteligencia de viaje
Agencias de cumplimiento de la ley y seguridad	Investigar, detectar y hacer valer	• Investigaciones en la escena del crimen • Inteligencia penal y de seguridad

Los listados de alerta pueden variar según el tamaño y la complejidad de su contenido. Algunos listados de alerta biométrica comprenderán bases de datos discretas de datos de referencia obtenidos de ciertas categorías de personas de interés. Otros listados de alerta biométrica pueden adicionar datos biométricos seleccionados de la escena del crimen para ampliar el alcance. Sin embargo, la interpretación más amplia del concepto del listado de alerta sería la integración legal de todas las bases de datos biométricos de los organismos de cumplimiento de la ley nacionales (véase la Sección 3.3.2) en un "listado de alerta nacional", como se ilustra en la Fig. 5. Esto expondría la cantidad de datos relevantes óptima para los listados de alerta y proporcionaría la máxima protección para el público que viaja y para la seguridad de la nación. Sin embargo, puede haber restricciones legales y reglamentarias nacionales que impidan tal solución.

3.3.1.3 Más allá de las fronteras nacionales

Un país puede tener activos en el extranjero que se consideran vulnerables a un ataque terrorista. La biometría puede formar una parte esencial de cualquier plan de mitigación de amenazas. Por ejemplo, puede ser un requisito seleccionar a los empleados del país anfitrión que trabajan en las instalaciones que son propiedad del país de origen, como una Embajada. Esto requeriría la cooperación entre los dos países e, idealmente, el acuerdo legal para buscar datos biométricos y biográficos en las bases de datos de ambos países para establecer que los empleados no tenían

[72] Para más detalles, remítase a la Guía sobre Gestión de Control de Fronteras del Programa de Identificación de Viajeros (TRIP) de la OACI, Montreal (2018).

antecedentes penales ni una conexión conocida con el terrorismo en ninguno de los dos países. De manera similar, si los ciudadanos del país anfitrión se hubieran involucrado en el terrorismo dentro del país de origen, ambos países se beneficiarían del intercambio y la búsqueda de datos biométricos entre sí para, en primer lugar, proteger los activos en el extranjero del país de origen, por ejemplo, operaciones comerciales, oficinas diplomáticas y actividades, etc. y, en segundo lugar, para ayudar al país anfitrión a identificar y gestionar el retorno de cualquiera de sus nacionales sospechosos de actividades terroristas. Esta forma de cooperación bilateral y otras opciones de intercambio de datos se describen en la Sección 3.3.2.

3.3.1.4 Datos biométricos de fuentes militares

Algunos países utilizan sus fuerzas militares para combatir el terrorismo dentro de sus fronteras nacionales o en el extranjero. La biometría a menudo se usa durante dichos despliegues para denegar el anonimato a los terroristas que pueden tratar de esconderse y mezclarse entre las poblaciones locales para evitar su detección o usarlos como "escudos humanos". Las fuerzas militares pueden usar técnicas similares a las empleadas por las agencias de cumplimiento de la ley tales como el despliegue de dispositivos de captura biométricos móviles o estáticos para obtener muestras de referencia de presuntos terroristas; o el examen forense de los artículos recuperados de detenidos o lugares de interés relacionados con actividades terroristas o insurgentes.

Los datos biométricos obtenidos de estas operaciones militares también pueden ser de gran valor para las agencias de cumplimiento de la ley en relación con sus investigaciones de terrorismo, pero puede haber restricciones sustanciales para compartir y usar dichos datos y esto dependerá en gran medida de:

- la autoridad legal para intercambiar dichos datos biométricos de acuerdo con la legislación nacional y la legislación internacional de derechos humanos
- la admisibilidad de los datos biométricos militares y otras pruebas en los tribunales civiles
- la compatibilidad de las normas de calidad de la ciencia forense y biométrica militar con las utilizadas por las autoridades civiles en ese país

Por lo tanto, aunque el intercambio de datos puede ser legal, puede que no alcance los estándares legales requeridos para ser admitido como prueba, aunque, por supuesto, puede tener un valor de inteligencia significativo (Véase la Sección 3.3.3).

Caso de estudio 9 – Centro analítico de dispositivos explosivos terroristas

El Centro de Análisis de Dispositivos Explosivos Terroristas (TEDAC, por su sigla en inglés) de la Oficina Federal de Investigaciones de EE.UU. es un ejemplo de este tipo de capacidad. El TEDAC coordina los esfuerzos de todo el gobierno, desde el cumplimiento de la ley hasta la inteligencia y el ejército, para recopilar y compartir datos forenses e inteligencia sobre dispositivos, tácticas, técnicas y procedimientos para desarmar e interrumpir los dispositivos explosivos improvisados (IED), vincularlos con sus creadores, y, lo más importante, evitar futuros ataques. Hasta la fecha, TEDAC ha recibido más de 100.000 presentaciones de IED de más de 50 países. La Unidad de Análisis Biométrico (BAU, por su sigla en inglés) respalda la capacidad global del gobierno de los EE.UU. y de los socios internacionales para contrarrestar y derrotar la amenaza del IED mediante la impresión

forense latente y el examen de ADN de los materiales del IED de manera oportuna y con alta calidad, a fin de generar una inteligencia para uso en la investigación.

3.3.1.5 Protección mutua garantizada

Los beneficios de los sistemas biométricos para rastrear y detectar a los terroristas solo se pueden realizar plenamente si las naciones cooperan y comparten datos. Un país puede tener sistemas biométricos nacionales integrales y efectivos dentro de sus fronteras e incluso ser parte de una red regional sofisticada, pero si no tiene acceso a datos terroristas de otros países fuera de esta red nacional y regional, entonces sigue siendo potencialmente vulnerable. El intercambio de datos nacionales, bilaterales y regionales (véase la Sección 3.3.2) proporciona una solución parcial, pero es imperativo que los datos biométricos terroristas se compartan internacionalmente, a escala global, para brindar protección mutua a todas las naciones. Esto también ayudará a disuadir e interrumpir a los terroristas que pueden basarse temporalmente en países con poca o ninguna capacidad biométrica para que puedan adoptar nuevas identidades u obtener documentos de viaje producidos de manera fraudulenta y luego viajar de incógnito a otros destinos. Se debe establecer un sistema sólido y completo de intercambio de datos biométricos internacionales para contrarrestar estas tácticas y negar a los terroristas el anonimato o los "refugios seguros" desde los cuales operar

Las bases de datos biométricos de Interpol son un buen ejemplo de este tipo de capacidad global. Están diseñadas para cumplir esta función vital y protectora al permitir que las naciones compartan datos biométricos relacionados con el terrorismo y, lo que es más importante, están sujetas a procedimientos de regulación acordados internacionalmente que están sujetos a supervisión independiente.

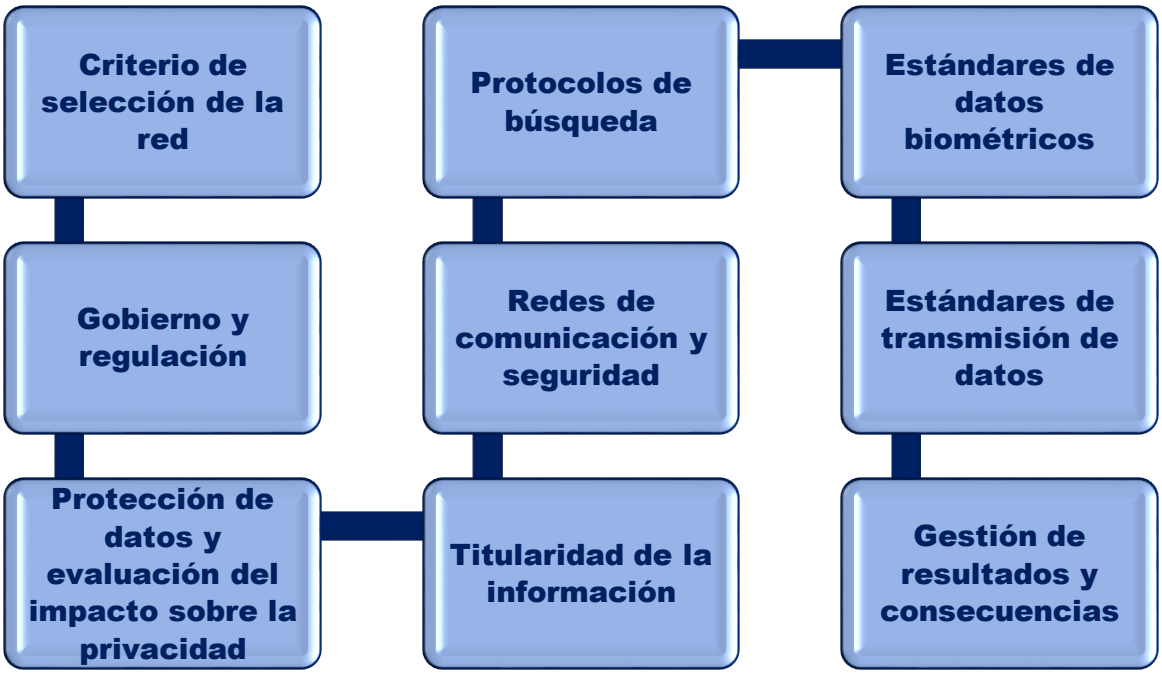
La Figura 6 muestra la amplia gama de *posibles* fuentes de datos biométricos, en poder de organizaciones públicas nacionales e internacionales, que podrían explotarse con fines de lucha contra el terrorismo. Los listados no son exhaustivos y el acceso a cualquiera de estas bases de datos está, por supuesto, sujeto a restricciones legales y reglamentarias nacionales. Sin embargo, muestra cómo los datos biométricos pueden, en teoría, estar conectados para brindar protección mutua contra la amenaza del terrorismo en términos de alcance nacional, regional y global.

