



UNITAT 6

SERVEIS DE SIGNATURA ELECTRÒNICA (ENVIAFIB)

CONTINGUTS

1 Serveis de signatura electrònica.....	2
Infraestructura de clau pública PKI.....	2
Què és un certificat electrònic?	2
Què és una autoritat de certificació?	2
Contingut d'un certificat electrònic.....	4
Marc normatiu de signatura electrònica.....	4
Conceptes bàsics de signatura electrònica.....	5
Tipologia de signatura electrònica	5
Validació i impressió de documents signats.....	6
Validar la signatura electrònica	6
Imprimir un document signat.....	7
2 Signatura de documents electrònic amb ENVIAFIB	9
Què és ENVIAFIB ?	9
Com funciona ENVIAFIB.....	9
Quins tipus de signatures puc fer amb ENVIAFIB?	11

OBJECTIUS

1. Aprendre què són els serveis de signatura: la infraestructura KPI, marc normatiu i conceptes bàsics de la signatura electrònica
2. Conèixer el funcionament de l'aplicació ENVIAFIB
3. Entendre el funcionament dels fluxos de firmes.



Autor/a: Departament de Desenvolupament Tecnològic

Data d'elaboració: 01/01/2026

Aquesta obra es difon mitjançant la llicència [Creative Commons Reconeixement-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/).



1 Serveis de signatura electrònica

Infraestructura de clau pública PKI

1..1 Què és un certificat electrònic?

És l'únic mitjà que permet garantir tècnicament i legalment la identitat d'una persona a Internet. Es tracta d'un requisit indispensable perquè les institucions puguin oferir serveis segurs a través d'Internet.

El certificat electrònic és un fitxer electrònic que conté un conjunt de dades per tal d'identificar el seu propietari.

Amb un certificat electrònic es pot intercanviar informació amb altres persones i entitats de forma segura, i signar electrònicament dades per a comprovar la seva procedència i integritat.



Figura 1: Propietats d'un certificat electrònic.

La normativa Europea eIDAS estableix les condicions que tots els Estats membres hauran de reconèixer els mitjans d'identificació electrònica de les persones físiques i jurídiques que pertanyin a un sistema d'identificació electrònica notificat d'un altre estat membre.

Defineix els següents tipus de certificats:

- **Certificats de signatura:** vincula les dades de validació d'una signatura amb una persona física i confirma, almenys, el nom o el pseudònim d'aquella persona.
- **Certificats de segell:** vincula les dades de validació d'un segell amb una persona jurídica i confirma el nom d'aquella persona.
- **Certificats d'autenticació web:** permet autenticar un lloc web i el vincula amb la persona física o jurídica a qui s'ha expedit el certificat.
- **Certificats no-qualificats** (SSL per establir connexions segures a Internet, certificats de component,...).

1..2 Què és una autoritat de certificació?

L'Autoritat de Certificació (AC) és una entitat de confiança, responsable d'emetre i revocar els certificats digitals, utilitzats en la signatura electrònica.



A part d'aquestes funcions bàsiques, l'Autoritat de Certificació pot proporcionar altres serveis, com la publicació de certificats, publicació de llistes de certificats revocats, serveis de comprovació de validesa dels certificats, etc.

