

Formación Digital para el Asociacionismo de Mujeres

1

El proyecto y su redacción

- ✓ **¿Un proyecto para qué?**
- ✓ **Esqueleto de un proyecto**
 - Errores comunes

2

E-administración: una realidad que no podemos eludir

- ✓ **Definición**
- ✓ **Normativas**
 - Respecto a la Administración
 - Respecto a la ciudadanía
- ✓ **¿Qué es necesario para materializar esta relación electrónica?**
 - Servidor seguro
 - Certificado digital
 - Firma electrónica avanzada
 - Prestador de Servicios de Certificación

- ✓ **Y... ¿Cómo nos identificamos nosotras?**

- Tarjeta ciudadana
- Representante de entidad
- B@k y B@kQ
- Juego de Barcos
- Dni Electrónico

- ✓ **Tenemos certificados...¿Y, ahora qué?**
 - Puesta en marcha de los certificados
 - Nuestros equipos ¿Necesitan algo más?

2

E-administración: una realidad que no podemos eludir

- ✓ **Proceso de firma electrónica con certificado**

 - Utilizando el applet de Id@zki

 - Utilizando Id@zki deskopt

- ✓ **Proceso de firma electrónica con Juego de barcos**

- ✓ **¡Vamos a tramitar!**

 - Ámbito Estatal

 - Ámbito Autonómico

 - Ámbito Provincial

¿Un proyecto para qué?

La necesidad de elaborar proyectos, en el ámbito asociativo, nace como consecuencia del **deseo de mejorar la realidad en la que vivimos.**

Supone un **avance anticipado de las acciones a realizar para conseguir unos determinados objetivos.** Es, por tanto, un plan de trabajo que tiene como misión la de **prever, orientar y preparar bien el camino** de lo que se va a hacer y cumple al menos alguna de las siguientes **funciones** (si no todas):

- ⦿ Ayudarnos a **definir y ordenar las actividades que queremos realizar** a lo largo de un periodo de tiempo (habitualmente un año)
- ⦿ Nos sirve de herramienta (por contener objetivos, personas destinatarias, actividades y metodologías...) para lograr la **colaboración de otras personas y/o entidades o administraciones** en la ejecución del mismo.
- ⦿ Hacer más sencillo el **seguimiento y la evaluación de resultados**



Esqueleto de un proyecto

Formular un proyecto exige **armonizar todos los hitos** que nos llevarán a la consecución del mismo; tanto la fase de diagnóstico de necesidades, de identificación de objetos, de especificación de actividades, de tiempo de ejecución, así como los recursos de que se dispone para llevar a cabo el proyecto.

Por lo tanto, **comporta dar respuesta a las siguientes cuestiones:**

¿QUÉ?

¿Qué se va a hacer?
→ **Naturaleza del proyecto**

Definición de la idea central del proyecto identificando el programa del que forma parte y la necesidad que lo origina.

¿POR QUÉ?

¿Por qué se va a hacer?
→ **Origen y fundamento**

Antecedentes que detectó el diagnóstico y la justificación.

¿PARA QUÉ?

¿Para qué se va a hacer?
→ **Objetivos**

Son los logros que se pretende alcanzar con la ejecución de una acción.

¿PARA QUIÉNES?

¿Para quienes?
→ **Personas destinatarias**
Identificar las personas destinatarias directas e indirectas.

¿HASTA DÓNDE?

¿Cuánto se quiere hacer?
→ **Metas**

Cuánto queremos alcanzar de cada objetivo y de que calidad es lo que queremos alcanzar.

¿DÓNDE?

¿Dónde se quiere hacer?
→ **Localización física**

Determinación restringida del territorio donde se ubicará, señalando el lugar específico.

¿CÓMO?

¿Cómo se quiere hacer?
→ **Actividades y tareas a realizar. Metodología**

Acciones y procedimientos necesarios para alcanzar las metas y objetivos propuestos.

¿CUÁNDO?

¿Cuándo se quiere hacer?
→ **Calendario y agenda de actividades**

¿QUIÉNES?

¿Quiénes lo van a hacer?
→ **Recursos humanos**

Cantidad y calidad de personas que son necesarias para la ejecución de las actividades.

¿CON QUÉ?

¿Con qué se va a hacer?
→ **Recursos materiales**

Instalaciones necesarias, los materiales, los instrumentos y los equipos.

¿CÚANTO?

¿Cómo se va a costear?
→ **Recursos financieros**

Presupuesto y la financiación

EVALUACIÓN

Eficacia y eficiencia

Cómo haremos la evaluación, en qué momentos, quiénes la realizarán y qué se analizará con sus respectivos indicadores.

Esqueleto de un proyecto

En la elaboración y redacción de un proyecto, a modo de ‘check-list’, podemos prever los siguientes puntos:

- Nombrar o denominar el proyecto
- Descripción del mismo
- Fundamentar o justificar
- Marco institucional
- Finalidad
- Objetivos (general, específicos y operativos)
- Personas destinatarias
- Localización física y ámbito territorial
- Actividades y tareas
- Metodología y estilo
- Calendario y Agenda de actividades
- Administración del proyecto
- Recursos (Humanos, materiales, técnicos y económicos)
- Presupuesto
- Evaluación
- Factores Externos

*Información basada en
“Redacción de proyectos”
publicado en la página web de
Bolunta*
[http://www.bolunta.org/manual-
gestion/proyectos2c.asp](http://www.bolunta.org/manual-gestion/proyectos2c.asp)

Errores comunes

Con la finalidad de minimizar la posibilidad de cometer errores muy comunes en la elaboración, redacción y justificación de proyectos para la institución de Emakunde distinguiremos entre:

1- Errores 'de base'

Son aquellos que se cometen como consecuencia de una **no lectura y posterior adecuación del proyecto**:

- ⊙ **A las [BASES de la convocatoria en curso](#)**. Las bases son modificadas todos los años y, es imprescindible, adecuar la redacción del proyecto tanto al objeto de la convocatoria como a los apartados más operativos; actividades subvencionables o no subvencionables, fechas de presentación, condiciones de pago o entidades subvencionables.
- ⊙ **Al Plan por la Igualdad entre mujeres y hombres de la CAE**. Está vigente aún al [VI Plan por la igualdad](#) pero se prevé que, en breve, se publicará el **VII Plan por la Igualdad**.

Errores comunes

Falta de adecuación del proyecto a las bases* de la convocatoria.

- ✓ Es imprescindible leérselas bien siempre ya que **son modificadas todos los años.**
- ✓ Especialmente el apartado que describe las actividades subvencionables o no. Este año pasado el apartado 4.

**Descarga correcta de PDFs contemplada más adelante.*

(ASOCIACIONISMO Y PARTICIPACIÓN) Subvenciones, durante el ejercicio 2017, para fomentar el asociacionismo y potenciar la participación de las mujeres en todos los ámbitos de la Comunidad Autónoma de Euskadi.

[ASM 2017]

Emakunde - Instituto Vasco de la Mujer

✘ Cerrado el plazo de presentación de solicitudes

Imprimir Enviar

Mostrar página completa

Resumen

Solicitud y otros trámites

Resolución y recursos

Contacto

Objeto

Es objeto de la presente Resolución la regulación de las subvenciones a conceder por Emakunde-Instituto Vasco de la Mujer a asociaciones y federaciones de mujeres sin ánimo de lucro y fundaciones cuyo único fin y ámbito de actuación sea el de la promoción de las mujeres, para la realización de proyectos concretos relacionados con los fines y objetivos del Instituto en el ejercicio de 2017 en los términos señalados en los artículos siguientes y dentro de los límites que determinan los créditos.

