

Licencia de Conducir Digital



Biométrica





¿Qué es una Licencia de Conducir?

El objetivo de este estudio es la elaboración de una nueva Licencia de Conducir Digital Biométrica Infalsificable haciendo para ello un análisis científico de Seguridad Documentaria Física, Lógica, Cadena de Custodia y Econométrica.

Debemos empezar entonces por definir que es una Licencia de Conducir y cuál es su función

Una Licencia de Conducir es un documento oficial que permite al titular operar uno o más vehículos motorizados, tales como una motocicleta, automóvil, ómnibus o semirremolque.

La mayoría de las Licencias de Conducir en el mundo son tarjetas ID-1 de polímeros plásticos con un tamaño y forma definidos por el estándar ISO/IEC 7810

En muchos países incluyendo Australia, Nueva Zelanda, Canadá, Reino Unido y Estados Unidos las Licencias de Conducir son aceptadas como el documento de identidad principal

La expedición de una licencia de conducir indica que el titular ha aprobado los exámenes que la autoridad de tránsito exige para operar determinado tipo de vehículos.

La Licencia de Conducir es un documento que las autoridades deben tomarse muy en serio, y así lo hacen en los países del primer mundo, y en los países de la OCDE donde pretendemos entrar algún día; a través de la dación de una Licencia de Conducir un estado asume la responsabilidad de que esa persona tiene las capacidades idóneas para conducir el vehículo de la categoría asignada.

De acuerdo a los estándares internacionales en Perú mueren al menos 2,000 personas por año, 5 personas por día en **accidentes de tránsito evitables**, (que nunca debieran suceder y no suceden en los países del Primer Mundo).

En el Perú mueren en total 4,000 personas por año, y sin embargo no mueren 4,000 por mala praxis médica, esto demuestra la importancia que el estado debe dar, y nunca dio, a los títulos que emite autorizando a conducir vehículos.

A esto se debe agregar las decenas de miles de ciudadanos que sufren todos los años lesiones e invalidez permanente como secuela de accidentes de tránsito, la estadística de los últimos 10 años revela que alrededor de **medio millón de personas terminaron "con algún tipo de lesión física"**.

Según datos de MINSA un cuarto de los discapacitados de Perú tiene su origen en los accidentes de tránsito

¿No nos preocuparíamos como nación si decenas o cientos de miles de médicos obtuvieran sus títulos sin estar debidamente capacitados, sin dar los exámenes y simplemente pagando una coima, o dando exámenes incompletos y poco rigurosos, o finalmente comprando un título falso en Azángaro?



Sin embargo es el caso de los títulos que entrega a “Nombre de la Nación” el estado peruano y que autorizan a conducir un vehículo, títulos sin ninguna garantía de idoneidad profesional, títulos que no son anulados por mala praxis, (conducir en estado etílico, incumplimiento reiterado de normas de tránsito, causar muertes, etc.), títulos que el estado entrega con datos falsos a cambio de una coima, títulos sin seguridad que se pueden falsificar fácilmente

Estos títulos que el estado ya no garantiza, y por los que ha resignado su función primaria de proteger al ciudadano, terminan “conduciendo” a la invalidez y la muerte de aquellos que el estado debió proteger.

Es obligación del estado garantizar la capacidad de los conductores del Perú

Accidentes de Tránsito

El Perú desde el año 2009 es el primer país del mundo en muertes por accidentes de tránsito por millón de vehículos, hasta el año 2006 el que ocupaba el primer lugar era Bolivia

¿Pero cuál es la causa de los accidentes de tránsito?

Las estadísticas mundiales coinciden en que el 90% de los accidentes de tránsito son responsabilidad de factor humano, error del chofer.

En cambio en aviación estas estadísticas indican que menos del 50% son responsabilidad del factor humano, error del piloto.

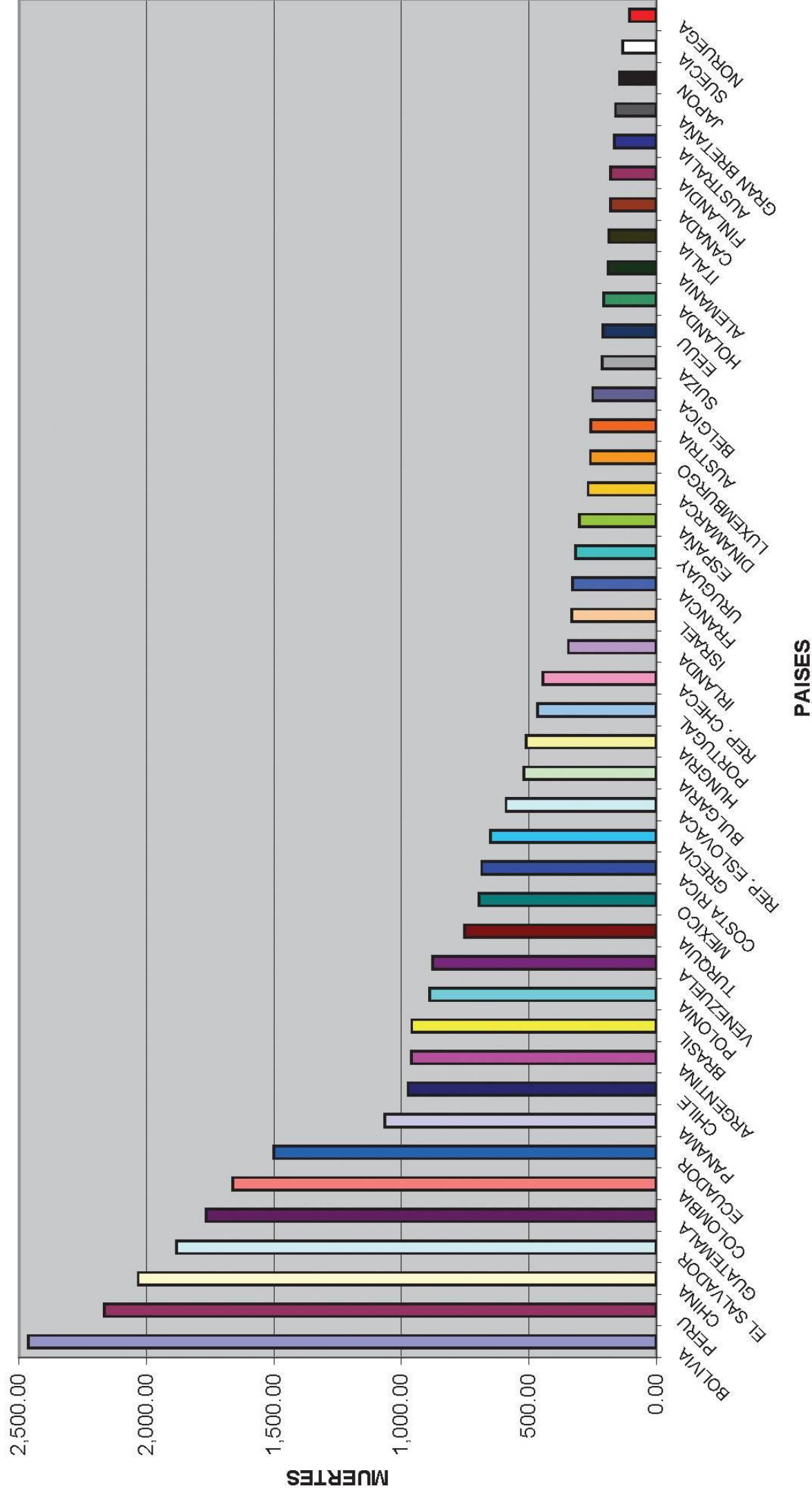
Esto explicaría los diferentes términos, unos son choferes de combi, choferes de “El Chosicano”, choferes de “Guapo Lindo”, y los otros son pilotos de US Airways, (Sully 2016), pilotos de Fórmula Uno.

Sin embargo en Perú es aún peor, esta proporción sube al 95% y si consideramos que el parque automotor de Perú no es el más moderno del mundo y las carreteras del Perú no son las mejores del mundo, podemos inferir que prácticamente todos los accidentes de Perú son responsabilidad de malos choferes.

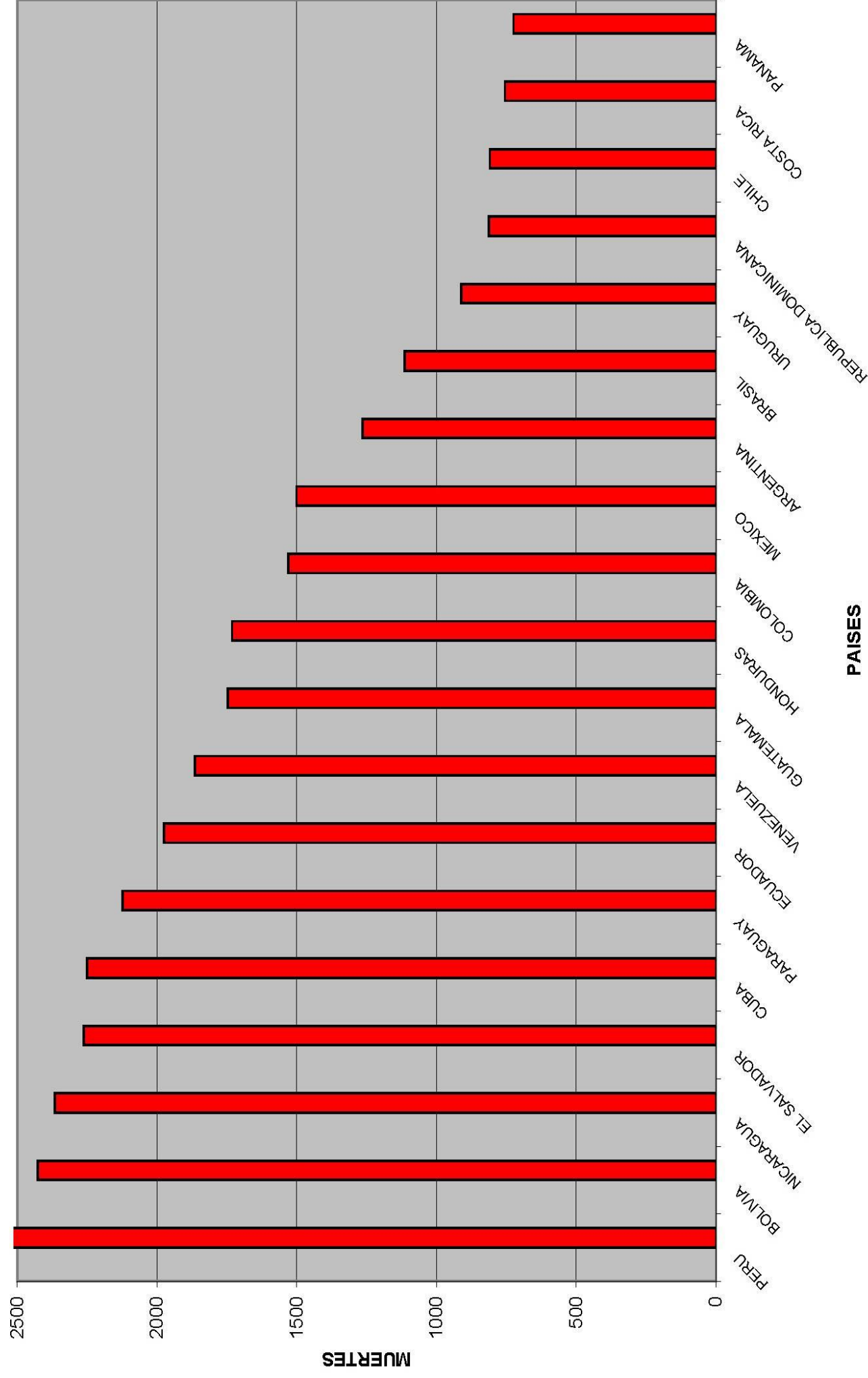
De esto se desprende una conclusión muy clara, si queremos disminuir la tasa de accidentes del Perú y la consecuente muerte e invalidez debemos ocuparnos de un solo factor, el factor humano, debemos tener buenos choferes, debemos capacitarlos y debemos tener un sistema para separar la paja del trigo.

Este sistema es el punto central de nuestro estudio, un sistema que usando las modernas tecnologías informáticas, usando Encriptación y Certificados Digitales, nos permita validar la capacitación de los choferes, avaluar a los instructores, asegurar la integridad de las Bases de Datos y finalmente consolidando todos estos datos emitir un “Título Seguro a Nombre del Estado Peruano” al que llamaremos Licencia de Conducir Digital Biométrica.

Muertes por Accidentes de Tránsito por Año y Millón de Vehículos



Muertes en Accidentes de Tránsito Millón de Vehículos*
Encuentro de Seguridad Vial Iberoamérica y el Caribe
Madrid 23 -24 de Febrero 2009



*En algunos países, generalmente de mayor siniestralidad, no incluyen los muertos en el lapso de 30 días del accidente, que es el estándar internacional, si la persona no muere en el lugar del siniestro, la causa de defunción será infarto, edema, etc.



Mientras que Perú alcanzaba el año 2009 el primer lugar en el mundo en muertes por accidentes de tránsito en Estados Unidos el “Department of Transportation” anunciaba el mínimo número de muertes por accidentes de tránsito desde 1961, avanzamos como el cangrejo.

Los datos compilados por el “DOT's National Highway Traffic Safety Administration” indicaban que el número de muertes el año 1961 fueron 37,313 mientras que las estadísticas del años 2009 indicaban 36,285.

En resumen podemos decir que los promedios de muertos y discapacitados permanentes de los últimos años son:

Muertes por accidentes de tránsito por año _____ 3,870

Discapacitados Permanentes por accidentes de tránsito por año _____ 29,745

Pero aunque las muertes y las discapacidades permanentes son el factor más visible y lamentable de los accidentes de tránsito hay otro aspecto muy negativo del que se habla menos, el costo económico de los accidentes de tránsito.

El costo de los accidentes de tránsito en el Perú es de **S/. 19,165 millones** lo que representa un **3.1% del PBI**, el promedio entre los países de ingresos bajos y medios de los accidentes de tránsito es de **1.5% del PBI**

En resumen el Perú gasta **10,000 millones de soles** más por año que el promedio mundial, perdemos **10,000 millones de soles por año**, ¿no es también de beneficio económico invertir en disminuir los accidentes de tránsito?

La pregunta humana y econométrica entonces es la siguiente:

¿Estamos dispuestos a invertir el esfuerzo y la tecnología necesarios en una Licencia de Conducir Segura, para salvar 2,000 vidas por año, 14,300 discapacitados permanentes por año y 10,000 millones de soles por año?

¿Saben cuántos hospitales, escuelas y carreteras se pueden hacer con 10,000 millones de soles por año?

La respuesta que demos dirá que sociedad somos y cual será nuestro futuro.

Hasta aquí hemos usado datos estadísticos de Perú y del mundo que muestran el vínculo fundamental entre la responsabilidad del chofer y los accidentes de tránsito, y que además en esta relación ocupamos el peor lugar del mundo, en resumen **nuestros choferes son los peores del mundo** y los responsables de nuestros muertos, nuestros discapacitados y nuestras millonarias pérdidas económicas.

Pero hay otro argumento objetivo y de ciencia pura que obliga al estado peruano a ser más cuidadoso en la entrega del “título de chofer en nombre de la nación” y en su control posterior.

La ciencia de la Cinemática, la Masa, y la Energía

Los estados no entregan licencias para portar armas o para manejar explosivos de manera indiscriminada, lo mismo debería ser con las licencias que autorizan a manejar vehículos. Los vehículos pueden ser armas mortales de alta peligrosidad que pueden matar en pocos segundos a decenas de personas como quedó demostrado en los recientes atentados terroristas en Europa Y Estados Unidos.

Este daño se produce por la Energía Cinética y el nivel de daño se explica fácilmente por una sencilla ecuación newtoniana de hace casi 300 años:

$$E = \frac{1}{2} MV^2$$

En resumen la energía de un cuerpo en movimiento, un vehículo o una bala, es directamente proporcional a la masa pero cuadráticamente proporcional a la velocidad.

Como una imagen vale más que mil palabras



Allí vemos gráficamente que cuando la velocidad pasa de 1 a 3 la energía pasa de 1 a 10 y queda claro que rápido aumenta la energía con la velocidad.

Pero esta relación cuadrática con la velocidad es hasta intuitiva, todos sabemos que si un vehículo choca contra una pared a 10 Km/h los daños son mínimos, pero si choca a 60 Km/h queda destrozado

Una forma usual de medir la energía en relación al daño que puede producir al liberarse casi instantáneamente, (que es el caso de un choque), es la unidad TNT (Trinitrotolueno), la bomba de Hiroshima por ejemplo es equivalente a 15 Kilotón (15 toneladas de TNT).

Veamos la energía en TNT que libera un choque a diferentes velocidades



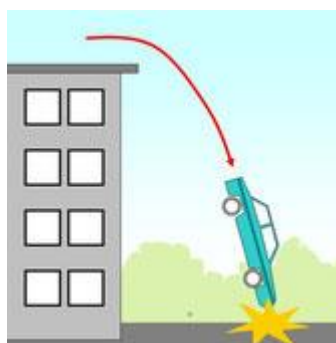
Automovil promedio a 80 Km/h	135 gramos TNT
Automóvil Promedio a 120 Km/h	300 gramos TNT
Camión de 40 toneladas a 100 Km/h	3.7 Kg TNT

Esta cantidad de explosivos es capaz de hacer mucho daño así que el estado tiene la obligación de analizar cuidadosamente a quien le entrega estos permisos para manipular explosivos y también tiene que tener un sistema para sacar de circulación a quienes hayan hecho mal uso de explosivos en las calles y carreteras del Perú.

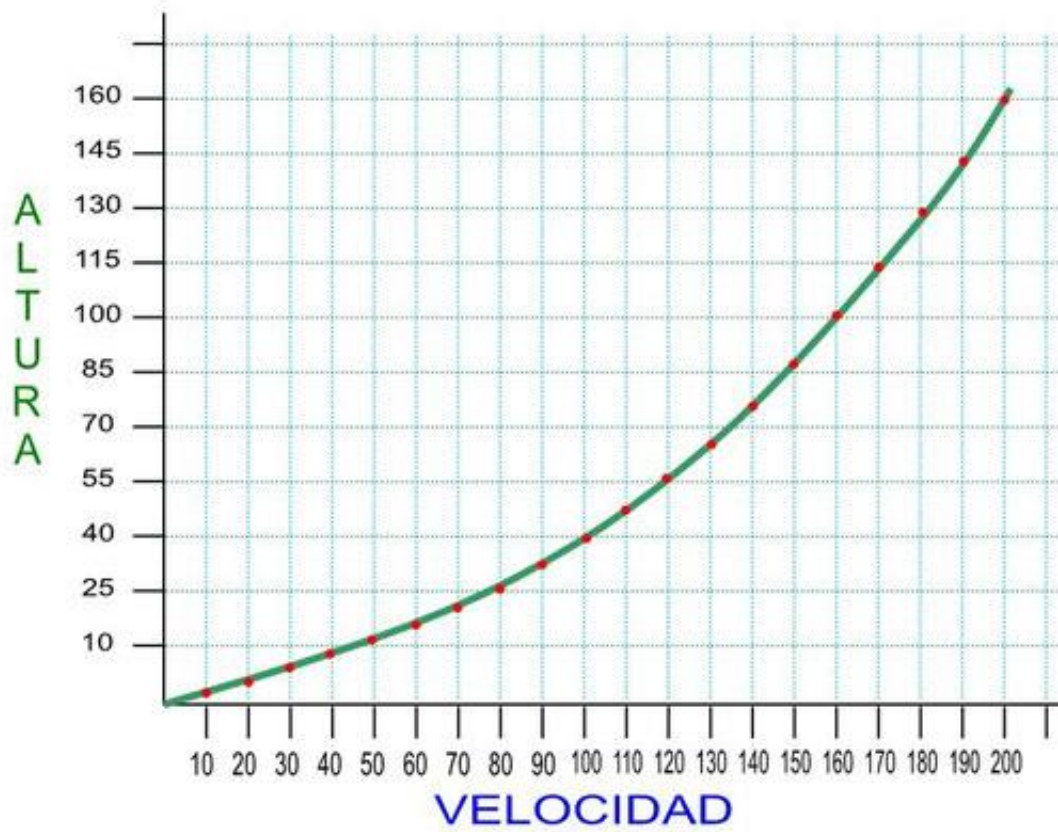
Si calculamos que el parque automor al año 2017 es de casi 2.8 millones de vehículos es fácil calcular que en cada momento circulan por el país **378 toneladas de TNT**, lo cual es equivalente a unos **800 misiles Tomahawk** o **25 bombas de Hiroshima**.

No es de extrañar entonces que en un contexto tan “explosivo” y “desregulado” muera un peruano cada 2 horas.

Para seguir ilustrando con ejemplos comparativos volvamos a nuestro vehículo que quedó destrozado al chocar con una pared a 60 Km/h, ese choque es equivalente a que el auto cayera de la azotea del quinto piso de un edificio



Y aunque parece claro que un chofer con un “Título a nombre del Estado” para conducir vehículos (brevete), debería manejar con mucho cuidado sobre una azotea en el quinto piso de un edificio, (equivalente a 60 Km/h), para no caerse, nuestros choferes como demuestran la frías estadísticas matemáticas son tan inconscientes que manejan sin cuidado aunque el edificio sea de 10, 50, o 100 pisos y el resultado es necesariamente la muerte.



Y esta gráfica nos ilustra otro peligro que deberían tener en cuenta los choferes en el Perú, los precipicios a los costados de las carreteras, vemos que caer 160 metros en un impacto directo es equivalente a chocar a 200 Km/h que significa necesariamente la muerte de todos los pasajeros.

Pero nuevamente los precipicios no son el problema sino los malos choferes, Suiza tiene muchos más precipicios que el Perú y las muertes por accidentes de tránsito son 20 veces menos.

Sería, para ponerlo en nuestra perspectiva como si en el Perú en vez de morir casi 4,000 personas por año murieran sólo 200, ¿será esto posible o es un sueño inalcanzable?

Pero integremos este cálculo con datos anteriores, si nuestros choferes fueron sólo 10 veces peores que los suizos salvaríamos de morir a 2,000 personas, salvaríamos de la discapacidad permanente a 14,300 personas y nos ahorraríamos 3,500 millones de dólares todos los años, podríamos hacer miles de kilómetros de carreteras nuevas todos los años.

Ahorrándonos la mitad de los accidentes de tránsito podríamos hacer una carretera de Tacna a Piura y otra de Lima a Huancayo todos los años y además 2,000 muertos que seguirían vivos y 14,300 discapacitados que ya no lo serían nos lo agradecerían.

Ya tenemos suficiente información y argumentos como para trazarnos una meta, queremos para empezar que nuestros choferes sean sólo 10 veces peores que los suizos

Lograr esta meta nos lleva de nuevo al “Título a nombre del Estado” para conducir vehículos, llamado Licencia de Conducir o Brevete



El Brevete “20 años de decadencia”

Y lograr esta meta nos lleva nuevamente a la increíble y triste historia de la licencia de conducir peruana y su mafia desalmada y criminal, y es importante conocer esta historia porque los pueblos que no la conocen están condenados a repetir los mismos errores, y a Perú este brevete ya le ha costado mucho.

Un análisis de los últimos 20 años nos revela que la licencia de conducir es el documento personal de identidad más falsificado en el Perú.

Su Seguridad Física no ha tenido mejoras reales desde el siglo pasado y en ese sentido es un documento cuya Seguridad Física es totalmente obsoleta a la luz de las tecnologías de falsificación disponibles en el año 2017.

Su Seguridad Lógica está totalmente ausente ya que la breve “primavera” con Seguridad Lógica de los años 2006 y 2007 fue totalmente inocua del punto de vista del control porque sólo incluyó a 280,000 brevets, nunca se desplegó el sistema de control en la Policía, (el MTC no entregó los dispositivos de control), y se borraron sus bases de datos, nunca se cumplió con la promesa de la renovación y depuración de todas las licencias profesionales.

Pero si algo aprendimos fue que la mafia se demoró más de un año para darse cuenta que no podía falsificar la Seguridad Lógica de la nueva licencia y que se debió coordinar la distribución del sistema de control con la Policía y los Inspectores desde la emisión de la primera licencia

La Cadena de Custodia parte fundamental de la Seguridad Documentaria nunca se cumplió como demuestran el caso de los 1000 hologramas robados en el 2008, y la denuncia de canal 9 ATV del 18 de octubre de 2011 “Licencias de conducir falsificadas utilizando insumos originales” donde la policía encontró hologramas y otros insumos verdaderos en manos de falsificadores que comprueban el continuo “robo hormiga” de los materiales del brevete.

Por último la seguridad del brevete cayó a su menor nivel histórico en el siglo XXI cuando en el año 2009 se procedió de manera anti técnica a una descentralización apresurada sin seguir los estándares internacionales de impresión, ni el proceso de emisión con el uso de un software de administración y un control eficiente y responsable.

El caso más escandaloso de esta segunda etapa del caos y la anarquía, fue la venta en Huánuco el año 2015 del mismo equipo e insumos que se usa para hacer los brevets de PVC de provincias, esta impresora térmica Fargo Modelo HDP-5000 fue vendida sin reparo ni control por la misma empresa que entrega los brevets e insumos para provincias.



El caso fue descubierto por la Inspectoría General de la Policía Nacional del Perú el 18 de junio de 2015 quién inició la investigación con Resolución Nº 230-2015-IN/TDP y Expediente 07103-15/485 y continúa en un juicio penal por falsificación.

Con esta máquina y los insumos se puede hacer un breveté falso que un experto no podría diferenciar de un original.....porque es un original

En el actual proceso de emisión no se puede garantizar la consistencia y validez de los datos por la falta del software y los mecanismos de control adecuados, no existe **Cadena de Custodia** ni responsabilidad por los documentos previos, que son el requisito indispensable para la emisión de un documento válido.

Por ello son comunes las denuncias de la prensa sobre ciegos con certificados médicos que los autorizan a conducir, firmados por oftalmólogos inescrupulosos, o de sociópatas al volante que han pasado el psicotécnico gracias a psicólogos negligentes, y por último escuelas de choferes que entregan certificados de capacitación falsos, ¿el único requisito?, llevar la huella y la firma en un papel bond, y suficiente dinero para nunca dar un examen.

