VI CONGRESO DERECHO NOTARIAL

COSTA RICA 2021

Dirección Nacional de Notariado

VI CONGRESO DERECHO NOTARIAL
COSTA RICA 2021

MESA #4

Proyecto de Reglamentación de documentos Notariales Extraprotocolares en soporte digital

DNN
Dirección Nacional de Notariado

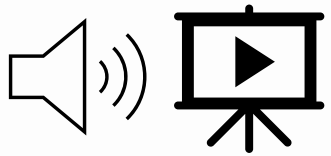
VI CONGRESO DERECHO NOTARIAL
COSTA RICA 2021

Aspectos tecnológicos sobre integridad e identidad

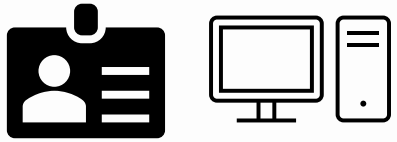
Juan Alejandro Herrera López

DNN Dirección Nacional de Notariado

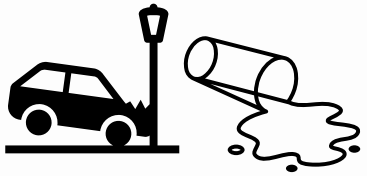
¿Qué servicios de valor agregado requeriría?



Generar pruebas de integridad archivos



Identificar personas o cosas



Acreditar eventos

¿Cómo podría ayudar la tecnología en estos servicios?

Integridad y autenticidad en el mundo digital requiere

Criptografía

HASH: Resumen criptográfico único de un archivo.

https://emn178.github.io/online-tools/sha256.html

Table 8 provides the approval status of the hash functions.

Table 8: Approval Status of Hash Functions

Hash Function	Use	Status
SHA-1	Digital signature generation	Disallowed, except where specifically allowed by NIST protocol-specific guidance.
	Digital signature verification	Legacy use
	Non-digital-signature applications	Acceptable
SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)	Acceptable for all hash function applications	
SHA-3 family (SHA3-224, SHA3-	Acceptable for all hash function applications	

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

F6419B5A71FE706D2B22D7BB6EBE91EE1860246D9A26AFECC20D3CACFA6081E4

onlinemd5.com

OnlineMD5

MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it. Examinar... quien-tiene-la-culpa-colision.jpg

Click to select a file, or drag and drop it here(max: 4GB).

Filename:	quien-tiene-la-culpa-colision.jpg
File size:	54,221 Bytes
Checksum type:	MD5 SHA1 SHA-256
File checksum:	F6419B5A71FE706D2B22D7BB6EBE91EE1860246D9A26AFECC20D3CACFA6081E4
Compare with:	F6419B5A71FE706D2B22D7BB6EBE91EE1860246D9A26AFECC20D3CACFA6081E4
Process:	100.00%

Compare Pause Stop

http://onlinemd5.com/

https://md5file.com/calculator

MD5 File — PAY ONCE USE FREE — Home Upload Calculator Email

HTML5 File Hash Online Calculator

This is html5 file hash online calculator, which supports an unlimited number of files and unlimited file size. Your files are not trar calculations are performed directly in the browser.

Drop files here or click to select

and hash them all

Fastest implementation for SHA-1, SHA-256, SHA-384 and SHA-512 (WebCrypto API) for files less than 512GB. Needs latest Chrome or Firefox and more memory. Microsoft Edge does not support SHA-1.

MD5 SHA-1 SHA-256 SHA-384 SHA-512 Examinar... quien-tiene-la-culpa-colision.jpg

quien-tiene-la-culpa-colision.jpg	(image/jpeg) - 54221 bytes
SHA-256	f6419b5a71fe706d2b22d7bb6ebe91ee1860246d9a26afecc20d3cacfa6081e4

Podría servir como herramienta para el notariado identificando de manera única un archivo (audio, video, software, registro base de datos) y asegurando su integridad en el tiempo.