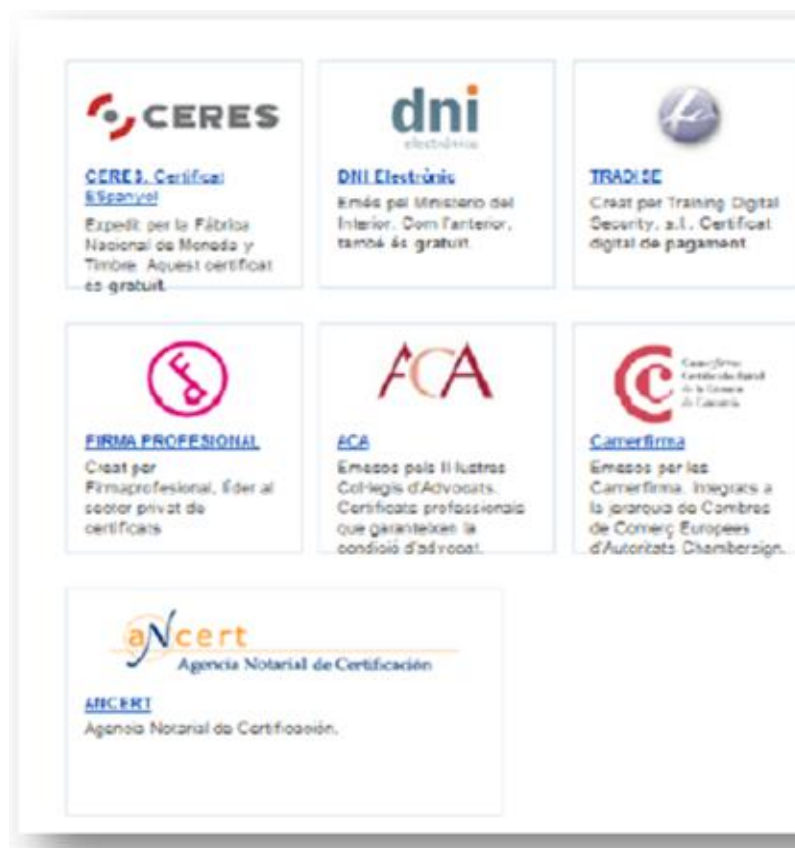


Figura 2: Autoritats de certificació.

L'AC disposa dels seus propis certificats amb els quals signa els certificats que emet organitzats de forma jeràrquica. Una jerarquia de certificació consisteix en una estructura jeràrquica d'AC en la qual es parteix d'una AC arrel, i a cada nivell, existeix una o més AC que poden signar certificats d'entitat final.

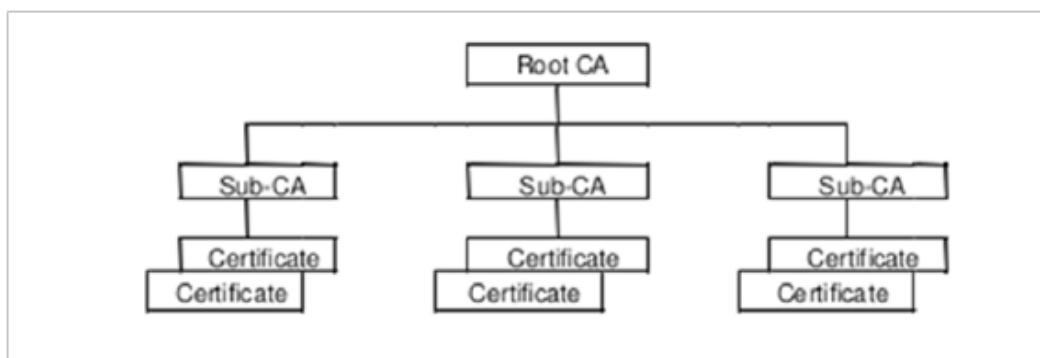


Figura 3: Jerarquia de certificació.



L'AC, per si mateixa o mitjançant la intervenció d'una Autoritat de Registre, verifica la identitat del sol·licitant d'un certificat abans de la seva expedició.

Finalment, l'AC, mitjançant funcions criptogràfiques, crea el certificat a partir de les dades verificades anteriorment i garanteix, mitjançant una signatura electrònica, la validesa del certificat creat. Si el certificat ha estat signat electrònicament per una AC, l'anomenem certificat reconegut.

1..3 Contingut d'un certificat electrònic

Si obrim el fitxer del certificat podem veure la informació de la clau pública. S'obren 3 pipelles:

- **General:** es pot veure el nom del propietari del certificat i la data de validesa.
- **Detalls:** conté informació tècnica sobre la generació del certificat i del seu contingut.
- **Ruta de certificació:** defineix la cadena jeràrquica de certificació que dona validesa al certificat. Normalment, aquesta cadena està formada per un certificat arrel que signa un certificat intermedi i aquest és el que s'utilitza per signar el nostre certificat.