Al no existir un software de control tampoco existe ninguna **Trazabilidad** del proceso que nuevamente es un requisito indispensable para emitir un documento válido y/o para encontrar una inconsistencia y al responsable de la misma.

Tampoco existen mecanismos y sistemas de control, ni cursos de capacitación para inspectores y policías sobre las medidas de seguridad de los documentos que emite e imprime el MTC.

¿Qué hemos aprendido?

20 años de batallas perdidas no servirían de nada si no hubiéramos aprendido algo de cada una de ellas y como dice Sun Tzu *“Conoce a tu enemigo y concóctete a ti mismo y podrás pelear en cien batallas sin un desastre”*, ahora ya conocemos al enemigo, tenemos una estrategia y cien tácticas, afrontaremos las próximas cien batallas sin ningún desastre.

Un ejemplo es La Licencia de Conducir Digital del año 2006 eliminada por la mafia con mucho dinero el año 2007.

Si el año 2006 se hubiera entregado los dispositivos para verificar la Nueva Licencia de Conducir Digital a la Policía Nacional del Perú y a los Inspectores de Tránsito, si se hubieran realizado talleres de instrucción, si se hubiera invitado a la prensa a estos talleres y se hubiera difundido la existencia y ventajas de la Nueva Licencia de Conducir Digital, hubiera sido un acontecimiento tan público que hubiera sido imposible para la mafia que se esconde hace años en las sombras del MTC, detener esta tecnología que ya era pública, este debe ser ahora el camino desde el inicio.



Ahora que aprendimos de los errores del pasado soltemos la pesadilla final de la mafia: **La Licencia de Conducir Digital y Biométrica; el Documento Absolutamente Infalsificable**

El ABC de la Seguridad Documentaria

La Seguridad Documentaria tiene ciertas reglas de oro, ninguna de ellas se puede soslayar en pos del documento ideal seguro en un momento histórico determinado.

Para que en el año 2018 todo documento de identidad de personas o bienes se pueda considerar un documento seguro se debe seguir estas 8 reglas fundamentales de la Seguridad Documentaria que son:

- 1. Seguridad Física**
- 2. Seguridad Lógica**
- 3. Cadena de Custodia y Trazabilidad**
- 4. MLDS (Multiple Layered Defense System) Sistema de defensa en capas múltiples**
- 5. Emisión Descentralizada pero Impresión Centralizada**
- 6. Cumplimiento de estándares actualizados**
- 7. Certificación de las empresas proveedoras de las tecnologías de seguridad**
- 8. Certificación e historial de la empresa integradora**

1.- Seguridad Física

La Seguridad Física es también llamada clásica porque tiene cientos de años y se basa simplemente en el gap (brecha) tecnológico (y económico) que separa generalmente al emisor oficial (Gobierno, Estado, Rey, Emperador, Casa de la Moneda, Imprenta de valores) del falsificador. La Seguridad Física se basa en técnicas y materiales especiales o exclusivos.

Materiales o substratos:

Papeles de composición especial, marcas de agua, plásticos como el Teslin y el Policarbonato

Técnicas de registro e impresión:

Tintas especiales (pigmentos de colores exclusivos, tintas UV, tintas PETQIL TD, tintas OVI), técnicas especiales de impresión (Intaglio, Láser Engraving, Impresión por Rayo de Electrones (Hologramas de Seguridad))

La fortaleza de la Seguridad Física reside en su uso extendido y que la mayoría de las personas aprende rápidamente a diferenciar lo verdadero de lo burdamente falsificado (si existe un gran gap tecnológico) y el ejemplo clásico son las monedas y el papel moneda

Las debilidades de la Seguridad Física están en el método que se usa para separar lo verdadero de lo falso y su alta subjetividad, el resultado es que cuando se reduce el gap tecnológico el 99.9 % de los usuarios no puede distinguir lo verdadero de lo bien falsificado.

Otra de las características de la Seguridad Física es que es genérica, todos los documentos o papel moneda de una clase tienen la misma seguridad. Eso es una grave deficiencia en el caso del brevete como los demuestran los robos de hologramas masivos, (1000 hologramas en el Touring) o el robo hormiga de pequeñas cantidades diarias que ocurre en el MTC y en los puntos de impresión en provincias.

Si no hay **Cadena de Custodia** todas las medidas de Seguridad Física carecen de valor, por eso la primera y fundamental medida de seguridad de un objeto de valor es la Impresión Centralizada, es el caso del dólar mundial que se imprimió en un solo lugar “United States Bureau of Engraving and Printing” en Washington, DC (300 14th St SW, Washington, DC.) por más de 100 años de 1877 a 1991 y fue recién en este año que se abrió una segunda imprenta en Fort Worth, Texas. Con la seguridad no se juega, con el dinero tampoco.

Asumiendo que hay una impresión centralizada con todas las normas de seguridad, que se cumplen todos los estándares de **Seguridad Documentaria** y **Cadena de Custodia** podemos definir genéricamente cuales son las medidas de **Seguridad Física** ideales.

La **Seguridad Física** ideal es aquella que por el “gap tecnológico” el falsificador no puede imitar para lograr que el observador promedio entrenado no pueda diferenciar del original.

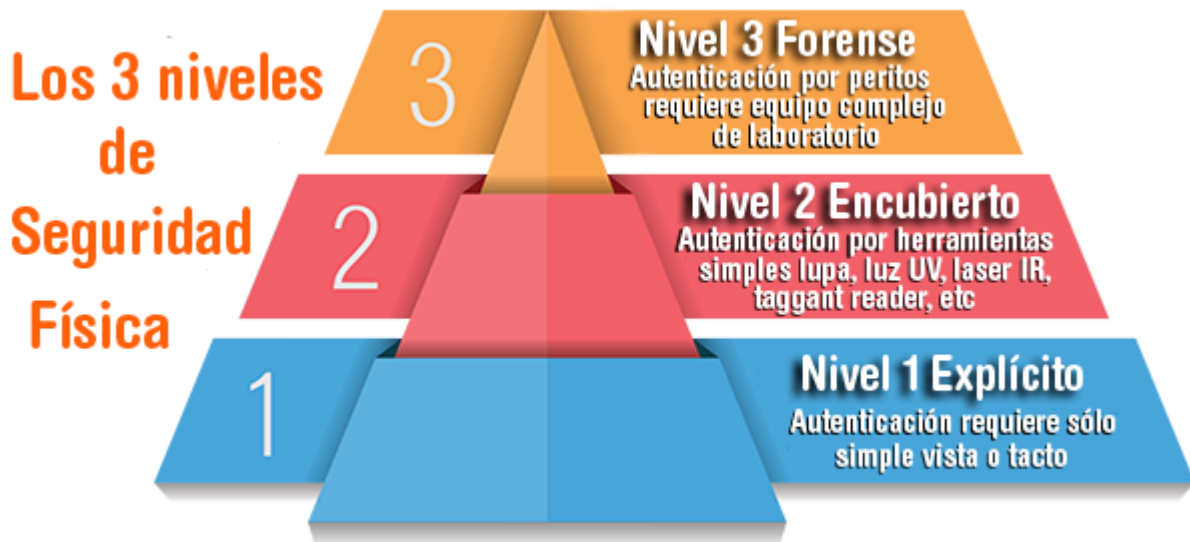
Es el caso del Intaglio que se usa para imprimir casi todos los billetes del mundo y la Licencia de Conducir de Brasil, pese a que es una técnica de hace 200 años es tan grande el “gap tecnológico” y la inversión de capital que ningún falsificador lo puede imitar, y no piensen en los bancos con sistemas de verificación sofisticados y luz UV, intenten pasar un billete falso a un cambista, van a ver que es imposible. El Intaglio se conoce fácilmente al tacto o a través de la Imagen Latente que genera con una luz a 45º



Algunos ejemplos de Seguridad Física son viendo las imágenes en el sentido de la agujas del reloj

1. Holograma de Seguridad con efectos cinéticos tipo Kinegram o similares, no es precisamente el caso del actual holograma de la Licencia de Conducir
2. Imagen oculta por difracción de burbujas ópticas con el logo del emisor
3. OVI (Optically Variable Ink), un buen OVI tiene que tener como se ve en la imagen un cambio notable al cambiar el ángulo de incidencia de la luz, no es el caso del OVI de la actual Licencia de Conducir

Otras técnicas de **Seguridad Física** incluyen tintas de colores exclusivos (SICPA), tintas UV, tintas IR, tintas PETQUIL-TD, y técnicas especiales de impresión como Intaglio, Laser Engraving, Impresión por Rayo de Electrones, Micro Textos, Marcas de Agua.



La elección de las tecnologías y niveles para un documento en particular se deciden de acuerdo con el estándar **ASTM F1448-16** Standard Guide for Selection of Security Technology for Protection Against Counterfeiting, Alteration, Diversion, Duplication, Simulation, and Substitution (CADDSS) of Products or Documents que se encuentra en proceso en el **Comité de Seguridad Documentaria de INACAL** con el fin de ser aprobado como **NTP (Norma Técnica Peruana)**

En resumen los 3 niveles de Seguridad Física son:

Nivel 1 Explícito: son características que se verifican a **Simple Vista** o al **Tacto** en forma instantánea. Son visibles y discernibles para la persona promedio que no tiene entrenamiento o instrucción especializada pero para mayor efectividad se requiere una instrucción básica. Son buenos elementos de este nivel los **Hologramas Cinéticos** y la estructura tridimensional del **Intaglio** con su **Imagen latente**



Nivel 2 Encubierto, las características de este nivel no son discernibles inmediatamente por la persona promedio y sólo pueden ser vistas por personal entrenado y el uso de herramientas simples de verificación. Algunos ejemplos serían el uso de luz UV invisible, Láser Infrarrojo Sintonizado, (de frecuencia determinada, 960nm. o 985nm.), lupas y microscopios hasta 50X

Nivel 3 Forense, las características de este nivel son características forenses. Características que son sólo discernibles por personas con una amplia capacitación en un entorno de laboratorio complejo. Los ejemplos aquí serían el análisis de estructuras ópticas que han sido manipuladas deliberadamente en una “huella digital” única o **Nanotexto** muy fino.

Nivel 4 Fabricante, este nivel es simplemente un nivel forense avanzado y son medidas exclusivas del fabricante que se incluyen como una garantía adicional de seguridad que no son reveladas ni siquiera al cliente

Todas estas características están explicadas en detalle en el documento de 90 páginas aprobado por el Comité de Seguridad Documentaria de INACAL Norma Técnica Peruana **NTP 620.000/2016 (R.D. N° 044-2016-INACAL/DN. Publicada el 2016-12-31)**

2.- Seguridad Lógica

La Seguridad Lógica también llamada Informática o Mecanizada consiste en agregar al documento datos codificados en un soporte óptico o electromagnético

La Seguridad Lógica, representada en el documento por un **Chip o un Código Óptico de Seguridad**, esta basada en algoritmos matemáticos, su verificación es objetiva y sólo admite 2 respuestas, verdadero o 1 y falso o 0, no hay lugar para la subjetividad o la interpretación del agente verificador, cómo consecuencia no se necesita de un inspector experto para obtener resultados confiables y puede incluir dispositivos de control anti corrupción.

Sus principales características son:

- a. Seguridad basada en algoritmos matemáticos comprobables y de dominio público.
- b. Seguridad basada en una llave secreta propietaria elegida entre un número de llaves mayor que los átomos de la galaxia y las estrellas del universo.
- c. Seguridad basada en códigos propietarios no comerciales llamados Códigos de Seguridad. Un Código de Seguridad es un lenguaje exclusivo, un ejemplo sería el lenguaje Navajo origen del Código Navajo y luego tema de la película “Windtalkers” con Nicholas Cage



- d. Seguridad individual y personalizada, cada documento incluye un código de seguridad único y exclusivo de ese documento.
- e. Cómo extensión del punto (d) algunos códigos de seguridad incluyen Biometría (foto del rostro, huella digital, Iris etc.) y la Firma Digital del ente emisor y/o el usuario
- f. Son sistemas de seguridad integrada y distribución controlada, su imposibilidad de falsificación obliga a llevar la seguridad al ente emisor y a la aplicación de estrictas normas de seguridad desde que se empieza a generar el documento hasta la entrega al usuario final, **(Cadena de Custodia)**.
- g. Incluyen Esteganografía de clase C (encubierta) o clase O (abierta) para impedir su clonación.
- h. Seguridad Dinámica, por su conexión natural con las bases de datos incorporan el factor tiempo a la seguridad del documento, un documento válido hoy puede estar anulado mañana por robo, inconducta del portador, etc. De ésta característica y enlace natural proviene la adjetivación de Informática aplicada a la **Seguridad Lógica**.
- i. Verificación electrónica y objetiva por elementos combinados de hardware y software que se deben desplegar de manera coordinada con la emisión de documentos. De ésta característica proviene la adjetivación de Mecanizada aplicada a la **Seguridad Lógica**.

La elección de cuál **Seguridad Física y Lógica** usar para un documento en particular depende de factores cómo el tipo de documento, forma y lugar de verificación, presupuesto asignado, etc. y su elección es tarea del experto en seguridad.

La cuna de la Seguridad Lógica

Todo comenzó a fines del siglo XX en la mente de matemáticos, físicos, ingenieros, expertos en seguridad, informática y comunicaciones. Los unía una tarea común, utilizar las nuevas tecnologías emergentes para crear documentos más seguros para sistemas de acceso de alta seguridad que luego se extendió a documentos de identidad y propiedad en general.

En los comienzos y por su origen tan lejano a la Seguridad Física sus creadores, jóvenes padres cegados por el orgullo, pretendieron que la Seguridad Lógica reemplazara a la Seguridad Física y su eslogan era que en un papel o plástico común y corriente se podía emitir un documento infalsificable agregando simplemente un código de seguridad, óptico o electromagnético.

Por fin hoy sabemos que la seguridad de un documento depende del matrimonio de la Seguridad Física y la Seguridad Lógica en un sistema de seguridad combinada MLDS (Multiple Layered Defense System).

El propósito de la **Seguridad Lógica** es impedir absolutamente la falsificación de un documento (identidad, propiedad, contrato, etc.) a través de un sistema de validación instrumental y objetivo.

La unión de la **Seguridad Física y la Seguridad Lógica en un Sistema MLDS**, bien aplicadas por un profesional documentario siguiendo los estándares internacionales actualizados, se materializa en documentos absolutamente infalsificables y objetivamente verificables, que son el paradigma de un sistema de seguridad documentaria.

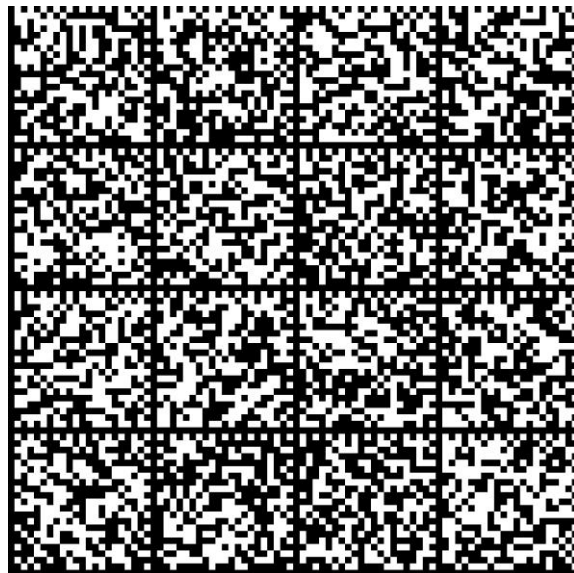
Dispositivos de Seguridad Lógica

Se clasifican en 2 clases y varias subclases

1. **Códigos Ópticos de Seguridad Encriptados**
2. **Chips Encriptados de Identificación**

Códigos Ópticos de Seguridad Encriptados

La primera clase son los Códigos 2D Encriptados y 2 ejemplos son los códigos tipo Datamatrix y los códigos tipo QR, no son códigos Datamatrix o QR comerciales sino códigos encriptados con encriptación nativa, de datos, o ambas.



Los códigos con encriptación nativa se logran modificando el SDK para la generación de los códigos, en este caso y aunque visualmente son códigos Datamatrix o QRcode en realidad no lo son. El arte del programador consiste en modificar el código sin alterar su capacidad (contenido de bytes), su densidad informática (número de bytes por unidad de área) su rapidez y facilidad de lectura, y lo que es aún más difícil, mantener el sistema de corrección de errores Reed–Solomon “Error Correcting Code” (ECC), cuyo algoritmo está basado en polinomios univariados sobre campos finitos, tarea que requiere a un programador y un matemático a la vez.

Por ello se prefiere no modificar el código 2D original y transformarlo en un Código de Seguridad 2D introduciendo la encriptación directamente en los datos, el siguiente es un diagrama esquemático de uno de los posible métodos a usar

Computer Science and Engineering 2016, 6(2): 19-24

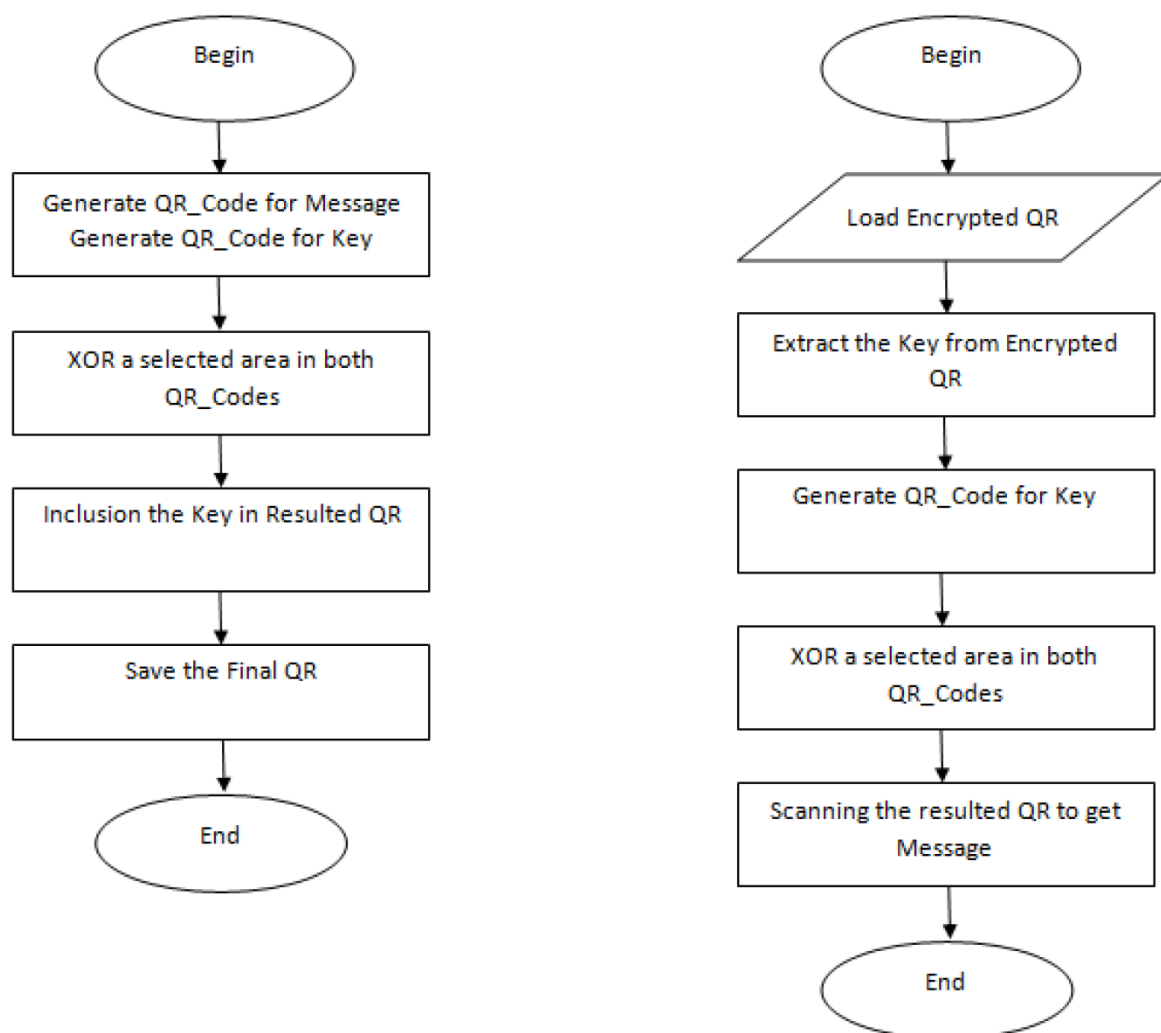
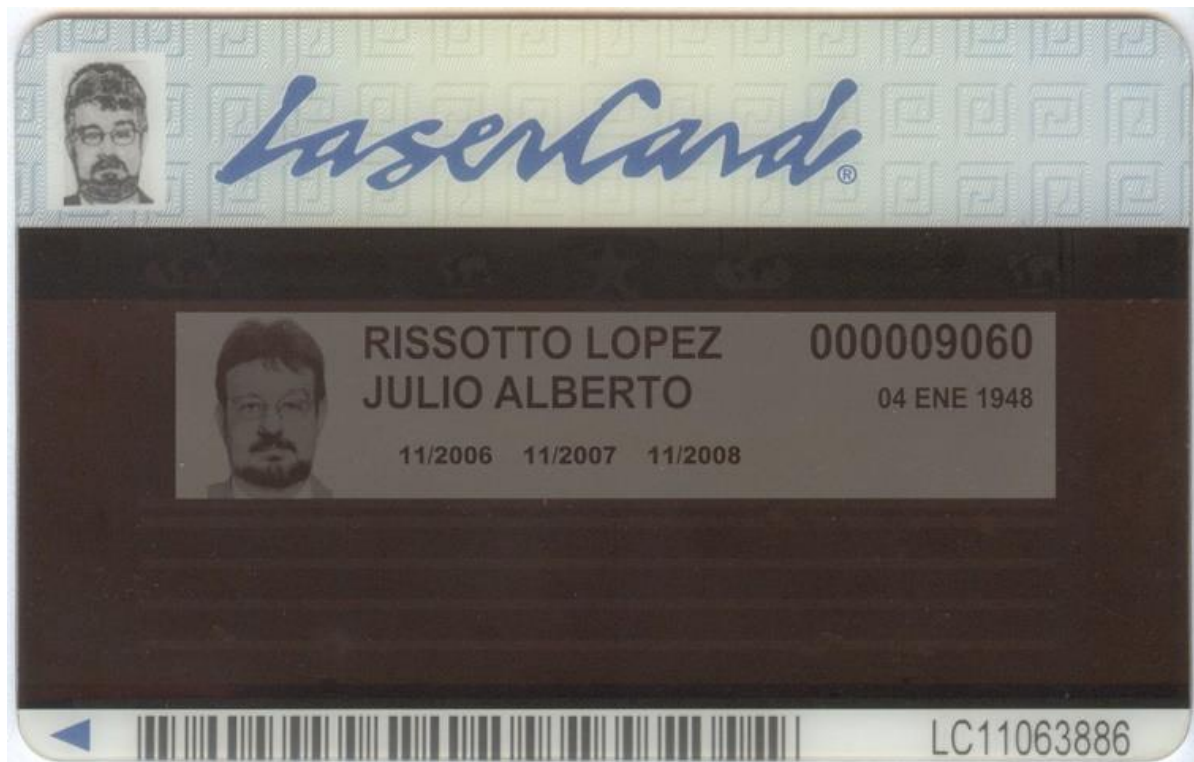


Figure 4. Encryption and decryption processes

La segunda clase de Códigos Ópticos de Seguridad se llaman Códigos de memoria óptica por método de grabación láser lineal, estándares ISO/IEC 11693, ISO/IEC 11694 y ISO/IEC 11695.

Son Códigos Ópticos que se imprimen con **Láser Engraving** sobre un sustrato de **Policarbonato**, en este caso si bien el código es encriptado para cada documento diferente con diferentes llaves, es uno para el Green Card de USA, otro para la Permanent Resident Card de Canadá, etc., la complejidad del sistema de grabación con láser lineal hace imposible la falsificación del código. El Green Card de USA no se ha falsificado nunca en más de 20 años



Es también el **Código Óptico de Seguridad** con mayor capacidad, tiene **40 veces la capacidad del Chip de un Pasaporte Electrónico actual**, y además incluye en el código la imagen de los datos del usuario y la foto en forma holográfica de acuerdo al estándar ISO/IEC 11695.

Chips Encriptados de Identificación

Es la segunda gran familia de dispositivos de Seguridad Lógica aplicado a la seguridad de los documentos

Chip es un nombre en inglés que en informática significa “pequeño procesador computacional” o microprocesador, es un Circuito Integrado donde se encuentran miles o millones de componentes electrónicos interconectados, (diodos, transistores, resistencias, capacitores, etc.), siguiendo un diseño para cumplir una función determinada.