Dotación presupuestaria

376.000

Normativa aplicable

RESOLUCIÓN de 22 de noviembre de 2016, de la Directora de Emakunde-Instituto Vasco de la Mujer, por la que se regula la concesión de subvenciones, durante el ejercicio 2017, para fomentar el asociacionismo y potenciar la participación de las mujeres en todos los ámbitos de la Comunidad Autónoma de Euskadi.

Normativa reguladora

Organismo que convoca

- Emakunde - Instituto Vasco de la Mujer / Dirección de EMAKUNDE > **Secretaría General de EMAKUNDE**

Organismo que resuelve

- Emakunde - Instituto Vasco de la Mujer / Dirección de EMAKUNDE > **Secretaría General de EMAKUNDE**

Apartado 4

Artículo 4.– Actividades subvencionables.

1.– En el marco del VI Plan para la Igualdad de Mujeres y Hombres en la CAE y en consonancia con los fines del Instituto, los proyectos o actividades a subvencionar, que se desarrollarán entre el 1 de enero y el 31 de diciembre de 2017, deberán ir dirigidos a la realización de:

- ✓ Programas de difusión de los derechos de las mujeres desde la diversidad, de la historia del movimiento de mujeres y del pensamiento feminista, en especial desde el marco internacional de la Convención sobre la Eliminación de Todas las Formas de Discriminación contra las Mujeres (CEDAW).
- ✓ Programas de generación de referencias y genealogías de las mujeres.
- ✓ Programas de actividades orientados a dinamizar, motivar e impulsar el movimiento asociativo de las mujeres que contribuyan a su empoderamiento y que creen, fomenten y fortalezcan las redes de asociaciones de mujeres que trabajen a favor de la igualdad de mujeres y hombres especialmente aquellos programas que contemplen la diversidad.
- ✓ Programas para potenciar, mediante la realización de actividades, la participación de todas las mujeres en todos los ámbitos de la vida política, económica, social y cultural, fomentando el asociacionismo de éstas, así como la coordinación del movimiento asociativo existente en la Comunidad Autónoma de Euskadi.
- ✓ Programas de información y sensibilización social sobre la igualdad de mujeres y hombres, así como iniciativas que promuevan una imagen igualitaria, diversa y no estereotipada de las mujeres y los hombres en los medios de información y comunicación.
- ✓ Programas que fomenten la corresponsabilidad de los hombres en las tareas y responsabilidades domésticas y de cuidados, y que persigan un reparto más racional e igualitario del tiempo personal, social, familiar y laboral.
- ✓ Programas formativos en materia de igualdad en los diferentes ámbitos: educación, cultura, deporte, formación-empleo, salud, participación social, diversidad etc.
- ✓ Los proyectos de aprendizaje de habilidades (artesanía, electricidad, cocina, carpintería, etc.) para ser susceptibles de ser subvencionados deberán ser complementados con otras actividades de sensibilización, información o formación en materia de igualdad de mujeres y hombres y/o tener integrada la visión de género.

Errores comunes

Apartado 4

2.– **No serán subvencionables más de tres proyectos por entidad** ni tampoco los siguientes:

- Proyectos que constituyan actividades de ocio exclusivamente.
- Proyectos que tengan como objetivo financiar servicios y otras acciones a ofertar a otras entidades.
- Proyectos que no incorporen el enfoque de género.

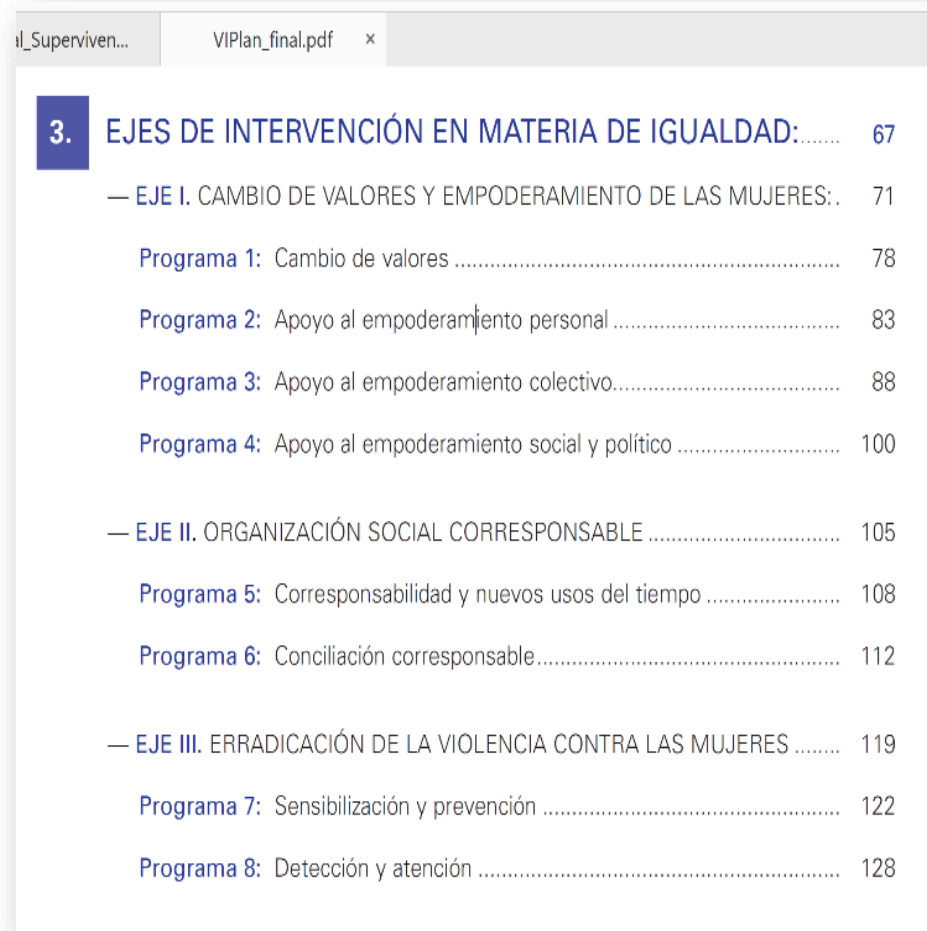
3.– En el supuesto en el que el objeto de una solicitud presentada no sea coincidente con el de esta línea subvencional, pero se considere por parte del órgano gestor que tiene encaje en otra línea de ayudas de Emakunde-Instituto Vasco de la Mujer que esté en fase previa a la resolución administrativa, podrá acordar la incorporación de la solicitud a la línea de ayudas que considere más ajustada a su objeto. La unidad gestora de la línea a la que se presentó inicialmente la solicitud dará traslado de ésta a la unidad gestora de la línea de ayudas en la que finalmente se va enmarcar, lo cual se notificará a la entidad solicitante, al objeto de que en el plazo de diez días a contar desde el siguiente a la recepción de la notificación pueda formular las alegaciones que estime pertinentes. Transcurrido dicho plazo sin mediar oposición por parte de la entidad solicitante se entenderá que el traslado de línea es aceptado.

Errores comunes

No adecuación al Plan de Igualdad

No ajustarse a alguno de los ejes de intervención que contempla el Plan vigente.