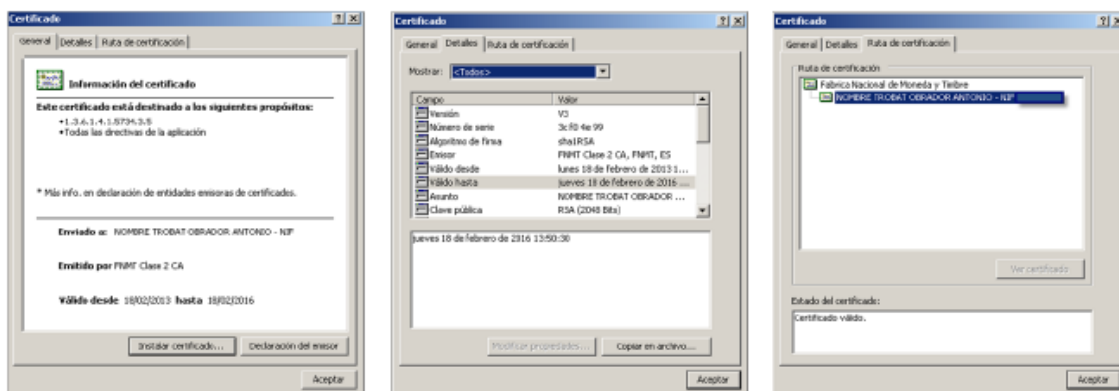


Figura 4: Informació de la clau pública del certificat electrònic.

Marc normatiu de signatura electrònica

L'article 10 (Llei 39/2015) regula els sistemes de signatura electrònica que pot emprar l'interessat. Els sistemes de signatura electrònica han d'acreditar l'autenticitat de la signatura, així com la integritat i la inalterabilitat del document. Aquests sistemes de signatura són:

- **Sistemes de signatura electrònica reconeguda o qualificada i avançada** basats en certificats electrònics reconeguts o qualificats.
- **Sistemes de segell electrònic reconeguts o qualificats i de segell electrònic avançat** basats en certificats electrònics reconeguts o qualificats.
- **Qualsevol altre sistema** que es consideri vàlid.

L'article 43 (Llei 40/2015) regula la signatura electrònica del personal de les administracions públiques. Diu que:



- Els documents electrònics s'han de signar amb signatura electrònica basada en certificats.
- La signatura electrònica podrà identificar el titular del lloc de treball i càrrec junt amb l'Administració per la qual fa feina. Aquest fet, dona lloc a la creació de certificats electrònics d'empleat públic.
- Per raons de seguretat, els sistemes de signatura es podran referir només a la identificació professional de l'empleat públic. Aquest fet, dona lloc a la creació de certificats d'empleat públic amb pseudònim.

Conceptes bàsics de signatura electrònica

Una signatura electrònica és un conjunt de dades electròniques que acompanyen o estan associades a un document electrònic i que:

- Identifiquen el firmant.
- Asseguren la integritat del document signat.
- Garanteixen el no-repudi en l'origen (el que ha signat no pot negar que hagi estat ell qui ha signat).

Per signar un document és necessari disposar d'un certificat digital o un DNI electrònic. Aquests contenen unes claus criptogràfiques (pública i privada) que són els elements necessaris per signar.

Aquestes claus són complementàries, això vol dir que tot allò que es xifra amb la clau privada només pot ser desxifrat amb la seva clau pública; per tant, podem saber sense dubte qui és l'emissor del missatge.

La clau privada s'emmagatzema en una targeta criptogràfica protegida per un PIN i no es pot compartir. En canvi, la clau pública s'emmagatzema en el certificat electrònic del signant i pot ser compartida.

Tipologia de signatura electrònica

Segons la normativa es distingeixen els següents tipus de signatura electrònica:

- **Signatura electrònica avançada.** És la signatura electrònica que està vinculada al seu signant de manera única i intransferible. Permet la seva identificació. Està basada sobre certificats electrònics, però no són certificats electrònics reconeguts o qualificats (emesos per una Autoritat de Certificació -AC). Garanteix l'autenticitat i integritat d'un document signat.
- **Signatura electrònica reconeguda o qualificada.** És la signatura electrònica avançada, però basada en un certificat electrònic reconegut o qualificat i està generada mitjançant un dispositiu qualificat de creació de signatures. **La signatura electrònica reconeguda o qualificada és la única que pot ser considerada equivalent a la signatura manuscrita.**



En resum, la signatura electrònica reconeguda o qualificada ha de:

1. Identificar el firmant.
2. Verificar la integritat del document signat.
3. Garantir el no-repudi en l'origen (el que ha signat no pot negar que hagi estat ell qui ha signat).
4. Comptar amb la participació d'un tercer de confiança (Autoritat de Certificació)
5. Estar basat en un certificat electrònic reconegut o qualificat.
6. Estar generada per un dispositiu qualificat de creació de signatures.