El campo que nos interesa es el de los Chips aplicados a las tarjetas de identidad en formato ID-1 ISO/IEC 7810 denominadas coloquialmente Smart Cards o Tarjetas Inteligentes

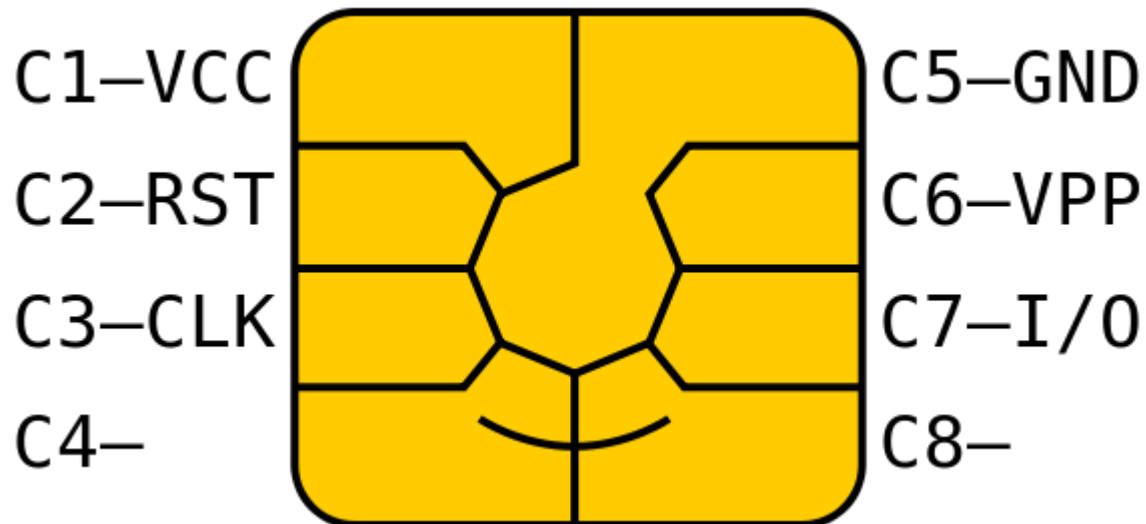
Las Smart Cards son tarjetas ID-1 ISO/IEC 7810 de un polímero plástico con un Chip incrustado en la masa del polímero (substrato) que es archivo de memoria ROM y RAM y que tiene además funciones de microcontrolador y microprocesador

De acuerdo a la interface de conexión las Smart Cards (Tarjetas con Chip) se clasifican en 4 categorías:

1. Contacto
2. Inalámbricas
3. Interface Dual
4. Híbridas

Smart Card de Contacto

Son tarjetas que tienen un cuadrado de color dorado que es la conexión del Chip, para funcionar se debe introducir la tarjeta en la ranura de un lector



En Perú este tipo de Chip de contacto se usa por ejemplo en las tarjetas de crédito, las tarjetas de los decodificadores de cable, y el DNI Electrónico

Detalles de Seguridad



Microtexto con error deliberado



Fondo numismático



Tinta ópticamente variable
Vista de frente



Tinta ópticamente variable
Vista inclinada



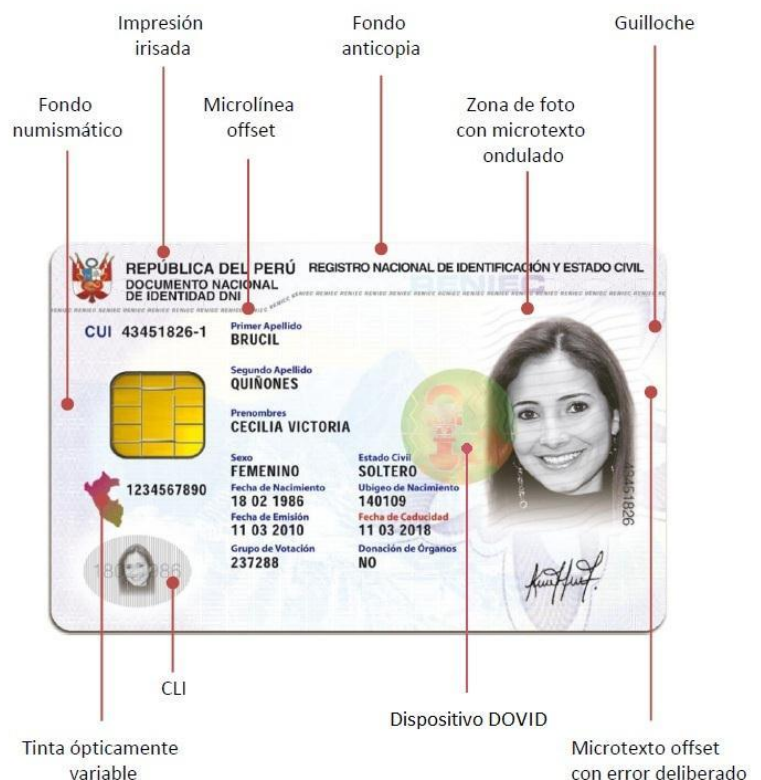
Efecto de color a 0°



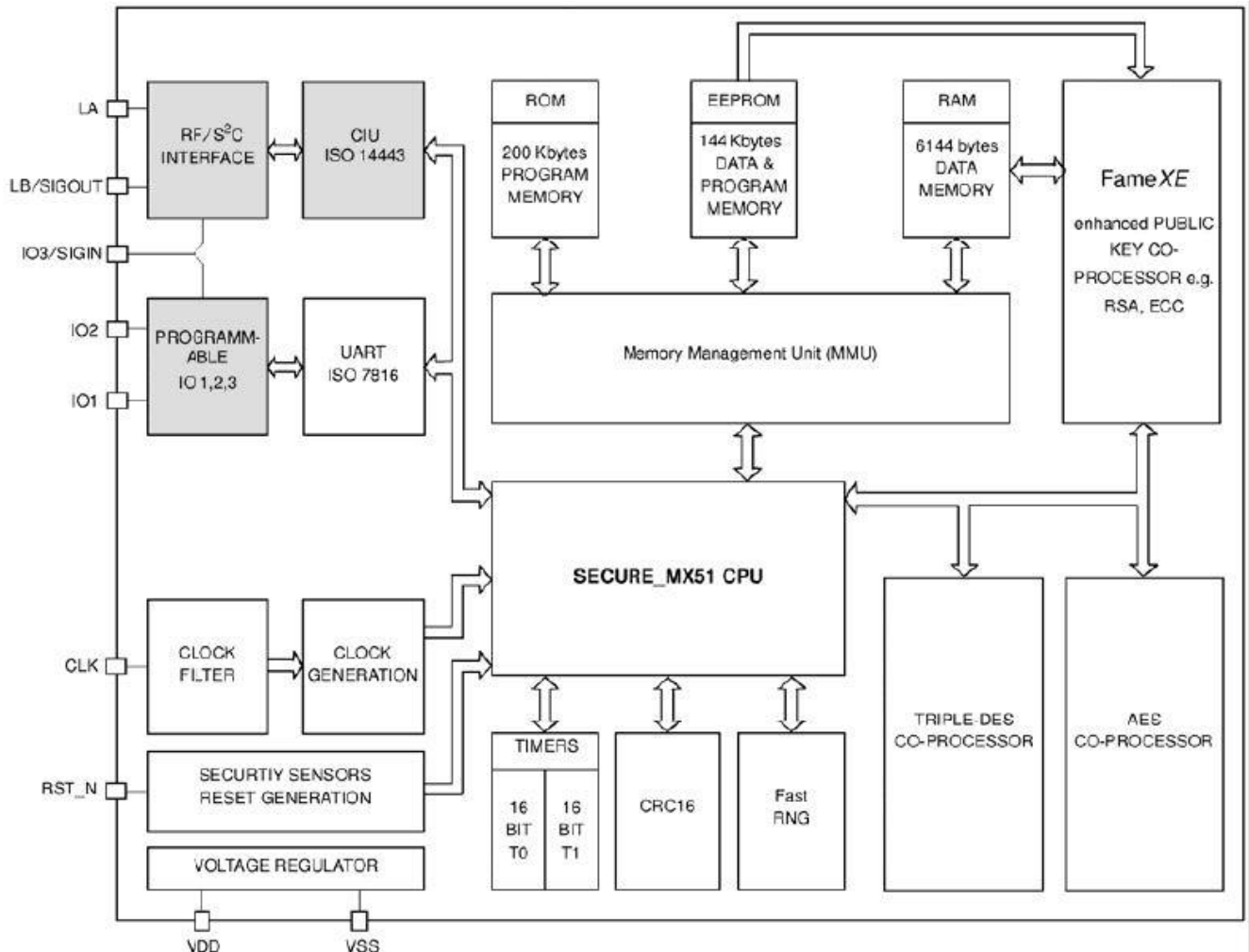
Efecto de color a 90°



CLI



Y como ejemplo de la estructura de un Chip de Documento de Identidad lo podemos ver en el siguiente diagrama del Chip NXP del DNI Electrónico



Smart Card Inalámbrico

Son tarjetas que incluyen el Chip pero no tienen contacto físico exterior, el intercambio de información es inalámbrico, hay muchas categorías, pero las 2 principales son:

1. RFID
2. NFC

RFID

RFID (Radio-Frequency Identification) son chips con un número de serie (ID) y la información está en una Base de Datos así que depende completamente de la conexión a la misma, esta puede estar en la nube o en una computadora local.

Siguen el estándar ISO/IEC 18000 y tiene un alcance de hasta 40 metros por lo cual se utiliza en los automóviles para control y peajes automáticos

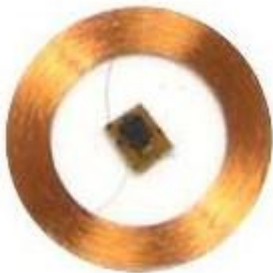
Hay 2 subclases, activos y pasivos, la única diferencia es que los activos tienen una batería que les proporciona energía y los pasivos reciben la energía en forma inalámbrica desde una antena.

Podemos pensar en los Chips RFID como una memoria inalámbrica de (lectura/escritura) con un único número de serie que identifica el documento.

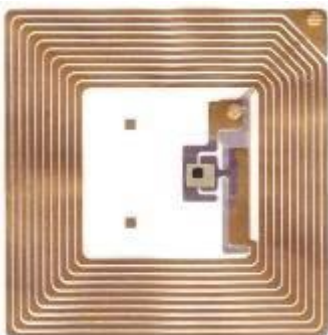


Hay 3 frecuencias principales que se evidencian por la cantidad de vueltas de la bobina de la antena, cuanto más alta la frecuencia menos vueltas la bobina.

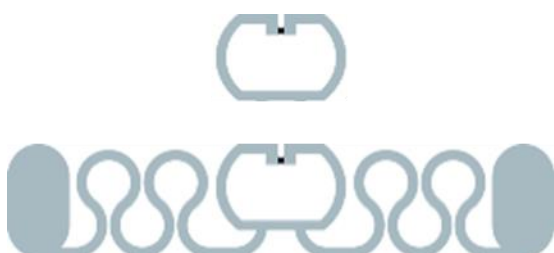
Baja Frecuencia LF



Alta Frecuencia HF



Ultra Alta Frecuencia UHF



Este último es el Chip RFID de la Tercera Placa ubicada en los parabrisas de los vehículos de Perú desde hace 9 años, esto nos enseña una lección para nuestro proyecto, hasta enero de 2018, no tiene ninguna aplicación ni uso, debería tenerlo y es una tarea pendiente.

NFC (Near-Field Communication)

Son chips pasivos, (sin batería) que como su nombre lo indica funcionan a poca distancia, menos de 10 cm y una frecuencia de 13.56 MHz.

Se basan en los estándares ISO/IEC 18092 y ISO/IEC 14443

El Chip NFC basado en el estándar ISO/IEC 14443-4 (Generación 4), es el de elección para documentos de identidad de **Alta Seguridad** y es el usado en todos los **Pasaportes Electrónicos y la nueva generación de DNI Electrónicos, por ejemplo España y Uruguay.**

¿Cuál es la importancia de un Chip NFC para la Licencia de Conducir?

Que es uno de los Activos fundamentales para cumplir con el Principio fundamental de la Seguridad Lógica Documentaria

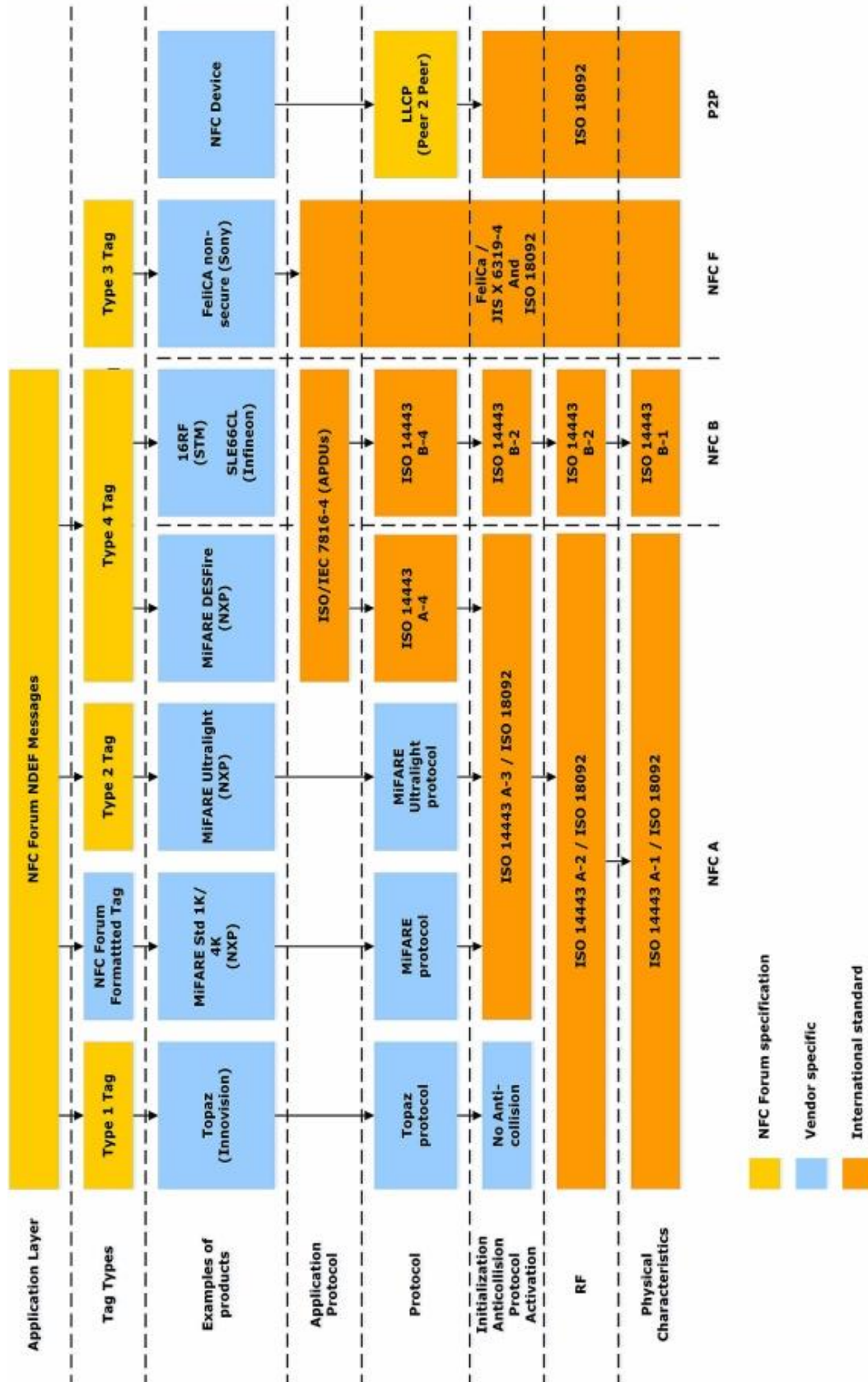
1. Es una de las medidas de Seguridad Lógica que funciona Offline-Online
2. Es una de las medidas de Seguridad Lógica que al año 2017 ya tiene una amplia base de sistemas de verificación-autenticación a precios razonables.



New Enhanced Driver License = NFC

En el caso del Chip NFC cumplir con el principio de mantener el actual costo del Brevete, es el mayor desafío para su aplicación

El siguiente cuadro indica las Clases y Protocolos NFC



3. Cadena de Custodia y Trazabilidad

La Cadena de Custodia Documentaria son todos los procedimientos, protocolos y buenas prácticas que se deben seguir con un documento desde su origen hasta su destino final.

La Cadena de Custodia puede ser Física, Lógica, o Mixta y debe proteger el documento a través del flujo completo.

La trazabilidad permite saber dónde se encuentra el documento y sus coordenadas espaciales y temporales.

La trazabilidad es conocer este conjunto de 4 coordenadas durante todo el proceso

La Cadena de Custodia y Trazabilidad se verán nuevamente en los procesos de Seguridad Física, Seguridad Lógica y Seguridad Informática

4. MLDS (Multiple Layered Defense System) Sistema de defensa en capas múltiples



Es la unión de todos los sistemas de Seguridad Documentaria Física y Lógica aplicados a un documento, es un principio físico básico que se aplica también a la resistencia de una soga, un chaleco antibalas, el blindaje de un tanque o de una nave espacial.



No hay una **Seguridad Física** objetivamente superior en todas las circunstancias, depende de donde se vaya a verificar, quién la vaya a verificar, quién la vaya a falsificar, en qué lugar y cómo se vaya a verificar, por eso es el experto documentario quién debe guiar la estrategia de que **Seguridad Física** se debe aplicar.

Por ejemplo una de las medidas de **Seguridad Física** más antigua y más usada es la Impresión Calcográfica o Intaglio y se usa en casi todos los billetes del mundo porque no se puede falsificar exactamente y la diferencia la puede notar desde una cajero de banco en ventanilla con Luz UV y un cambista en la calle con sol o poca luz sin instrumentos, hasta la cajera de un supermercado.

Yo mismo he probado las mejores falsificaciones de soles con mi cambista de confianza y siempre se ha demorado menos de un segundo en detectar el billete falso simplemente al tacto.

Sin embargo nuestro proyecto está enfocado en la **Licencia de Conducir**, y que nosotros sepamos la única Licencia de Conducir del mundo que emplea la Impresión en **Intaglio tipo Papel Moneda es la de Brasil**.

Pero no todos tienen esa habilidad del cambista, por eso un billete de banco tienes otras capas de **Seguridad Física, Papel Insensible al Yodo, Tintas Fluorescentes a la Luz Ultravioleta, Tintas Magnéticas, Hologramas de Seguridad OVD, Tintas OVI (Optical Variable Ink)**

Como el detalle de las capas **MLDS** depende del tipo de documento y el costo lo volveremos a ver específicamente en el capítulo de **Seguridad Física de la Licencia de Conducir**.

En todos los casos las capas de **Seguridad Física y Seguridad Lógica** son decididas por el experto documentario siguiendo una **Matriz como la del estándar ASTM F1448**, su objetivo es decidir el número y tipo de capas siguiendo un esquema **MLDS de Costo-Beneficio**

5. Emisión Descentralizada pero Impresión Centralizada

La Seguridad Documentaria Moderna ha optado por este sistema porque es el sistema más seguro y el de menor costo ya que bajan los costos de equipos por la producción a por economía de escala, y se reduce el costo de la **Cadena de Custodia**. El único país en el mundo que usa un sistema de impresión descentralizada es España por razones políticas, el costo de los equipos de **Laser Engraving** y la **Cadena de Custodia** son extremadamente caros y el documento está subvencionado por el estado

6. Cumplimiento de estándares actualizados

Seguir los estándares es la única garantía para los procesos que desarrollan las Imprentas de Valores, estos estándares pueden ser consultados en el **Comité de Seguridad Documentaria de INACAL**



7. Certificación de las empresas proveedoras de las tecnologías de seguridad

Las empresas que proporcionan los insumos deben ser Certificadas, lo cual es sinónimo de empresas de prestigio internacional, para seguir con el ejemplo de los Hologramas, hay Hologramas y **Hologramas de Seguridad (Kinegram o DOVID)**, no se puede usar un Holograma el nivel de los que se usan en las cajas de cereales, parece de Ripley pero sucede

8. Certificación e historial de la Empresa Integradora

La Empresa Integradora (EI) es donde se juntan todas las tecnologías Físicas y Lógicas para obtener el producto final, en nuestro caso la Licencia de Conducir Digital, allí llegan los materiales de los substratos, las tintas especiales de venta restringida, las **Tintas Fluorescentes IR y UV, OVI, DOVID Chips NFC, etc.**

Pongamos un solo ejemplo que demuestra la necesidad en la Empresa Integradora, el caso del paquete de 1,000 hologramas que se robaron del punto de impresión del MTC en el Touring, y en todos los demás lugares se roban hologramas todos los días, en una empresa con procesos certificados eso no puede pasar.

Tomemos como ejemplo nuestro paradigma el BEP (Bureau of Engraving and Printing) que tiene los ISO 9001 y ISO 14001, debemos pretender que nuestra EI tenga estos estándares y muchos más pero nuestra experiencia demuestra que a veces hasta estos papeles se falsifican, por ello la solución que indican las buenas prácticas internacionales es una inspección a la planta de la Empresa Integradora antes de tomar una decisión.

Otro aspecto muy importante sobre todo ahora con Google es buscar el historial de las candidatas a **Empresa Integradora**, solo un historial y un pasado libre de malas prácticas puede garantizar que depositemos nuestra confianza hacia el futuro

Principio fundamental de la Seguridad Lógica Documentaria

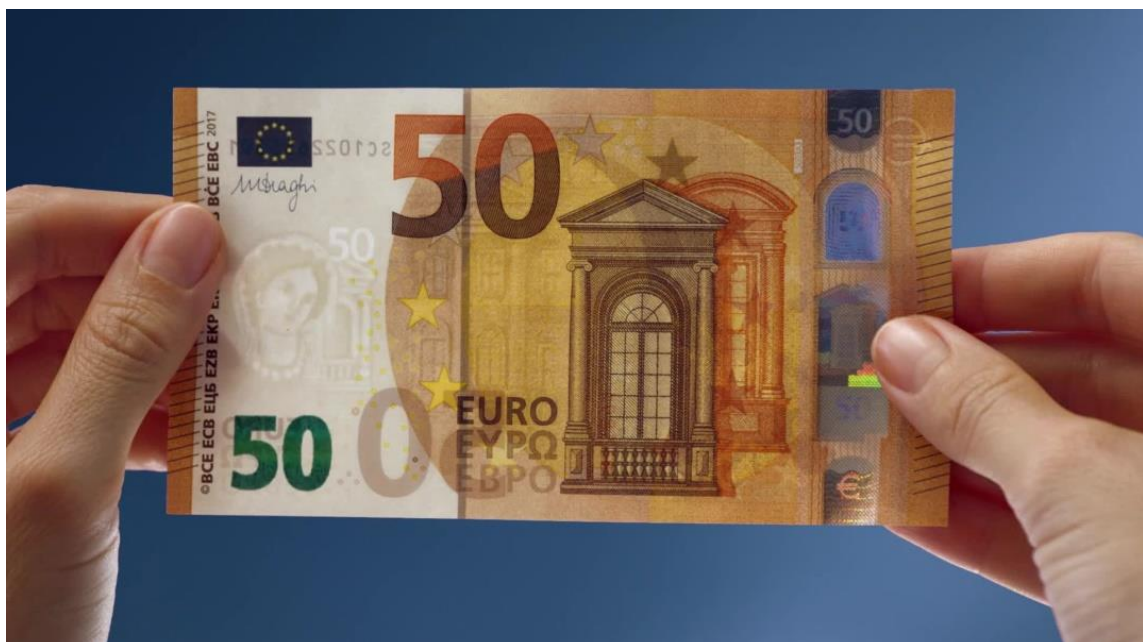
La Seguridad Lógica de todo documento debe cumplir con éste principio, el Activo, o la suma de Activos, de Seguridad Lógica debe tener características Offline-Online.

Aclaremos que este principio no quiere decir que todas las características tengan esta propiedad, sino que al menos una de ellas debe poder verificarse Offline

Esto se analizará en detalle en la sección específica sobre la Seguridad Lógica de la Licencia de Conducir.



Seguridad Física



Seguridad Física de la Licencia de Conducir

Como ya hemos visto antes la definición y características de la Seguridad Física, sabemos que también se llama Seguridad Documentaria Clásica ya que fue la primera Seguridad Documentaria que apareció en la historia, sabemos que era la única Seguridad Documentaria hasta fines del siglo XX, sabemos que sigue siendo la principal seguridad de todo el papel moneda del mundo, ahora debemos analizar la **Seguridad Física de la Licencia de Conducir**

Es cierto que nuestro objetivo es diseñar una Licencia de Conducir poniendo especial énfasis en la Seguridad Lógica, pero también es cierto que los dólares, euros y soles tienen sólo Seguridad Física, y que el DNI Electrónico y el Pasaporte Electrónico tienen un máximo nivel de Seguridad Física.

No existe en este momento ningún documento en el mundo, ni estándar de Seguridad Documentaria, que elimine la Seguridad Física, de hecho es el primer punto de los 8 principios básicos de Seguridad Documentaria y primera capa del sistema MLDS

Pero el DNI Electrónico y el Pasaporte Electrónico tienen un costo mucho mayor que el fijado para este proyecto, nuestro desafío es entonces alcanzar el máximo de Seguridad Física con el costo asignado.

¿Por qué debemos incluir Seguridad Física?

Porque así lo indican todos los estándares de Seguridad Documentaria, pero la explicación es muy sencilla, al igual que el papel moneda un documento debe poder ser verificado con total seguridad sin equipo electrónico especial, (Computadoras, Smartphones) y estos equipos son imprescindibles para la verificación de la **Seguridad Lógica Offline** y además adicionalmente conexión a la red para la **Seguridad Lógica Online**.

Tomaremos como Paradigma los DNI Electrónicos, que ya vimos que siendo un documento de Seguridad Lógica tienen el máximo de Seguridad Física.

Todos ellos son documentos en **Policarbonato** por impresión usando **Láser Engraving** y con Dispositivos DOVID (Diffractive Optically Variable Image Device) el primero de los cuales fue Kinegram y como ya mencionamos se usó para la **Visa Schengen**.