VI CONGRESO DERECHO NOTARIAL
COSTA RICA 2021

Autenticación de personas

DNN Dirección Nacional de Notariado

Modelo determinista

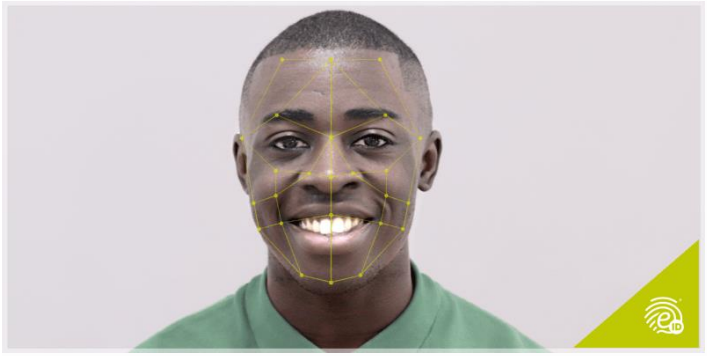
Un **modelo determinista** es un modelo matemático donde las mismas entradas o condiciones iniciales producirán invariablemente las mismas salidas o resultados, **no contemplándose la existencia de azar, o incertidumbre en el proceso modelado mediante dicho modelo**.

https://es.wikipedia.org/wiki/Modelo_determinista

$$\frac{1}{4} + \frac{3}{4} = \frac{4}{4} = 1$$

Modelo probabilístico

Estos modelos identifican la distribución de probabilidad de una función determinada que relaciona las variables predictoras con las de clase y la utiliza para realizar predicciones en el futuro.



En casos en los que se requiere una alta seguridad, se limita el uso de otras soluciones de autenticación por la siguientes razones:

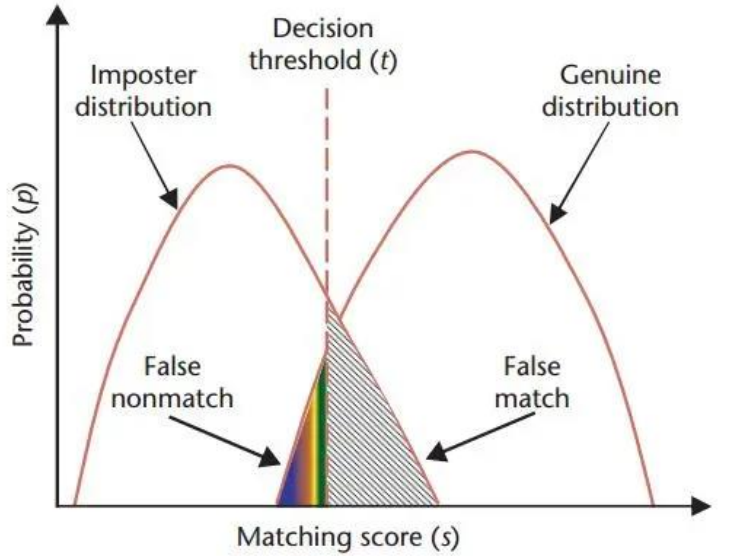
1. **El Ratio de Falsos Positivos (RFP)** no provee una fiabilidad total en la autenticación de la persona por sí mismo.

2. **La comparación biométrica es probabilística**, donde otros factores (por ejemplo, usuario/contraseña) son determinísticos.

3. **Las características biométricas no constituyen secretos**. Los datos biométricos pueden obtenerse online, tomando una imagen (cara) o a través del conocimiento de las personas, obtenida de objetos que alguien toca (huellas) o capturados con cámaras de alta resolución (iris).

https://www.electronicid.eu/es/blog/post/autenticacion-biometrica-facial-smileid/es

$$\frac{1}{4} + \frac{3}{4} = \frac{4}{4} = 1$$



https://semiengineering.com/biometrics-for-the-iot/

CÓDIGO NOTARIAL

ARTÍCULO 39.- Identificación de los comparecientes

Los notarios deben identificar, cuidadosamente y **sin lugar a dudas**, a las partes y los otros intervinientes en los actos o contratos que autoricen. Los identificarán con base en los documentos legalmente previstos para el efecto y cualquier otro que consideren idóneo.

Table 2. The comparison of approaches for fingerprint liveness detection.

