HUVI – Expediente Fundacional

Autor: Francisco Corbacho Madera

Carta Universal de la Identidad Humana(1)

CARTA UNIVERSAL DE LA IDENTIDAD HUMANA

Propuesta para la protección de la persona en la era digital

España, 2026

PREÁMBULO

A lo largo de la historia, la humanidad ha tenido que adaptarse a grandes cambios tecnológicos, sociales y culturales.

Cada avance ha traído nuevas oportunidades, pero también nuevas responsabilidades.

La imprenta transformó el conocimiento.

La electricidad transformó la industria.

Internet transformó la comunicación.

La inteligencia artificial transformará la forma en que los seres humanos se relacionan con la información, con las máquinas y entre sí.

Nos encontramos ante una nueva etapa de la civilización en la que la capacidad de reproducir imágenes, voces, comportamientos e incluso decisiones humanas mediante sistemas artificiales plantea desafíos inéditos.

Por primera vez, una persona puede ver comprometida no solamente su privacidad o sus datos, sino también la propia autenticidad de su identidad.

Ante esta realidad, consideramos necesario reconocer y proteger la identidad humana como un bien fundamental que merece especial protección jurídica, ética y tecnológica.

La presente Carta constituye una propuesta abierta dirigida a ciudadanos, instituciones, empresas, universidades y gobiernos para promover un marco común de principios destinado a preservar la autenticidad de la persona en la era digital.

PRINCIPIOS GENERALES

Artículo 1. Dignidad humana

Toda persona posee una identidad propia, única e irrepetible que constituye una expresión de su dignidad como ser humano.

Ninguna tecnología podrá justificar la negación o menoscabo de dicha dignidad.

Artículo 2. Derecho a la autenticidad

Toda persona tiene derecho a ser reconocida como un ser humano auténtico y a disponer de mecanismos que le permitan acreditar dicha condición cuando resulte necesario.

Artículo 3. Derecho a la protección frente a la suplantación

Toda persona tiene derecho a ser protegida frente a la falsificación de su identidad, la utilización fraudulenta de su imagen, su voz, sus datos biométricos o cualquier otro elemento destinado a representarla.

Artículo 4. Derecho a la identidad vital

Toda persona tiene derecho a que existan procedimientos seguros que permitan verificar, de forma proporcionada y respetuosa con sus derechos, su existencia física y presencia real cuando ello resulte necesario para proteger intereses legítimos.

Artículo 5. Derecho al control de los datos personales

La información utilizada para acreditar la identidad de una persona deberá permanecer bajo el máximo control posible de su titular.

Su utilización requerirá bases legítimas, transparencia y garantías adecuadas.

GARANTÍAS TECNOLÓGICAS

Artículo 6. Principio de proporcionalidad

Los sistemas de identificación deberán utilizar únicamente los datos estrictamente necesarios para cumplir su finalidad.

Artículo 7. Principio de minimización

La protección de la identidad humana no podrá convertirse en una excusa para la recopilación masiva e indiscriminada de información personal.

Artículo 8. Transparencia

Las personas tendrán derecho a conocer qué tecnologías intervienen en los procesos de verificación de identidad y cuáles son sus principales características y limitaciones.

Artículo 9. Supervisión independiente

Los sistemas de identificación de gran impacto social deberán estar sometidos a mecanismos de supervisión técnica, jurídica y ética independientes.

Artículo 10. Seguridad

Toda tecnología destinada a la protección de la identidad humana deberá diseñarse priorizando la seguridad, la resiliencia y la protección frente al fraude.

LÍMITES Y PROHIBICIONES

Artículo 11. Prohibición de la discriminación

Ningún sistema de identificación podrá utilizarse para discriminar a personas o colectivos por razones de origen, nacionalidad, sexo, edad, religión, ideología, condición económica o cualquier otra circunstancia personal o social.

Artículo 12. Prohibición de usos abusivos

La protección de la identidad humana no podrá utilizarse como instrumento de persecución, represión, control arbitrario o limitación ilegítima de derechos fundamentales.

Artículo 13. Respeto a la libertad individual

Toda aplicación de tecnologías de identificación deberá respetar los principios democráticos, el Estado de Derecho y las libertades fundamentales reconocidas internacionalmente.