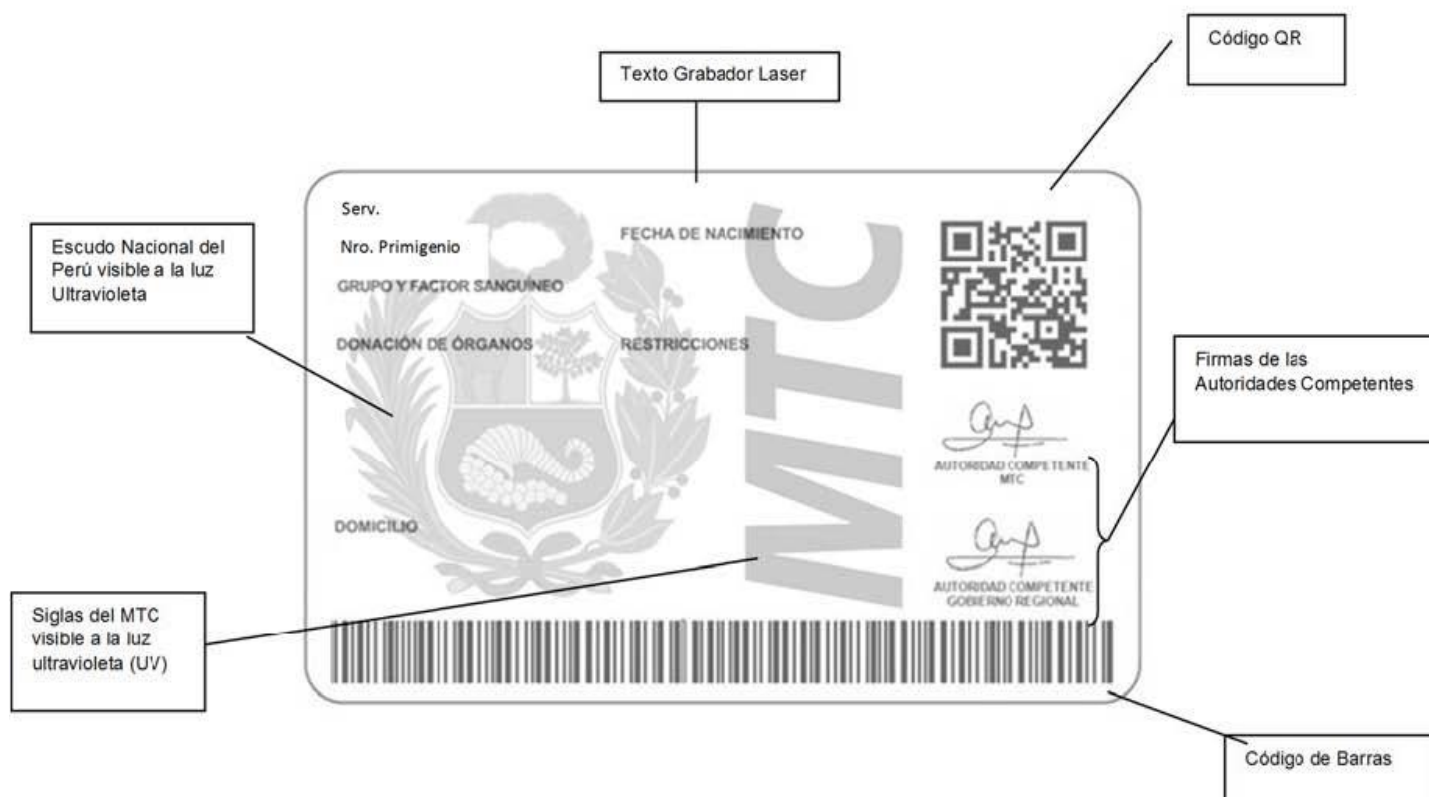
Sabemos que este Paradigma no es alcanzable por un tema de costos ya que la **Resolución Directoral n° 305-2017-MTC Policarbonato del 17 de enero de 2017** fue descartada en abril del mismo año por el nuevo Director General de la Dirección General de Transporte Terrestre.

El desafío es lograr la Seguridad Física más cercana al Policarbonato con Láser Engraving, sin incurrir en esos costos ya descartados

DATOS Y MEDIDAS DE SEGURIDAD DE LA
LICENCIA DE CONDUCIR EN POLICARBONATO



REVERSO
DATOS Y MEDIDAS DE SEGURIDAD DE LA
LICENCIA DE CONDUCIR EN POLICARBONATO





- 1.- La imagen Láser Variable (MLI o CLI) debe descartarse porque es exclusiva del Policarbonato y la Técnica de Laser Engraving.
- 2.- Relieves deben descartarse porque son una característica del Láser Engraving o Intaglio
- 3.- La Tinta Ópticamente Variable (OVI) puede y debe ser aplicada en otros soportes diferentes al Policarbonato, pero debemos acercarnos lo más posible a la calidad del OVI de los billetes de banco o el papel moneda, es el caso del billete de 10 soles que cambia en forma evidente del color magenta al verde

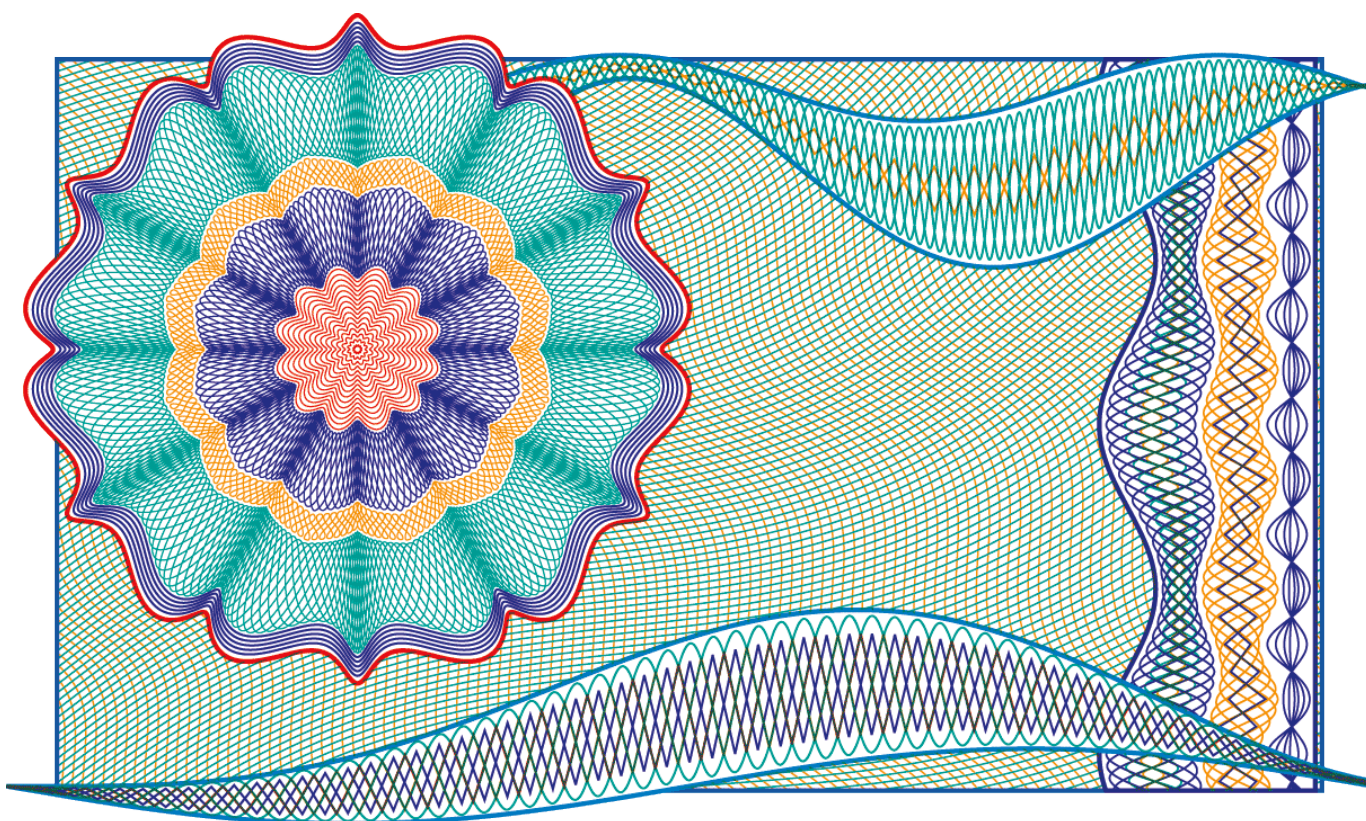


- 4.- Fotografía por impresión con Láser Engraving que no puede ser borrada o alterada con solventes químicos, debemos buscar otras tecnologías que protejan la foto en otros soportes como PVC Compuesto o Teslin

5.- Fondo de colores difuminados que no se pueden fotocopiar con fidelidad, es una tecnología que tienen todos los Documentos de Seguridad pero aunque no se pueda imitar exactamente la gente no nota fácilmente la diferencia, se incluirá pero no es especialmente relevante para nuestro proyecto. Se puede aplicar en Policarbonato, PVC Compuesto, Teslin o Papel Moneda

6.- Imágenes y texto impresos con Tinta Fluorescente a la Luz Ultravioleta o Infrarroja, se puede aplicar en todos los soportes y de hecho es una medida de Seguridad Documentaria que se aplica en todos los documentos y se va a aplicar en la nueva Licencias de Conducir. No la consideramos una medida de seguridad relevante porque a diferencia de los bancos y otras instituciones financieras, puntos de control migratorio, y hasta oficinas comerciales nunca hemos visto a un policía o inspector de tránsito con una Lámpara Ultravioleta Portátil. Las Licencias de Conducir falsificadas son fácilmente detectables bajo la Luz Ultravioleta, **si se usara y fuera de noche.**

7.- Fondos de Seguridad: Guilloches y Tramas de Seguridad, son aplicables a todos los sustratos y es una medida de Seguridad Documentaria que se aplica en todos los documentos de seguridad, en los DNI Electrónicos y los Pasaportes, se aplicará también en nuestro diseño de Licencia de Conducir.



Es generado por software especial que sólo tienen las Imprentas de Valores, no se puede fotocopiar ni imprimir con tecnologías convencionales de impresión y se puede verificar con una lupa cuentahílos de 5 soles, es una buena medida de seguridad **si se entrena al personal encargado de fiscalizarla.**



La lupa cuentahílos es un dispositivo de bajo costo que permite verificar la medida de seguridad anterior (7) y la siguiente (8)

8.- Microescritura o Microtexto es la impresión de caracteres, (alfanuméricos o símbolos) a una escala que requiere de amplificación óptica para ser leído. A simple vista el texto aparece como una línea sólida. Los intentos de reproducirlo por Fotocopia, Escaneo o Pantógrafo, se traducen típicamente en una línea sólida o de puntos, a menos que el método de reproducción tenga la capacidad de identificar y recrear estos patrones a esa escala, lo que implica altísima tecnología, no Azángaro. La Microescritura es una medida anti falsificación de gran importancia debido a que es imposible de ser reproducida por métodos digitales convencionales. La Microescritura puede ser variable y personalizada, un texto diferente para cada documento, en este caso se convierte en un mecanismo de seguridad de robustez formidable, es nativo del sistema de Policarbonato con Láser Engraving, pero afortunadamente puede ser aplicada también en PVC Compuesto y Teslin.

En estos substratos sin Láser Engraving se usan impresoras especiales para Microescritura Digital y Fonts y Tintas especialmente diseñadas para este propósito. La tinta más usada es de partículas de tóner MICR (Magnetic Ink Character Recognition), pero también se pueden usar tóner con base de poliéster, tóner con base de styrene acrylate polymer. También se pueden usar tóner en color y tóner más especializado que contiene tintas sensibles a la luz ultravioleta o diferentes frecuencias de infrarrojo que producen fluorescencia al ser expuestos a la radiación adecuada.

9.- DOVID (Diffractive Optically Variable Image Device) es un tipo de Holograma especial de Seguridad Dinámico (con efectos cinéticos, cambio y movimiento). Dispositivo óptico variable también conocido como “holograma de seguridad” y que es emitido únicamente por las imprentas de seguridad registradas en la IHMA International Hologram Manufacturers Association Ltd:

Más allá de cada técnica particular para crear estos efectos, (movimiento, imágenes ocultas, etc.) todos tienen en común que no son creados por impresión de Rayo Láser, sino por el uso de Haz de Electrones que permite más resolución y un detalle más fino para los efectos de difracción.

Optaglio (Optical Microstructure Technologies) ha impreso en un DOVID de 15 mm un mapa con todas las calles de la ciudad de Praga.

El DNI Electrónico y todos los pasaportes del mundo incluyen DOVID, uno de los primeros en salir al mercado en 1980 fue el Kinegrama de la empresa suiza Kinegram



La característica de los DOVID es su alta resolución y los efectos cinéticos que no pueden ser imitados. En el caso de la Licencia de Conducir debemos tener en cuenta.

1. El costo debe ajustarse a nuestro presupuesto
2. El efecto cinético debe ser notable para cualquiera

Una de las principales características de una medida de Seguridad Documentaria efectiva es que la diferencia entre la imitación y la original deben ser claramente discernibles para todo público, y este no es el caso del Holograma de la Licencia de Conducir actual



Es claro que este holograma falso es simplemente una lámina de aluminio difractiva donde se ha impreso MTC con tipografía de 2 tamaños, pero debido a que el original carece de efectos cinéticos claramente distinguibles el holograma falso cumple con el papel de engañar.

También hay casos de Licencias de Conducir falsas con hologramas verdaderos, esto sucede por los robos masivos de hologramas, hasta por mil hologramas de una vez, y el robo hormiga de todos los días, esto sucede en las decenas de puntos de impresión en todo el país.

La solución entonces para el DOVID es usar uno con efectos cinéticos claros para cualquier observador, controlar la Cadena de Custodia con un sistema de Emisión Descentralizada e Impresión Centralizada, como es el estándar mundial, y asignar un solo responsable de su control que debe tener todas las seguridades que exigen los estándares de la industria de Seguridad Documentaria.

Con esto agotamos las medidas de Seguridad Física que podemos migrar desde la tecnología de Substrato de Policarbonato y de impresión por Láser engraving que pueden migrar a otras tecnologías de substrato e impresión.

TABLA 1 Matriz de Lista de Control para Definir Requerimientos Tecnológicos (MLCDRT)

Sustitución	Simulación	Duplicación	Desvío	Alteración	Falsificación	Parámetros
						Durabilidad
						Selección y Verificación visual simple
						Validación sin instrumentos
						Validación con instrumento simple de campo
						Validación con instrumento complejo de campo
						Fácil de incorporar y aplicar
						Rentable en función del riesgo potencial
						Resistente a la alteración o la alteración deja evidencia
						Características de seguridad expuestas
						Características de seguridad ocultas
						Suficiente tiempo disponible para la autenticación
						Autenticación en cualquier momento y lugar que sea necesaria
						Facilidad de integración con el sistema actual
						Se requiere capacitación para la validación
						Es necesaria capacidad disuasiva simple
						Requiere trazabilidad (Seguridad Lógica)
						Información variable incluida en las características de seguridad (Seguridad Lógica)
						Requiere de laminado en caliente
						Requiere adhesivo sensible a la presión
						Requiere de sustratos especiales
						Requiere de tintas especiales
						Requiere una sola característica de seguridad
						Requiere de múltiples características de seguridad
						Validación uno a uno
						Requiere de cierre o sello
						Requiere de la verificación de un experto
						Se requiere cómo evidencia en una corte
						Requiere de una tecnología exclusiva
						Debe ser fácil de detectar una alteración

Es estándar ASTM F1448 indica en el inciso 10 el procedimiento matricial que debe usarse en manos de un experto documentario para decidir el tipo de seguridad que se debe aplicar a un documento en particular.

10 Matriz (Tabla 1)

10.1 El eje vertical (Y) de la matriz identifica el problema potencial. El eje horizontal (X) identifica el posible requerimiento tecnológico que ayudará en la evaluación de las tecnologías

10.2 La persona responsable de la selección analiza cada parámetro para elegir el adecuado al fin de crear un sistema de seguridad efectivo, teniendo en cuenta lo que se requiere para su aplicación.

10.3 El analista coloca una marca "X" en el lugar apropiado de la tabla, bajo el parámetro y a través de uno de los CADDSS.

11.1 CADDSS; (counterfeit protection); (product protection); security; (document protection); security analysis.

Una vez elegidas las medidas de Seguridad Física debemos analizarlas y crear la matriz de eficiencia para un documento determinado.

Esta Matriz de Eficiencia CADDSS debe analizar:

1. Valor objetivo y absoluto de la Medida de Seguridad Física.
2. Documento específico donde se va a aplicar
3. Instrumental requerido para su verificación.
4. Capacitación del personal
5. Costo de los sistemas de autenticación
6. Medidas verificadas por los inspectores y su frecuencia
7. Métodos usados por los falsificadores

Se le asignan puntajes y pesos en una escala de 1 a 10 y se obtiene un promedio ponderado

Y las medidas que vamos a migrar a nuestro sustrato y tecnología de impresión son

3.- Tinta Ópticamente Variable (OVI)

5.- Fondo de colores difuminados

6.- Imágenes y texto impresos con Tinta Fluorescente a la Luz Ultravioleta o Infrarroja

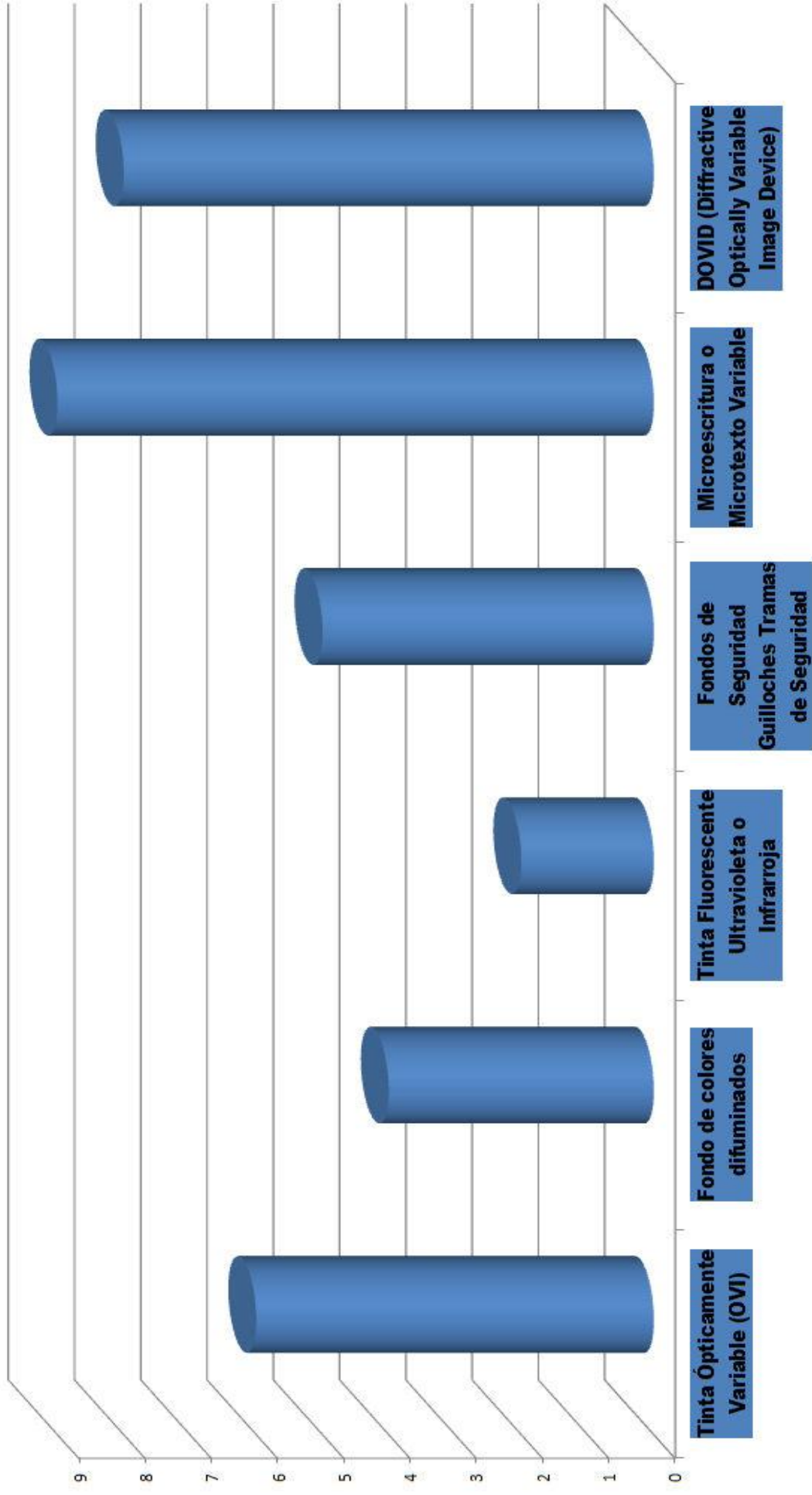
7.- Fondos de Seguridad: Guilloches y Tramas de Seguridad

8.- Microescritura o Microtexto Variable de caracteres, (alfanuméricos o símbolos)

9.- DOVID (Diffractive Optically Variable Image Device)

En la siguiente página se presenta en forma gráfica la importancia ponderada de las principales medidas de Seguridad Física de la nueva Licencia de Conducir, no se incluyen medidas de nivel 3 como las Fallas Técnicas, porque, aunque se aplicarán son medidas de estricto nivel forense, es notorio que las 3 medidas más importantes son

- 1. Microescritura**
- 2. DOVID**
- 3. OVI**



Matriz de Eficiencia CADDSS

Conclusiones sobre la Seguridad Física

La Matriz de Eficiencia CADDSS que vemos en el gráfico es la Matriz específica para la Seguridad Física de la Licencia de Conducir de Perú.

Las conclusiones se basan en todos los análisis e informes forenses de 25 años de falsificación para un Brevete que no ha variado en 25 años, **conocemos los métodos de Azángaro y los falsificadores.**

Un ejemplo de este análisis son las tintas fluorescentes, que siguen siendo importantes en otros documentos de aún más alta seguridad como el Pasaporte Electrónico y ocupa el último lugar en la Licencia de Conducir de Perú, los falsificadores saben que no se usa, nunca se ha visto a un policía con una Lámpara UV portátil y mucho menos con un Láser Infrarrojo, los falsificadores de brevete hace más de 10 años que no incluyen tintas fluorescentes en sus falsificaciones porque saben que nadie las verifica.

En el otro extremo de alta puntuación tenemos el punto 8 (Microescritura Variable) y el punto 9 DOVID (Diffractive Optically Variable Image Device) que son dos tecnologías ausentes en la actual Licencia de Conducir.

La Microescritura Variable tiene un ponderado levemente superior por ser personalizada, es decir que cada documento es diferente, y se necesita sólo de un simple cuentahílos para ser verificada, se puede autenticar su información comparándola con el DNI y es independiente de la Cadena de Custodia de la Seguridad Física.

El DOVID (Diffractive Optically Variable Image Device) se puede verificar a simple vista, pero al igual que el actual holograma depende de la Cadena de Custodia de la Seguridad Física que hace más de 10 años que es una “coladera”

La solución obvia para cumplir el estándar de Cadena de Custodia Física, y que además se usa el todo el mundo es la Centralizada, donde todo el proceso es confinado a una “Fortaleza”, el mejor ejemplo es el BEP (Bureau of Engraving and Printing)



Desde el siglo XIX hasta el 26 de abril de 1991 todos los dólares del mundo se imprimieron únicamente en esta imprenta, desde esa fecha hay una segunda imprenta del BEP en Fort Worth; Texas a 1,210 Km.

El único caso en el mundo donde no se sigue éste estándar universal es el DNle Español y esto debido a las autonomías, esto implica una Cadena de Custodia de muy alto costo que solo es factible por la subvención del gobierno español que dice literalmente *“el Gobierno promoverá la norma legal de rango adecuado para la adecuación de la tasa que haya de percibirse por la expedición del Documento Nacional de Identidad, de acuerdo con su coste y en consideración a los beneficios que proporciona a la comunidad”*

Pero la norma peruana para la Licencia de Conducir dice que el valor se determinará respetando los límites establecidos en el artículo 45° de la Ley del Procedimiento Administrativo General. Ley N° 27444, no incluye ninguna subvención y dice que el costo para el usuario no será en ningún caso mayor al valor que se encuentra vigente.

Siguiendo esta norma la única solución de una Cadena de Custodia Física que cumple el estándar mundial es el sistema universal centralizado de insumos físicos, cualquier otra solución requiere de una subvención del estado.

Aunque nuestro objetivo es una Licencia de Conducir Digital Biométrica, eso pertenece al capítulo de la Seguridad Lógica que trataremos más adelante, pero la Seguridad Lógica requiere de instrumental de verificación, que aunque el año 2018 será más asequible, no debemos olvidar que estamos en un país complejo de geografía muy compleja, entonces mejorar la Seguridad Física de la Licencia de Conducir sin alterar su costo es un principio fundamental de Buenas Prácticas de Seguridad Documentaria para nuestro territorio y nuestra realidad.

Con respecto a la Cadena de Custodia de Seguridad Física dependerá del lugar, edificio e infraestructura, los procedimientos, los estándares y buenas prácticas de la locación que concentre los insumos físicos, sin llegar a ser un BEP debe parecerse a los estándares de un banco o financiera, lo más común y parecido a una Imprenta de Valores.

En el caso de nuestro paradigma que es el BEP debemos pensar que al igual que ellos lo ideal es que el impresor cumpla con las normas ISO 9001 y ISO 14001, con respecto a estándares de Seguridad Física de bancos y financieras 4 de los más completos son:

- **Manual General de Seguridad para Entidades Financieras (Ministerio de Seguridad Pública de Costa Rica)**
- **Importancia de la estandarización de la seguridad física en las entidades financieras en Colombia (Universidad Militar Nueva Granada 2016)**
- **Manual de seguridad bancaria, España**
- **Manual de seguridad bancaria, México**

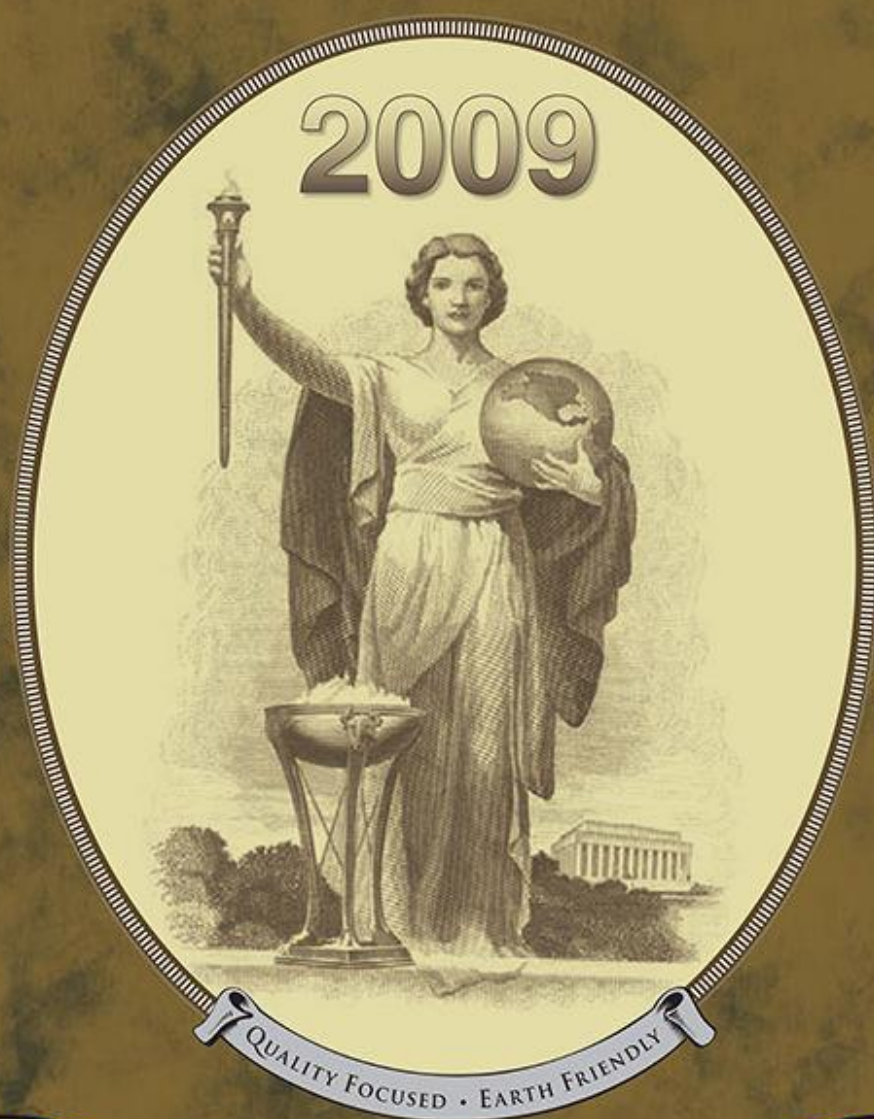
En definitiva lo más seguro para juzgar la seguridad es una inspección actualizada a las instalaciones de todos los posibles candidatos y cuanto más parecido sea al BEP, sus estándares y Buenas Prácticas mejor.