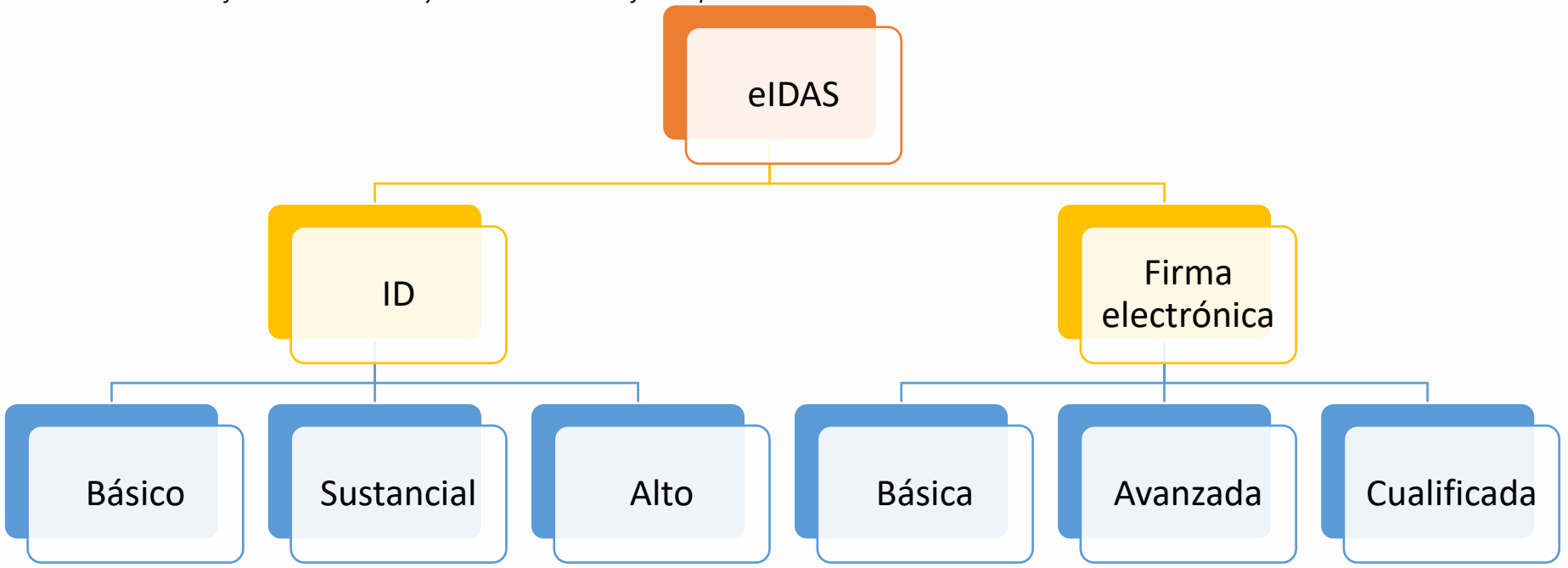
Approaches	Year of Publication	Category or Technique	Databases	Sensors	Best Performance (Correct Classification Rate)
Tan and Schuckers [24]	2006	Wavelet transform	Michigan State University (MSU) gummy finger database	Capacitive DC, optical, and electro-optical	80%–100%
Coli et al. [25]	2008	Both static and dynamic features	Private database	Optical	75.35%
Galbally et al. [26]	2012	Fingerprint parameterization based on 1uality related features	ATVS	Optical	90%
Kim [27]	2017	Difference of the dispersion in the image gradient field	LivDet 2009 and ATVS	Optical	95.63% (ATVS) 86.83% (LivDet 2009)
Jung and Heo [28]	2018	Convolutional neural network (CNN)	2015 competition set	Optical	98.60%
Kundargi and Karandikar [29]	2018	Completed local binary pattern (CLBP) and wavelet transform (WT)	LivDet 2011	Optical	91.7%
Xia et al. [30]	2018	Weber local binary and Support Vector Machine (SVM)	LivDet 2011, 2013, 2015	Optical	94.04%
Yuan et al. [31]	2018	BP neural network	LivDet 2013	Optical	93.22%

https://link.springer.com/article/10.1007%2Fs00500-018-3182-1

Existen **tres** "**factores**" principales para la **autenticación**: un **factor** de conocimiento (algo que conoces, por ej., una contraseña o un PIN), un **factor** de posesión (algo que tienes, por ej., un dispositivo móvil o una tarjeta de id.) y un **factor** de inherencia (algo que eres, por ej., una huella digital o tu voz).
https://experience.dropbox.com/es-la/resources/what-is-2fa