RESPONSABILIDAD COMPARTIDA

Artículo 14. Responsabilidad de los desarrolladores

Quienes diseñen tecnologías relacionadas con la identidad humana deberán actuar con prudencia, responsabilidad y respeto a los derechos de las personas.

Artículo 15. Responsabilidad de las instituciones

Los poderes públicos deberán promover marcos normativos que protejan a los ciudadanos frente a la suplantación digital y los riesgos derivados del uso indebido de tecnologías avanzadas.

Artículo 16. Cooperación internacional

La protección de la identidad humana constituye un desafío global que requiere cooperación entre Estados, organizaciones internacionales, empresas, universidades y sociedad civil.

DISPOSICIÓN FINAL

La identidad humana constituye uno de los fundamentos de la libertad, de la responsabilidad y de la convivencia.

En una época en la que las tecnologías permiten reproducir con creciente precisión las características de una persona, resulta necesario reforzar los mecanismos destinados a preservar la autenticidad humana.

La presente Carta no pretende ofrecer respuestas definitivas.

Pretende iniciar una reflexión colectiva.

Porque el progreso tecnológico será verdaderamente valioso únicamente si continúa estando al servicio de las personas.

Y porque ninguna innovación tendrá sentido si olvidamos aquello que buscamos proteger: el ser humano.

Francisco _____

España

2026

HUVI - Reivindicaciones Iniciales de Patente(1)

HUVI

HUMAN UNIVERSAL VITAL IDENTITY

DOCUMENTO Nº 6

REIVINDICACIONES INICIALES DE PATENTE

VERSIÓN FUNDACIONAL

REIVINDICACIÓN 1 (PRINCIPAL)

Sistema y método de autenticación humana caracterizado por verificar simultáneamente la identidad biométrica de un individuo, la existencia de vida del mismo y la generación de una credencial dinámica asociada a una acción concreta.

REIVINDICACIÓN 2

Sistema según la reivindicación anterior en el que la identidad del individuo se determina mediante uno o varios parámetros biométricos.

Dichos parámetros podrán comprender:

huella digital;

huella tridimensional;

reconocimiento facial;

iris;

retina;

patrón vascular;

voz;

ADN;

biometría conductual;

cualquier sistema biométrico presente o futuro.

REIVINDICACIÓN 3

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por incorporar una prueba de vida obtenida mediante uno o varios parámetros fisiológicos.

Dichos parámetros podrán comprender:

pulso;

frecuencia cardíaca;

variabilidad cardíaca;

temperatura;

oxigenación;

perfusión sanguínea;

actividad eléctrica;

parámetros neuromusculares;

otros indicadores fisiológicos.

REIVINDICACIÓN 4

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque la autenticación requiere simultáneamente identidad válida y prueba de vida válida.

REIVINDICACIÓN 5

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por generar una credencial dinámica distinta para cada operación realizada.

REIVINDICACIÓN 6

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque cada credencial dinámica se calcula utilizando una combinación de:

identidad validada;

parámetros fisiológicos;

fecha;

hora;

identificador de dispositivo;

identificador de operación;

componente aleatoria;

algoritmo criptográfico.

REIVINDICACIÓN 7

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque la credencial generada tiene una validez temporal limitada.

REIVINDICACIÓN 8

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque una credencial utilizada no puede volver a emplearse para una operación posterior.

REIVINDICACIÓN 9

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque una credencial generada para una acción concreta no podrá utilizarse para una acción distinta.

REIVINDICACIÓN 10

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque la autenticación incorpora análisis contextual de riesgo.

REIVINDICACIÓN 11

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por determinar un nivel de confianza asociado a la autenticación.

REIVINDICACIÓN 12

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por clasificar la autenticación en distintos niveles de seguridad.

REIVINDICACIÓN 13

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por incorporar análisis de estado funcional del individuo.

REIVINDICACIÓN 14

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por evaluar la capacidad del individuo para emitir una autorización válida.

REIVINDICACIÓN 15

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por detectar condiciones incompatibles con una autorización válida.

REIVINDICACIÓN 16

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por detectar posibles situaciones de:

coacción;

amenaza;

miedo extremo;

incapacidad cognitiva;

pérdida de consciencia;

alteraciones fisiológicas incompatibles con una decisión libre.