**Ejemplo del último plan vigente; VI Plan*



3.	EJES DE INTERVENCIÓN EN MATERIA DE IGUALDAD:.....	67
—	EJE I. CAMBIO DE VALORES Y EMPODERAMIENTO DE LAS MUJERES:.	71
	Programa 1: Cambio de valores	78
	Programa 2: Apoyo al empoderamiento personal	83
	Programa 3: Apoyo al empoderamiento colectivo.....	88
	Programa 4: Apoyo al empoderamiento social y político	100
—	EJE II. ORGANIZACIÓN SOCIAL CORRESPONSABLE	105
	Programa 5: Corresponsabilidad y nuevos usos del tiempo	108
	Programa 6: Conciliación corresponsable.....	112
—	EJE III. ERRADICACIÓN DE LA VIOLENCIA CONTRA LAS MUJERES	119
	Programa 7: Sensibilización y prevención	122
	Programa 8: Detección y atención	128

2- Errores procedimentales

Son aquellos errores que cometemos bien por ‘despiste’ o por desconocimiento del procedimiento en sí mismo. Sirva como ejemplo:

- ⦿ **No seleccionar** los apartados que facilitan consultar mediante **interoperabilidad** con otras Instituciones de la Administración (Hacienda y Seguridad Social en concreto)
- ⦿ **No comunicar mediante el “Alta de Terceros”** cualquier posible cambio de cuenta o en la titularidad de las mismas.



Errores comunes

En conclusión,

Tener un buen proyecto, bien fundamentado y bien procedimentado será el pilar sobre el que se basará tanto nuestra petición de financiación como la ejecución del mismo

Por ello, es importante **dedicarle el tiempo previo suficiente para reflexionar, analizar, prever y recopilar** toda la información necesaria.

Una vez redactado, de cara a la solicitud de subvenciones será igualmente importante, *analizar los documentos de solicitud y/o justificación* para ver qué partes de nuestro proyecto deben integrarse en cada campo requerido *y tener preparada toda la documentación* antes de iniciar el proceso de solicitud.

Errores comunes

EUSKO JAURLARITZA  GOBIERNO VASCO

Imprimir

ANEXO II PROYECTO DE ACTIVIDADES

Nombre de la entidad solicitante:

Identificación del proyecto en el VI Plan de Igualdad de Mujeres y Hombres

Ejes de intervención:

Programas del eje seleccionado:

Tipo de programa según artículo 4 de la Resolución:

Denominación del proyecto:

Justificación del proyecto. Análisis previo de la necesidad existente:

Objetivos:

Metodología:

Actividades concretas del Proyecto:

Criterios/Indicadores de evaluación:

Resultados esperados:

Necesario haber leído tanto las Bases de la convocatoria como el Plan de Igualdad vigente

Beneficio social del programa y efecto multiplicador del mismo:

Fomento de la accesibilidad y de elementos facilitadores de la conciliación:

Personas destinatarias de la actividad:

Nº de personas previstas en la participación de la misma:

Ámbito territorial de la actividad:

Local Territorio Histórico Comunidad autónoma

Lugar o lugares de realización de la actividad:

Calendario de la actividad:

Nº de horas:

Fecha de inicio:

Fecha de finalización:

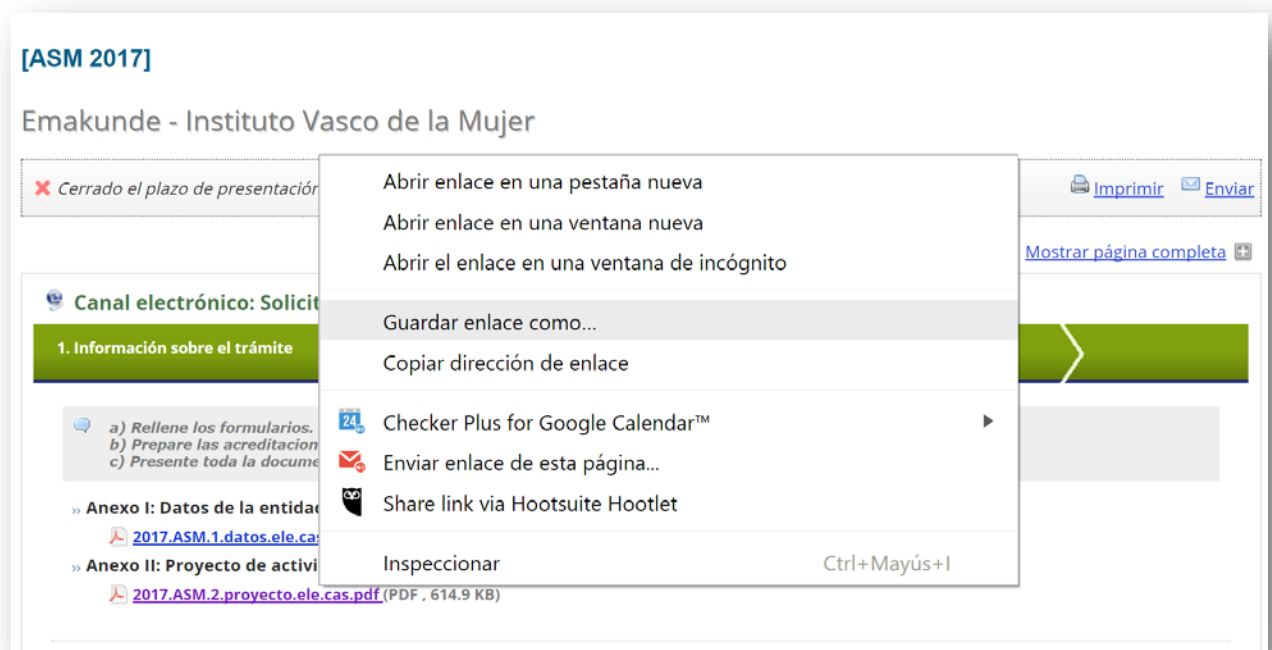
La actividad se realizará en:

Euskara Castellano Bilingüe Otra

Descarga correcta de archivos PDF

Los documentos **rellenables e imprimibles** necesarios tanto para la solicitud de subvención como para la justificación se encuentran siempre en la página de Emakunde. En ocasiones, nuestros navegadores no pueden abrir estos documentos pdfs por no tener la última versión de los lectores PDF actualizados. Para poder descargarlos, poderlos abrir y que se vean bien:

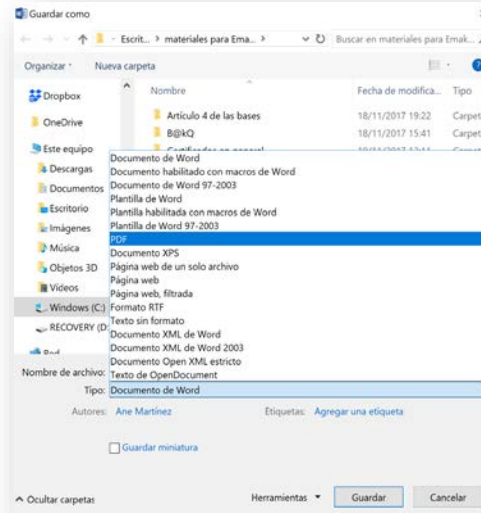
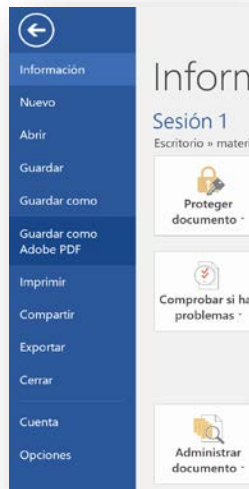
1. **Botón derecho del ratón** sobre el enlace (azúl)
2. Pinchamos en **guardar enlace como**
3. Elegimos la carpeta destino para nuestros archivos en el pc.
4. Guardamos



Creación correcta de archivos PDF

La mejor manera para ‘subir’ o adjuntar nuestros proyectos ya redactados al aplicativo de Emakunde es haber convertido nuestros documentos base (hojas de cálculo o documentos de texto) en PDF. Hay varias maneras de crear un pdf.