Identificación(autenticación) y firma no es lo mismo

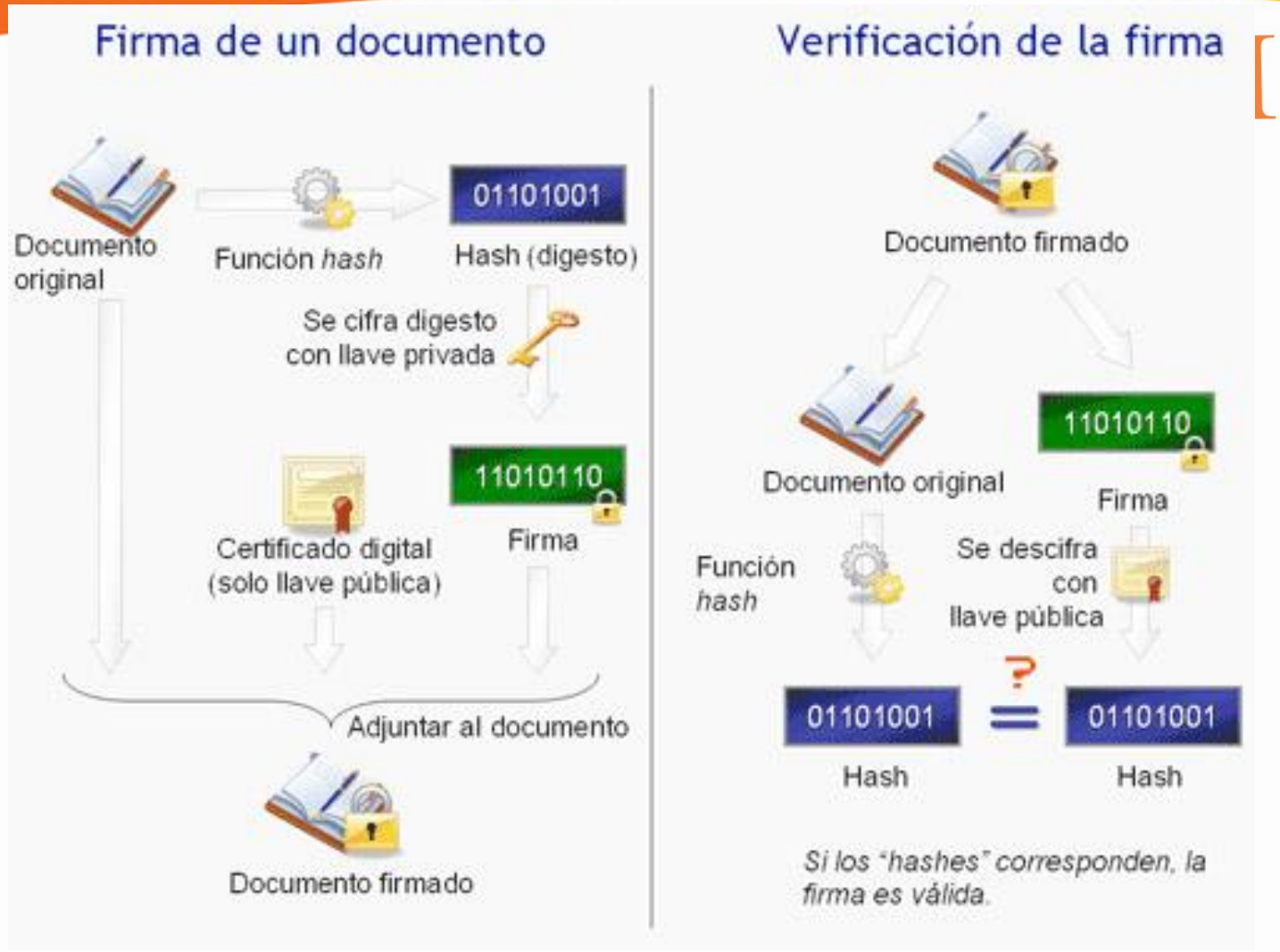
Reglamento relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior



https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910&from=ES#d1e1274-73-1

Situación en Costa Rica (ley 8454):

- Sólo regula firma digital, no firma electrónica
- Se excluyen áreas de aplicación de firma digital
- Se da valor equivalente a la firma manuscrita a la firma digital (no habla de certificada)
- Se da presunción de autoría a la firma digital certificada, pero no dispensa formalidades de autenticación



https://www.soportefirmadigital.com/web/es/que-es-firma-digital.html

Conclusiones :

- Todo mecanismo de identidad biométrico es probabilístico.

- El único modelo determinista (punto de vista técnico y legal) de identidad al día de hoy, tanto en Costa Rica como en la normativa comparada europea es la firma digital certificada.

- Existen retos regulatorios porque Costa Rica sólo norma un mecanismo específico de firma –sujeto a discusión-, no regula ningún mecanismo de identificación.

Recomendaciones:

- Interpretar el concepto de “sin lugar a dudas” de la legislación.

- Valorar los espacios que una norma secundaria como un reglamento; puede cubrir en concordancia con la legislación, sobre definiciones de niveles aceptables de identificación de personas.

- Valorar el uso de mecanismos tecnológicos como herramientas para identificar y garantizar la integridad de archivos o cosas.

VI CONGRESO DERECHO NOTARIAL
COSTA RICA 2021

Muchas gracias….

DNN Dirección Nacional de Notariado