Y un detalle que a veces se olvida y el BEP toma en cuenta, no bastan los muros, las bóvedas, el aislamiento perimetral, las cámaras, las alarmas, las puertas dobles, la biometría, las revisiones, el Factor Humano es fundamental, y por ello la elección de personal y el buen trato son fundamentales (ISO/IEC 18001)



DEPARTMENT OF THE TREASURY
BUREAU OF ENGRAVING AND PRINTING

CHIEF FINANCIAL OFFICER
PERFORMANCE AND ACCOUNTABILITY REPORT

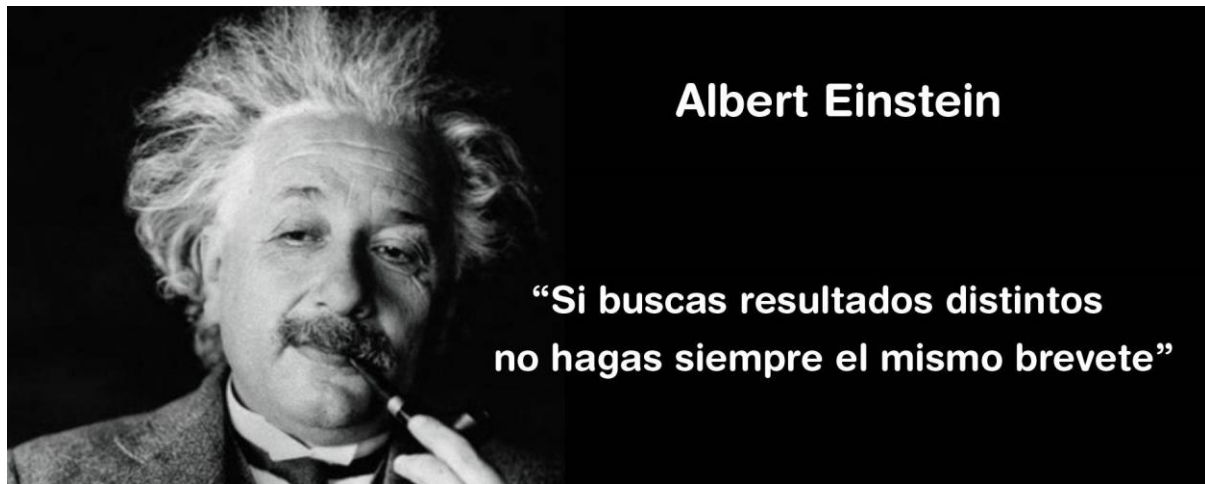


Hay otro detalle que se debe mejorar en la Seguridad Física aunque no sea una de las medidas de Seguridad Física de los DNI Electrónicos, los Substratos de Policarbonato con Laser Engraving, ni los Pasaportes Electrónicos.

No está entre las tecnologías que hemos elegido para migrar a nuestro substrato y tecnología de impresión de la Licencia de Conducir Digital

Tampoco está en la Matriz CADSS del estándar ASTM-F1448

Se trata de Lógica Pura y ya lo dijo hace muchos años el gran sabio Albert Einstein



Y Alberto tiene razón, hace más de 25 años que hacemos el mismo Brevete, no debemos esperar resultados distintos, sólo cada vez más falsificación, porque cada día es más fácil para los falsificadores, a ellos le basta hacer lo mismo que hacen hace más de 25 años.

Las medidas de seguridad son las mismas desde el milenio pasado cuando los celulares de alta tecnología eran los Motorola de sapito



Pero aunque parece que algunas personas no se han dado cuenta, o no quieren darse cuenta por intereses subalternos, (es un eufemismo para el informe); ya estamos en el Tercer Milenio.

Sí, estamos en el año 2018, y aunque todos amamos los “sapitos”, las computadoras Radio Shack TRS-80, las Commodore, las Atari, pero más allá de la nostalgia el mundo ha cambiado.

Por eso hemos diseñado la Nueva Licencia de Conducir Digital con nuevas tecnologías de Seguridad Física del Tercer Milenio que hará imposible el trabajo a los falsificadores, serán eliminados por las inmutables leyes de la evolución y la selección natural.

Pero podemos hacer cambios fuera de la “matrix” y las nuevas medidas de Seguridad Física. Cambiemos el obsoleto y fácilmente imitable diseño.

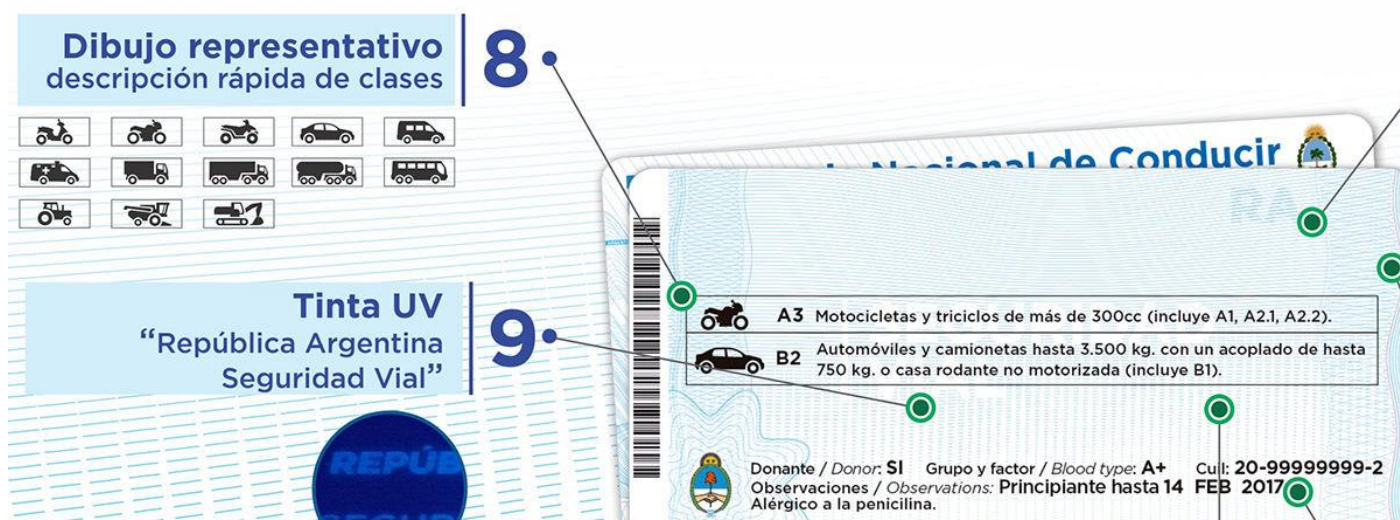
Pero ya que cambiaremos el diseño para tristeza de Azángaro podemos hacer un cambio que facilite las labores de fiscalización de inspectores y policías, cambiemos el absurdo sistema en el cual las categorías apenas se notan y ocupan menos del 1% de la Licencia de Conducir.

Ya vimos al principio de este estudio la fórmula de la energía cinética:

$$E = \frac{1}{2} MV^2$$

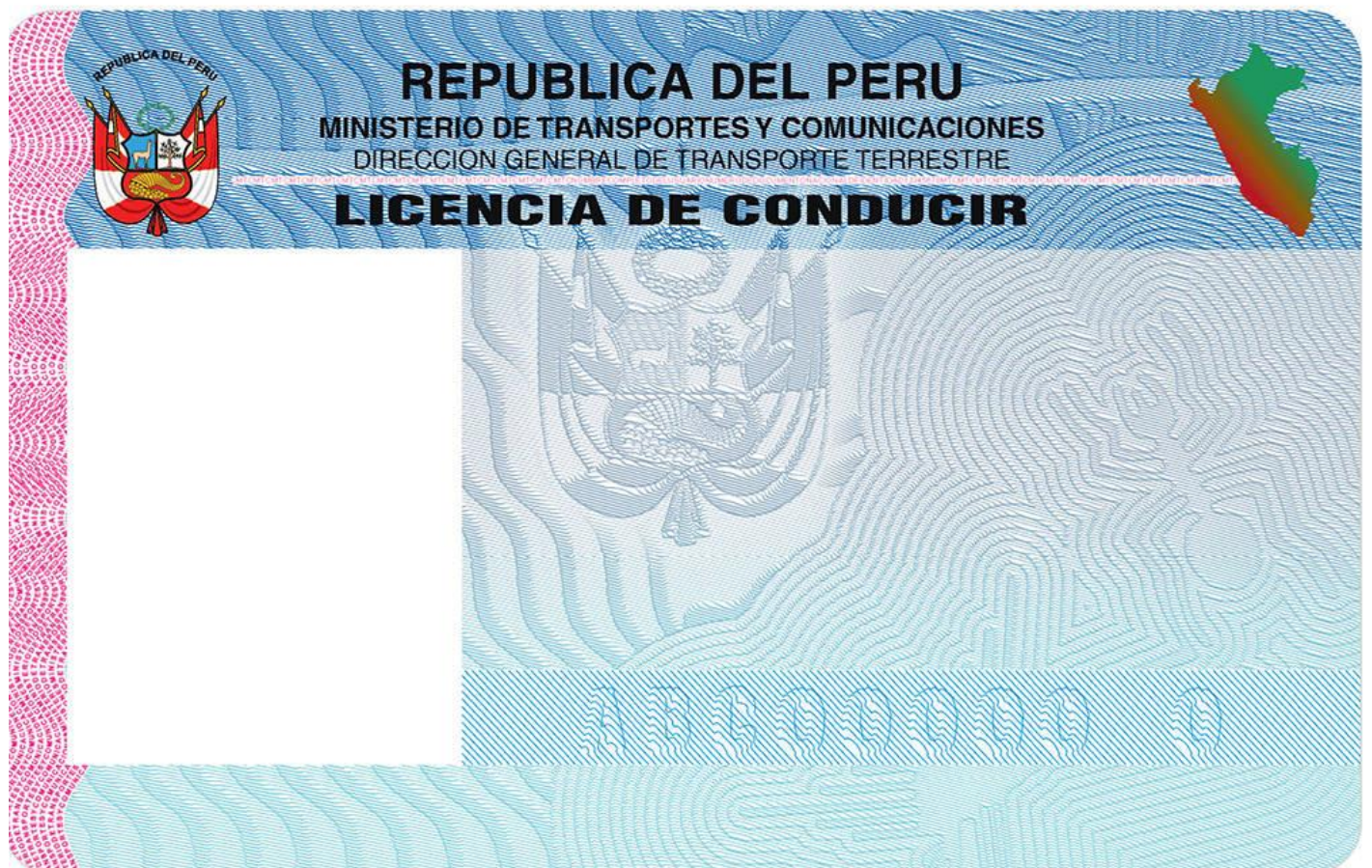
Que demuestra que la relación entre manejar un automóvil de 2 toneladas un autobús de 18 toneladas o un camión de 40 toneladas no es lineal sino cuadrática.

Tampoco es lo mismo la responsabilidad de un chofer que lleva 1 o 4 pasajeros que la del chofer que lleva 60 pasajeros, por eso la Nueva Licencia de Conducir Argentina consideró necesario hacer más evidente esta característica de la nueva Licencia de Conducir destacando las Clases o Categorías



Nosotros tomaremos en cuenta esta consideración, pero lo haremos mejor como se ve en la propuesta de nuevos diseños

Anverso Clase A



CLASE A



Ciclomotores
hasta 50 cc.



Motocicletas
hasta 150 cc.
Incluidos: triciclos,
ciclomotores
y cuatriciclos.



Motocicletas
hasta 300 cc.
Incluidos: triciclos,
ciclomotores
y cuatriciclos.

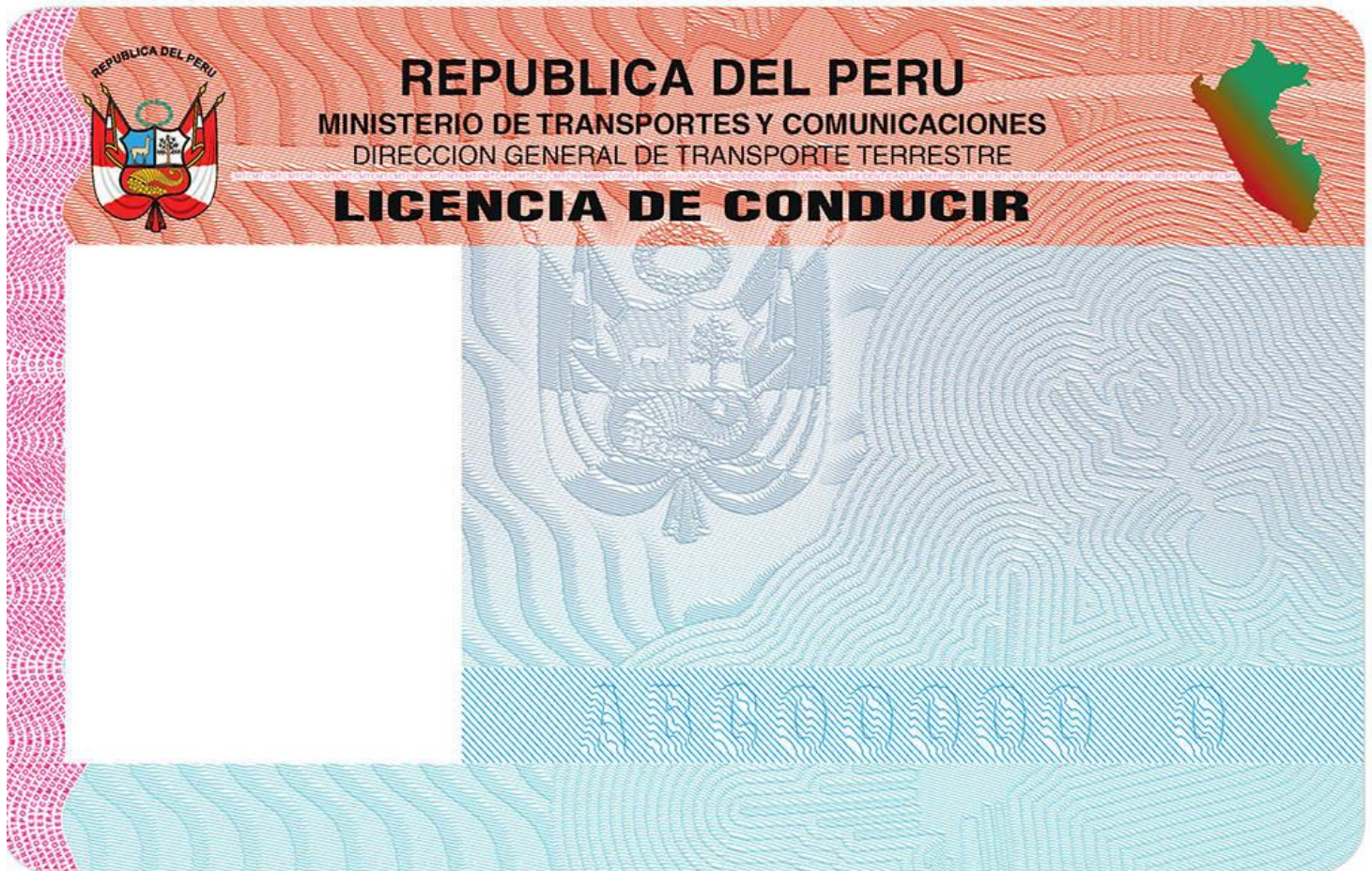


Motocicletas de
más de 300 cc.
Incluidos: triciclos,
ciclomotores
y cuatriciclos.



Categorías
anteriores que
sean dedicadas
para actividades
comerciales.

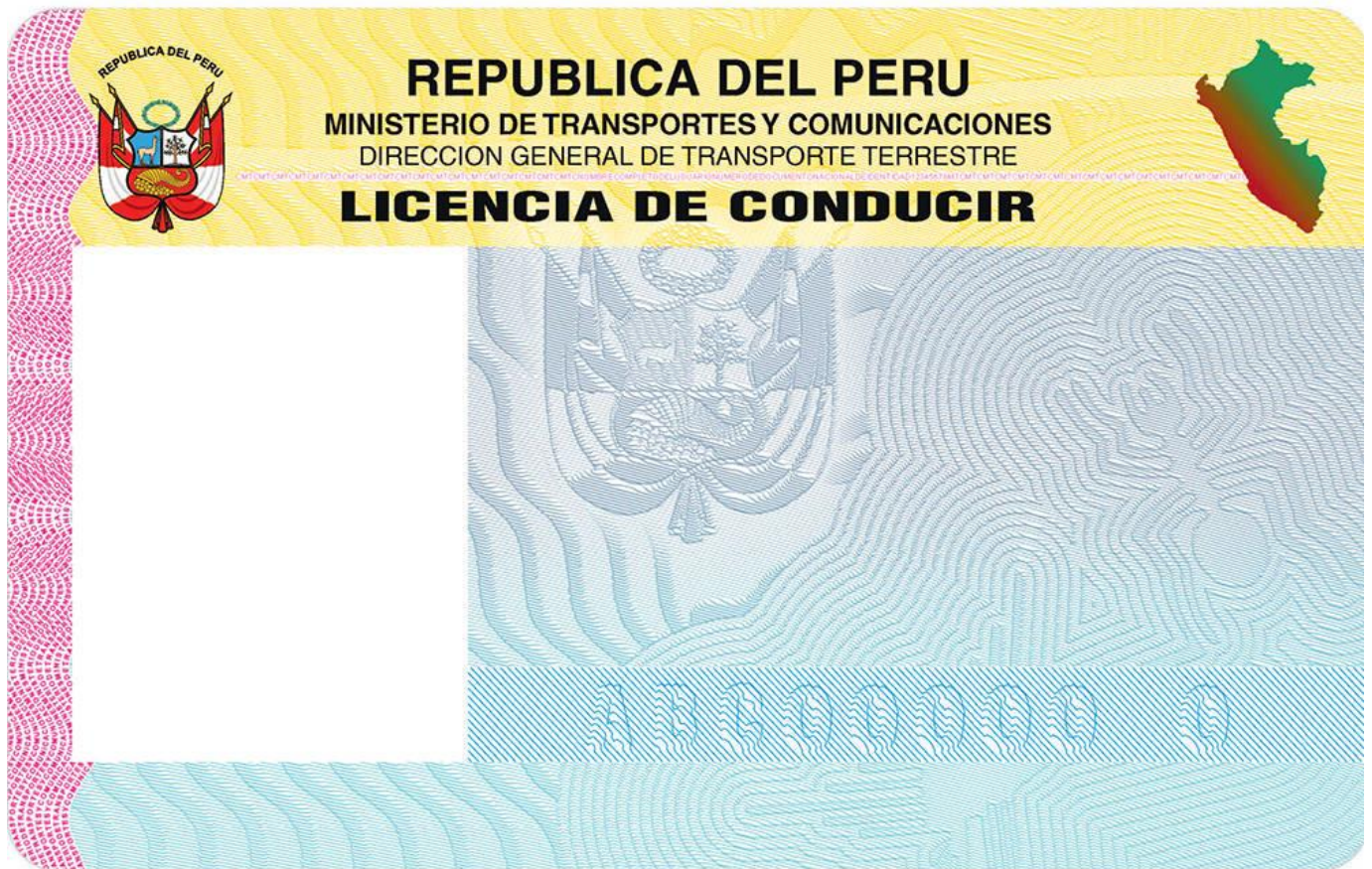
Anverso Clase B



CLASE B

			
Autos, utilitarios, camionetas y casas rodantes hasta 3.500 kg de peso total.	Automóviles y camionetas hasta 3.500 kg y acoplado hasta 750 kg.	Camiones y casas rodantes de más de 3.500 kg y los comprendidos en la clase B1.	Transporte de pasajeros hasta 8 plazas y los comprendidos en la clase B1.

Anverso Clase C



CLASE C



Transporte de pasajeros hasta 8 plazas y los comprendidos en la clase B1.



Transporte de pasajeros de más 8 plazas y los comprendidos en la clase B, C y D1.



Servicios de urgencia, emergencia y similares.

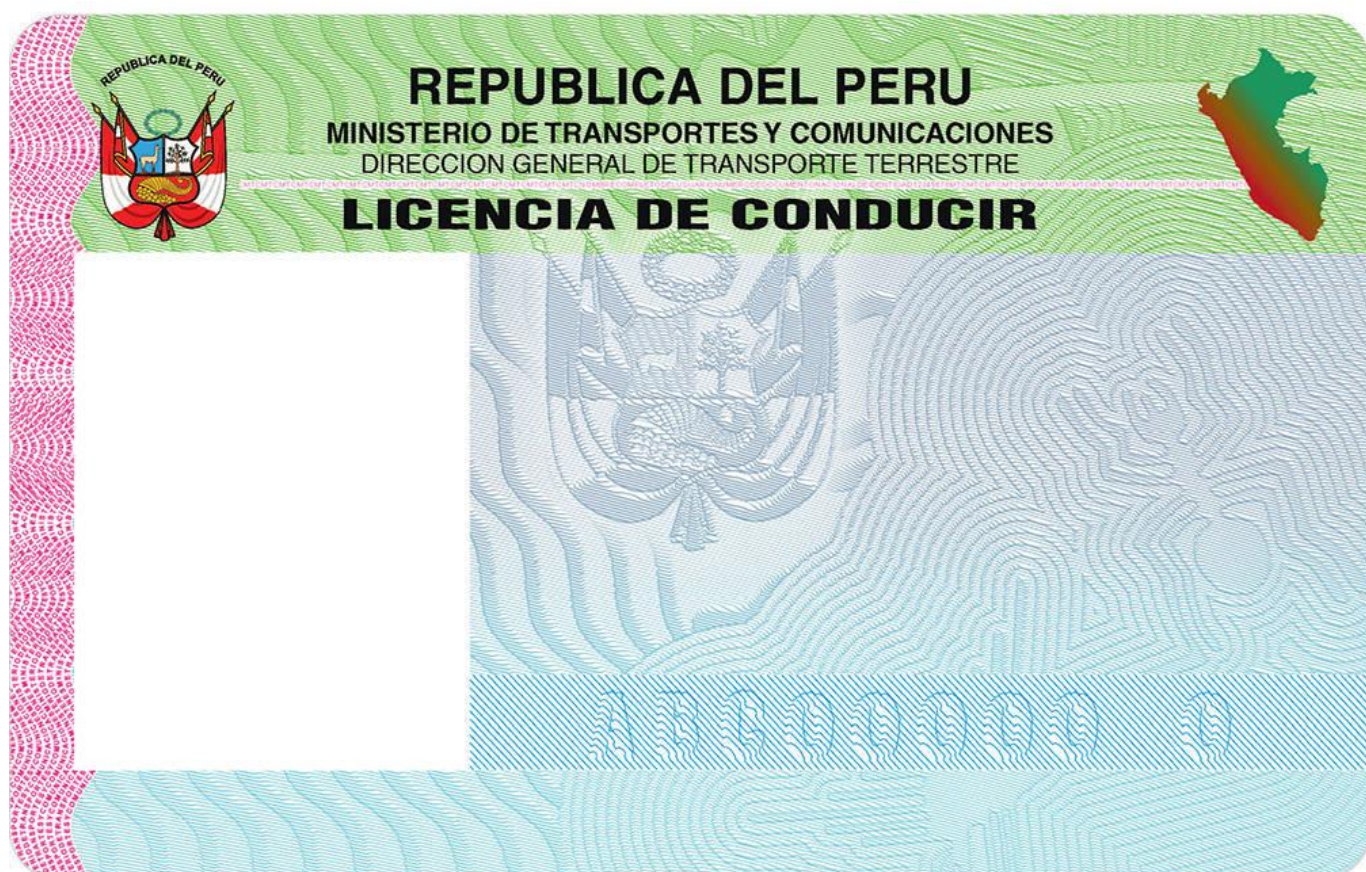


Camiones Articulados y/o con acoplado y los comprendidos en las clases B y C;



Vehículos afectados al transporte de cargas peligrosas;

Anverso Clase D



CLASE D



Maquinaria especial
no agrícola.



Incluye las clases B
y profesionales.
Casos de
discapacidad,
con la descripción
adecuada del titular.



Tractores agrícolas.



Maquinaria especial
agrícola.

Reverso Digital Común



El Reverso Digital es sólo para mostrar la idea que se quiere transmitir, la Licencia de Conducir Digital, no se ha desarrollado en un “Software Numismático” por razones de costo, y porque además a diferencia de la foto del Anverso no hemos podido dejar los espacios blancos de impresión porque no tenemos el tamaño del Código de Seguridad Offline-Online ni del Código de Color (Human Readable).

Del primero sabemos que es cuadrado aunque no sabemos el tamaño, del segundo no sabemos si será cuadrado o rectangular ya que la elección será el resultado de una selección posterior.

La selección de estas medidas de seguridad se hará siguiendo estrictamente las Buenas Prácticas de Jurisprudencia Documentaria reflejadas en el caso Visa Schengen vs Kinegram y las políticas y estrategias generales de Sun Tzu, Adam Smith, John Locke, Adam Galinsky, Alejandro Hernández.