- ✓ A la hora de guardar nuestros documentos usaremos la opción **“Guardar como PDF”**.
- ✓ También es posible desde la opción **“Guardar como”** y elegir luego el **tipo de archivo** en el que lo queremos guardar el formato PDF.
- ✓ Y, por último, podemos darle a **imprimir** y en vez de elegir una impresora, le damos a cambiar y ponemos **“imprimir como pdf”**



Aviso:

Si nuestros documentos contienen enlaces a algún sitio web o a alguna parte en concreto del documento (caso de documentos navegables) debemos evitar la opción de imprimir como PDF porque quedaría como impreso en papel.

¿Qué es la e-administración?

La Unión Europea ha definido la Administración electrónica como

“el uso de las Tecnologías de la Información y las Comunicaciones (TIC) en las Administraciones Públicas, unido a cambios en la organización, con el propósito de mejorar los servicios públicos y los procesos democráticos, y de reforzar el apoyo a las políticas públicas. ”



Normativa

Respecto a la Administración

Existe, además, una normativa específica al respecto, *La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*, señala que **la tramitación electrónica debe constituir la actuación habitual de las Administraciones**. Esta obligación general se desarrolla a lo largo de la Ley, estableciendo derechos y obligaciones concretas:

- ✓ Derecho y obligación de relacionarse electrónicamente con las Administraciones públicas.
- ✓ Derechos de la ciudadanía como interesados/as.
- ✓ Identificación y firma de los interesados/as en el procedimiento.
- ✓ Derecho de asistencia de los interesados/as.
- ✓ Derechos de información.
- ✓ Registros electrónicos.
- ✓ Archivos de documentos.
- ✓ Tramitación electrónica de los procedimientos.

Normativa

Respecto a la Ciudadanía

La ciudadanía también tenemos obligación de relacionarnos electrónicamente con las Administraciones Públicas ya que mediante la La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece, desde el pasado **2 de octubre de 2016, la obligación para las **personas jurídicas** de relacionarse electrónicamente con las Administraciones Públicas (Art. 14)**

Artículo 14. Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.

2. En todo caso, estarán obligados/as a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos:

- a) Las personas jurídicas.
- b) Las entidades sin personalidad jurídica.
- c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios/as y registradores/as de la propiedad y mercantiles.
- d) Quienes representen a una persona interesada que esté obligada a relacionarse electrónicamente con la Administración.
- e) Los empleados/as de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado/a público, en la forma en que se determine reglamentariamente por cada Administración.

Normativa

Respecto a la Ciudadanía

Una administración así entendida necesita, de manera paralela, **de una ciudadanía no sólo empoderada tecnológicamente** en el uso de esas nuevas vías de comunicación sino, sobre todo, **comprometida y participativa**.

Por lo tanto, existe **un compromiso a doble banda**:

- ✓ Por una parte, la Administración que para ser electrónica ha de implementar:
 - Un **sistema de acreditación**, con el fin de que tanto la Administración como la ciudadanía puedan llevar a cabo procesos de tramitación electrónica que cumplan todos los requisitos legales.
 - La existencia de **un registro electrónico**, que permita procesar las transacciones y la documentación que se genera en la prestación de cualquier servicio público.
- ✓ Por otra, una ciudadanía comprometida, participativa y **acreditada**.

Normativa

Realidad actual

Mediante la Administración electrónica, actualmente, la ciudadanía pueden realizar, entre otras, las **siguientes gestiones**:

- ✓ Iniciar procedimientos administrativos.
- ✓ Obtener duplicados de solicitudes.
- ✓ Adjuntar documentos a una solicitud.
- ✓ Acceder a servicios de respuesta inmediata.
- ✓ Declaración y pago de impuestos y tasas.
- ✓ Pedir citas médicas o de otra naturaleza.
- ✓ Formular quejas y sugerencias.
- ✓ Participar en las distintas iniciativas públicas.

¿Qué es necesario para materializar esta relación electrónica?

El hecho de que se hayan tenido que regular los derechos y las obligaciones de la ciudadanía con respecto a la tramitación electrónica indica **que algo ha cambiado y que su nivel de implantación es suficiente como para tener que regularlo.**

Ahora mismo existe la posibilidad de interactuar con la Administración, vía telemática, **las 24 horas** de los 365 días a través de las **‘ventanillas virtuales’** o **‘sedes electrónicas’** que se han implementado en los sitios webs de las diferentes administraciones (locales, provinciales, autonómicas y nacionales).

La tramitación telemática es por tanto una realidad y ello conlleva que nos veamos obligadas y obligados a hacer un **intercambio de datos personales a través de internet.**

Necesitamos, para ello, de un **entorno de transacciones seguras en el alojamiento** de esas ‘Sedes electrónicas’ y disponer **de una identificación electrónica segura y admitida** de las personas usuarias (**certificado electrónico**). Hoy en día, los sistemas basados en los certificados digitales o electrónicos garantizan la seguridad en las comunicaciones.

Nota:

Es importante **no confundir un servidor seguro con un certificado digital o una firma digital.**

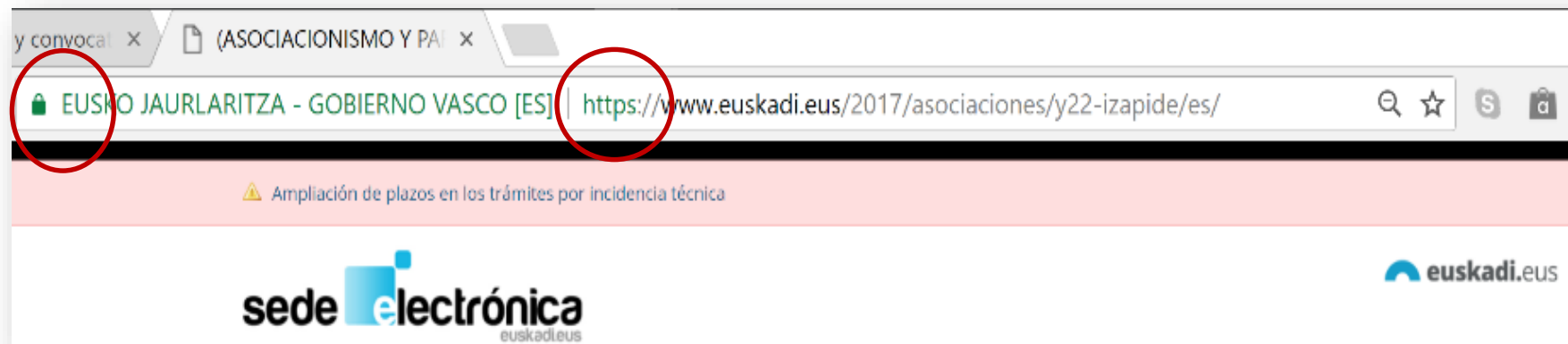
¿Qué es necesario para materializar esta relación electrónica?

Servidor seguro

Un servidor seguro **garantiza** que las personas usuarias están verdaderamente conectadas al sitio web que se declara.

Es, por tanto, un servidor de páginas web en el que la información que intercambian el cliente y el servidor viaja encriptada a través de la red, de modo que se garantice la privacidad de los datos que se transmiten.

Visualmente lo identificamos por utilizar un protocolo de internet propio (**https://**) y un candado en la barra de direcciones.



¿Qué es necesario para materializar esta relación electrónica?