Els 4 primers punts són possibles gràcies a l'ús de claus criptogràfiques contingudes en el certificat i a l'existència d'Autoritats de Certificació. A més a més, ha d'estar basada en un certificat reconegut o qualificat.

El dispositiu segur ha de garantir que les claus siguin úniques, que la clau privada no es pugui deduir de la pública i viceversa, que el signant pugui protegir de forma fiable les claus, que no s'alteri el contingut del document original i que el signant pugui veure què és el que va a signar.

Validació i impressió de documents signats

1..4 Validar la signatura electrònica

Per això, és més recomanable utilitzar qualche servei qualificat per validar la signatura. Per exemple, podem fer servir el [servei VALIDE](#) de validació de certificats i signatura electrònica, que permet una validació completa de la signatura.

Figura 5: Interfície gràfica de Valide.

1.5 Imprimir un document signat

La impressió d'un document signat per una administració ha de proporcionar alguna manera de poder validar que el document original que té l'administració és el mateix que està imprès. Per això el procés d'impressió del document signat reflectirà en el document en paper, a banda del contingut del document, la informació següent:

- **Codi segur de verificació (CSV)**, per la seva posterior verificació a la seu electrònica
- **Dades de representació de la signatura.**

L'exemplar imprès del document electrònic constituirà el justificant de signatura del document electrònic.

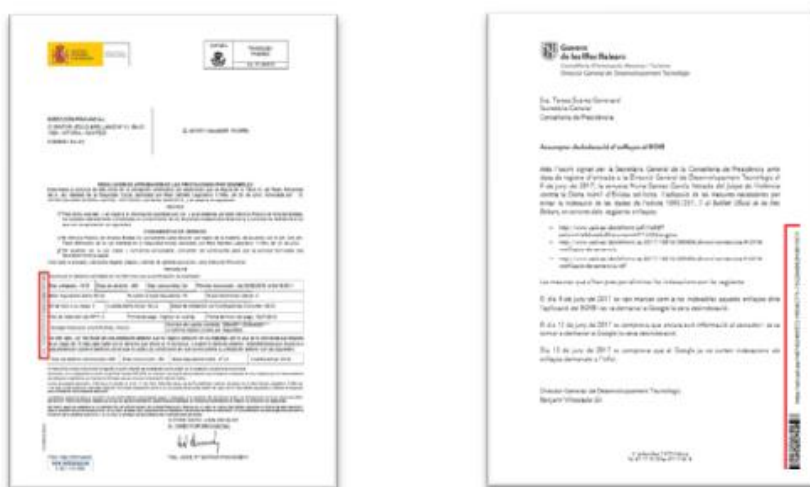


Figura 6: Document signat amb CSV.

El CSV haurà de ser únic i estarà associat a un únic document. A més, es requereix una ordre o resolució del titular de l'organisme públic, que ha de descriure el funcionament del sistema que s'utilitza per generar el CSV.

Al GOIB l'eina per validar el document imprès s'anomena CONCSV i es troba disponible a la Seu Electrònica (<https://csv.caib.es>).



Figura 7: Interfície gràfica de CONCSV.



Mitjançant aquesta eina, l'interessat pot introduir el codi CSV del document i si hi ha un document electrònic associat a ell, es mostrarà a l'usuari una vista del document juntament amb informació de la validesa de la signatura electrònica. D'aquesta manera, l'interessat pot accedir al document, verificar la seva integritat i contrastar-lo amb el que ell té imprès.



2 Signatura de documents electrònic amb ENVIAFIB

Què és ENVIAFIB ?