El objetivo es siempre el mismo y muy claro, el máximo de seguridad para la Nueva Licencia de Conducir Digital Biométrica, a un precio justo

En resumen: en este estudio hemos hecho los cambios necesarios para aumentar considerablemente la Seguridad Física de la Licencia de Conducir de Perú, modernizándola, dejando atrás 25 años de hacer lo mismo, y sin aumentar su costo.

Lo hemos hecho siguiendo la Matriz de Eficiencia CADDSS para obtener el máximo de seguridad al menor costo.

Se ha cambiado el diseño que se repitió millones de veces por más de 25 años; por un diseño más moderno, que transmite su carácter Digital, que es más seguro y que destaca las Clases por tipo de vehículo.

La Seguridad Física de la Nueva Licencia de Conducir Digital Biométrica será una pesadilla para Azángaro por muchos años en el futuro.

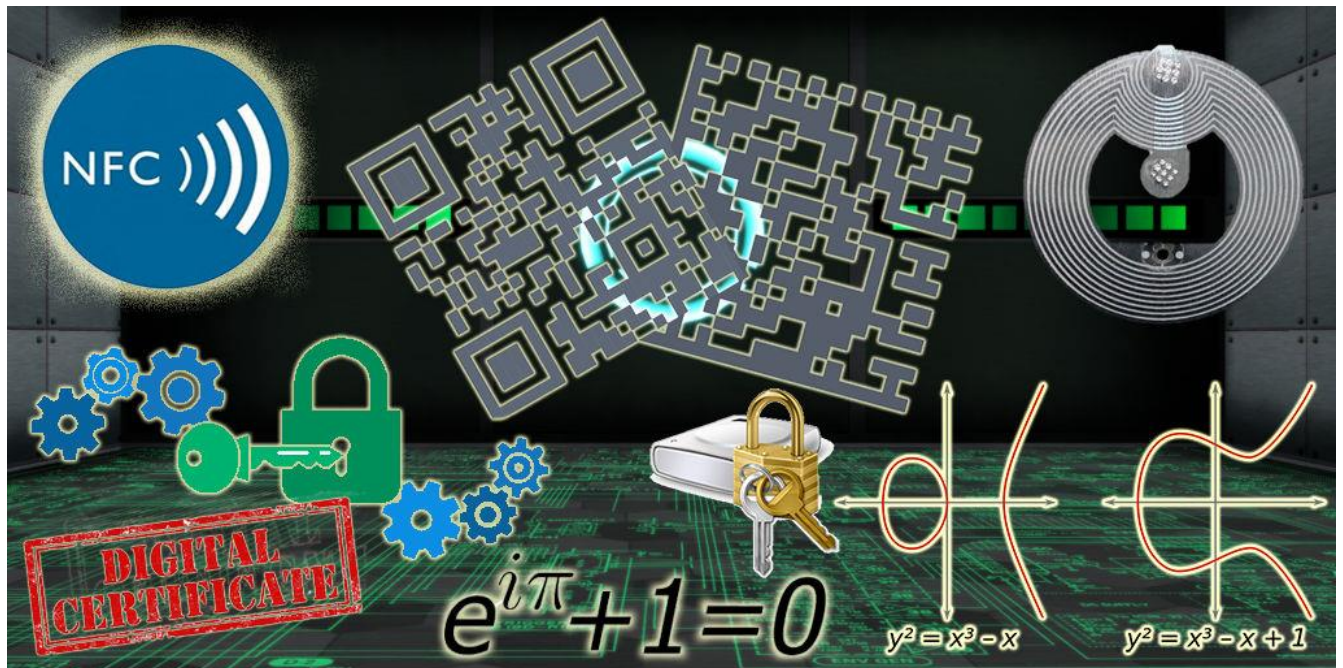
Pero esto es sólo una parte de la seguridad dentro del sistema MLDS, se le agregará la Seguridad Lógica y Biométrica con 7 niveles más de seguridad.

Será una fortaleza inexpugnable de múltiples muros, uno detrás de otro, muros físicos y muros lógicos, será como atravesar un juego de video de n dimensiones, nadie llegará al final del juego al menos en los próximos 25 años

Y para los muchachos de Azángaro, aunque no lo hayan leído será como las infinitas puertas de “El Proceso” de Franz Kafka, cada puerta, (MLDS), detrás de cada puerta, (MLDS), tendrá un guardián más fuerte y poderoso.



Y al final, con el advenimiento de los años, cuando el enrolamiento biométrico haya terminado y el despliegue de equipos sea generalizado, el Brevete no se podrá falsificar, como no se puede falsificar un hombre, porque miraremos al hombre y al Brevete, al Brevete y al hombre, pero no podremos distinguirlos porque ya serán lo mismo. (Desmaterialización)



SEGURIDAD LÓGICA



Simbolo que indica Chip NFC ICAO-OACI

After AddRoundKey	aa	61	82	68
	8f	dd	d2	32
	5f	e3	4a	46
	03	ef	d2	9a
	48	67	4d	d6
	6c	1d	e3	5f
	4e	9d	b1	58
	ee	0d	38	e7
	e0	c8	d9	85
	92	63	b1	b8
	7f	63	35	be
	e8	c0	50	01
	f1	c1	7c	5d
	00	92	c8	b5
	6f	4c	8b	d5
	55	ef	32	0c
	26	3d	e8	fd
	0e	41	64	d2
	2e	b7	72	8b
	17	7d	a9	25

Seguridad Lógica de la Licencia de Conducir

Como se ha definido en la sección general la Seguridad Lógica, también llamada Informática o Mecanizada, consiste en agregar al documento datos codificados en un soporte óptico o electromagnético

La Seguridad Lógica, representada en el documento por un chip o un código óptico de seguridad, está basada en algoritmos matemáticos, su verificación es objetiva y sólo admite 2 respuestas, verdadero o 1 y falso o 0, no hay lugar para la subjetividad o la interpretación del agente verificador, cómo consecuencia no se necesita de un inspector experto para obtener resultados confiables y puede incluir dispositivos de control anti corrupción.

Vamos a presentar en esta parte del estudio 7 medidas de Seguridad Lógica y 2 medidas mixtas Lógicas y Biométricas

1. Código de Integridad Digital

Es un código único de 11 dígitos, generado para cada documento, que permite verificar la integridad de sus datos. Se verifica Offline-Online.

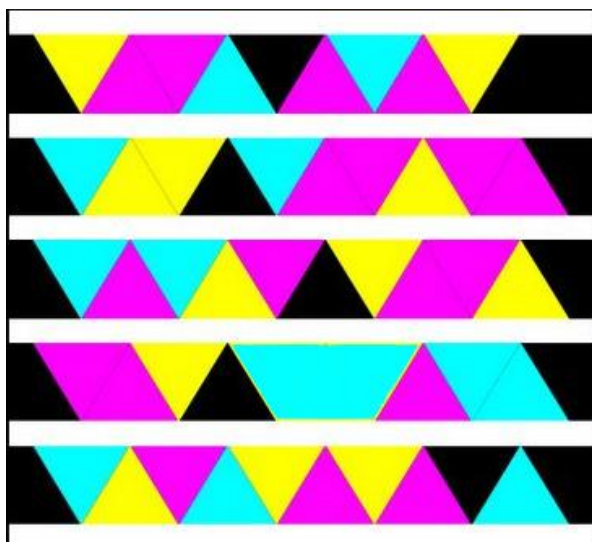
fy0YGW9gDvM

El código se imprime en el documento usando técnicas de Seguridad Física Numismática, al leer el Código Óptico de Seguridad, o el Chip NFC del documento, con un Smartphone aparece un código en pantalla, si el código que presenta el Smartphone y el impreso en el documento son iguales el documento es original

Verificación Offline-Online

Posibilidad de falsificación 0%

2. Código de Color HR (Human Readable)



Es un código único anti falsificación del documento, es la huella dactilar del documento, es una sumatoria de la data del documento que se transforma en un código único para cada documento que se imprime y es reconocible a simple vista

Al leer con un Smartphone el Código Óptico de Seguridad del Documento, el Código Esteganográfico, o el Chip si lo hubiera, aparece en la pantalla del Smartphone, junto con los demás datos el código de colores.

Se compara la imagen en pantalla con el código impreso en el documento., si son iguales es porque el documento es original.

Verificación Online

Posibilidad de Falsificación 0%

3. Código Esteganográfico

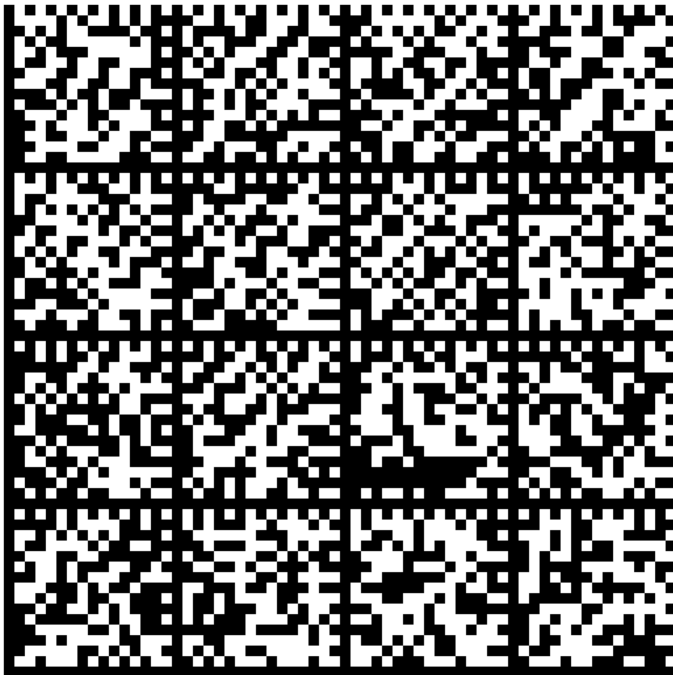


Es un código de seguridad "invisible", y por lo tanto absolutamente infalsificable, se imprime en el Anverso del documento usando técnicas esteganográficas junto con la foto y los datos, a través de su lectura con un Smartphone y el software de descryptación correspondiente muestra todos los datos del tarjeta habiente (Alfanumérico, Foto, Record del Conductor)

Verificación Online y Parcial Offline (sólo autenticación)

Posibilidad de Falsificación 0%

4. Código de Seguridad 2D Encriptado



Es un código bidimensional encriptado que se lee con un Smartphone y el software de descryptación, se verifica a través de un Certificado Digital y muestra Offline todos los datos del conductor y su foto.

Tiene la capacidad de conectarse Online y mostrar el Record del Conductor

Verificación Offline-Online

Posibilidad de Falsificación 0%

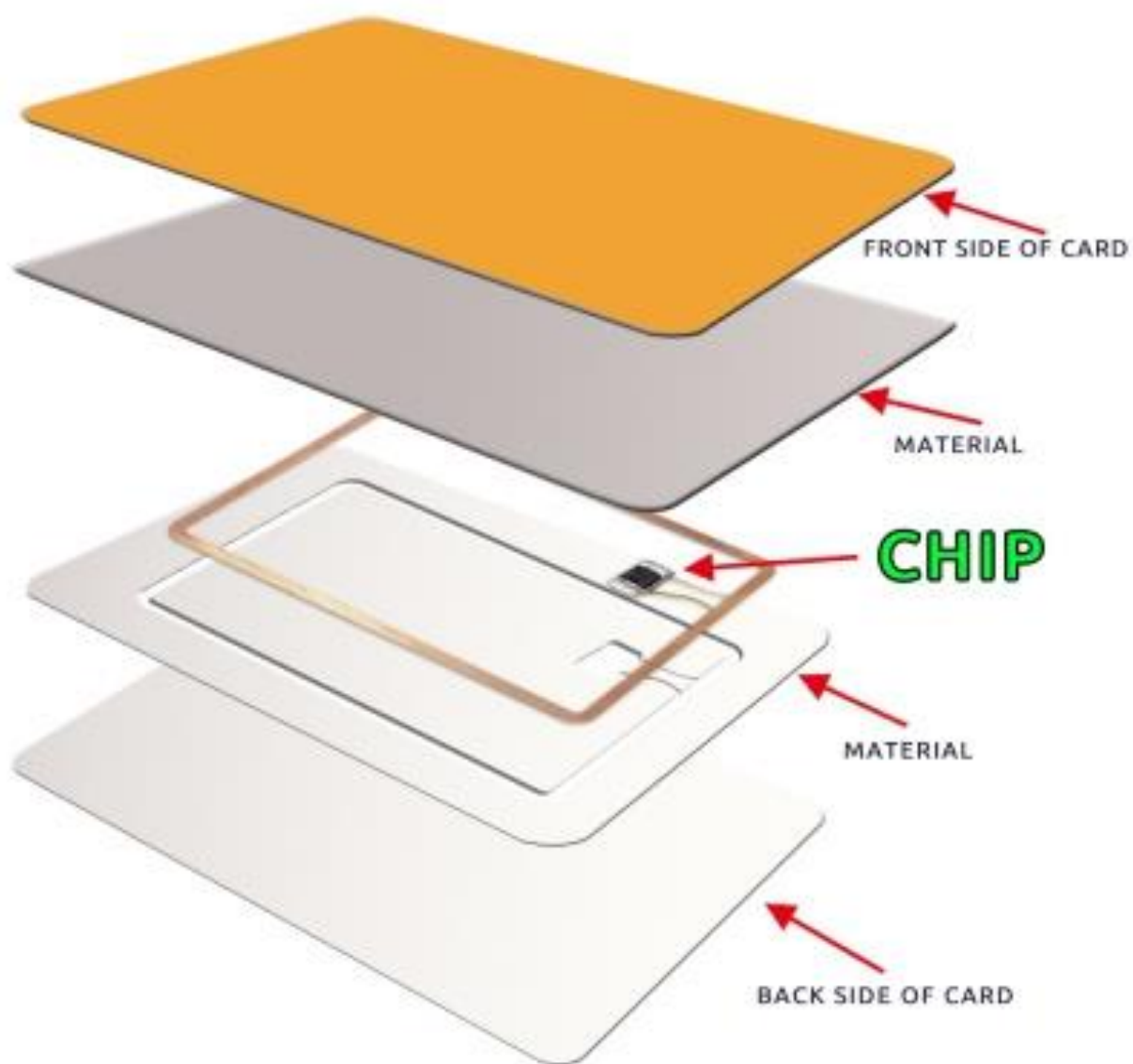
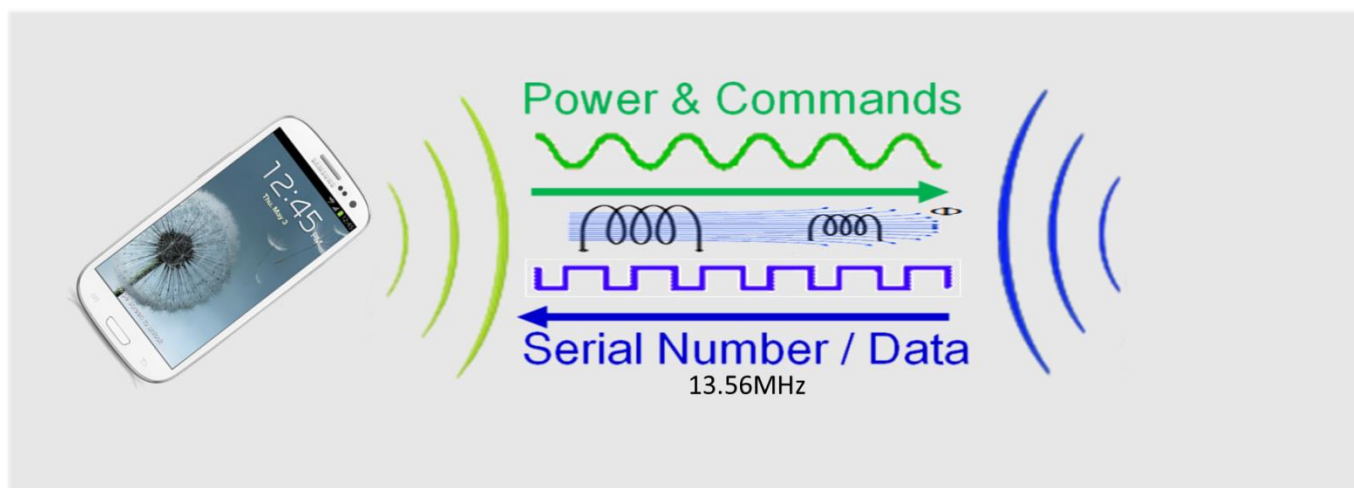
5. Chip Encriptado Inalámbrico NFC

Es un dispositivo electrónico de lectura por proximidad que contiene la información del conductor, (Datos Alfanuméricos y Foto), que se lee con un Smartphone con NFC y un software especial que lee y descrypta los datos.

Tiene la capacidad de conectarse Online al Record del Conductor.

Está basado basado en el estándar ISO/IEC 14443-4 (Generación 4) que es el de elección para documentos de identidad de Alta Seguridad

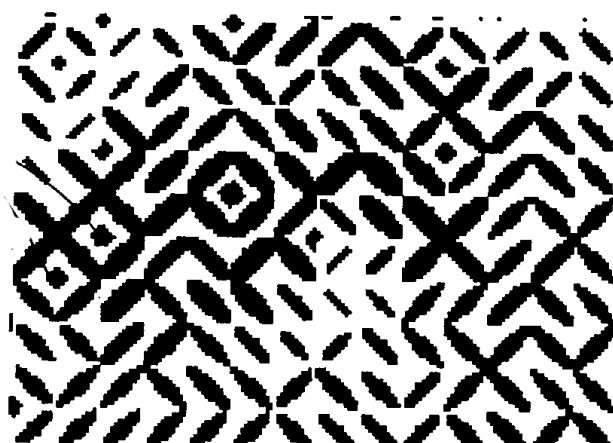
Es el sistema del actual de todos los Pasaportes Electrónicos y de los nuevos DNI Electrónicos de España y Uruguay



Verificación Offline-Online

Posibilidad de Falsificación 0%

6. Código para verificación de Foto



Es un código que usa un algoritmo de encriptación cuya llave de acceso está en la imagen fotográfica. Cuando se observa la fotografía del carné con un Smartphone y el software de descryptación lee el código, si la llave privada generada por la foto y la llave pública del código coincide, la foto es autenticada.

Este sistema permite confirmar que la foto observada en el carné es la foto originalmente impresa en ese carné, es imposible sustituir o modificar la foto ya que la foto y el código son una sola entidad

Verificación Offline-Online

Puede incluir Biometría

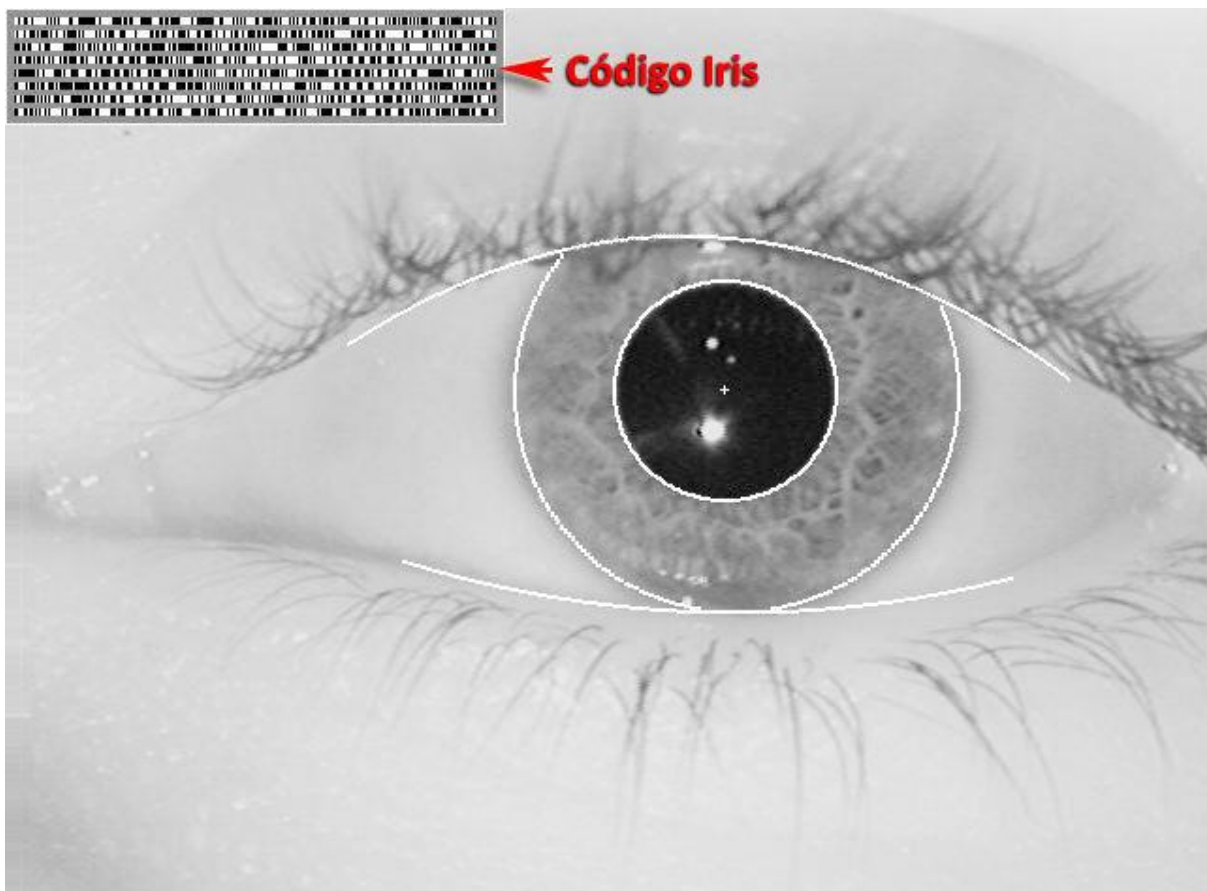
Posibilidad de Falsificación 0%

7. Biometría del Iris

Es el “séptimo sello” para los falsificadores, si las 6 medidas Anteriores de Seguridad Lógica (MLDS) son una barrera impenetrable para cualquier falsificador del mundo, la biometría pone el clavo final en su viaje al más allá.

Hay muchas biometrías a considerar, Huellas Dactilares, Reconocimiento Facial, Estructura Venosa de la Mano, Reconocimiento de Iris, Perfil de ADN.

De todas ellas elegimos RI (Riconoscimento dell'Iride) por ser la más exacta, rápida, y verificable con dispositivos móviles de costo razonable



El sistema extrae el código único del Iris y se usa directamente para el reconocimiento, la lectura del Código Iris nos muestra todos los datos del conductor, datos personales alfanuméricos, foto y Record de Conductor

Verificación Online y Offline si se usa una computadora Windows con Base de Datos

Desmaterialización: No se necesita la Licencia de conducir con conexión a la Base de Datos

Posibilidad de Falsificación 0%

El sistema de verificación usa un Smartphone con luz infrarroja y lector infrarrojo, se conecta Online a la base de Datos central o por Bluetooth a una Base de Datos local, por ejemplo la computadora de un patrullero, presenta todos los datos Alfanuméricos del conductor, su foto y su récord de conductor





360°

**Cadena de
Custodia**

Cadena de Custodia de la Licencia de Conducir

Ya hemos analizado el concepto fundamental de Cadena de Custodia y su relación transversal con la Seguridad Documentaria en sus componentes de Seguridad Física, Seguridad Lógica y Seguridad Informática.

Ahora veremos un resumen para el caso específico de la Nueva Licencia de Conducir Digital en el Perú

Cadena de Custodia Seguridad Física

En nuestra propuesta seguimos el estándar mundial de Impresión Centralizada para los documentos de Alta Seguridad en este caso toda la Cadena de Custodia de la Seguridad Física depende de una sola Empresa Integradora, físicamente está ubicada en un solo lugar, y hay un solo responsable, nuestro paradigma y ejemplo es el **BEP (Bureau of Engraving and Printing)**

1. Custodia de Insumos

Trata de los insumos antes de su integración en el documento final, la empresa no sólo debe cumplir con las referencias anteriores de Protección del Edificio y sus cercanías, Vigilancia Perimétrica, Sistemas de Alarma, Cámaras de Vigilancia Diurna y Nocturna, Vigilantes Armados, Puertas Dobles, Sistema de Incendios, Cámaras en todas la zonas de producción, Bóveda de Seguridad, Selección de personal con múltiples filtros de control sino que los Protocolos de Seguridad se deben extender a la llegada de los insumos a la planta desde otra planta productora local o la aduana en vehículos blindados



Con un Sistema de seguridad con estándares internacionales y un solo responsable podemos asegurar que nunca más habrá un robo de hologramas.

2. Custodia de la Licencia de Conducir Impresa

La Empresa Integradora deberá tener un Sistema de Cadena de Custodia desde la Planta de Producción hasta los puntos de entrega en todo el territorio nacional siguiendo los estándares internacionales. Estos sistemas permiten la trazabilidad del producto hasta la llegada al punto de destino con sistemas de empaque especiales, códigos de barras y sistemas informáticos en línea. También se puede optar por un sistema directo de entrega a domicilio pagando el costo correspondiente. Este debería ser el sistema de elección en el futuro ya que permite verificar el domicilio del poseedor de la Licencia de Conducir y se tiene la confirmación de recepción en ese domicilio.

El sistema debe incluir la eliminación inmediata de un grupo de licencias de conducir en caso la mismas se perdieran por accidente para así poder autorizar una nueva impresión.

Las tecnologías de Seguridad de la Nueva Licencia de Conducir Digital Biométrica hacen completamente inútil una licencia perdida ya que toda la licencia es absolutamente personalizada para una sola persona, haciendo imposible su uso aún para un hermano gemelo (Código de Integridad, Huella Dactilar, Iris).

Cadena de Custodia Seguridad Informática y Lógica

Consiste en la protección de los datos que se grabarán en la Licencias de Conducir en forma Física o Lógica, esto se ha analizado en la sección de Seguridad Informática

The background is a vibrant blue gradient. It features a pattern of binary code (0s and 1s) in a lighter blue shade, scattered across the surface. Overlaid on this is a grid of intersecting lines in two shades of blue, creating a spherical or globe-like effect. The lines are thicker and more prominent, forming a wireframe structure.