Figura 6 – Fuentes de datos biométricos

3.3.2 Protocolos para compartir datos e integración legal de las bases de datos

Tradicionalmente, las bases biométricas de los organismos de cumplimiento de la ley operaban como sistemas "independientes" porque cada aplicación respondía a una necesidad empresarial distinta e independiente y no se percibía ninguna ventaja al compartir datos entre estos sistemas. Estas bases de datos se diseñaron específicamente para las funciones comerciales asociadas con la vigilancia policial, la gestión de fronteras o las prisiones. Sin embargo, la creciente amenaza del terrorismo global, durante las últimas décadas, ha obligado a muchos gobiernos a reconsiderar la forma en que se utilizan sus bases de datos y cómo podrían compartir datos entre ellos para brindar mayor protección a sus ciudadanos. Esto ha dado como resultado una mayor conectividad e interoperabilidad entre las bases de datos a nivel nacional y el desarrollo de redes bilaterales, multilaterales y regionales de bases de datos a nivel internacional. Esto comenzó con la agregación de bases de datos dispares de modo único y ha evolucionado, en algunos países y regiones, a redes de reemplazo de vanguardia que cuentan con bases de datos multimodales interconectadas diseñadas para dar servicio a una gama de las necesidades comerciales a través de la aplicación de la ley, la gestión de fronteras y otras funciones gubernamentales a nivel nacional e internacional. Los requisitos para este tipo de conectividad son los siguientes:

Figura 7 – Requisitos de conectividad de red biométrica



Criterio de selección de la red: Los propietarios de datos biométricos deben evaluar su pertenencia a una red biométrica basándose no solo en sus propios requisitos comerciales y objetivos operacionales, por importantes que sean, sino también desde una perspectiva más amplia que tenga en cuenta el valor agregado potencial para su país o región así como los otros socios en la red. Este enfoque es esencial y fundamental en el desarrollo de bases biométricas de datos contra el terrorismo en red. También es poco probable que los propietarios de datos que buscan participar en una red internacional corran el riesgo de compartir sus datos con socios sin principios o no confiables, y estas preocupaciones deben ser administradas adecuadamente por cualquier red que tenga una gran cantidad de miembros internacionales, por ejemplo, véase la Sección 3.1.2. Aplicaciones de la policía e INTERPOL.

Gobierno y regulación: Las redes biométricas deben operar dentro de un marco legal que permita la transferencia de datos biométricos y otros metadatos asociados. Cada base de datos existente ya debería estar operando de acuerdo con las leyes nacionales y las leyes internacionales de derechos humanos, pero es posible que se requiera más legislación para permitir la búsqueda entre diferentes bases de datos dentro de un país o internacionalmente. En el caso de las redes internacionales, esto normalmente se logrará a través de acuerdos formales, como los Memorandos de Entendimiento, entre las entidades o países participantes. La búsqueda legal se puede restringir a búsquedas individuales iniciadas caso por caso (por ejemplo, para delitos específicos) o más ampliamente aplicadas, como en la búsqueda automática de todos los datos registrados a través de una red.

Un marco regulatorio debe proporcionar una supervisión independiente de toda la red y prestar especial atención a las funciones de administración de datos y los propósitos para los cuales se utilizarán los datos para evitar cualquier extensión no autorizada del alcance, por ejemplo, la búsqueda de conjuntos de datos dentro o fuera de la red que están prohibidos por la ley o bajo los protocolos operativos actuales. Algunos países han designado funcionarios para llevar a cabo esta

función, por ejemplo, Reguladores o Comisionados Biométricos. Además, otros reguladores, como el Regulador de Ciencias Forenses del Reino Unido, tienen la responsabilidad de supervisar los procesos científicos, incluidos los utilizados para crear los datos y perfiles biométricos forenses que se utilizan en estas bases de datos. Esto significa que tanto la operación de la base de datos como la información biométrica forense que contiene están sujetas a un escrutinio y supervisión independientes y esto incluye el trabajo de comités de revisión ética u organismos similares. (Véase la Sección 2.1.1.)

Protección de datos y evaluación del impacto sobre la privacidad: (Véase las Secciones 2.2.3. y 2.2.4.).

Titularidad de la información: Cada registro biométrico debe tener un propietario de datos definido (Véase la Sección 2.2.6.) que asume la responsabilidad, según la ley, de la inscripción, el uso, la retención y la eliminación de esos datos. Esto es de particular importancia cuando se trata de una red de bases de datos biométricos que contienen grandes volúmenes de datos de diversas fuentes.

Redes de comunicaciones y seguridad: El flujo de datos biométricos y otra información debe ser eficiente y oportuno. La red debe ser segura debido a la naturaleza de los datos que posee y tener niveles adecuados de seguridad para proteger al personal y al entorno operativo, incluidos los datos, el hardware, el software y la red de comunicaciones. Es una buena práctica conservar solo los datos biométricos en el sistema de red. Los datos personales y biográficos que están vinculados a los datos biométricos respectivos deben archivarse en un sistema separado. Esta protección impide que se acceda a la información personal y a los datos biométricos desde una aplicación. Por lo tanto, los datos biométricos generalmente solo tienen un número de referencia único para poder vincularlos a sus datos biográficos correspondientes, utilizando procedimientos operativos seguros, cuando surja la necesidad.

Protocolos de búsqueda: la red debe tener colas de búsqueda y protocolos de búsqueda sistemáticos y sincronizados que controlen el tiempo y la secuencia de cada búsqueda para garantizar que esté expuesta al conjunto completo de datos en cada base de datos en la red, es decir, no se pierda nada, incluso en momentos de máxima demanda (véase el párrafo siguiente: - Bases de datos biométricos en red: protocolos de búsqueda).

Estándares de datos biométricos: Las búsquedas solo se pueden realizar en una red cuando los socios presentan datos biométricos de un tipo compatible. Por ejemplo, se han utilizado diferentes composiciones químicas de perfilado de ADN en todo el mundo, como por ejemplo en el caso de Australia, Europa y los Estados Unidos. Cada una de sus composiciones químicas utilizó STR-loci únicos específicos además de STR-loci que eran comunes a todos. Sin embargo, siempre que hubiera un número suficiente de loci comunes fue posible buscar perfiles de estas diferentes composiciones químicas en cualquiera de sus bases de datos de ADN. Las últimas composiciones químicas de perfilado utilizan un número aún mayor de STR-loci, por lo que hay proporcionalmente más loci que son comunes a todos los socios.

Los estándares técnicos y científicos (por ejemplo, ISO 17025) que se describen en la Sección 2.4 deberían sustentar todas las características operativas de la red.

Estándares de transmisión de datos: La calidad de imagen por debajo de lo normal puede exponer a la red biométrica a riesgos graves e innecesarios, como un mayor número de rechazos falsos o incluso identificaciones erróneas. Con el fin de garantizar que la calidad de las imágenes, como el rostro o las huellas dactilares, no se degrade durante la transmisión a través de la red, se debería contar[73] con estándares que aborden los requisitos de resolución de imagen. Esto significa que la imagen conservará la misma claridad y definición, independientemente de dónde se vea en la red.