Servidor seguro




Pero el hecho de que una página web disponga de conexión segura no quiere decir que el sitio sea de confianza o seguro.

Para ello **un servidor seguro debe emplear un certificado digital**, por el que **una tercera parte de confianza avale la autenticidad de la relación entre ese servidor seguro y el organismo que lo posee.**

<https://support.google.com/chrome/answer/95617?hl=es>




Comprobar si la conexión de un sitio web es segura

Para saber si es seguro acceder a un sitio web, puedes consultar la información de seguridad de ese sitio. Chrome te avisa si no puedes acceder al sitio web de forma segura o privada.

1. En Chrome, abre una página.
2. Para comprobar la seguridad de un sitio web, consulta el estado de seguridad en el icono situado a la izquierda de la dirección web:
 -  Es seguro.
 -  Información o No es seguro.
 -  No es seguro o Peligroso.
3. Para consultar los permisos y la información del sitio web, selecciona el icono. Chrome te indica de forma resumida el grado de privacidad de la conexión.

Significado de cada símbolo de seguridad

Estos símbolos te permiten saber si es seguro visitar y utilizar un sitio web y te indican si tiene certificados de seguridad, si Chrome confía en él y si este navegador tiene una conexión privada con un sitio web.

 Es seguro	▼
 Información o No es seguro	▼
 No es seguro o Peligroso	▼

Corregir el error "La conexión no es privada"

Si aparece un mensaje de error "La conexión no es privada" que ocupa toda la página, significa que hay un problema con el sitio web, con la red o con tu dispositivo. Más información sobre cómo [solucionar errores del tipo "La conexión no es privada"](#)

¿Qué es un certificado de seguridad?

Al acceder a un sitio web que utiliza HTTPS (seguridad de conexión), su servidor utiliza un certificado para demostrar la identidad del sitio web a los navegadores (como Chrome). Cualquier usuario puede crear un certificado para hacerse pasar por el sitio web que quiera.

Para que puedas navegar por la Web de forma segura, Chrome exige a los sitios web que utilicen certificados de organizaciones de confianza.

¿Qué es necesario para materializar esta relación electrónica?

Certificado digital

El **Certificado Digital** es el **único medio que permite** garantizar técnica y legalmente la identidad de una persona, jurídica o no, en Internet. Los certificados digitales son, por tanto, **credenciales electrónicas** que **se usan para certificar las identidades en línea** de personas físicas o jurídicas, equipos y otras entidades no jurídicas en internet. Funcionan de forma similar a los documentos de identificación, como pasaportes y licencias de conducir.

Además, el certificado digital permite:

- ✓ **La firma electrónica de documentos.**
- ✓ **Cifrar las comunicaciones**

Por ello, son de uso imprescindible en la tramitación telemática con la Administración ya que se requiere autenticación, cifrado y firma digital.

¿Qué es necesario para materializar esta relación electrónica?

Certificado digital

Un Certificado Digital consta de una **pareja de claves** criptográficas, una pública y una privada, creadas con **un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede** descifrar con su clave pareja. La persona titular del certificado debe mantener bajo su poder la **clave privada**, ya que, si ésta es sustraída, se podría suplantar su identidad en la red. En este caso la persona titular debe **revocar el certificado*** lo antes posible.

En conclusión, **un Certificado Digital** en sí, es un documento digital que contiene la clave pública junto con los datos de la persona titular, todo ello firmado electrónicamente por una **Autoridad de Certificación**, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos de la persona titular. Las terceras partes encargadas de otorgar certificados digitales se conocen como Prestadores de Servicios de Certificación. **Izenpe** es el Prestador de Servicios de Certificación de la Administración Pública Vasca.

*La vulnerabilidad ROCA detectada en el chip de algunas tarjetas electrónicas de Izenpe ha provocado que la Entidad Certificadora revocara esos certificados y obligara a su reemisión por nuestra seguridad, a pesar de no haberse detectado ninguna suplantación de identidad ya que, utilizando ROCA, un atacante podría suplantar identidades, firmar malware con un certificado malicioso o descifrar mensajes que utilicen claves vulnerables.

¿Qué es necesario para materializar esta relación electrónica?

Certificado digital

Tipos de certificados aceptados en la sede electrónica del Gobierno Vasco

La relación de medios de identificación electrónica admitidos a partir del 31 de agosto de 2013, de acuerdo con la [política de firma](#) aprobada es la siguiente:

Para las personas físicas



[Juego de Barcos / B@kQ](#)



[Izenpe - Certificado de ciudadano](#)



[DNI electrónico](#)



[Izenpe - Certificado de empleado público](#)



[FNMT - Certificados de persona física](#)



[CAMERFIRMA - Certificados de persona física](#)



[FIRMA PROFESIONAL - Certificados de persona física](#)

Para los Representantes de entidades:



[Izenpe - Certificado de Representante de entidad](#)



[FNMT - Certificado de representante](#)



[FIRMA PROFESIONAL - Certificado de representante legal](#)



[CAMERFIRMA - Certificados de representante \(PR\)](#)

¿Qué es necesario para materializar esta relación electrónica?

Firma electrónica avanzada

En España existe la *Ley 59/2003, de Firma electrónica*, que define tres tipos de firma:

1. **Firma electrónica simple:** Incluye un método de identificar al firmante (autenticidad)
2. **Firma electrónica avanzada:** Además de identificar al firmante permite garantizar la integridad del documento.
3. **Firma electrónica reconocida:** es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

¿Qué es necesario para materializar esta relación electrónica?

Firma electrónica avanzada

En el uso cotidiano se tiende a usar indistintamente los términos firma digital y firma electrónica si bien, en esencia no son lo mismo.

La **Firma Electrónica** es un concepto más amplio que el de Firma Digital:

- ✓ La firma digital hace referencia a una serie de métodos criptográficos.
- ✓ El concepto de “Firma Electrónica” es de naturaleza fundamentalmente legal, ya que confiere a la firma un marco normativo que le otorga validez jurídica, es **un concepto jurídico y un método de identificación, equivalente o análogo a la firma manuscrita, que se sirve de diversos soportes electrónicos distintos**. La Firma Electrónica, puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido

¿Qué es necesario para materializar esta relación electrónica?

Firma electrónica avanzada

¿Cómo funciona la firma digital?

(Para explicar este funcionamiento utilizaremos parte del material que [Kzgunea](#) utiliza en su taller de firma electrónica por parecernos un material didáctico muy gráfico y claro)

1. La firma digital es el conjunto de **caracteres que se añaden al final de un documento o cuerpo de un mensaje** para informar, dar fe o mostrar validez y seguridad. La firma digital sirve para asegurar:
2. La **confidencialidad** o secreto de la información enviada.
3. La **integridad** de dicha información, avalando que ha permanecido inalterable en el envío.
4. La **autenticidad**, que identifica a la persona emisora.
5. El **no repudio**, de modo que la persona emisora reconoce la transmisión y no puede negar ante terceros el envío de dichos datos en un momento concreto puesto que **esta firma implica la existencia de un certificado oficial emitido por un organismo o institución que valida la firma y la identidad** de la persona que la realiza.

¿Qué es necesario para materializar esta relación electrónica?