Seguridad Informática

Seguridad Informática para la Licencia de Conducir

No es el ámbito de esta consultoría un análisis a nivel de ingeniería de detalle del Sistema Informático, pero hemos creado una Licencia de Conducir Absolutamente Infalsificable y es nuestra obligación proponer una tecnología de avanzada que impida la generación y emisión de Licencias de Conducir verdaderas con datos falsos. Ello se logra a través del uso de un Workflow basado en Certificados Digitales, Firma Digital, Encriptación y Biometría.

EL MTC no puede impedir que alguien a cambio de una coima introduzca datos falsos en el sistema, pero debemos impedir que estos datos sean anónimos, que puedan ser descubiertos y denunciados, debemos crear sistemas de seguridad que sea disuasivo y castigue al mal funcionario.

Esto es también un problema legal que el MTC debe analizar con el Poder Ejecutivo y el Congreso

Tampoco hasta ahora el MTC ha podido impedir que “manos mágicas”, como lo viene haciendo hace más de 10 años modifique temporalmente la Base de Datos Oracle para emitir una licencia a un chofer que está impedido por faltas graves.

La Seguridad Informática tiene ciertos estándares como el ISO/IEC 27001:2013 y el ISO/IEC 27002:2013, no podemos esperar a que el MTC y todas las regiones cumplan con este estándar auditado para tener una Licencia de Conducir segura. Lo importante es ver cómo funciona el mundo real y aplicar partes de estos estándares a las zonas críticas.

El esperar la perfección siempre ha sido un buen pretexto para no hacer nada

También es cierto que muchas medidas de seguridad que se aplicarían en estos procesos se harán usando productos que cumplen estos estándares o son procesos y empresas acreditados por INDECOPI

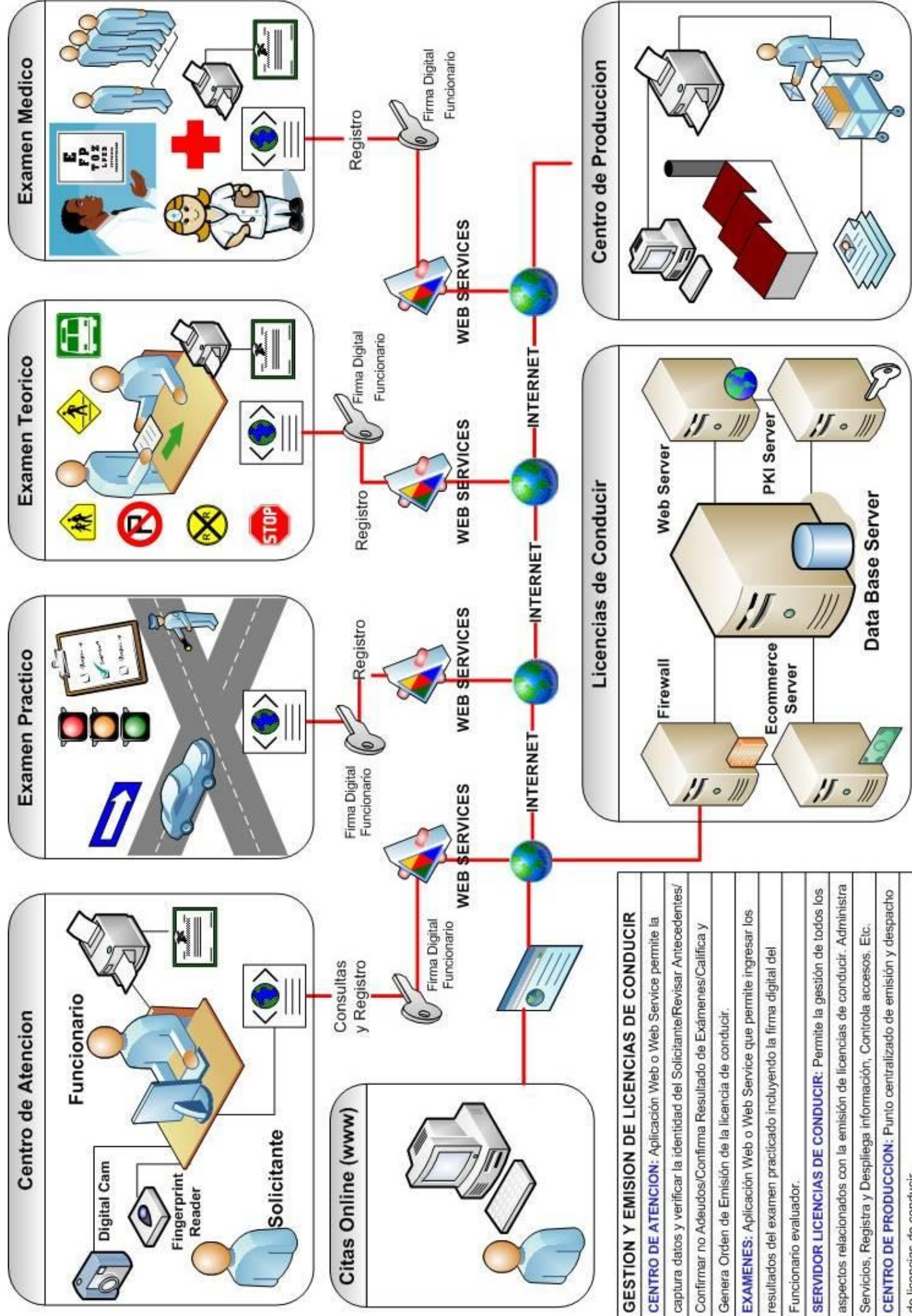
Debemos entonces focalizarnos donde están los problemas, que no son los mismos que tiene una entidad bancaria o financiera que aplica los ISO/IEC 27001:2013 y el ISO/IEC 27002:2013.

Más de 20 años de estudios forenses nos muestran que el principal problema del MTC y las regiones no es ser atacado por hackers, sino el trabajo interno, y es en esto donde debemos enfocarnos primero y en pocos meses, 2 o 3 resolver el problema.

Podemos ver 2 problemas claros y principales:

- 1. Introducción de Datos Falsos en los puntos de Emisión**
- 2. Modificación de la Base de Datos por trabajo interno**

Para el punto uno ponemos como ejemplo el sistema completo desarrollado en Buenos Aires y un boceto inicial de un sistema desarrollado local



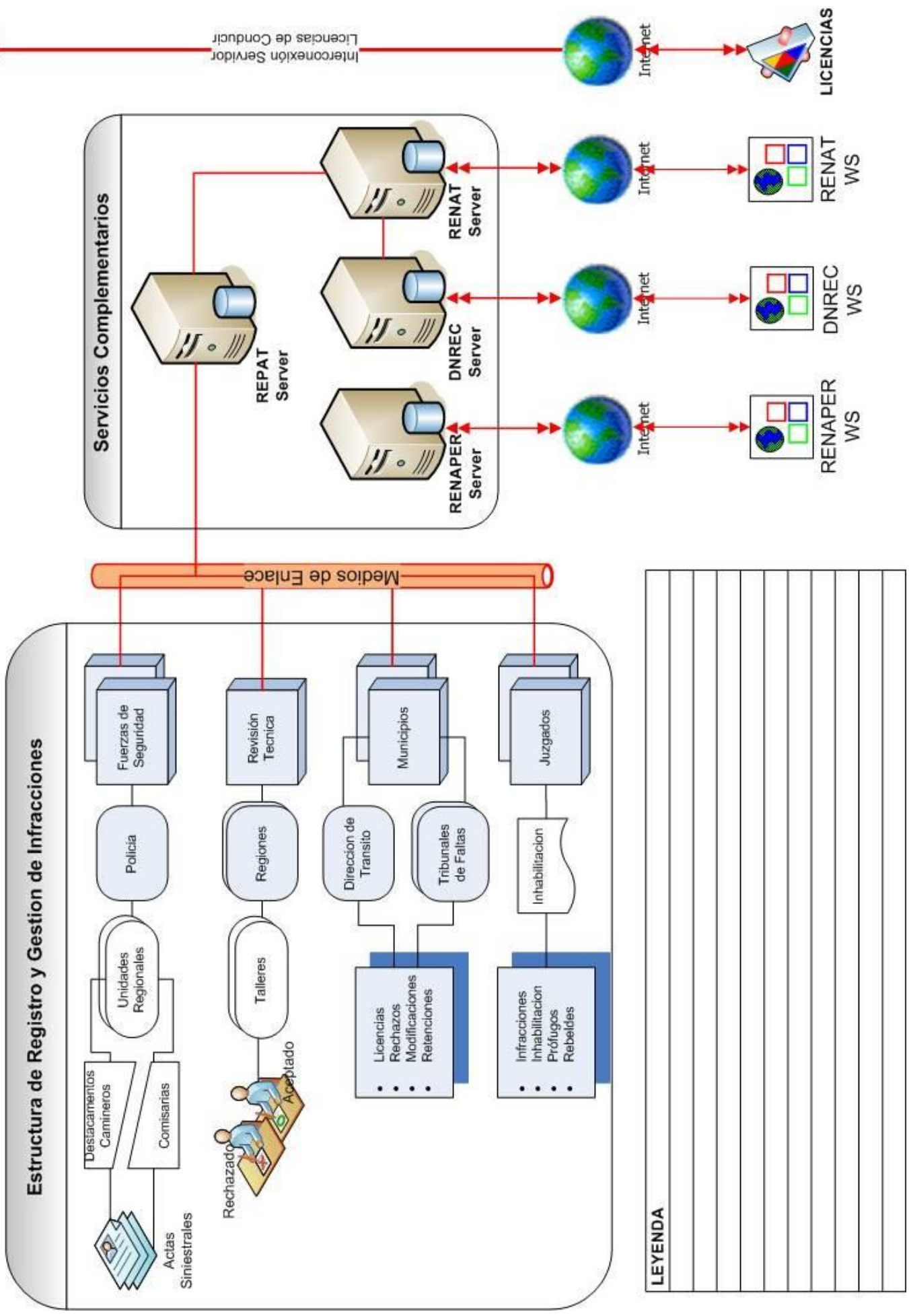
GESTION Y EMISION DE LICENCIAS DE CONDUCIR

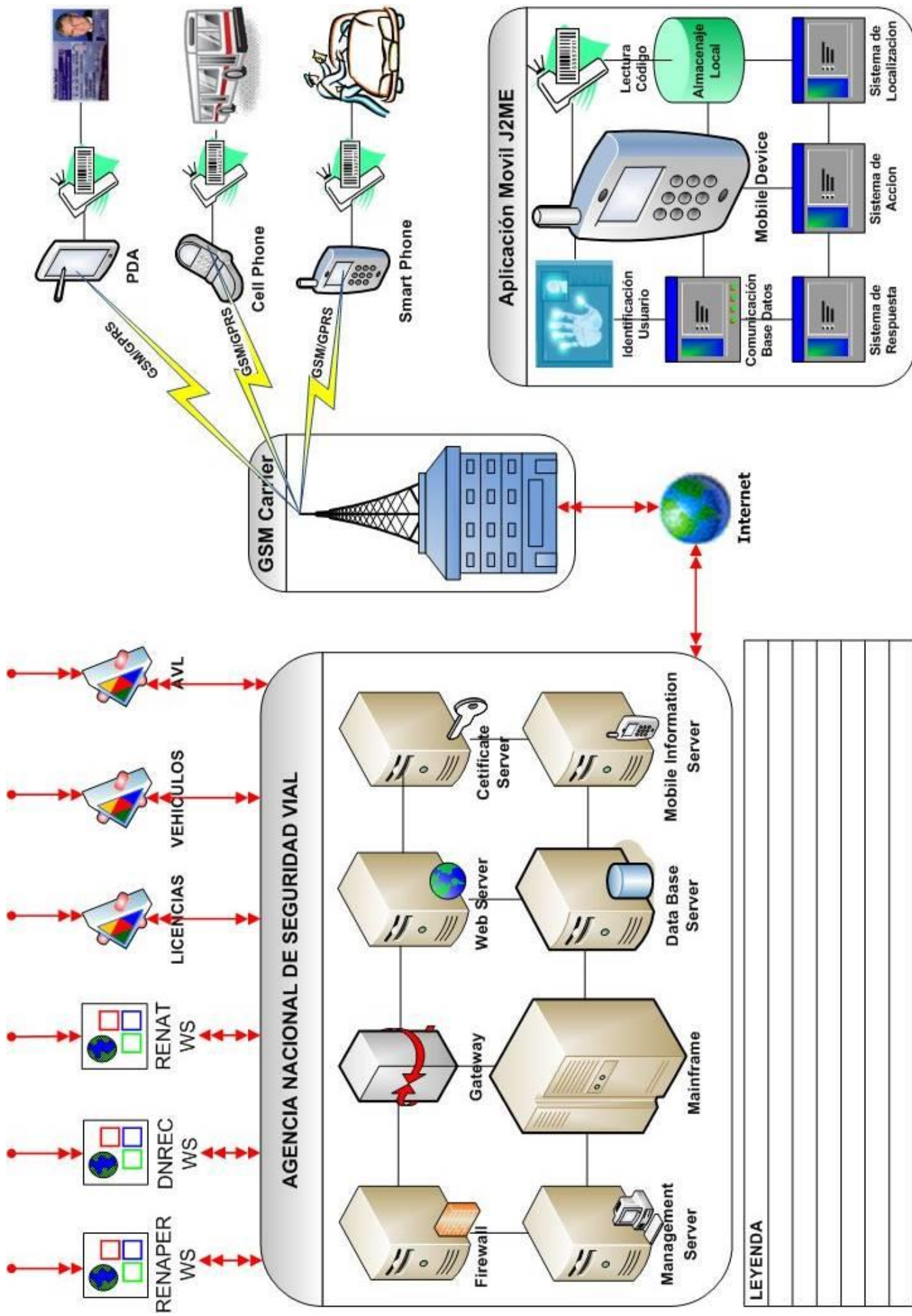
CENTRO DE ATENCION: Aplicación Web o Web Service permite la captura datos y verificar la identidad del Solicitante/Revisar Antecedentes/ Confirmar no Adeudos/Confirma Resultado de Exámenes/Califica y Genera Orden de Emisión de la licencia de conducir.

EXAMENES: Aplicación Web o Web Service que permite ingresar los resultados del examen practicado incluyendo la firma digital del Funcionario evaluador.

SERVIDOR LICENCIAS DE CONDUCIR: Permite la gestión de todos los aspectos relacionados con la emisión de licencias de conducir. Administra Servicios, Registra y Despliega información, Controla accesos. Etc.

CENTRO DE PRODUCCION: Punto centralizado de emisión y despacho de licencias de conducir.





Estos diagramas nos muestran cómo funciona un sistema completo de Emisión y Control, desde la solicitud del ciudadano a la emisión e impresión, las etapas principales son las siguientes:

- 1. Solicitud de Cita, que puede ser personal u online, (pagalo.pe) del Banco de la Nación y otros bancos afiliados al sistema.**
- 2. Centro de Atención y Enrolamiento (Lima y Regiones)**
- 3. Examen Práctico (Lima y Regiones)**
- 4. Examen Teórico (Lima y Regiones)**
- 5. Sistemas y Base de Datos (MTC Lima)**
- 6. Centro de Producción (Imprenta Lima)**

El sistema completo deberá funcionar dentro del ISO/IEC 27001:2013 y el ISO/IEC 27002:2013, pero desde el principio, dentro de unos pocos meses, podrá funcionar usando Certificados Digitales acreditados por INDECOPI y Biometría proporcionada por RENIEC, este sistema garantizaría la integridad de todos los datos, identificando además al autor de los mismos.

Por ejemplo si fuera un Examen Médico hay 2 responsables, la entidad o clínica que toma el examen y cobra por el mismo y el médico que toma el examen en la clínica.

Por ejemplo tomemos el caso de una de las entidades médicas que toman los exámenes para las Licencias de Conducir, digamos SERVIMEDIC, para entrar al sistema deberá tener un Certificado Digital de Persona Jurídica y este tendrá todos los ISO necesarios ya que será generado por una EC (Entidad de Certificación) acreditada por INDECOPI y será registrado por una ER (Entidad de Registro) acreditada por INDECOPI.

La entidad a su vez generará Certificados Digitales para los médicos que trabajan en la entidad que a su vez deberán estar acreditados en el Colegio Médico del Perú.

Cuando una persona pasa el examen médico su habilitación se firma con un Certificado Digital y Biometría, el Certificado Digital es de SERVIMEDIC, de un médico, (avalado por el Colegio Médico del Perú) y es un médico de SERVIMEDIC.

Si la información proporcionada por el médico resulta falsa el médico que la firma es responsable, también lo es solidariamente la entidad, en este caso SERVIMEDIC de cualquier sanción que se pueda aplicar.

Si además el título de médico resulta falso el Colegio Médico del Perú es responsable ya que un Certificado Digital de un médico no puede ser emitido sin la autorización del Colegio Médico.

Lo mismo sucede con todas las demás etapas y entidades, examen teórico, examen práctico, etc., siempre habrá una entidad y una persona responsables indubitadamente ya que la Firma Digital no se puede negar ni requiere pericia forense

Con este sistema no podemos garantizar que un funcionario de una empresa no va a mentir, pero podemos garantizar que la mentira tendrá consecuencias para la persona y para la persona jurídica.

¿Cuáles son estas consecuencias?

Está en manos del MTC determinar cuáles son estas consecuencias, y sus costos para funcionarios y entidades.

Por supuesto que un sistema completo como el mostrado para Buenos Aires incluye un sistema de Gestión de Infracciones y el Sistema de Control de las Licencia de Conducir.

Sistema que debe ser desplegado desde un principio, aunque en los primeros meses sean pocos los nuevos documentos, podemos considerarlo una “marcha blanca” para entrenamiento de los policías y los inspectores.

Para que el sistema sea desplegado se deben dar cursos a la policía y a los inspectores en la instalación y uso de las diferentes App en Android y Windows.

Justamente esta política se deduce del análisis forense del fracaso de los sistema anteriores, que nos muestran las causas del fracaso, veamos un caso.

Hasta el año 2007 hubo una nueva Licencia de Conducir con Seguridad Lógica y se emitieron 280,000 licencias.

El sistema de autenticación era Offline, la Base de Datos estaba incluida en el sistema portátil de lectura y era actualizada todos los días, la fortaleza del sistema es que al ser Offline podía funcionar en las zonas más alejadas del Perú.

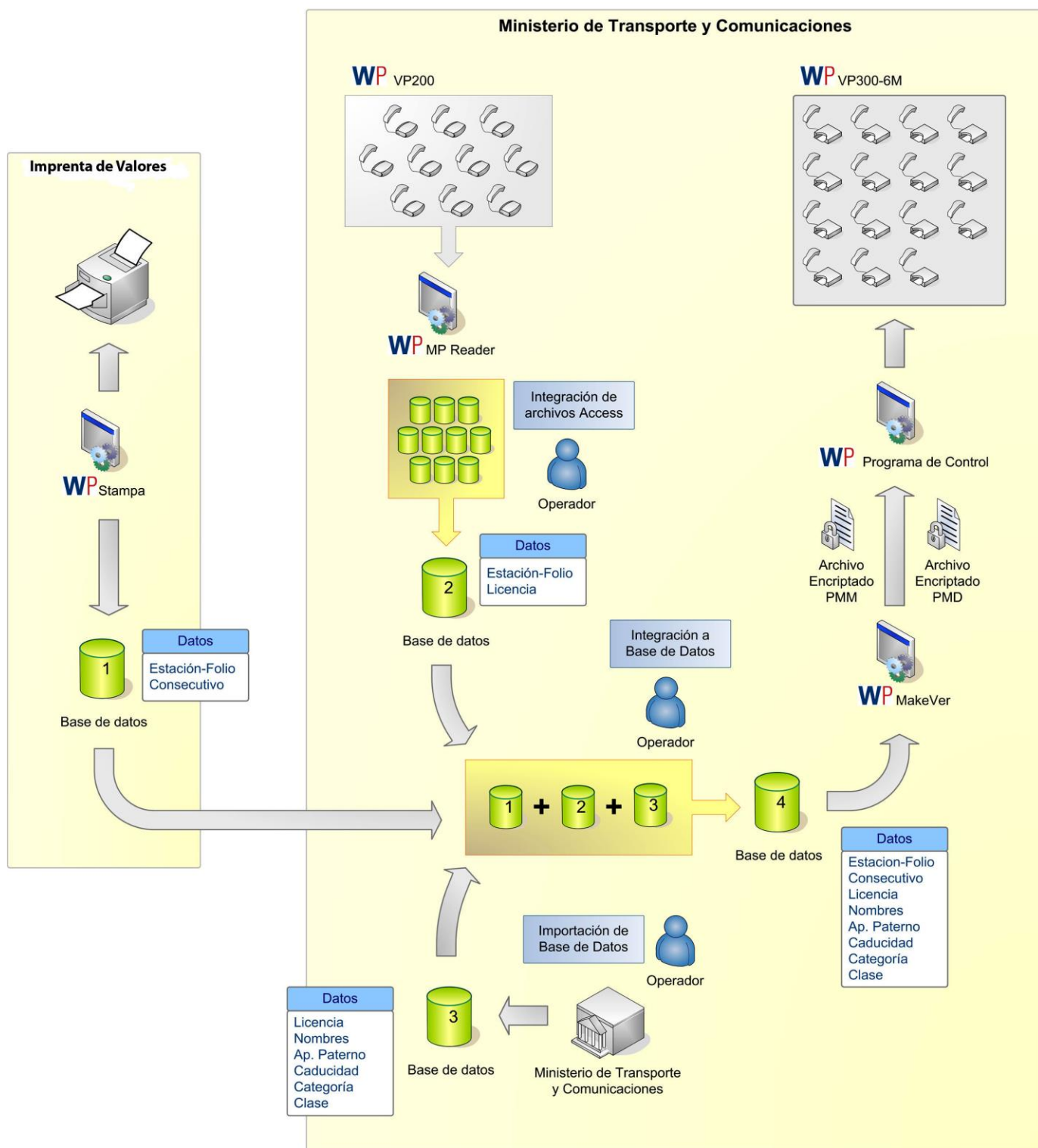
La desventaja fue el costo, varios miles de dólares por equipo, se entregaron 50 equipos que “desaparecieron” en el MTC.

Nunca fueron entregados a la policía y tampoco el MTC dio cursos a la policía para su uso, fue muy fácil para la mafia eliminar el sistema.

Los ingenieros norteamericanos que instalaron el sistema conocían de la manipulación de la Base de Datos Oracle y por ello crearon una Base de Datos de Control en SQL Server Encriptada que no podía ser manipulada

No contaron con el hecho extremo, que la mafia eliminaría no sólo el servidor SQL, sino el sistema completo, lo ilustramos como experiencia a tomar en cuenta en 2 páginas

WernerPegasus VP1000			
Procesador MIPS 200 Mhz 64 Mb. FlashROM 64 Mb. SDRAM Pantalla LCD 64K colores Resolución 240 x 320 Pantalla Táctil 3.5" QVGA Batería Lithium 800mAh Bat. Extendida 1200mAh Bocina y Micrófono	Impresora 	Terminal 	COAS 
Especificación	SmartCards 	GPRS 	RFID 
FingerPrint 	Impresora móvil Bluetooth	Terminal de Datos	Lector de SmartCards



Como dijo Jorge Santayana, el filósofo madrileño nacionalizado estadounidense:

“Aquellos que no pueden aprender de su pasado están condenados a repetirlo”

Por eso este informe incluye las experiencias del pasado en el desarrollo de la **Nueva Licencia Digital Biométrica del siglo XXI**, para demostrar que hemos aprendido

Con esto terminamos el análisis del primer punto de alteración de datos

1. Introducción de Datos Falsos en los puntos de Emisión

Pasemos analizar el segundo punto

2. Modificación de la Base de Datos por trabajo interno

Nuevamente si cumplimos con los principales estándares de Seguridad Informática eventualmente tendremos un sistema acreditado, pero si pensamos en unos 30 puntos en todo el Perú, eso llevará más tiempo del deseable.

Por eso debemos crear un sistema seguro para nuestros fines de garantizar la coherencia e intangibilidad de la Base de Datos de la Licencia de Conducir, para ellos debemos usar las herramientas disponibles y hacerlo en un máximo de 3 meses.

La problemática encontrada en el MTC es común a la que encontramos en otras Entidades públicas como privadas: la data contenida en las Bases de Datos es corrompida por diversas razones de manera no autorizada.

En efecto muchos de los denominado “ataques” de seguridad informática son realizados por el propio personal de la organización –según estudios generales alrededor del 70%- mientras que los restantes son realizados por hackers ajenos a estas.

En el caso del MTC hasta ahora no hay pruebas de hackers o ataques externos, siendo el 100% trabajos internos, aunque el sistema debe también proteger la base de datos de futuros ataques externos

Los daños que se pueden dar por utilizar data corrupta van desde pérdidas económicas directas hasta daños a la reputación y pérdida de credibilidad e imagen de la institución.

Pero en el caso que nos ocupa es fundamentalmente la alteración de datos de las Licencias de Conducir el mayor blanco de estos ataques en el MTC

Mejor alternativa de solución

Esta es la que toma en cuenta como factores tanto los aspectos técnicos de la ingeniería como los aspectos legales de su gestión y el valor probatorio en el marco de la Infraestructura Oficial de Firma Electrónica.

En efecto la solución contempla la provisión de librerías de software de **Firma Digital** acreditados de **Bases de Datos integradas** a estas según las reglas de negocio de la Entidad, para garantizar la integridad de la base de datos y los reportes que allí se generen de un lado.

Esto garantiza nuestros datos para la Nueva Licencia de Conducir Digital y Biométrica Absolutamente Infalsificable y toda la Base de Datos del MTC

Adicionalmente se ha previsto emplear sistemas de Notificaciones Electrónicas Acreditados con la finalidad de remitir los informes y reportes previos a los Oficiales de Seguridad de la Información o funcionarios autorizados ante eventos presumiblemente no autorizados a fin de que se tomen las acciones respectivas previamente determinadas por la organización.

De esa forma se automatiza y se delegan las responsabilidades por casos de seguridad informática relacionados con la **Base de Datos** con actuaciones enmarcadas en la **Infraestructura Oficial de firma electrónica**, que la otorgan de validez probatoria y jurídica a los documentos y transacciones electrónicas.