ENVIAFIB És una aplicació web que permet enviar a signar documents electrònics administratius que es troben fora de l'àmbit de gestió d'un expedient administratiu. Permet a l'usuari signar documents ell mateix i enviar a signar un o varis documents a tercers persones. Aquestes persones poden ser tant personal intern de GOIB com persones externes.

ENVIAFIB facilita la gestió de peticions de signatura i la descàrrega dels documents firmats. A més està integrada amb l'Arxiu Electrònic del Govern per tal de garantir l'arxivat i conservació al llarg del temps dels documents signats. No és necessari tenir coneixements tècnics avançats per emprar ENVIAFIB, ja que ha estat dissenyada per ser intuïtiva i fàcil d'utilitzar per tots els usuaris.

Govern de les Illes Balears | EnviaFIB | DRASSANA

GOVERN DE LES ILLES BALEARS | USUARI | [usuari] | [Enviar document a signar] | [FAQs]

Llistat de Peticions de Firma

Eliminar seleccionats

Títol: [] Creada des de... [] Fins a... [] Cercar Neteja [x]

Estat: [] Finalitzada des de... [] Fins a... []

Mostrant registres del 1 al 9 de 9 registres

ID	Títol	Creada	Finalitzada	Tipus documental	Estat	Accions
14553	Autorització PINBAL AEAT procediment CODSVDR_GBA_20121107	25/10/2024 9:13:50	25/10/2024 11:56:34	TD14-001 Sol·licitud	[Verde]	[Accions]
1221	Autorització PINBAL AEAT Pel procediment 2893190 (corregit)	9/1/2024 12:40:22	10/1/2024 6:00:03	TD14-001 Sol·licitud	[Verde]	[Accions]
1200	Autorització PINBAL AEAT Pel procediment 2893190	27/12/2023 10:20:14	29/12/2023 6:00:03	TD14-001 Sol·licitud	[Verde]	[Accions]
1141	Test firma personalitzada b2	11/12/2023 10:50:50	12/12/2023 6:00:08	TD10-001 Acta	[Verde]	[Accions]
1140	Test Autofirma 3	11/12/2023 10:48:30	12/12/2023 6:00:05	TD10-001 Acta	[Verde]	[Accions]
1060	Test-DI_Catastro_Bienes_e_inmuebles_v2.9.pdf	21/9/2023 9:23:56		TD10-001 Acta	[Amarillo]	[Accions]
1002	Test plantilla de firma-Test FIRMA 1.pdf	14/9/2023 13:05:43	14/9/2023 13:16:37	TD02-001 Acord	[Verde]	[Accions]
1001	Test Firma Personalitzada-TEST_FIRMA.pdf	14/9/2023 12:49:44	14/9/2023 12:52:04	TD02-001 Acord	[Verde]	[Accions]
1000	Test Autofirma 1	14/9/2023 12:39:16	14/9/2023 12:48:05	TD02-001 Acord	[Verde]	[Accions]

1

Elements per pàgina: 10

EnviaFIB v2.0.1
Buitat: 02/12/2024 13:19
J2K: 118.16.1-1475-1
Revisió: 38/2018
Desenvolupat per Data de Govern Digital (Fundació DT)

DRASSANA

Necessites Ajuda?

Figura 8: Pantalla principal d'ENVIAFIB.

Com funciona ENVIAFIB

L'aplicació **ENVIAFIB** ofereix una interfície d'usuari intuïtiva i fàcil d'utilitzar per tal de facilitar la gestió de les peticions de firma. A continuació, es detallen els elements clau de la interfície de l'aplicació:

Menú superior

La barra de menú es troba a la part superior de la pantalla i conté les opcions de navegació i les funcionalitats principals de l'aplicació. Aquí trobareu els següents botons:

- **"Enviar document a signar"**: Aquest botó us permetrà iniciar el procés d'enviament d'una nova petició de firma. Al fer clic sobre aquest botó, s'obrirà un desplegable



amb els diferents tipus de peticions disponibles. Podeu seleccionar el tipus de petició desitjat des d'aquest desplegable.

- **Botó de FAQ's:** Aquest botó us permetrà accedir a l'ajuda en línia de l'aplicació.
- **Desplegable de configuració:** Aquest desplegable us ofereix diverses opcions de configuració de l'aplicació. Podeu editar les dades d'usuari o sortir de l'aplicació des d'aquest desplegable.