REIVINDICACIÓN 17

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por incorporar biomarcadores bioquímicos.

Dichos biomarcadores podrán comprender:

cortisol;

adrenalina;

noradrenalina;

dopamina;

serotonina;

glucosa;

lactato;

hormonas;

metabolitos;

biomarcadores futuros.

REIVINDICACIÓN 18

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por incorporar biomarcadores genéticos.

REIVINDICACIÓN 19

Sistema según cualquiera de las reivindicaciones anteriores caracterizado por registrar cada autenticación realizada.

REIVINDICACIÓN 20

Sistema según cualquiera de las reivindicaciones anteriores caracterizado porque dicho registro incorpora:

identidad;

fecha;

hora;

acción autorizada;

dispositivo utilizado;

nivel de confianza;

firma criptográfica.

REIVINDICACIÓN 21

Sistema según cualquiera de las reivindicaciones anteriores implementado mediante teléfono móvil.

REIVINDICACIÓN 22

Sistema según cualquiera de las reivindicaciones anteriores implementado mediante dispositivo portátil.

REIVINDICACIÓN 23

Sistema según cualquiera de las reivindicaciones anteriores implementado mediante reloj inteligente.

REIVINDICACIÓN 24

Sistema según cualquiera de las reivindicaciones anteriores implementado mediante terminal fijo.

REIVINDICACIÓN 25

Sistema según cualquiera de las reivindicaciones anteriores utilizado para:

banca;

pagos;

firma electrónica;

inteligencia artificial;

redes sociales;

vehículos;

robots;

maquinaria;

infraestructuras críticas;

procesos electorales;

sistemas gubernamentales.

REIVINDICACIÓN FUNDACIONAL HUVI

Método universal de autenticación humana caracterizado por combinar identificación biométrica, verificación vital, análisis funcional del individuo y generación de credenciales dinámicas irrepetibles para autorizar acciones físicas o digitales de manera segura, verificable y no reutilizable.

HUVI CORE(1)

HUVI

DOCUMENTO Nº 7

HUVI CORE

MOTOR UNIVERSAL DE IDENTIDAD VITAL

ARQUITECTURA CONCEPTUAL FUNDACIONAL

1. DEFINICIÓN

HUVI CORE constituye el núcleo de inteligencia del sistema HUVI.

Su función es transformar información humana, fisiológica y contextual en una credencial dinámica única capaz de autorizar una acción física o digital.

HUVI CORE no verifica únicamente identidad.

HUVI CORE verifica identidad, existencia vital, capacidad funcional y validez de autorización.

2. PRINCIPIO FUNDAMENTAL

La identidad humana no será considerada una condición binaria.

La identidad será calculada mediante una puntuación dinámica de confianza.

HUVI CORE evaluará simultáneamente:

identidad;

vitalidad;

contexto;

consentimiento;

riesgo.

3. VARIABLES DE ENTRADA

BLOQUE A

IDENTIDAD

Variables posibles:

huella digital;

huella 3D;

iris;

retina;

rostro;

voz;

ADN;

biometría conductual;

futuros sistemas biométricos.

BLOQUE B

VIDA

Variables posibles:

pulso;

frecuencia cardíaca;

temperatura;

oxigenación;

flujo sanguíneo;

actividad eléctrica;

perfusión;

biomarcadores futuros.

BLOQUE C

ESTADO FUNCIONAL

Variables posibles:

estrés;

capacidad cognitiva;

estado emocional;

nivel de atención;

capacidad de respuesta;

nivel de consciencia;

orientación temporal;

orientación espacial.

BLOQUE D

CONTEXTO

Variables posibles:

fecha;

hora;

ubicación;

dispositivo;

tipo de operación;

historial;

nivel de riesgo;

frecuencia de uso.

4. MATRIZ DE CONFIANZA HUVI

HUVI CORE calculará una puntuación denominada:

HUVI TRUST SCORE

Escala:

0 - 1000

0 = autenticación imposible

1000 = autenticación máxima

5. FACTORES DE CÁLCULO

Ejemplo conceptual:

IDENTIDAD = 40 %

VIDA = 25 %

ESTADO FUNCIONAL = 20 %

CONTEXTO = 15 %

La ponderación podrá variar dinámicamente.

6. ANÁLISIS DE COHERENCIA

HUVI CORE verificará la coherencia entre todas las variables.