[73] Por ejemplo, Publicación especial de NIST 1152 'Latent Interoperability Transmission Specification' www.nist.gov

Gestión de resultados y consecuencias: Las coincidencias de datos biométricos producidas por la red de búsqueda (resultados) y las acciones tomadas como resultado de dichas coincidencias (consecuencias) deben gestionarse con cuidado y de acuerdo con los requisitos legales, estándares científicos sólidos y estrictos protocolos organizativos (Véase la Sección 3.3.3.). Las coincidencias biométricas deben ser revisadas por pares, como parte de un Sistema de Gestión de Calidad, por otro experto o preferiblemente dos expertos antes de que se publique el resultado. Esto evita el riesgo de que solo una persona realice una identificación incorrecta.

Bases de datos biométricos en red: protocolos de búsqueda. Existen dos métodos fundamentales para sincronizar las búsquedas entre las bases de datos:

Búsqueda unidireccional: los datos biométricos (a) se registran y se buscan en la base de datos 1. Si no se encuentran coincidencias, los datos se archivan en la base de datos 1 y se envían a la base de datos 2 para su búsqueda y nuevamente si no hay coincidencias se archivan en la base de datos 2.

Nota: Se pueden perder coincidencias potenciales si los datos (a) *solo* se buscan y no se *archivan* en la base de datos 2 porque el resultado de la búsqueda se limitaría a la hora exacta de la búsqueda. Por ejemplo, si los datos de búsqueda adicionales (b), que coinciden con los datos biométricos (a), se incorporan y se buscan en la base de datos 2 *después* del momento de la búsqueda de datos (a), no se encontrará ninguna coincidencia porque los datos (a) no fueron archivados y por lo tanto no están expuestos a la búsqueda de datos (b). Por lo tanto, en las transferencias unidireccionales de datos entre dos o más bases de datos es importante que cada base de datos registre los datos después de la búsqueda para asegurar que sean discernidos por búsquedas posteriores y, por lo tanto, mantener una cobertura continua.

La gestión de datos también puede ser un problema con las transferencias de una vía, especialmente si las bases de datos se encuentran en diferentes jurisdicciones o países. Cada propietario de los datos debe buscar un acuerdo formal con los otros socios con respecto al tiempo de retención y la política de eliminación de los datos compartidos. En ausencia de un acuerdo de este tipo, no existe ninguna obligación de cumplimiento por parte de los propietarios de las otras bases de datos, que pueden no estar sujetos a las mismas leyes que la base de datos de acogida. También pueden ser reacios a llevar a cabo las eliminaciones solicitadas por otras razones, tales como limitaciones financieras, de recursos o de tiempo.

Búsqueda bidireccional recíproca: Los datos biométricos (a) se registran y se buscan en la base de datos 1. Si no se encuentran coincidencias, los datos se archivan en la base de datos 1 y se envían a la base de datos 2 para la búsqueda pero los datos (a) no son retenidos por la base de datos 2. De la misma manera, si los datos biométricos (b) se registran y se buscan en la base de datos 2 y luego se envían a la base de datos 1 para su búsqueda, no son retenidos por la base de datos 1. Este método se replica para cualquier cantidad de bases de datos en la red, ya que cada base de datos busca sus nuevos registros de datos a través de las otras bases de datos. El riesgo de perder coincidencias potenciales (como en la búsqueda unidireccional) se evita al archivar los datos en la base de datos de acogida antes de buscarlos en la red para evitar brechas en el tiempo que de otra manera permitirían que las búsquedas entrantes simultáneas en la red se pierdan entre sí.

Nota: A este sistema a menudo se le conoce como 'búsqueda múltiple de registro único' o 'ingresar una vez una búsqueda de muchos'. La base de datos que posee los mismos los archiva después de la búsqueda, pero todas las demás bases de datos solo realizan una búsqueda. Esto simplifica la gestión de datos porque los datos del propietario se almacenan solo en su base de datos y esto también reduce la cantidad de datos archivados en la red. La secuencia de búsquedas entre bases de datos debe gestionarse cuidadosamente, particularmente cuando varias bases de datos en una jurisdicción se incorporan a una base de datos en otra jurisdicción. Por ejemplo, las combinaciones de búsqueda

entre las bases de datos en la jurisdicción (1) deben agotarse por completo antes de que cualquiera de ellas envíe búsquedas a la jurisdicción (2), de lo contrario, las coincidencias se pueden divulgar en la jurisdicción (2) que ya deberían haberse encontrado en la jurisdicción (1). Esto se puede evitar enviando búsquedas desde la jurisdicción (1) a la jurisdicción (2) a través de un único cauce gestionado.

3.3.2.1 Biometría predictiva: el uso proactivo de las redes biométricas de datos para prevenir ataques terroristas

La integración de las bases de datos biométricos en el amplio espectro de la aplicación de la ley y de la gestión de fronteras (y los datos biométricos militares, si están disponibles) permite analizar los resultados colectivos de la red no solo desde la perspectiva de las necesidades comerciales discretas, por ejemplo, detección de delitos o controles de identidad en la frontera, etc., sino también como una serie o patrón mucho más amplio de "eventos biométricos" por derecho propio. En términos de una amenaza terrorista, cada evento puede tener una relevancia directa o indirecta o quizás parecer completamente inocuo y no tener un valor aparente, pero cuando se coloca dentro del contexto de otra información o evento biométrico, puede contribuir significativamente a la imagen de inteligencia más amplia de los movimientos y actividades terroristas. Algunas de estas consecuencias pueden ser bastante explícitas, como revelar acuerdos de viaje sospechosos o establecer vínculos con delitos de terrorismo, pero otras pueden ser más sutiles y matizadas, pero aun así proporcionar indicadores valiosos cuando se toman en consideración con otro material pertinente. Este método, que se muestra a continuación en la Figura 8, se basa en el uso tradicional, reactivo y en gran parte pasivo de las bases de datos biométricos con fines de investigación e intenta salvar vidas mediante la prevención de ataques terroristas antes de que ocurran mediante el uso de datos biométricos de la más amplia gama de fuentes junto con otros productos de inteligencia.

Figura 8 – El modelo biométrico predictivo

Las bases de datos biométricos tradicionales (descriptas en la Sección 1) se diseñaron para ser reactivas y plantear preguntas de investigación basadas en la identidad y en actividades actuales o pasadas, tales como "*¿Te conocemos, quiénes son tus asociados y qué has hecho?*" Las bases de datos biométricos integradas obviamente pueden responder a las mismas preguntas, pero también pueden usarse de manera proactiva para inferir y predecir posibles acciones y asociaciones futuras, es decir, "*¿Qué estás planeando con tus asociados o es probable que hagan y cuándo y dónde*?". Por lo tanto, un análisis cuidadoso de todos los resultados a través de la red es esencial y puede ser un factor crítico de éxito en la evaluación y anticipación de la actividad terrorista cuando se combina con otra inteligencia. Esto se aplica igualmente a la gestión posterior de los resultados.

3.3.3 Gestión de los resultados

3.3.3.1 Evaluación contextual de resultados

En los sistemas biométricos independientes, los resultados pueden automatizarse en gran medida con una interacción humana mínima (Véase la Sección 1), pero cuando los datos contenidos en estos sistemas se integran en una red de bases de datos biométricos multifuncionales y se realizan búsquedas cruzadas, es absolutamente vital que los resultados se revisen y comprendan a fondo antes de tomar cualquier acción. La evaluación contextual de estos resultados y aquellos que gestionan las consecuencias resultantes deben tener en cuenta los siguientes factores:

Asegurar una respuesta proporcional legal y gestionar identificaciones incorrectas o colaterales: es natural que quienes reciben y manejan los resultados de cualquier tipo de base de datos biométrica, y especialmente una relacionada con el terrorismo, formen opiniones peyorativas y asuman que

cualquier persona identificada por ese sistema debe ser un terrorista. Sin embargo, este no es siempre el caso por las siguientes razones:

1. un error humano o del sistema puede identificar erróneamente a una persona y, aunque esto es muy raro, debería formar parte integral de cualquier protocolo de revisión, especialmente si otros datos o pruebas parecen arrojar dudas sobre el resultado
2. Los gobiernos u otras partes pueden querer hacer un mal uso de los resultados biométricos al hacer alegaciones falsas de actividades terroristas con el fin de perturbar a su oposición, activistas políticos o activistas de derechos humanos (véase la Sección 2.2.5.)
3. La persona identificada puede no estar involucrada en el terrorismo de manera alguna. Es por esta razón que el valor contextual y relativo de cualquier resultado debe evaluarse adecuadamente *antes* de tomar cualquier acción.