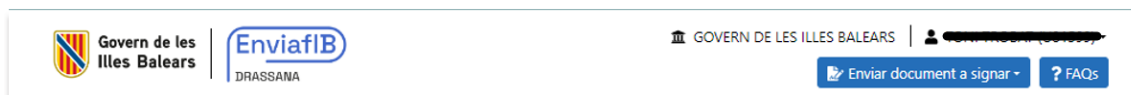


Figura 9: Menú superior d'ENVIAFIB.

Llistat de peticions

El llistat de peticions és una de les vistes principals de l'aplicació **ENVIAFIB**, on es mostren les diferents peticions creades i el seu estat actual. Aquesta secció proporciona una descripció del llistat de peticions i les funcionalitats disponibles.

- **Visualització de les peticions:** En aquesta vista, es mostra un resum de cada petició, incloent informació com l'estat de la petició, el destinatari, la data d'enviament i altres detalls rellevants. Cada fila del llistat representa una petició individual.
- **Ordenació i filtrat:** Per facilitar la gestió de les peticions, el llistat permet l'ordenació i el filtrat dels resultats. Es poden ordenar les peticions segons diferents criteris, com la data d'enviament o l'estat. A més, hi ha opcions de filtrat per mostrar només les peticions d'un estat determinat o d'un destinatari específic.

ID#	Títol#	Creada#	Finalitzada#	Tipus documental#	Estat#	Accions
517010	Carta certificació regweb	27/11/2025 13:39:24	27/11/2025 13:40:51	TD06-002 Carta	Firmada	Accions
451228	Formulari per actualitzar dades de contacte a la Plataforma de Intermediación de Datos (PID)	24/10/2025 9:13:07	24/10/2025 9:41:05	TD14 Sol·licitud	Firmada	Accions
439956	Formulari AEAT per autoritzar consulta de serveis de PINBAL a l'entorn de preproducció	17/10/2025 10:14:11	17/10/2025 12:57:45	TD14 Sol·licitud	Firmada	Accions
273908	Test 20MB	20/6/2025 8:57:31	20/6/2025 8:59:38	TD06-010 Nota interna	Firmada	Accions
162094	Comunicació sol·licitud usuari representant/auditor PINBAL	7/4/2025 10:39:18	7/4/2025 10:41:04	TD06 Comunicació	Firmada	Accions

Figura 10: Llistat de peticions d'ENVIAFIB.

Accions disponibles:

- **Visualitzar detalls:** Al fer clic en una fila de la taula, es pot accedir als detalls de la petició. Aquí es mostrarà informació més completa sobre la petició, incloent l'historial d'estats i altres dades relacionades.
- **Descarregar fitxers:** Si una petició està en estat "Firmada", l'usuari té l'opció de descarregar els fitxers relacionats amb la petició. Això pot incloure la versió imprimible del document, la versió en format ENI (intercanvi electrònic de documents) i el document original signat.
- **Consular estat de signatura:** En cas que una petició estigui en estat "Pendent" es pot consultar quins usuaris han signat la petició de signatura.



- **Enviar per correu electrònic:** Si una petició està en estat "Firmada", l'usuari té l'opció d'enviar el document signat a un altra usuari per correu electrònic.

Quins tipus de signatures puc fer amb ENVIAFIB?

ENVIAFIB permet fer diversos tipus d'enviaments de firma depenent de qui és el destinatari o destinataris que han de firmar el document:

- **Autofirma.** És una opció on el mateix usuari signa un document des de la mateixa aplicació **d'ENVIAFIB**. Aquesta opció de firma només permet signar documents d'un en un. A continuació podeu veure un vídeo de com podeu signar un document amb aquesta opció: <https://youtu.be/GYRnw2kIVSo>
- **Enviar al Director General / Enviar al Secretari General.** Permet enviar a signar un o varis documents al director general de la unitat orgànica on està adscrit l'usuari **d'ENVIAFIB** o en el cas, al secretari general de la conselleria on està ubicada la unitat orgànica on està adscrit l'usuari **d'ENVIAFIB**. A continuació podeu veure un vídeo de l funcionament d'aquesta opció: <https://youtu.be/VYAq7awXXXg>
- **Enviar a signar un document a una altra persona.** La Firma personalitzada permet enviar a signar un o varis documents a una persona. Per això haurem d'utilitzar l'assistent de fluxos de signatura seleccionar l'usuari al que volem enviar el document a signar. L'usuari destinatari de l'enviament de signatura ha de ser usuari de **PORTAFIB**. A continuació es pot veure un vídeo de com enviar un document a signar a una altra persona https://youtu.be/3e08R6fk_48
- **Enviar a signar un document a varis signants establint un ordre en els signants.** La Firma personalitzada permet enviar a signar un o varis documents a varies persones definint l'ordre en el que han de signar el document. Per això haurem d'utilitzar l'assistent de fluxos de signatura seleccionar els usuaris que volem que signin i definir l'ordre dels signants. Els usuaris destinataris de l'enviament de signatura han de ser usuaris de **PORTAFIB**. A continuació es pot veure un vídeo explicatiu de com fer-ho: https://youtu.be/_GrJr-nOhpTQ
- **Enviar a signar un document sense establir un ordre en els signants.** La Firma personalitzada permet enviar a signar un o varis documents a varies persones de forma que sigui indiferent l'ordre dels signants. Per això haurem d'utilitzar l'assistent de fluxos de signatura i seleccionar els usuaris que volem que signin el document. Els usuaris destinataris de l'enviament de signatura han de ser usuaris de **PORTAFIB**. A continuació es pot veure un vídeo explicatiu de com fer-ho: <https://youtu.be/e61S5hpaTss>
- **Enviar a signar un document a persones externes a GOIB.** La Firma Personalitzada permet enviar a signar un o varis documents a varies persones entre elles persones externes a GOIB. Per això haurem d'utilitzar l'assistent de fluxos de signatura i seleccionar els usuaris que volem que signin el document. Com a part del flux l'assistent de creació fluxos de signatura ens deixarà definir un usuari extern a GOIB que formarà part del flux de signatura. Prèviament per poder definir l'usuari extern hem de conèixer el seu NIF, nom complet i correu



electrònic. Quan hagi de signar el document l'usuari extern rebrà un correu electrònic amb un enllaç a una pàgina web des d'on podrà signar el document. A continuació es pot veure un vídeo explicatiu de com fer-ho:

<https://youtu.be/U1KevkqwsXo>

- **Els meus fluxos:** permet fer peticions de firma utilitzant fluxos de firma que ja ha creat i guardat abans l'usuari. Amb aquesta opció podem agilitzar el procés de signatura quan l'usuari envia a signar els documents als mateixos signants. Per això haurem d'utilitzar l'opció de Plantilles de flux de firmes, accessible des del mateix botó d'enviar a signar, per configurar els nostres propis fluxos de firma i després, per enviar el document o documents a signar l'usuari utilitzant aquestes plantilles de flux de firma, ha d'anar a la opció de Els meus fluxos per crear l'enviament de signatura amb la plantilla de flux que ha definit amb anterioritat. A continuació es pot veure un vídeo explicatiu de com fer-ho:

<https://youtu.be/-mcmEyT5aB4>





BIBLIOGRAFIA

Llei 39/2015 del procediment administratiu comú de les administracions públiques.
<https://boe.es/buscar/act.php?id=BOE-A-2015-10565>

RD 3/2010 pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330

Reglamento UE 910/2014 del parlamento europeo y del consejo 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/PDF/?uri=CELEX:32014R0910&from=IT>

Jerarquia entitats de certificació
<https://www.securityartwork.es/2013/06/12/fundamentos-sobre-certificados-digitales-iii-cadena-de-confianza/>

Criptografia asimétrica
https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

Función de Hash https://es.wikipedia.org/wiki/Funci%C3%B3n_hash

Proceso de signatura electrónica. https://arturomesc.files.wordpress.com/2012/10/proceso_signatura_electronica.png

Validació de signatura electrònica. <https://valide.redsara.es/valide/validarFirma/ejecutar.html>

Eina per a la signatura de documentació electrònica ENVIAFIB https://www.caib.es/sites/administracioelectronica/ca/n/enviafib_substituira_a_ibkey_per_a_signar_documents/