Ejemplos:

Huella correcta + pulso inexistente

Resultado:

DENEGADO

Huella correcta + pulso correcto + nivel extremo de estrés + operación de alto valor

Resultado:

VERIFICACIÓN ADICIONAL

Huella correcta + pulso correcto + contexto normal

Resultado:

AUTORIZACIÓN

7. DETECCIÓN DE ANOMALÍAS

HUVI CORE incorporará un motor de detección de anomalías.

Detectará:

suplantaciones;

duplicidades;

comportamientos atípicos;

patrones incompatibles;

automatización sospechosa;

posibles ataques.

8. DETECCIÓN DE COACCIÓN

Uno de los elementos diferenciales de HUVI.

El sistema podrá detectar indicadores compatibles con:

secuestro;

amenaza;

miedo extremo;

coacción;

incapacidad temporal.

Variables potenciales:

variabilidad cardíaca;

respuesta fisiológica;

biomarcadores;

comportamiento anómalo;

patrones de estrés.

9. DECISIÓN HUVI

HUVI CORE podrá emitir:

AUTORIZADO

AUTORIZADO CON RESTRICCIONES

VERIFICACIÓN ADICIONAL

DENEGADO

DENEGADO POR RIESGO

DENEGADO POR COACCIÓN

10. GENERACIÓN DE HUVI KEY

Una vez tomada la decisión:

HUVI CORE generará una credencial única.

La credencial incorporará:

identidad verificada;

instante temporal;

contexto;

dispositivo;

operación;

componente aleatoria;

firma criptográfica.

11. PRINCIPIO DE NO REPETICIÓN

Ninguna HUVI KEY podrá repetirse.

Dos operaciones consecutivas de la misma persona producirán credenciales diferentes.

Incluso si:

utiliza el mismo dispositivo;

realiza la misma operación;

se encuentra en el mismo lugar.

12. PRINCIPIO DE NO TRANSFERENCIA

Una HUVI KEY generada para una operación concreta no podrá utilizarse para una operación distinta.

Una autorización bancaria no servirá para acceder a una red social.

Una autorización de vehículo no servirá para firmar un contrato.

13. APRENDIZAJE EVOLUTIVO

HUVI CORE podrá incorporar sistemas de inteligencia artificial.

Su finalidad será:

mejorar la detección de fraude;

mejorar la detección de coacción;

mejorar la detección de identidad;

mejorar la puntuación de confianza.

14. OBJETIVO ESTRATÉGICO

Convertir HUVI CORE en el estándar universal de decisión de identidad humana para:

personas;

empresas;

bancos;

gobiernos;

robots;

inteligencia artificial;

infraestructuras críticas.

DEFINICIÓN FUNDACIONAL

HUVI CORE es un motor de decisión capaz de transformar identidad humana, prueba de vida, estado funcional y contexto operativo en una autorización dinámica única, verificable, irrepetible y vinculada a una acción concreta.

HUVI Trust Engine(1)

HUVI

DOCUMENTO Nº 8

HUVI TRUST ENGINE

MOTOR DE CONFIANZA Y GENERACIÓN DE AUTORIZACIÓN

DOCUMENTO FUNDACIONAL DE FUNCIONAMIENTO

1. OBJETIVO

HUVI TRUST ENGINE constituye el núcleo operativo del sistema HUVI.

Su finalidad es determinar si una acción solicitada puede ser autorizada por un individuo concreto en un instante determinado.

El sistema no pretende únicamente identificar personas.

Su objetivo es verificar:

identidad;

existencia vital;

autenticidad;

consentimiento;

nivel de confianza.

2. PRINCIPIO FUNDAMENTAL

HUVI considera que una autorización válida solamente existe cuando concurren simultáneamente cinco condiciones:

CONDICIÓN 1

Identidad válida.

CONDICIÓN 2

Vida verificada.

CONDICIÓN 3

Presencia real.

CONDICIÓN 4

Consentimiento válido.

CONDICIÓN 5

Contexto aceptable.

Si cualquiera de estas condiciones falla, la autorización podrá ser rechazada.

3. VARIABLES DE ENTRADA

HUVI TRUST ENGINE recibirá información procedente de múltiples fuentes.