Por ejemplo, un elemento o lugar clave en una investigación sobre terrorismo puede haber sido inocentemente contaminado por alguien que no está involucrado en ninguna actividad terrorista o por personal policial descuidado. El material forense luego es recogido por los investigadores de la escena del crimen y científicos forenses y se registra en la red de base de datos apropiada. Esta información forense "colateral" podría responder a las búsquedas en toda la red y generar una coincidencia, por ejemplo, cuando el individuo posteriormente proporciona un dato biométrico para cruzar una frontera. Las acciones tomadas por esas autoridades fronterizas, por lo tanto, deben basarse en el contexto completo de cualquier coincidencia biométrica y no en un supuesto automático de que la persona es un terrorista solo debido a la coincidencia biométrica. La respuesta de los organismos encargados de hacer cumplir la ley debe ser medida y proporcionada de conformidad con el derecho internacional en materia de derechos humanos. Estos procedimientos de evaluación contextual deben estar sujetos a una supervisión sólida e independiente para evitar posibles detenciones ilegales o posibles errores judiciales.

Estrategia de comunicación: Con el fin de garantizar que las evaluaciones contextuales se apliquen de manera coherente y eficaz a la gestión de los resultados, las autoridades deben establecer líneas de comunicación claras, seguras y continuas entre quienes evalúan los resultados biométricos y el personal operativo de primera línea y los responsables de la toma de decisiones que deben actuar sobre la información. Esto implicará facilitar el diálogo urgente entre los propietarios de datos de la escena del crimen (una agencia de cumplimiento de la ley) y los funcionarios que tratan con una persona detenida debido a una coincidencia con los datos de la escena del crimen. El intercambio de este y otros tipos de información es bastante frecuente y normalmente es un procedimiento operativo estándar en los círculos nacionales e internacionales de aplicación de la ley. La red de comunicaciones también deberá priorizar los resultados de la base de datos y operar dentro de los plazos acordados, especialmente cuando las personas son arrestadas o detenidas debido a una coincidencia biométrica. La estrategia de comunicación también debe establecer la lista completa de destinatarios de los resultados biométricos de la red y establecer criterios de no conflicto para prevenir o resolver disputas entre dos destinatarios con respecto a cuestiones como la primacía jurisdiccional o las prioridades de investigación.

Modalidades, estándares de informes de datos de inteligencia forense e interpretación científica: algunas redes de base de datos biométricos pueden usar una sola modalidad, pero es más habitual y efectivo tener un rango de modalidades que operan en paralelo a través de una red biométrica, por ejemplo, huellas dactilares, ADN y rostro. Los resultados de los sistemas multimodales brindarán una visión más amplia de la actividad cuando se combinen con los sistemas multifuncionales que contendrán datos de inteligencia forense de las escenas del crimen, así como datos de referencia de una variedad de fuentes. El material forense recuperado de la escena del crimen no siempre proporciona una coincidencia "completa" con los datos de referencia debido a los factores que se

describen en la Sección 1, pero aún puede ser de inmenso valor probatorio para una investigación. Estos dos componentes deben ser completamente apreciados y comprendidos por aquellos que recopilan las salidas de la base de datos. La fuerza relativa del emparejamiento y su potencial valor probatorio o de investigación, junto con cualquier otra información relevante obtenida durante la evaluación contextual, deben compilarse e informarse al funcionario, investigador o analista correspondiente para que se puedan tomar las medidas adecuadas y proporcionadas. Por lo tanto, es una buena práctica solo registrar datos que puedan presentarse como evidencia en un tribunal de justicia. Esto permite que todas las coincidencias se utilicen por completo en una investigación y se divulguen o presenten en el tribunal.

Caso de estudio 10 – Procedimientos que regulan los avisos de INTERPOL
Ejemplo operativo de la gestión del intercambio de datos internacional

Aunque el sistema de Aviso Rojo de INTERPOL no aborda los resultados biométricos, tiene fuertes paralelos con los procesos de evaluación estipulados en la Sección 3.3.3.1. y proporciona un modelo sólido para la gestión de datos a escala global. Está obligado a operar de acuerdo con el estado de derecho internacional y las reglas de la organización y garantiza que se facilite la comunicación efectiva entre las partes clave y que exista un sistema establecido para tratar de manera independiente y sólida las quejas y apelaciones de aquellos que están sujetos a los procedimientos de Aviso Rojo.

Un Aviso Rojo es una solicitud para arrestar provisionalmente a una persona mientras se encuentre pendiente la extradición emitida por la Secretaría General a solicitud de un país miembro sobre la base de una orden de arresto nacional válida. Los avisos rojos también pueden emitirse a pedido de los tribunales internacionales.

Además de los avisos rojos, INTERPOL emite otros tipos de avisos, por ejemplo, un aviso azul que se emite a solicitud de un país miembro con el fin de buscar información en el contexto de una investigación penal. Los países miembros también pueden emitir difusiones, que son solicitudes de cooperación que se distribuyen directamente entre los países miembros.

INTERPOL no puede insistir ni obligar a ningún país miembro a arrestar a una persona que sea objeto de un Aviso Rojo. INTERPOL tampoco puede exigir a ningún país miembro que tome ninguna acción en respuesta a la solicitud de otro país miembro. Cada país miembro de Interpol decide por sí mismo qué valor legal otorgar al Aviso Rojo dentro de sus fronteras. Al tomar la decisión de actuar sobre una notificación o cualquier otra solicitud, un país asume toda la responsabilidad de esa decisión. La efectividad operativa de los acuerdos del Aviso Rojo depende de que las referencias entre las Oficinas Centrales Nacionales (NCB, por su sigla en inglés) puedan gestionarse 24/7/365.

Todos los avisos y difusiones deben cumplir con las normas y regulaciones de INTERPOL. Esto incluye el Artículo 2 de la Constitución de Interpol, que hace una referencia explícita al espíritu de la Declaración Universal de Derechos Humanos, y el Artículo 3 de la Constitución de Interpol, según el cual está "estrictamente prohibido que la organización realice cualquier intervención o actividad de un carácter político, militar, religioso o racial". Las Normas de INTERPOL sobre el procesamiento de datos establecen criterios adicionales para la publicación de cada tipo de aviso, la asignación de responsabilidades entre las distintas entidades, es decir, el país solicitante, la Secretaría General, los países receptores, etc.

Supervisión regulatoria: existen varios niveles de control para garantizar el cumplimiento de las regulaciones de INTERPOL. El primero son las NCB que envían la solicitud de cooperación policial

(por ejemplo, una solicitud de Aviso Rojo). Son totalmente responsables de cualquier información que proporcionen a las bases de datos de Interpol o que circulen utilizando el sistema de información de INTERPOL. Deben asegurarse de que la información sea precisa, relevante y actualizada, y que su procesamiento sea acorde a la Constitución de la Organización, así como a su legislación nacional.

La segunda es la sede de la Secretaría General de INTERPOL. En noviembre de 2016, la Secretaría General estableció un grupo de trabajo especializado que comprende una unidad multidisciplinaria que incluye abogados, oficiales de policía, analistas y especialistas operativos para revisar todos los niveles de procesamiento de datos, incluso en relación con los Avisos Rojos y las difusiones. Todas las solicitudes son examinadas cuidadosamente por el equipo de trabajo para garantizar que cumplen con la constitución o las normas de INTERPOL. Como parte de la revisión por el equipo de trabajo, se puede solicitar información adicional de todas las fuentes relevantes para decidir si se emite un Aviso o no. Además, un país miembro puede plantear inquietudes con respecto a la información procesada por otro país miembro, incluida la publicación de un Aviso Rojo, si considera que esto no se realizó de conformidad con las normas de Interpol.

Gestión de refugiados: desde junio de 2014, INTERPOL ha implementado una nueva política en relación con los casos relacionados con refugiados. Esto permite a Interpol ayudar a los países miembros a evitar que los delincuentes abusen de la condición de refugiado, al tiempo que ofrece garantías adecuadas y efectivas para proteger los derechos de los refugiados. Cada Aviso Rojo y solicitud de difusión contra un refugiado es evaluada por la Secretaría General o, cuando corresponda por la Comisión para el Control de los Archivos de INTERPOL (Véase la Sección 3.1.2.), caso por caso. En general, no se permitirá el procesamiento de Avisos Rojos y las difusiones contra los refugiados si el estatus de refugiado o solicitante de asilo ha sido confirmado y el aviso/difusión ha sido solicitado por el país donde la persona teme la persecución.

Derechos de las personas sujetas a un aviso/difusión: la decisión de publicar un aviso o registrar información en las bases de datos de INTERPOL no tiene ningún efecto sobre los derechos de la persona, incluido su derecho a ser presuntamente inocente, el derecho a impugnar el caso ante las autoridades pertinentes del país que emitió la orden de arresto y solicitó la asistencia de INTERPOL, o el derecho de impugnar el caso ante las autoridades nacionales que consideran la solicitud de extradición.
Un individuo tiene al menos las siguientes tres opciones a través de las cuales puede impugnar un Aviso o difusión:

- Defender su caso ante las autoridades nacionales del país solicitante, ya sea directamente o mediante la contratación de representación legal. Dado que un aviso rojo se basa en una orden de arresto válida, si las autoridades nacionales competentes retiran la orden de arresto, se eliminará el aviso rojo.
- Contactar a la Comisión de Control de los Archivos de INTERPOL
- Solicitar a su país que tome el caso por sí mismo y objete el Aviso Rojo.