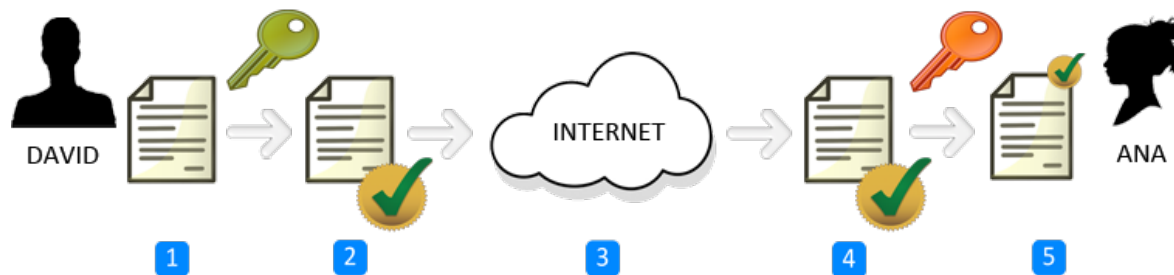
Firma electrónica avanzada

¿Cómo funciona la firma electrónica?

Cuando usamos el sistema de firma electrónica, cada persona física o jurídica dispone de un par de claves:

La **clave privada**, que debe permanecer bajo el exclusivo control de la persona física o jurídica propietaria. Esta característica permite que una firma digital identifique en forma unívoca a quien firma.

La **clave pública**, que es conocida por las demás personas. Posibilita al destinatario verificar quien es el autor del mensaje y la integridad de los datos enviados.

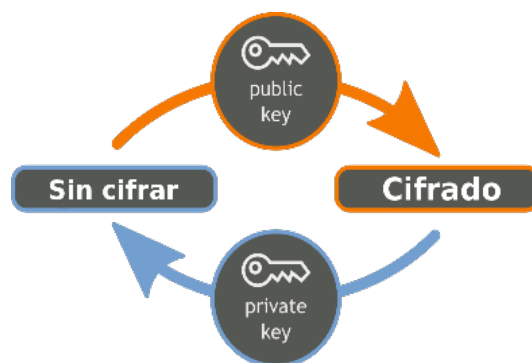


¿Qué es necesario para materializar esta relación electrónica?

Firma electrónica avanzada

¿Cómo funciona la firma electrónica?

Estas claves actúan de forma complementaria: **lo que cifra una, sólo puede ser descifrado por la otra, y viceversa.** De este modo:



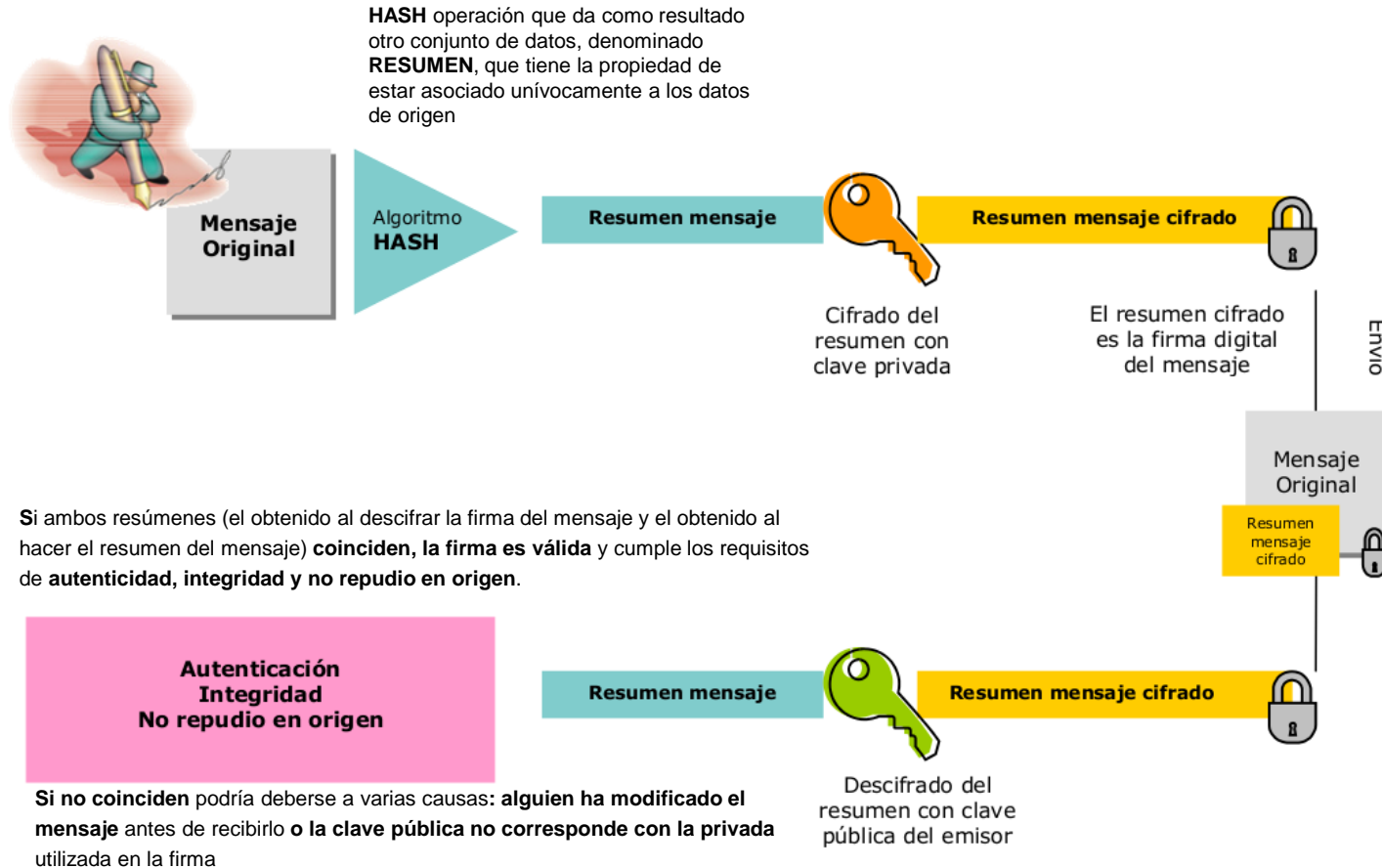
Por tanto, podemos tener plena seguridad de que el mensaje descifrado con esa clave pública solamente pudo cifrarse utilizando la privada, es decir, proviene de la persona a quien está asociada esa clave, o lo que es lo mismo, podemos saber sin lugar a dudas quién es el emisor de ese mensaje.

¿Qué es necesario para materializar esta relación electrónica?

Firma electrónica avanzada

¿Cómo funciona la firma digital?

(Se ha utilizado de ejemplo un mensaje, pero podría aplicarse a un archivo cualquiera, una factura en formato pdf, una imagen, un texto, etc.)



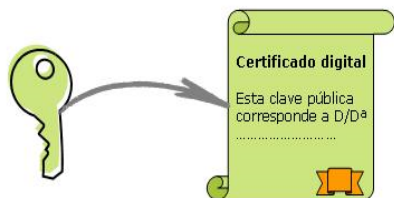
¿Qué es necesario para materializar esta relación electrónica?

Firma electrónica avanzada

¿Quién y dónde se guardan las claves?

En este punto somos conscientes de la importancia de la custodia de esas claves. De ello dependerá, en gran parte, la seguridad de todo el proceso.

La clave privada, empleada para firmar mensajes, debe estar **exclusivamente bajo el poder de quien firma**. Para ello, dicha clave se guarda en un dispositivo seguro; puede ser en una tarjeta criptográfica, en un token que no se puede duplicar y está protegida por un número de identificación personal (PIN).