IDENTIDAD

Variables posibles:

huella;

huella 3D;

iris;

retina;

rostro;

voz;

ADN;

biometría conductual.

VIDA

Variables posibles:

pulso;

ritmo cardíaco;

temperatura;

oxigenación;

flujo sanguíneo;

actividad fisiológica.

PRESENCIA

Variables posibles:

interacción física;

movimiento;

respuesta en tiempo real;

detección de vida;

liveness detection.

CONSENTIMIENTO

Variables posibles:

respuesta consciente;

confirmación activa;

comportamiento coherente;

ausencia de anomalías graves.

CONTEXTO

Variables posibles:

dispositivo;

ubicación;

fecha;

hora;

historial;

riesgo de operación.

4. MATRIZ DE CONFIANZA

HUVI no trabaja mediante respuestas binarias.

Trabaja mediante niveles de confianza.

Cada variable genera una puntuación parcial.

Las puntuaciones parciales se integran en una puntuación global denominada:

HUVI TRUST SCORE

5. HUVI TRUST SCORE

La puntuación podrá expresarse en cualquier escala.

Ejemplo:

0 - 1000

0-250

Confianza insuficiente.

251-500

Confianza limitada.

501-750

Confianza elevada.

751-1000

Confianza máxima.

6. PONDERACIÓN DINÁMICA

La importancia de cada variable podrá modificarse automáticamente.

Ejemplo:

Una red social puede exigir:

70 % identidad.

30 % vida.

Mientras que un banco puede exigir:

40 % identidad.

30 % vida.

30 % consentimiento.

El sistema adaptará automáticamente los pesos.

7. DETECCIÓN DE COACCIÓN

HUVI podrá evaluar indicadores compatibles con situaciones de presión externa.

Posibles indicadores:

estrés extremo;

comportamiento anómalo;

incoherencia fisiológica;

alteraciones emocionales;

biomarcadores.

Cuando exista sospecha de coacción:

HUVI podrá:

bloquear;

retrasar;

requerir confirmación adicional.

8. DETECCIÓN DE FRAUDE

El sistema analizará:

duplicidad de identidad;

comportamientos imposibles;

patrones automatizados;

ataques de suplantación;

ataques de repetición.

9. DECISIÓN

Una vez procesadas las variables:

HUVI podrá emitir:

AUTORIZADO

AUTORIZADO CON RESTRICCIONES

AUTORIZADO CON SUPERVISIÓN

VERIFICACIÓN ADICIONAL

DENEGADO

DENEGADO POR RIESGO

DENEGADO POR COACCIÓN

10. GENERACIÓN DE LA HUVI KEY

Una vez autorizada la operación:

HUVI genera una credencial temporal.

La credencial se construye utilizando:

identidad validada;

estado vital;

contexto;

operación solicitada;

instante temporal;

componente aleatoria;

firma criptográfica.

11. PRINCIPIO DE IRREPETIBILIDAD

La HUVI KEY deberá ser diferente en cada operación.

Dos autorizaciones consecutivas nunca producirán la misma credencial.

12. PRINCIPIO DE VINCULACIÓN

Cada HUVI KEY quedará vinculada a:

una persona;

una acción;

un instante;

un dispositivo;

un sistema receptor.

13. PRINCIPIO DE CADUCIDAD

Toda HUVI KEY tendrá una duración limitada.

Transcurrido dicho plazo quedará invalidada.

14. APRENDIZAJE EVOLUTIVO

HUVI TRUST ENGINE podrá incorporar inteligencia artificial.

La finalidad será mejorar continuamente:

detección de fraude;

detección de coacción;

validación de identidad;

cálculo de confianza.

15. DEFINICIÓN FUNDACIONAL

HUVI TRUST ENGINE es un sistema de decisión capaz de transformar identidad humana, existencia vital, consentimiento y contexto operativo en una autorización digital dinámica, única, verificable, irrepetible y temporalmente limitada.

HUVI - Sistema de Creación y Certificación de Identidad(1)

HUVI

DOCUMENTO Nº 9

SISTEMA DE CREACIÓN Y CERTIFICACIÓN DE IDENTIDAD HUVI

NACIMIENTO DE LA IDENTIDAD VITAL DIGITAL

Documento Fundacional

1. PRINCIPIO FUNDAMENTAL

La fortaleza de una identidad digital depende de la fiabilidad de su origen.