Toda vez que se cancele un Aviso Rojo o difusión, por el motivo que sea, se enviará un mensaje a todos los países miembros para informarles de la decisión y se les solicitara que eliminen cualquier información relacionada de sus bases de datos nacionales.

Estas salvaguardas aseguran un proceso transparente y estructurado para abordar y resolver tales problemas y para evitar el posible uso indebido de Avisos Rojos.

3.3.3.2 Objetivos estratégicos y directrices de los investigadores

Las estrategias nacionales y regionales de lucha contra el terrorismo deberían reflejar la importancia de la ciencia forense y la biometría. Los organismos encargados de hacer cumplir la ley y la administración de las fronteras deberían apoyar activamente estas estrategias empleando todos los recursos forenses y biométricos disponibles y manteniendo bases de datos efectivas.

Las estrategias forenses y biométricas también se pueden establecer a nivel de investigación y esta práctica debería fomentarse a través de la capacitación y la doctrina operacional. El funcionario superior a cargo de una investigación sobre terrorismo debería establecer los principales objetivos forenses y biométricos al comienzo de la investigación y las características biométricas deberían incluir rutinariamente:

- Todas las muestras de referencia biométricas del arrestado obtenidas durante la investigación deben ser de calidad óptima
- Todas las escenas del crimen deben someterse a exámenes forenses exhaustivos y totalmente secuenciales para maximizar el rendimiento de ADN y huellas dactilares para establecer asociaciones terroristas más amplias además de los requisitos forenses específicos de la investigación
- Todos los datos biométricos pertinentes, recuperados durante la investigación, deben registrarse y/o buscarse en todas las bases de datos nacionales e internacionales relevantes

Estos tres elementos de la estrategia biométrica abordan:

1. *las necesidades de la investigación*, es decir, datos de referencia biométricos de alta calidad para una comparación efectiva 1: 1 con el material de la escena del crimen y el registro y la búsqueda en las bases de datos para avanzar en la investigación y
2. *los requisitos de otras investigaciones sobre terrorismo y operaciones de inteligencia* al tener una visión más amplia de las escenas del crimen y la recolección de material biométrico que puede no ser necesariamente relevante para la investigación central, pero puede revelar asociados, células o redes previamente desconocidos y
3. los datos biométricos recopilados de una investigación pueden no solo ayudar a resolver o establecer vínculos con otras investigaciones, sino que también podrían *prevenir futuros ataques terroristas* y, al hacerlo, salvar muchas vidas.

3.4 Prácticas recomendadas

a) Los Estados deberían contrarrestar la amenaza que representa el movimiento continuo de terroristas a través de las fronteras internacionales mediante el empleo de sistemas biométricos para proteger sus fronteras y activos nacionales y compartir legalmente datos biométricos con socios internacionales.

b) La seguridad de la frontera se puede administrar de manera más efectiva mediante el uso de técnicas de verificación biométrica 1: 1 combinadas con las comprobaciones de los listados de alerta biométrica 1:n para rastrear y detectar a los terroristas y sus asociados. Los listados de alerta biométrica se pueden crear a cualquier escala, desde pequeñas colecciones de referencia hasta la conectividad total con la gestión de la identidad de las fuerzas del orden público y las bases de datos de detección de delitos, sujetas a la legislación nacional, las restricciones reglamentarias y el derecho internacional en materia de derechos humanos.

c) Se recomienda encarecidamente a los Estados que maximicen su uso de las bases de datos biométricos de Interpol (rostro, huellas dactilares y ADN) para contrarrestar la amenaza del terrorismo y los combatientes terroristas extranjeros.

d) El intercambio de datos biométricos a nivel internacional es una herramienta vital para combatir el terrorismo, pero debe realizarse de conformidad con el derecho internacional en materia de derechos humanos. Los gobiernos deben asegurar que, al compartir datos biométricos, no facilitarán arrestos que conducirán a la tortura o la imposición de la pena de muerte.

e) Es imperativo que el contexto completo de todas las coincidencias biométricas se investigue exhaustivamente antes de tomar cualquier acción, asegurando el pleno cumplimiento de la legislación internacional en materia de derechos humanos.

f) Las estrategias nacionales y regionales de lucha contra el terrorismo deben reflejar la importancia de la ciencia forense y la biometría al asignar una responsabilidad a las agencias de cumplimiento de la ley y de gestión de fronteras para maximizar su recopilación y uso legal de material forense o biométrico y mantener bases de datos efectivas y protocolos de intercambio de datos.

3.4.1 Documentos de referencia

Guía sobre Gestión de Control de Fronteras del Programa de Identificación de Viajeros (TRIP) de la OACI, Montreal (2018)

Guías de Implementación de Mensajes PNRGOV EDIFACT & XML:
www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

Pautas sobre PNR de WCO/IATA/ICAO (Doc 9944)

Documento 9303 de ICAO: Documentos de viajes de lectura mecánica

www.interpol.int/INTERPOL-expertise/I-Checkit

www.interpol.int/INTERPOL-expertise/databases

The INTERPOL ADN Gateway – Publicación Oficial, febrero de 2017

Guía de mejores prácticas de imágenes faciales de INTERPOL de octubre de 2015 y hoja de datos de reconocimiento facial

Directrices de INTERPOL sobre transmisión de huellas dactilares 2012

Normas de INTERPOL sobre procesamiento de información a los fines de cooperación con la policía internacional

ETIAS
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

www.un.org/sc/ctc/

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/fact-sheets/docs/20161116/factsheet_-_etias_en.pdf

http://europa.eu/rapid/press-release_MEMO-16-3706_en.htm

Publicación Especial 1152 de NIST 'Latent Interoperability Transmission Specification'
www.nist.gov

4. APÉNDICES

4.1 Acrónimos

ABC	Control Automatizado de Fronteras
AFIS	Sistema Automatizado de Identificación de Huellas Dactilares
API	Información Anticipada sobre Pasajeros
BCP	Puntos de Cruce de Frontera
BMS	Sistema Informático de Gestión de Fronteras
CCF	Comisión de Control de Archivos de Interpol
CCTV	Circuito Cerrado de Televisión
eBMS	Sistema Informático de Gestión de Fronteras Electrónico
EER	Tasa de Error Igual
ETS	Sistemas Electrónicos de Viaje
FAR	Tasa de Falsa Aceptación
FRR	Tasa de Falso Rechazo
FTA	Tasa de Falla de Obtención
FTF	Combatientes Terroristas Extranjeros
IEC	Comisión Electrotécnica Internacional
OACI	Organización de Aviación Civil Internacional
iAPI	Información Anticipada sobre Pasajeros Interactiva
ISO	Organización Internacional de Normalización
LDS	Estructura de Datos Lógicos
MRZ	Zona de Lectura Mecánica
PKI	Infraestructura de Clave Pública
PNR	Registro de Nombre del Pasajero
QMS	Sistema de Gestión de Calidad
SIS	Sistema de Información de Schengen
STR	Repeticiones Cortas en Tándem
TAR	Tasa de Aceptación Verdadera
TRR	Tasa de Rechazo Verdadero
VIS	Sistema de Información de Visas

4.2 Glosario de términos biométricos

Acreditación: ISO define la acreditación como "el reconocimiento formal por un organismo independiente, generalmente conocido como organismo de acreditación, respecto de que un organismo de certificación opera de conformidad con las normas internacionales".

Sistema Automatizado de Identificación de Huellas Dactilares: un sistema electrónico diseñado para almacenar y realizar búsquedas de grandes volúmenes de (1) conjuntos de impresiones de dedos y palmas de referencia y (2) marcas de dedos y palmas tomadas en la escena del crimen. Las Búsquedas de Gestión de Identidad generalmente generan sólo una respuesta o un resultado sin rastros. En la Búsqueda de Detección de Delitos los resultados se presentan como un listado de posibles coincidencias. Un perito en huellas dactilares analiza las respuestas y confirma las coincidencias arrojadas por el sistema.

Modalidad Biométrica: el tipo de datos biométricos utilizado por un sistema o contexto operativo, tal como huellas dactilares, rostro, iris, etc.

Certificación: ISO define la certificación como "la emisión por parte de una organización independiente de una declaración escrita (un certificado) respecto de que un producto, servicio o sistema cumple con los requisitos especificados".