Por su parte, la **clave pública debe ser conocida por el resto de personas**. Para ello, **se incluye en un certificado digital, público y accesible**. Este certificado avala que la clave contenida en él pertenece a la persona indicada en el mismo, esto es, le identifica indubitablemente

Recuerda:

Un certificado digital es un documento electrónico firmado electrónicamente por un **Prestador de Servicios de Certificación** (ej: Izenpe) que asocia una clave pública con su propietario. Se pueden consultar las [preguntas más frecuentes de la firma electrónica](#).

¿Qué es necesario para materializar esta relación electrónica?

Prestador de Servicios de Certificación

Un prestador de servicios de certificación es una **organización que proporciona servicios de certificados digitales**.

De esta manera, podremos confiar en el certificado digital de una persona a la que no conocemos, si dicho certificado está avalado por una entidad en la que sí confiamos; es decir, si está avalado por un Prestador de Servicios de Certificación en el que confiamos (Ej: Izenpe)

El Prestador de Servicios de Certificación garantiza que el certificado es de fiar mediante su firma digital en el mismo.

¿Qué es necesario para materializar esta relación electrónica?

Prestador de Servicios de Certificación

Izenpe

Izenpe S.A, empresa de certificación y prestadora de servicios de confianza, es decir, una organización que proporciona servicios de firma electrónica. Fue constituida como sociedad anónima en 2002 y supone un proyecto impulsado por el Gobierno Vasco y las Diputaciones Forales, constituida a través de sus sociedades informáticas: EJIE, LANTIK, IZFE y CCASA.



RECUERDA:

La firma electrónica se puede definir como un conjunto de procedimientos técnicos y jurídicos que permiten “sustituir” la firma manual convencional con el fin de poder realizar a través de Internet y del teléfono tramites que antes debían hacerse de forma presencial.

Y...¿Cómo nos certificamos nosotras?

Hemos visto hasta ahora qué es la E-administración, qué supone tramitar de manera telemática con ella, cuáles son los requisitos para hacerla posible (servidor seguro, certificados digitales, firma electrónica avanzada), qué agentes se ven implicados (Administración, ciudadanía, Entidad certificadora) pero... ¿cómo podemos nosotras, desde nuestras diferentes realidades iniciar una tramitación telemática?

En principio, con cualquiera de los certificados digitales citados anteriormente se podría tramitar, pero atendiendo a la realidad de nuestros territorios:

Tarjeta ciudadana

El certificado de Ciudadanía es un certificado de firma electrónica, con la consideración legal de certificado reconocido, el más seguro de los certificados digitales y su firma es legalmente reconocida como la manuscrita.

Este certificado Izenpe permite relacionarse telemáticamente con las distintas administraciones (locales, forales, autonómicas y estatales) y cada día con más entidades, como las financieras. En su reverso contiene un juego de barcos



Y...¿Cómo nos certificamos nosotras?

Representate de Entidad

Es un certificado de firma electrónica cualificado que permite relacionarse de forma telemática (autenticarse y firmar) con las distintas administraciones (locales, forales, autonómicas y estatales) y viene a cubrir el espacio al que antes se accedía con el certificado de persona jurídica o entidad sin personalidad jurídica.

Pueden solicitarse en soporte tarjeta, Token USB o formato SOFTWARE.



Para solicitar un certificado de firma electrónica del tipo representante de entidad o entidad sin personalidad jurídica, el solicitante deberá ser un representante legal o un apoderado general con facultad inscrita para representar a la organización ante toda clase de personas privadas o públicas.

Y...¿Cómo nos certificamos nosotras?

Representate de Entidad

Renovación de estas tarjetas (ciudadana y de representante)

Estos certificados tienen una validez de 4 años, 60 días antes de la fecha de caducidad del certificado Izenpe remitirá un correo electrónico a la dirección cedida en el momento de la solicitud para informar del proceso de renovación. En las renovaciones se emitirá un certificado nuevo con fecha de inicio posterior a la de caducidad de su actual certificado para que se puedan usar de forma continua.

Además existen otras posibilidades especialmente indicadas para factura electrónica como solicitando un [certificado de SELLO de entidad en SOFTWARE](#) »

AVISO: El solicitante de un certificado de Representante de Entidad o Entidad SPJ deberá tener en cuenta los plazos requeridos para su emisión. La documentación exigida conlleva la petición de certificaciones registrales y/o poderes notariales que pueden demorar la fecha final de expedición del certificado.

Y...¿Cómo nos certificamos nosotras?

B@k y B@kQ

Son un nuevo medio de identificación electrónica muy sencillo de usar y que permite relacionarse telemáticamente con las administraciones.

B@k nivel básico es un medio de identificación electrónica de nivel básico, válido para trámites y servicios sin criticidad, formado por:



- ✓ Un número de referencia coincidente con el DNI/NIE de la persona usuaria.
- ✓ Una contraseña.
- ✓ Y un certificado no cualificado emitido en un repositorio centralizado seguro de Izenpe, la “nube”, que servirá para los actos de firma.

Además, puede ser complementado para todos o algunos de sus usos por un código enviado a un dispositivo móvil.

B@k exige un **proceso de emisión y de activación online** para la puesta en marcha y para preparar su uso. Es un proceso sencillo que se debe hacer desde un ordenador o cualquier dispositivo móvil.

Y...¿Cómo nos certificamos nosotras?

B@k y B@kQ

B@kQ será necesario cuando el nivel de seguridad exigido sea medio (sustancial) y está formado por:



- ✓ Un identificador coincidente con el DNI/NIE de la persona usuaria.
- ✓ Una contraseña. (compartida con B@k)
- ✓ Un juego de coordenadas con 16 posiciones
- ✓ Y un certificado cualificado emitido en un repositorio centralizado que servirá para los actos de firma.

En realidad, es B@k con un elemento de seguridad añadido: **las coordenadas**. Y un **certificado en la “nube” de mayor consideración jurídica**.

B@kQ también se debe solicitar y además se emite al tener asociada la generación de un certificado de firma electrónica, pero al ser un certificado cualificado **requiere IDENTIFICACIÓN PRESENCIAL o mediante otro medio de identificación electrónica válido**.

Tanto con B@k y B@kQ será posible la consulta y tramitación online en distintos servicios de las administraciones vascas.

Y...¿Cómo nos certificamos nosotras?

Juego de barcos

Es una **herramienta de firma electrónica de persona física**, que combina los juegos de barcos con una contraseña y la gestión por parte de Izenpe, como tercero de confianza, de la firma que permite a la persona usuaria autenticarse y realizar firma electrónica avanzada.

Ventajas

- ✓ Consideración de Firma Electrónica Avanzada.
- ✓ No necesita Software.
- ✓ Elimina la necesidad de lector.
- ✓ Verificación por parte de Izenpe (PSC).
- ✓ PIN asociado.
- ✓ Posibilidad de pérdida y recuperación de PIN



Y...¿Cómo nos certificamos nosotras?

Dni electrónico

Desde el año 2006 todos los Documentos Nacionales de Identidad que se expiden en España son documentos electrónicos, coexistiendo actualmente dos versiones:

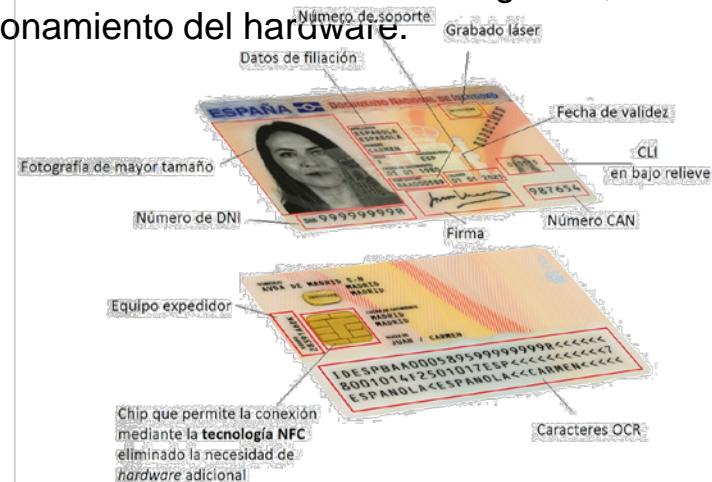
DNle

El **primer DNle**, expedido desde 2006 hasta finales de 2015 incorporaba, a diferencia de su predecesor, un chip en el anverso con información digital que permiten a la ciudadanía conectar con la Administración de forma digital, hacer uso de su identidad electrónica, firmar documentos digitalmente y de forma remota.