HUVI establece que ninguna identidad puede considerarse plenamente válida si no existe una relación verificable entre:

la persona física;

la identidad legal;

la identidad biológica;

la identidad digital.

2. CONCEPTO DE IDENTIDAD HUVI

La Identidad HUVI constituye una identidad vital digital única asociada a una persona humana concreta.

Dicha identidad se genera una sola vez y permanece vinculada al individuo durante toda su vida.

3. CREACIÓN INICIAL

La creación de una identidad HUVI requerirá una fase de verificación fundacional.

Durante dicha fase se comprobará simultáneamente:

Identidad legal

Mediante documentos oficiales.

Ejemplos:

DNI.

Pasaporte.

Documento nacional de identidad extranjero.

Permiso de residencia.

Documento gubernamental equivalente.

Identidad biométrica

Mediante:

huella digital;

huella tridimensional;

iris;

rostro;

voz;

patrones biométricos adicionales.

Identidad vital

Mediante:

pulso;

temperatura;

oxigenación;

flujo sanguíneo;

prueba de vida.

4. GENERACIÓN DEL HUVI ID

Una vez completadas las verificaciones iniciales, el sistema generará:

HUVI ID

Este identificador será:

único;

permanente;

global;

intransferible;

asociado exclusivamente a una persona.

5. CERTIFICACIÓN DE ORIGEN

La identidad HUVI deberá incorporar evidencia verificable de su creación.

Dicha evidencia podrá incluir:

organismo certificador;

autoridad emisora;

fecha de creación;

país de origen;

método de verificación utilizado;

nivel de confianza inicial.

6. NIVELES DE CERTIFICACIÓN

HUVI C1

Verificación documental básica.

HUVI C2

Verificación documental más biométrica.

HUVI C3

Verificación documental, biométrica y vital.

HUVI C4

Verificación presencial certificada por entidad autorizada.

HUVI C5

Verificación reforzada con múltiples fuentes oficiales.

7. PRINCIPIO DE UNICIDAD

Cada persona podrá disponer de una única identidad HUVI principal.

El sistema deberá incorporar mecanismos destinados a detectar:

duplicidades;

identidades múltiples;

intentos de fraude;

registros repetidos.

8. ACTUALIZACIÓN DE IDENTIDAD

La identidad HUVI podrá evolucionar durante la vida del individuo.

El sistema podrá actualizar:

biometría;

documentación;

información vital;

niveles de certificación.

Sin alterar la identidad HUVI original.

9. RECUPERACIÓN DE IDENTIDAD

En caso de:

pérdida de dispositivo;

robo;

deterioro biométrico;

accidente;

enfermedad;

la identidad podrá recuperarse mediante procedimientos reforzados de verificación.

10. HERENCIA DIGITAL Y FINALIZACIÓN

El sistema podrá incorporar procedimientos para:

inhabilitación por fallecimiento;

conservación histórica;

transmisión de determinados derechos digitales;

cancelación de credenciales activas.

11. REGISTRO FUNDACIONAL HUVI

Toda identidad HUVI deberá quedar inscrita en un registro seguro.

El registro contendrá:

HUVI ID;

fecha de creación;

nivel de certificación;

país de origen;

historial de actualizaciones.

12. PRINCIPIO DE SOBERANÍA HUMANA

HUVI reconoce que la identidad pertenece al individuo.

Ninguna organización podrá apropiarse de la identidad HUVI de una persona.

La identidad vital digital permanecerá vinculada exclusivamente a su titular.

DEFINICIÓN FUNDACIONAL

HUVI ID es una identidad vital digital única, permanente e intransferible creada mediante la vinculación verificable entre identidad legal, identidad biométrica, identidad vital e identidad digital, permitiendo autenticar a una persona humana de forma segura durante todo su ciclo de vida.

HUVI - Casos de Uso(1)

HUVI

DOCUMENTO Nº 10

CASOS DE USO Y ESCENARIOS DE FUNCIONAMIENTO

HUMAN UNIVERSAL VITAL IDENTITY

Aplicaciones Prácticas del Sistema HUVI

INTRODUCCIÓN

HUVI ha sido concebido como un estándar universal de identidad humana verificable.