Evaluación de Conformidad: IEC define la evaluación de conformidad con la "demonstración del cumplimiento de los requisitos especificados respecto de un producto, proceso, sistema, persona u organización".

Búsqueda de Detección de Delitos: un protocolo de búsqueda con una interfaz de doble sentido que realiza búsquedas (1) de datos de referencia contra los datos de la escena del crimen y (2) de datos de la escena del crimen contra los datos de referencia.

Datos de la Escena del Crimen: generados a partir de las muestras y artículos recuperados en las escenas del crimen.

Tasa de Error Igual (EER): hace referencia a la configuración del límite específico en donde la Tasa de Falsa Aceptación y la Tasa de Falso Rechazo son iguales.

Gestión de Excepciones: medidas contingentes implementadas en caso de falla de un sistema biométrico, por ejemplo intervención humana, sistemas de back-up, etc.

Tasa de Falla de Obtención (FTA): es la proporción de todas las operaciones registradas que no pueden completarse debido a fallas en la presentación (no se capturó la imagen), extracción de características o etapas de control de calidad.

Tasa de Falsa Aceptación (FAR): la cantidad de aceptaciones falsas como proporción de la cantidad total de averiguaciones biométricas que deberían haberse rechazado, es decir, la cantidad de no coincidencias *generadas y presentadas como coincidencias por el sistema* como proporción de las no coincidencias genuinas.

Tasa de Falso Rechazo (FRR): la cantidad de rechazos falsos como proporción de la cantidad de averiguaciones biométricas que deberían haberse aceptado, es decir, la cantidad de coincidencias *generadas y presentadas como no coincidencias por el sistema* como proporción de las coincidencias genuinas.

Identificación (también conocido como comparación uno de muchos o 1:n): esta es una función de búsqueda que no depende de una identidad sugerida y por lo tanto interroga a toda la base de datos para obtener una posible coincidencia.

Búsqueda de Gestión de Identidad: determina si un sujeto ya se encuentra registrado en una base de datos mediante la comparación de sus datos de referencia contra todos los datos de referencia archivados en la base de datos.

Transformación: muestras biométricas (por ejemplo imágenes faciales) de dos o más donantes que se fusionan para permitir la verificación exitosa de cualquiera de los sujetos donantes contra la identidad transformada.

Sistema de Gestión de Calidad: protocolo formal que define y documenta procesos, procedimientos y responsabilidades para satisfacer los objetivos de calidad. El sistema está diseñado para coordinar y dirigir las actividades de la organización a fin de satisfacer los requisitos del cliente y regulatorios, abordar las no conformidades y fomentar una cultura de mejora continua.

Datos de Referencia: recogidos bajo condiciones controladas, de aquellas personas arrestadas por un delito o sospechadas de haberlo cometido, por ejemplo, las huellas dactilares de los 10 dedos de la mano tomadas en forma electrónica mediante un escáner o mediante el método tradicional de la tinta y el papel; hisopados bucales extraídos de la cara interna de la mejilla de la persona arrestada o una muestra de cabello o sangre que se procesan para crear un perfil de ADN completo; fotografías digitales del rostro, etc.

Búsqueda de Delitos/Eventos Seriales: la búsqueda de datos biométricos o de la escena del crimen a través de una base de datos que contiene datos de escenas del crimen similares para identificar cualquier coincidencia y por lo tanto establecer conexiones entre delitos o conexiones entre eventos en una única investigación.

Suplantación: (también denominada ataque de presentación) es la presentación de una biometría falsificada (como una máscara de látex, fotografía, dedo falso o grabación de voz) de un usuario legítimo registrado para obtener acceso no autorizado a un sistema de reconocimiento biométrico.

Límite: una configuración ajustable para los sistemas biométricos. Regula el equilibrio entre la aceptación y el rechazo de una aplicación determinada.

Tasa de Rendimiento: el volumen de gente que usa un sistema biométrico dentro de un plazo de tiempo determinado.

Tasa de Aceptación Verdadera (TAR): la medida de la capacidad del sistema de hacer coincidir correctamente los atributos de identidad de una misma persona.

Tasa de Rechazo Verdadero (TRR): la medida de la cantidad de veces en que el atributo de identidad biométrica de una persona *no* coincide correctamente con los atributos de identidad biométrica de otras personas incluidas en la base de datos, es decir, la frecuencia de no coincidencias correctas.

Verificación: (también conocido como comparación uno a uno o 1:1). Este modelo utiliza una identidad declarada para seleccionar sólo una plantilla de la base de datos para comparación con la plantilla consultada. Esencialmente, es un proceso que compara la plantilla consultada con la plantilla

de la base de datos y confirma que las dos plantillas se originan en la misma persona o que no lo hacen.

4.3 Directorio de Organismos Internacionales

Biometrics Institute www.biometricsinstitute.org

Organización de Aviación Civil Internacional www.icao.int

Comité Internacional de la Cruz Roja www.icrc.org

Organización Internacional de Policía Criminal (INTERPOL) www.interpol.int

Comisión Electrotécnica Internacional www.iec.ch

Organización Internacional de Normalización www.iso.org

4.4 Oficina de Lucha contra el Terrorismo de las Naciones Unidas (UNOCT)

La Secretaría de las Naciones Unidas, agencias, fondos, programas y organizaciones afiliadas contribuyen a la implementación de la Estrategia Global contra el Terrorismo de las Naciones Unidas tanto en forma individual como a través de su participación en el Equipo Especial de Coordinación Global contra el Terrorismo de las Naciones Unidas (GCTCCTF).

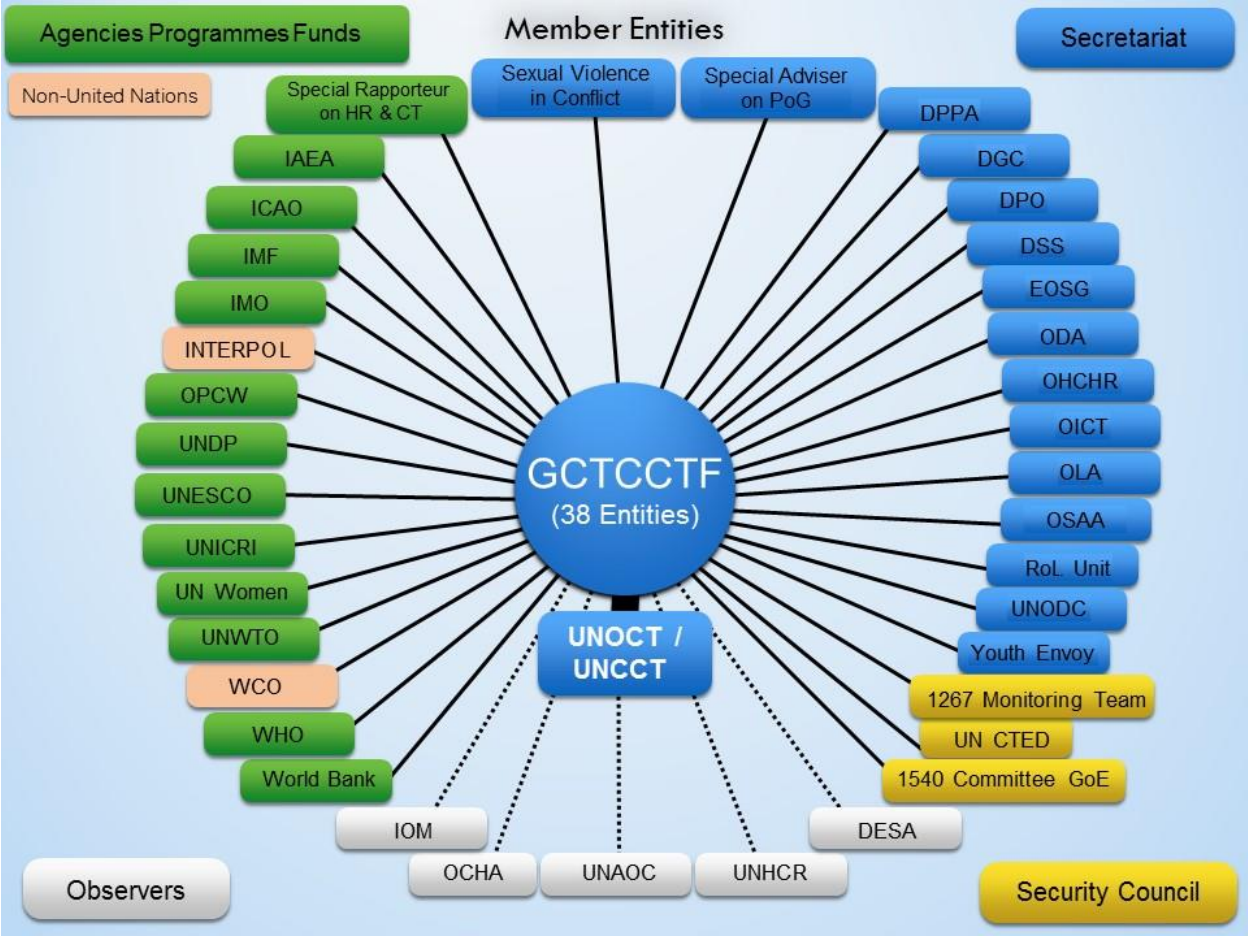
El Equipo Especial está integrado por 38 entidades internacionales e INTERPOL que en virtud de su trabajo tienen una participación en los esfuerzos multilaterales contra el terrorismo. Cada entidad realiza aportes acordes a su mandato. Los miembros del Equipo Especial incluyen a la UNOCT y a las siguientes entidades:

1. Equipo de Vigilancia sobre Al-Qaeda y los Talibanes
2. Director Ejecutivo del Comité contra el Terrorismo (CTED)
3. Departamento de Operaciones de Mantenimiento de la Paz (DOMP)
4. Departamento de Asuntos Políticos y de Consolidación de la Paz (DAPCP)
5. Departamento de Comunicación Global (DCG)
6. Departamento de Seguridad (DSS)
7. Grupo de Expertos del Comité 1540
8. Organismo Internacional de Energía Atómica (OIEA)
9. Organización de Aviación Civil Internacional (OACI)
10. Organización Marítima Internacional (OMI)
11. Fondo Monetario Internacional (FMI)
12. Organización Internacional de Policía Criminal (INTERPOL)
13. Oficina de Asuntos de Desarme (ODA)
14. Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH)
15. Oficina de Asuntos Jurídicos (OAJ)
16. Oficina del Secretario General (OSG)
17. Oficina del Asesor Especial para la Prevención del Genocidio

18. Oficina del Representante Especial del Secretario General para la Cuestión de los Niños y los Conflictos Armados (CNCA)
19. Oficina del Representante Especial del Secretario General sobre la Violencia Sexual en los Conflictos (VSC)
20. Oficina del Enviado Especial del Secretario General para la Juventud
21. Organización para la Prohibición de las Armas Químicas (OPAQ)
22. Relator Especial sobre la promoción y la protección de los derechos humanos en la lucha contra el terrorismo
23. Programa de las Naciones Unidas para el Desarrollo (PNUD)
24. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)
25. Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI)
26. Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)
27. Oficina del Asesor Especial para África (OSAA)
28. Dependencia de las Naciones Unidas sobre el Estado de Derecho
29. ONU Mujeres
30. Organización Mundial del Turismo (OMT)
31. Organización Mundial de Aduanas (OMA)
32. Banco Mundial
33. Organización Mundial de la Salud (OMS)

Observadores

34. Organización Internacional para las Migraciones (OIM)
35. Oficina de Coordinación de Asuntos Humanitarios (OCAH)
36. Departamento de Asuntos Económicos y Sociales (DAES)
37. Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR)
38. Alianza de Civilizaciones de las Naciones Unidas (UNAOC)



4.5 Grupo de Trabajo de la UNOCT sobre Gestión de Fronteras y Cumplimiento de la Ley en relación con la Lucha contra el Terrorismo de las Naciones Unidas

Este Grupo de trabajo Interinstitucional de las Naciones Unidas tiene como objetivo brindar orientación a los Estados Miembros sobre la implementación de las medidas legales, institucionales y prácticas requeridas de lucha contra el terrorismo relacionadas con el control de fronteras. Se enfoca particularmente en las siguientes áreas: movilidad terrorista; integridad y seguridad de los documentos de viaje; movimiento ilícito de efectivo e instrumentos negociables al portador; movimiento y procesamiento de bienes; movimiento ilícito de armas pequeñas, armas ligeras, municiones, explosivos y armas de destrucción masiva; aviación y seguridad marítima; sistemas de advertencia temprana y alerta; y control de las fronteras abiertas.

Competencia

El Grupo de Trabajo se creó para ayudar a los Estados Miembros a reforzar la gestión de fronteras y sus sistemas de control de fronteras de conformidad con lo estipulado en Pillar II, párrafos 4, 5, 7, 8, 13 a 16 y Pillar III, párrafos 2, 4 y 11 a 13 de la Estrategia Global de Lucha contra el Terrorismo de las Naciones Unidas (A/RES/60/288).

Se han desarrollado los Términos de Referencia del Grupo de Trabajo sobre Gestión de Fronteras Relacionado con la Lucha contra el Terrorismo.

Estado

El Grupo de Trabajo está implementando actualmente un proyecto sobre gestión coordinada de fronteras, que recopila todos los convenios internacionales, normas y mejores prácticas relevantes en un formato fácil de usar para ayudar a los Estados interesados a construir los mecanismos institucionales y de procedimiento para un sistema de gestión de fronteras efectivo. El Grupo de Trabajo ha finalizado una plantilla de trabajo sobre la gestión coordinada de las fronteras. Esta plantilla continuará mejorándose a través del diálogo y las consultas continuas con Estados Miembros y organizaciones internacionales.

Entidades

Presidentes conjuntos:

- Dirección Ejecutiva del Comité contra el Terrorismo (DECT) (Líder)
- Organización Mundial de Aduanas (OMA)
- Organización Internacional de Policía Criminal (INTERPOL)

Entidades centrales:

- Oficina de Lucha contra el Terrorismo de las Naciones Unidas (UNOCT)
- Equipo Especial de Coordinación Global contra el Terrorismo de las Naciones Unidas (GCTCCTF)
- Organización de Aviación Civil Internacional (OACI)
- Organización Marítima Internacional (OMI)
- Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)
- Organización Internacional para las Migraciones (OIM)
- Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH)
- Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI)
- Oficina de Asuntos de Desarme (OAD)
- Equipo de Supervisión 1267
- Grupo de Expertos del Comité 1540
- Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR) (Observador)

Otras entidades miembro:

- Departamento de Operaciones de Mantenimiento de la Paz (DOMP)
- Organización para la Prohibición de Armas Químicas (OPAQ)
- Programa de Naciones Unidas para el Desarrollo (PNUD)
- Organización Mundial de la Salud (OMS)
- Departamento de Asuntos Económicos y Sociales (DAES)

El Grupo de Trabajo lleva a cabo actividades sobre un número de temas clave:

- Movilidad y procesamiento de personas
- Integridad y seguridad del proceso de emisión de documentos
- Movimiento de efectivo y otros instrumentos negociables al portador
- Movimiento y procesamientos de bienes
- Movimiento de armas pequeñas, armas ligeras, municiones, explosivos y CBRN

- Seguridad marítima
- Seguridad aeronáutica
- Sistemas de advertencia temprana y alerta
- Control de la frontera abierta
- Necesidad general de respetar los derechos humanos

Movilidad y procesamiento de personas

Una consecuencia importante de los ataques terroristas llevados a cabo en todo el mundo en los últimos años es el mayor vínculo entre el movimiento de personas a través de las fronteras y las medidas adoptadas para salvaguardar la seguridad nacional. Debido a que los procesos que facilitan los viajes y los intercambios económicos y culturales también son explotados por terroristas, las medidas dirigidas a prevenir el terrorismo se han vinculado explícitamente a la gestión y regulación de los movimientos transfronterizos. Estas medidas incluyen la implementación de sistemas integrados de gestión de fronteras de pasajeros, la emisión de documentos de viaje seguros, la promoción del intercambio de información entre las partes interesadas, la capacitación y el desarrollo de capacidades. Las mejoras en estas áreas pueden ayudar a mejorar los sistemas de seguridad e inmigración y, al mismo tiempo, facilitar el movimiento transfronterizo de personas. Algunas de estas medidas son tecnológicamente complejas y altamente innovadoras, pero se pueden implementar varias medidas más simples en las áreas tradicionales de gestión de la migración con el fin de mejorar la capacidad general. Tales medidas siempre deben estar justificadas por el nivel de amenaza al que se enfrentan, en particular porque una mayor seguridad puede llevar a una mayor obstrucción y una posible intrusión en la privacidad y los derechos civiles.