Notificación de documentos digitales con valor legal.-

La normativa sobre firmas y certificados digitales regula también las condiciones requeridas para la notificación de documentos digitales con pleno valor legal. Para ello, será indispensable que:

- a. Se emplee un **Sistema de Intermediación Electrónico (SIE)** para el envío de la notificación al domicilio electrónico del destinatario, el mismo que deberá estar acreditado ante el INDECOPI.
- b. El domicilio electrónico del destinatario es el equivalente al domicilio físico del destinatario de una notificación, permitiendo el empleo del sistema de notificación acreditado por el INDECOPI y así tener certeza de la fecha/hora/minuto/segundo en que fue realizada la notificación.

Bases técnicas y legales

- **Ley Nº 27269 - Ley Firmas y Certificados Digitales, Reglamento de la Ley de Firmas y Certificados Digitales aprobado por D. S. Nº 052-2008-PCM (18JUL2008) y normas complementarias.**
- **Normativa sobre Notificaciones Electrónicas: se consigna un cuadro con la evolución normativa sobre notificaciones electrónicas en la Ley No. 27444 – Ley del procedimiento administrativo general**

Librería de protección de la Integridad de Registros de Bases de Datos

Es una librería que permite generar evidencias de integridad y autenticidad para los registros de una base de datos, por ejemplo, mediante el mecanismo de firma digital.

Esta librería permite proteger la integridad de los registros de una base de datos a nivel de cada registro o fila, de tal manera que si se realizara una modificación en algún registro directamente en la base de datos esta modificación podría ser detectada y se podría generar una alerta o notificación apropiada. Mediante el uso de esta librería solo la aplicación legítima conectada a la base de datos es la que podría generar y actualizar los registros en la base de datos.

Adicionalmente, esta librería soporta el proceso de evolución de los registros a proteger (ej. adición o eliminación de columnas), mediante el concepto de versionado de registros soportado por su API de programación y permite la generación de reportes del estado de integridad de una base de datos (ej. con firma digital por parte de un agente automatizado) En relación a las claves utilizadas para la generación de las protecciones de registro, se pueden utilizar claves almacenadas en software en formato PFX (PKCS #12), así como claves almacenadas en módulos de seguridad hardware (HSM) mediante el protocolo PKCS#11.

En relación a la compatibilidad de esta librería, esta es compatible con cualquier motor de base de datos (ej. MS SQL Server, Oracle Database, etc.) y puede ser invocada desde cualquier aplicación basada en .NET o Java.

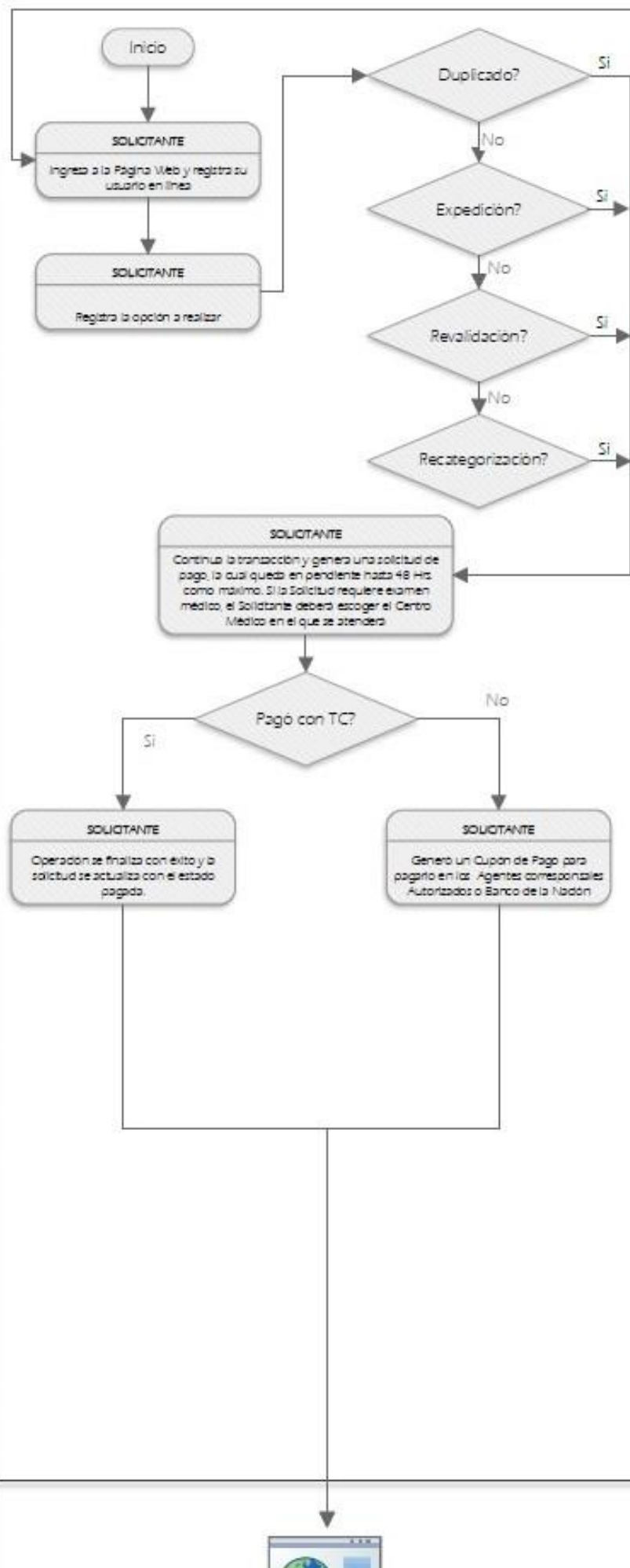
- Medios de almacenamiento de claves soportados:
 - PKCS #12 (software).
 - HSM (Hardware Security Module).
 - Tarjetas inteligentes o tokens criptográficos.
- Plataformas/lenguajes soportados:
 - .NET
 - Java

El modo de licenciamiento del sistema de protección es por servidor o por dispositivo que emplee la librería. A requerimiento específico pueden ser consideradas versiones a ser desarrolladas y personalizadas para otras plataformas o aplicaciones en otros lenguajes de programación. También podrían ser necesarias interfaces de software o componentes de terceras partes (proveedores) que permitan una adecuada optimización del producto.

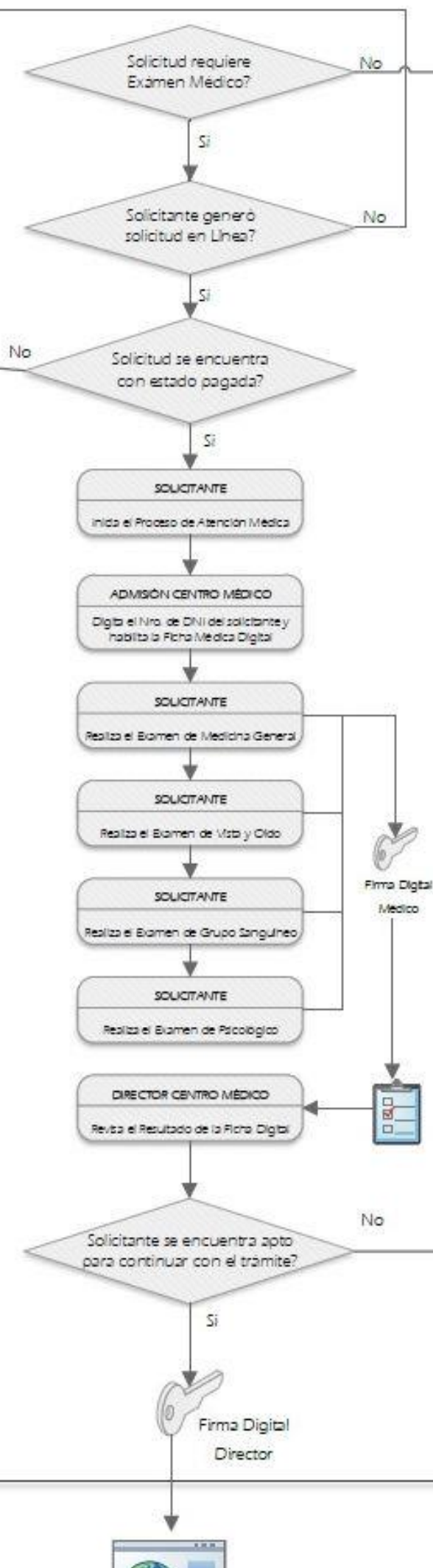
El principal impacto para nuestro fin de la emisión de **la Nueva Licencia de Conducir Digital Biométrica Infalsificable** es que logra básicamente la eliminación de la corrupción en el proceso, la disminución de los costos de transacción, y la eficacia de la seguridad mediante los siguientes:

1. Ahorro de costos (eliminación de uso de papel, notificaciones en papel, etc.).
2. Reducción de tiempo (requerido para la ubicación de las adulteraciones, realización de las diligencias de notificaciones, obtención del resultado de la notificación (cargo) etc.)
3. Eliminación del riesgo de pérdida/destrucción de data de la Bases de Datos.
4. Eliminación de los problemas de rechazo/cuestionamiento de las notificaciones como argumento de "defensa" en procedimientos sancionadores.
5. Garantías de integridad y **Bases de Datos "limpias"**.

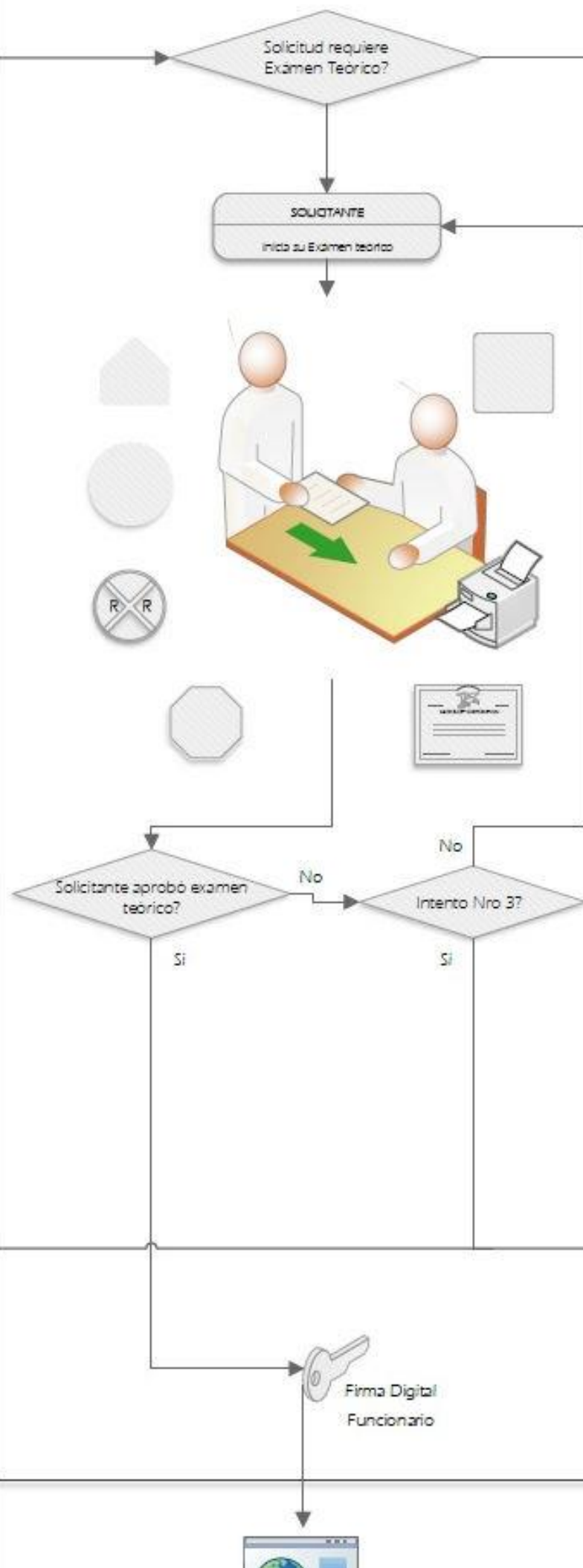
Esto resume un método eficiente para asegurar la no alteración de la Base de Datos de nuestra Nueva Licencia de Conducir Digital Biométrica

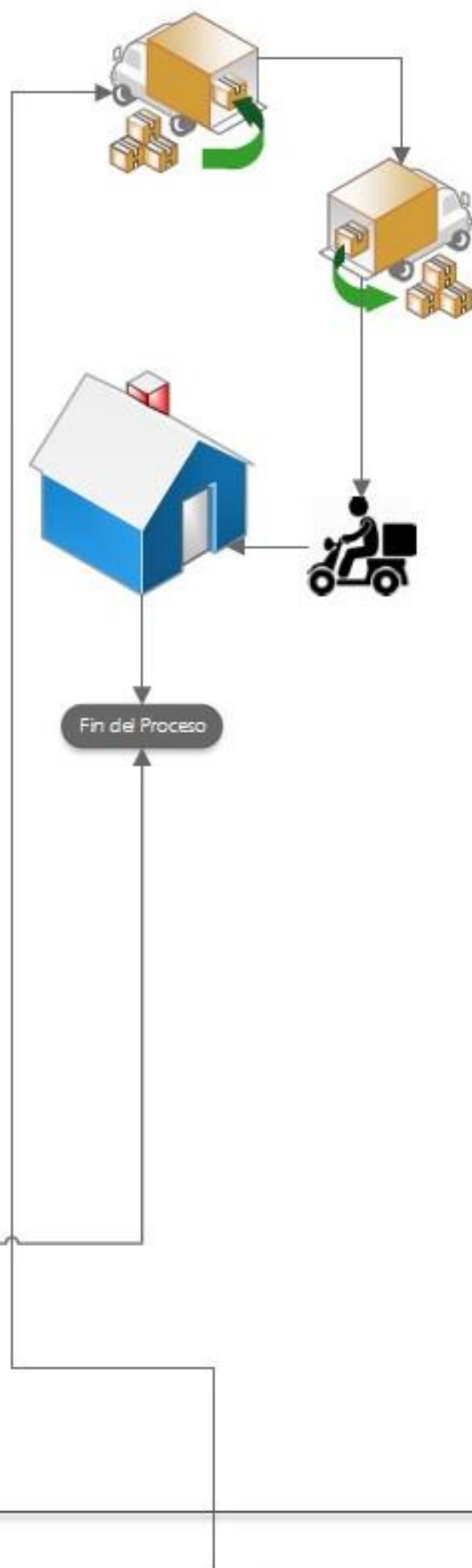
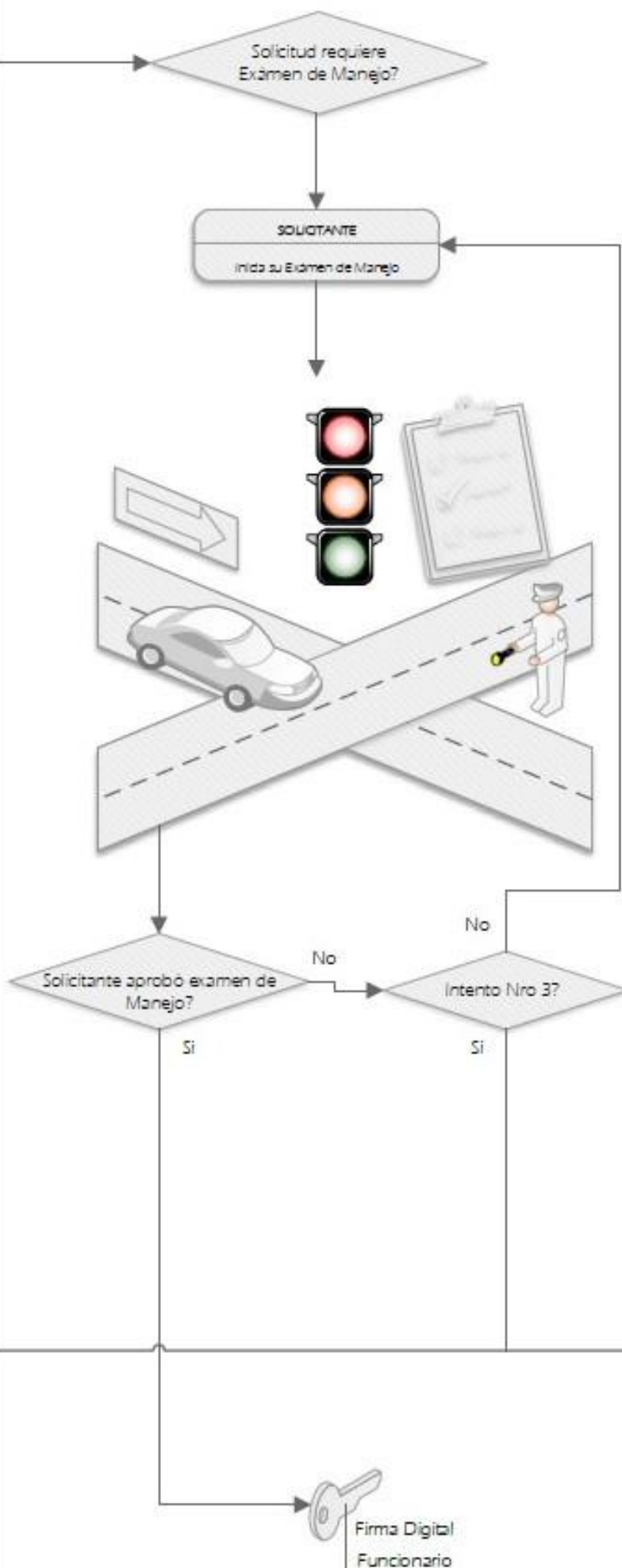


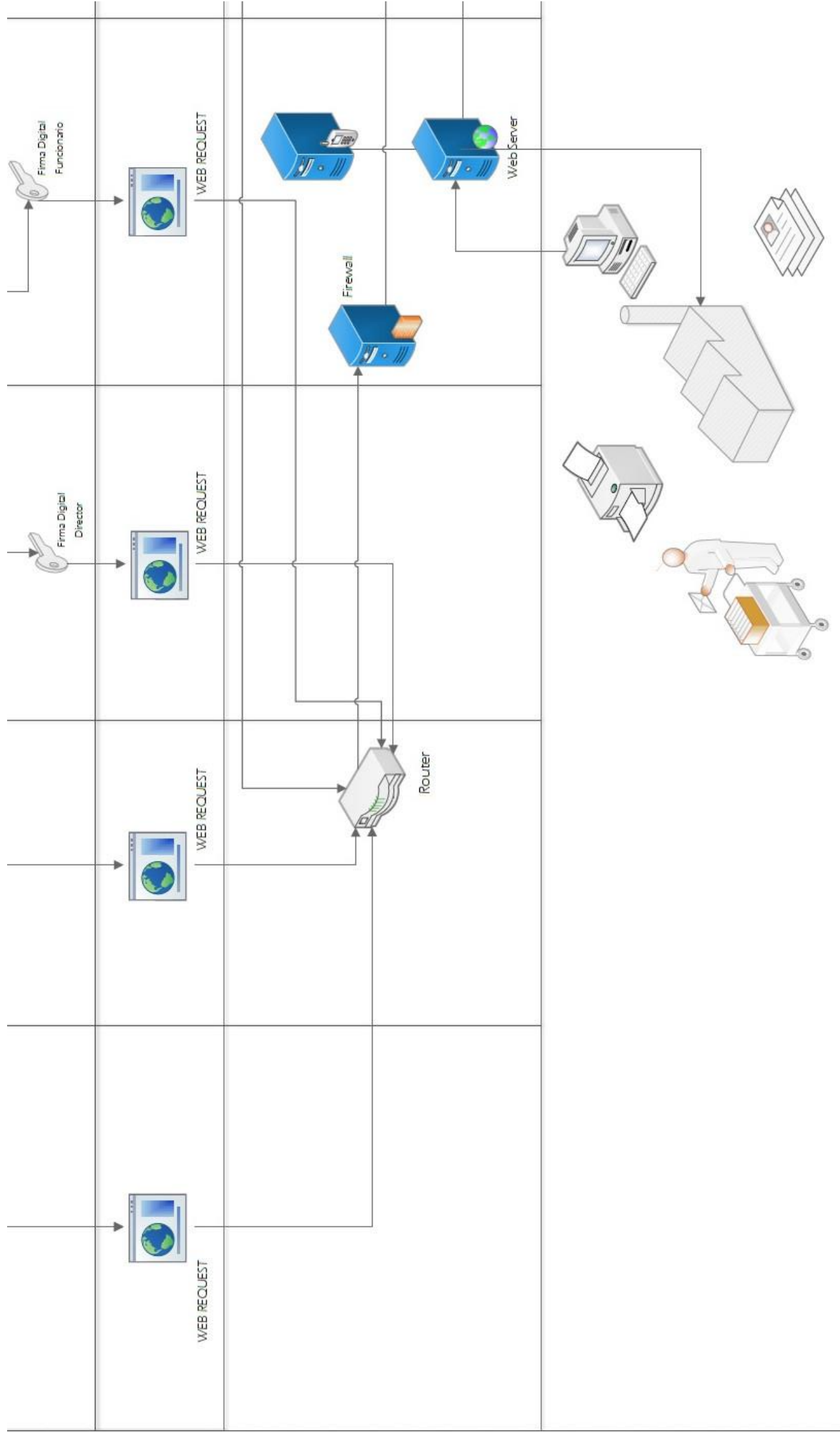
Centro de Salud

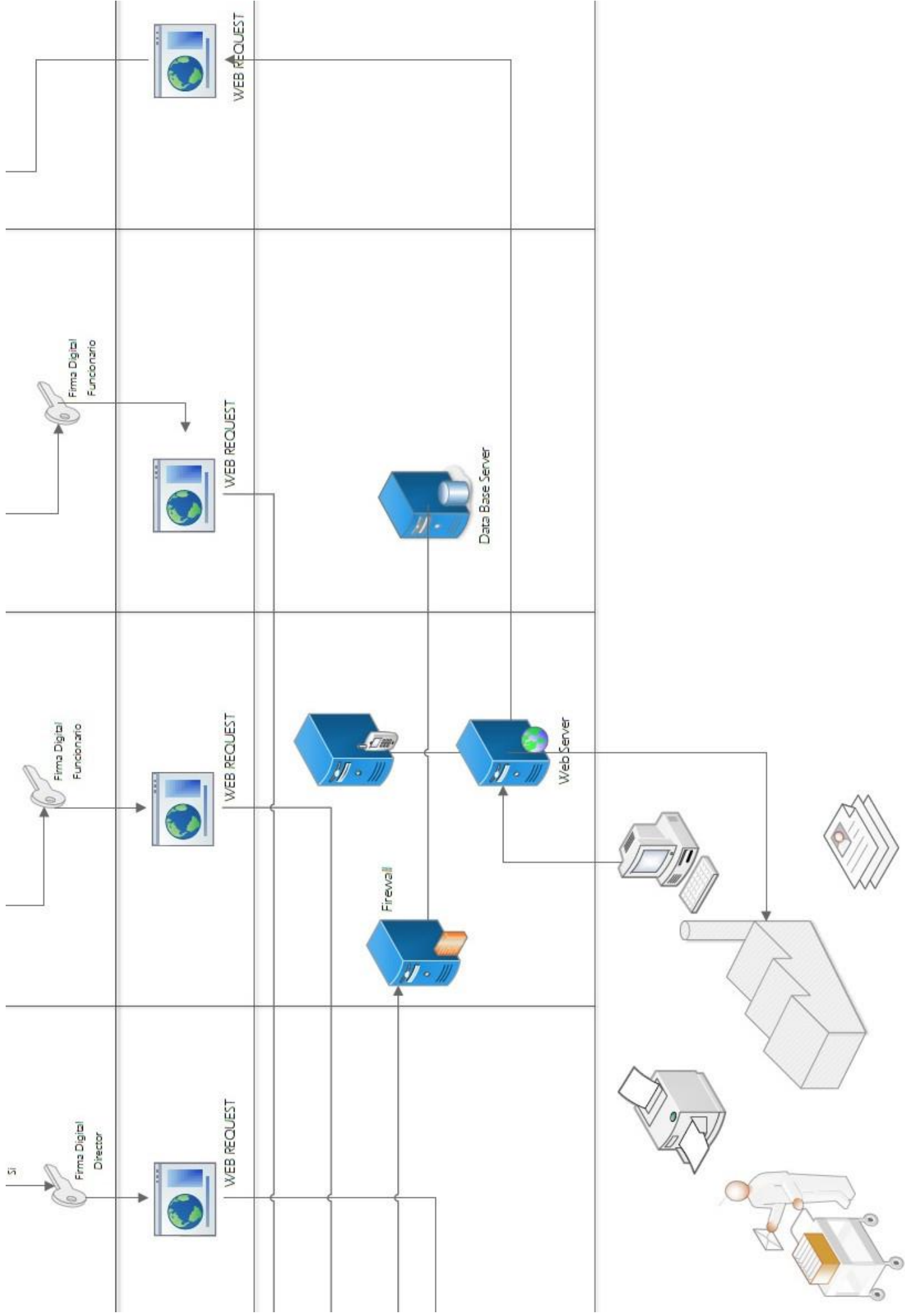


Centro de Evaluación Touring









Hemos realizado este análisis de Seguridad Informática porque para una Licencia de Conducir Digital Biométrica que tiene la característica de “Absolutamente Infalsificable” necesitamos Datos Confiables y estos dependen de un Sistema Informático con Certificados Digitales, Firmas Digitales y una Topología inspirada en los principios de la Seguridad Documentaria

Para ello hemos consultado a especialistas en Buenos Aires, Brasil y Perú y todas las opiniones han sido convergentes, los diagramas son una expresión de esta convergencia.

La otra consulta fue el tiempo para desarrollar el sistema, el estimado fue de 60 a 90 días contando con el Total Apoyo del Departamento Informático del MTC.

La consulta sobre el tiempo estimado para el desarrollo del sistema para la protección de la Integridad de Registros de Bases de Datos da un estimado de 30 a 60 días, siempre contando con el apoyo del MTC.

Lo mismo sucede con todos los 7 sistemas de Seguridad Lógica y Biometría, el tiempo promedio es de 60 días.

El Gant de todos los procesos es paralelo no secuencial, entonces si los procesos comienzan simultáneamente en enero deben estar terminado con total seguridad en abril.

En el mes de mayo se podría empezar a emitir la Nueva Licencia de Conducir Digital Biométrica en todo el Perú