Su finalidad es permitir que cualquier sistema físico o digital pueda determinar con un elevado nivel de confianza:

quién realiza una acción;

si dicha persona está viva;

si se encuentra presente;

si se encuentra en condiciones válidas para actuar;

si la autorización emitida es auténtica.

Los siguientes escenarios describen posibles aplicaciones del sistema.

CASO 1

BANCA Y OPERACIONES FINANCIERAS

Situación actual

Las transferencias bancarias se autorizan mediante:

contraseñas;

SMS;

aplicaciones;

códigos temporales.

Todos estos sistemas pueden ser robados, interceptados o manipulados.

Funcionamiento HUVI

El usuario inicia una transferencia.

La entidad bancaria solicita autenticación HUVI.

El usuario activa HUVI Mobile.

HUVI verifica:

identidad;

prueba de vida;

contexto;

consentimiento.

HUVI genera una HUVI KEY.

El banco valida la autorización.

Beneficio

La autorización queda vinculada a:

una persona;

una operación;

un instante concreto.

CASO 2

FIRMA DIGITAL DE CONTRATOS

Problema actual

Las firmas electrónicas demuestran autenticación.

No siempre demuestran:

presencia;

consciencia;

consentimiento real.

Funcionamiento HUVI

Antes de firmar:

Verificación biométrica.

Verificación vital.

Evaluación de consentimiento.

Generación de HUVI KEY.

Firma del documento.

Beneficio

Mayor seguridad jurídica.

CASO 3

REDES SOCIALES

Problema actual

Existencia de:

bots;

perfiles falsos;

identidades suplantadas;

cuentas automatizadas.

Funcionamiento HUVI

La plataforma solicita validación HUVI.

El sistema verifica:

existencia humana;

identidad;

prueba de vida.

Beneficio

Diferenciación entre:

personas;

sistemas automáticos;

inteligencia artificial.

CASO 4

INTELIGENCIA ARTIFICIAL

Problema actual

Las IA desconocen quién se encuentra al otro lado.

Funcionamiento HUVI

La IA recibe una validación HUVI.

Puede determinar:

identidad;

nivel de confianza;

condición humana verificada.

Beneficio

Creación de entornos de interacción humana verificada.

CASO 5

VEHÍCULOS

Funcionamiento

Antes del arranque:

identificación;

prueba de vida;

estado funcional.

Beneficio

Prevención de uso indebido.

Posibilidad de impedir el uso en situaciones incompatibles con la conducción.

CASO 6

CAJAS FUERTES Y ACTIVOS CRÍTICOS

Funcionamiento

La apertura requiere:

identidad válida;

presencia física;

autorización HUVI.

Beneficio

La clave no puede copiarse ni reutilizarse.

CASO 7

ROBOTS Y MAQUINARIA INDUSTRIAL

Funcionamiento

HUVI verifica:

identidad del operador;

autorización;

estado funcional.

Beneficio

Reducción de errores y accesos no autorizados.

CASO 8

SISTEMAS ELECTORALES

Funcionamiento

El votante:

Verifica identidad.

Verifica vida.

Genera autorización única.

Beneficio

Reducción del fraude electoral.

CASO 9

SANIDAD

Funcionamiento

HUVI verifica identidad de:

pacientes;

médicos;

personal autorizado.

Beneficio

Mayor trazabilidad y seguridad.

CASO 10

INFRAESTRUCTURAS CRÍTICAS

Aplicable a:

centrales energéticas;

defensa;

telecomunicaciones;

transporte.

Beneficio

Control reforzado de acceso y autorización.

CASO 11

HUVI COMO IDENTIDAD UNIVERSAL

Escenario futuro.

La identidad HUVI se convierte en una credencial universal.

Un único identificador permite interactuar con:

bancos;

administraciones;

empresas;

IA;

vehículos;

dispositivos.

CASO 12

VERIFICACIÓN DE INTENCIÓN HUMANA

Escenario diferencial HUVI.

El sistema no verifica únicamente identidad.

También verifica:

vida;

presencia;

consentimiento;

intención de actuar.

PRINCIPIO FINAL

Toda acción relevante en el entorno digital o físico puede asociarse a una identidad humana viva, presente, consciente y verificable mediante el sistema HUVI.

Esta capacidad constituye la base del concepto de Identidad Vital Universal.