Integridad y seguridad del proceso de emisión de documentos

La seguridad de los documentos de viaje y la gestión de la identidad son herramientas importantes para prevenir la movilidad de los terroristas y para combatir la delincuencia transfronteriza. En manos de terroristas, un documento de viaje fraudulento puede ser tan peligroso como un arma. A medida que los pasaportes modernos se han vuelto más seguros y más difíciles de falsificar, los criminales y los terroristas intentan cada vez más falsificar documentos de respaldo (certificados de nacimiento, tarjetas de identificación nacionales, etc.) o solicitar pasaportes "emitidos oficialmente". Por lo tanto, es esencial que los Estados desarrollen e implementen especificaciones universales para la gestión de identidades y la seguridad de los documentos de viaje (incluso en el proceso de emisión) para hacer frente a estas vulnerabilidades.

Movimiento de efectivo y otros instrumentos negociables al portador

El contrabando de efectivo y/o instrumentos negociables al portador (BNI) a través de las fronteras es uno de los métodos preferidos empleados por los terroristas para mover fondos a través de las fronteras internacionales, ya sea con fines de financiamiento del terrorismo o para el lavado de las ganancias de actividades ilícitas. Los gobiernos confían a sus servicios de aduanas la implementación de medidas de control fronterizo que cumplen con las normas internacionales, como un medio para detectar y prevenir el movimiento ilícito de efectivo y BNI. El cumplimiento riguroso de estas normas mejoraría la efectividad del control fronterizo en esta área. La lucha contra la financiación del terrorismo es una parte integral del enfoque antiterrorista de las Naciones Unidas, como se refleja en muchas de sus resoluciones y convenciones.

Movimiento y procesamiento de bienes

El comercio mundial y la cadena de suministro internacional son particularmente vulnerables a la manipulación por parte de terroristas. Con el fin de minimizar esta vulnerabilidad, se deben tomar una serie de medidas, que incluyen garantizar la recepción de información de carga electrónica anticipada sobre los envíos entrantes, salientes y en tránsito; emplear un enfoque coherente de gestión de riesgos para abordar las amenazas a la seguridad de la carga; utilizar equipos de detección no intrusivos; promover la cooperación entre las administraciones de aduanas (por ejemplo, mediante la inspección saliente de contenedores y carga de alto riesgo); y establecer asociaciones con el sector privado para la implementación de prácticas seguras en cada etapa de la cadena de suministro, a través de los programas de Operador Económico Autorizado (OEA). La implementación de estas y otras medidas relacionadas es esencial para aumentar la seguridad del comercio internacional y facilitar el flujo de mercancías a través de las fronteras internacionales.

Movimiento de armas pequeñas, armas ligeras, municiones, explosivos y CBRN

El tráfico y movimiento ilícito de armas pequeñas, armas ligeras, municiones convencionales y explosivos, así como materiales químicos, biológicos, radiológicos y nucleares (CBRN) y los bienes de doble uso, agravados por los cambios en los patrones en el comercio de armas y la participación de actores no comerciales, presentan problemas importantes que deben ser abordados por los esfuerzos globales contra el terrorismo. En manos de los terroristas, estas municiones y materiales se convierten en los ingredientes para los ataques terroristas. La regulación efectiva, los controles de exportación y la gestión de las fronteras, incluidas las medidas legislativas y de cumplimiento, pueden minimizar el riesgo de que dichos elementos sean desviados o adquiridos ilícitamente por actores no estatales. Estas medidas deben respetar la necesidad de mantener un equilibrio adecuado entre los controles de exportación y la facilitación del comercio legítimo.

Seguridad marítima

Más del 90 por ciento del total de bienes comercializados internacionalmente se transporta desde el origen hasta el destino a lo largo de las principales rutas mundiales de comercio marítimo. La seguridad del dominio marítimo es, por lo tanto, una cuestión de importancia mundial. Los objetivos de la seguridad marítima son detectar y disuadir amenazas de seguridad; tomar medidas preventivas contra incidentes de seguridad que afecten a buques o instalaciones portuarias; y salvaguardar a los pasajeros, las tripulaciones, los buques y sus cargamentos, las instalaciones portuarias y las personas que trabajan y viven en las zonas portuarias, y a su vez permitir el movimiento seguro y eficiente del comercio marítimo. La implementación efectiva de las medidas de seguridad legislativas y prácticas pertinentes es necesaria para prevenir actos ilegales contra los pasajeros y la tripulación de los barcos que realizan viajes internacionales y contra las instalaciones portuarias que los atienden.

Seguridad aeronáutica

Los actos de terrorismo siguen siendo amenazas graves y constantes para la aviación civil internacional. Para hacer frente a estas amenazas se requiere el establecimiento de políticas y medidas de seguridad integrales y responsables destinadas a garantizar la seguridad física de las aeronaves y los aeropuertos. La adopción de disposiciones legislativas para penalizar los actos de interferencia ilícita contra la aviación civil, y la aplicación y el cumplimiento efectivos de las normas

y prácticas de seguridad de la aviación pertinentes, aumentarían significativamente la capacidad de los Estados para defenderse de estas amenazas.

Sistemas de advertencia temprana y alerta

La seguridad fronteriza es un proceso dinámico y en evolución. Debido a que el movimiento ilegal de personas a través de la frontera afecta negativamente no solo a la seguridad, sino también al bienestar político, económico y social de los Estados, los gobiernos ahora se centran en los esfuerzos cooperativos de seguridad, en el entendimiento de que las acciones unilaterales ya no son efectivas. Los sistemas integrales de advertencia temprana y alerta son, por lo tanto, componentes clave de los sistemas eficaces de gestión de fronteras. Fortalecen la capacidad colectiva de los Estados para detectar, prevenir y combatir el terrorismo, ya que facilitan la cooperación interinstitucional y el intercambio oportuno de información relevante y confiable, lo que permite que las decisiones críticas se tomen de manera responsable.

Muchas organizaciones internacionales competentes para controlar las fronteras utilizan o promueven sistemas de advertencia temprana y alerta, ya sea con herramientas desarrolladas por la organización individual o con herramientas desarrolladas para el uso de la comunidad internacional. Esas herramientas incluyen las redes CEN y RILO de la OMA; IMO SOLAS, LRIT y AIS; las Listas Consolidadas de los comités de "sanciones" del Consejo de Seguridad y el sistema de comunicaciones global seguro I-24/7, la base de datos SLTD y el régimen de Avisos de la Organización Internacional de Policía Criminal (INTERPOL).

Control de la frontera abierta

La frontera abierta (la frontera entre los puntos de control oficiales de las fronteras terrestres y marítimas) sigue facilitando el movimiento ilegal de personas a través de la frontera, incluidos los terroristas y delincuentes, y de bienes (incluidas las armas pequeñas, armas ligeras, municiones y explosivos, y materiales químicos, biológicos, radiológicos y nucleares). Los gobiernos reconocen la importancia de asegurar la frontera abierta e intentan hacerlo a través de una variedad de medidas, que incluyen vigilancia, patrullas, barreras físicas, operaciones de control y patrullaje conjunto, intercambio de información, evaluaciones de inteligencia y compromiso con las comunidades fronterizas en temas de control y vigilancia policial. Se requieren esfuerzos de control concertados por parte de las autoridades pertinentes para abordar de manera efectiva los riesgos que presenta la frontera abierta.

Necesidad general de respetar los derechos humanos

La Estrategia global de las Naciones Unidas contra el terrorismo refleja una clara afirmación, por parte de los Estados Miembros, de que las medidas eficaces contra el terrorismo y la protección de los derechos humanos no son contradictorias, sino más bien objetivos complementarios y que se refuerzan mutuamente, y que los derechos humanos y el estado de derecho constituyen la base fundamental del esfuerzo global contra el terrorismo. Al adoptar la Estrategia Global y su Plan de Acción, los Estados Miembros resolvieron “reconocer que la cooperación internacional y todas las medidas que adoptemos para prevenir y combatir el terrorismo deben ajustarse a las obligaciones que nos incumben en virtud del derecho internacional, incluida la Carta de las Naciones Unidas y los convenios y protocolos internacionales pertinentes, en particular las normas de derechos humanos,

el derecho relativo a los refugiados y el derecho internacional humanitario"(A/RES/60/288, Anexo, párrafo 3 del preámbulo, reafirmado en A/RES/64/297). La Asamblea General también ha enfatizado la necesidad general de garantizar el respeto de los derechos humanos en los esfuerzos contra el terrorismo en más de 60 resoluciones sobre el terrorismo internacional. Específicamente respecto del control fronterizo, la Asamblea exhorta a los Estados "a que se aseguren de que en todas las operaciones de control de fronteras, al igual que en los mecanismos previos a la entrada, se sigan directrices y prácticas claras y se respeten plenamente las obligaciones que tienen de conformidad con el derecho internacional, en particular el derecho de los refugiados y las normas de derechos humanos, respecto de quienes soliciten protección internacional" (A/RES/62/159, párrafo 8, reafirmado por A/RES/64/221).