Para ello, las personas han de disponer de un dispositivo hardware que permita la lectura de los certificados contenidos en el chip, y posibilite la conexión a los distintos servicios digitales, así como instalar los diferentes drivers necesarios para el funcionamiento del hardware.

DNI 3.0.

El DNI 3.0, que desde diciembre de 2015, es el único documento que se expide en todas las Oficinas de Expedición del territorio nacional, es una tarjeta de un material plástico, que incorpora un chip con interface dual que permite la conexión mediante el contacto o de forma inalámbrica mediante la tecnología NFC



Y...¿Cómo nos certificamos nosotras?

¿Para qué puedo utilizarlo?

Tal y como recoge la Declaración de Prácticas de Certificación del DNI, los certificados electrónicos podrán utilizarse:

✓ **Como medio de Autenticación de la Identidad.**

El Certificado de Autenticación (*Digital Signature*) asegura al titular, en la comunicación electrónica, acreditar su identidad frente a cualquiera.

✓ **Como medio de firma electrónica de documentos.**

Mediante la utilización del Certificado de Firma (*non Repudition*), la persona receptora de un mensaje firmado electrónicamente puede verificar la autenticidad de esa firma, pudiendo de esta forma demostrar la identidad del firmante sin que éste pueda repudiarlo.

✓ **Como medio de certificación de Integridad de un documento.**

Permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación.

✓ **Como Documento de Viaje.**

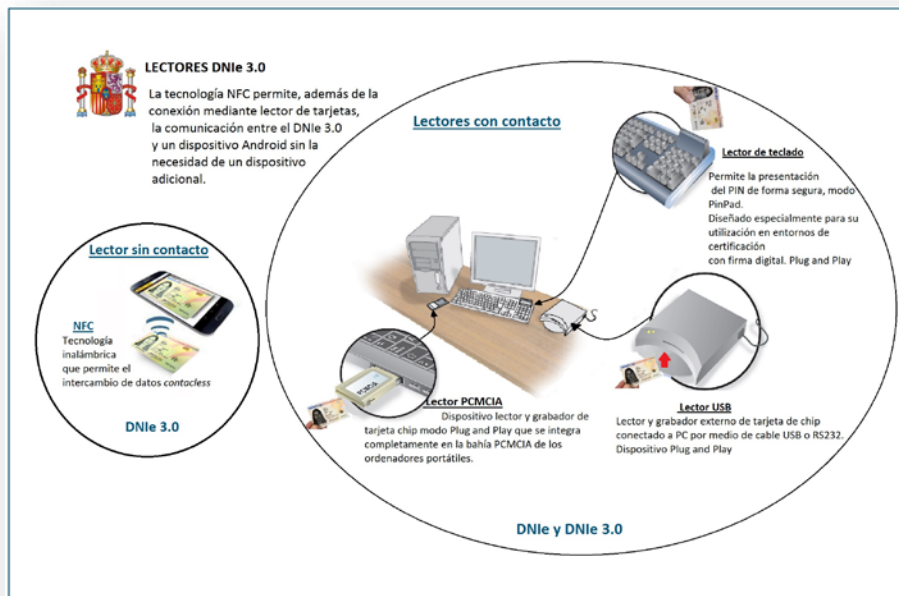
El DNI 3.0 tiene una estructura de datos equivalente al pasaporte. En este sentido, el DNI 3.0 puede realizar funciones de Documento de Viaje en los países que lo acepten como tal, y se permite su uso en los Pasos Rápidos de Frontera (*ABC Systems*) de forma totalmente equivalente a un pasaporte.

Y...¿Cómo nos certificamos nosotras?

¿Qué necesitamos para poder utilizarlo?

Para la utilización, del DNI, es necesario contar con determinados elementos hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

Mientras que el DNle sólo permite el acceso mediante contacto, el DNI 3.0 dispone de un chip *Dual interface*, que permite también la conexión inalámbrica a través de la antena NFC.



Para aplicativos Microsoft como **Internet Explorer** o para **Google Chrome** basta con tener el equipo conectado a Internet e insertar la tarjeta en el lector. El servicio Windows Update buscará automáticamente el driver de la tarjeta y lo instalará al tratarse de un dispositivo Plug & Play.

Y...¿Cómo nos certificamos nosotras?

¿Qué necesitamos nosotras para tramitar con el Dni Electrónico?

En el área de descargas de la página web del Dni electrónico podemos encontrar los enlaces a todos los software y drivers necesarios para hacer funcionar los certificados digitales.



The screenshot shows the 'Área de Descargas' (Download Area) of the Dni electrónico website. The browser address bar shows the URL: https://www.dnielectronico.es/PortalDNIE/PRF1_Cons02.action?pag=REF_1100. The page header includes the 'Cuerpo Nacional de Policía' logo and navigation buttons for 'Ciudadanos', 'Empresas', 'Administraciones', and 'Oficina Técnica'. The main content area is titled 'Área de Descargas' and lists several download links:

- ☒ Sistema Windows
- ☒ Sistemas GNU/Linux y Sistemas MacOS
- ☒ Certificados x509, Autoridades de Certificación y Autoridades de Validación
- ☒ Código fuente completo de aplicaciones Android, y documentación para desarrolladores, para uso de DNIE 3.0 en dispositivos móviles con tecnología NFC
- ☒ ActiveX para DNIE para entorno PC

At the bottom, there is contact information for the Oficina Técnica: oficinatecnica@dnielectronico.es.

Y...¿Cómo nos certificamos nosotras?

¿Cómo verificamos que nuestro certificado es válido?

El proceso de comprobación de un certificado implica en primer lugar la obtención de los datos del certificado y en segundo lugar la consulta a un servicio denominado Autoridad de Validación (AV) . El navegador presentará su certificado al servidor y éste lanzará una consulta a la AV.

El resultado de esta consulta es el estado actual del certificado: activo o revocado. Simultáneamente se mostrarán los datos incorporados al certificado (nombre y apellidos del titular, número de DNI,...).

Antes de intentar esta prueba deberá:

- ✓ Si usamos Windows (a partir del win7), únicamente introducir la tarjeta DNle en el lector de tarjetas y el Sistema Operativo instala el driver del DNle de forma rápida y automática.
- ✓ Instalar en su equipo el software adecuado en función del sistema operativo que esté usando teniendo en cuenta para ello lo indicado en el párrafo anterior, encontrará éste software en el área de [descargas](#).
- ✓ Comprobar que puede ver los certificados en el navegador de su equipo:
 - **Internet Explorer:** herramientas-opciones-contenido-certificados.
 - **Firefox:** herramientas-opciones-avanzado-ver certificados.
 - **Chrome:** configuración-mostrar opciones avanzadas-https/ssl-administrar certificados.

La comprobación de los certificados puede realizarse accediendo a cualquiera de los siguientes prestadores de servicio de validación:

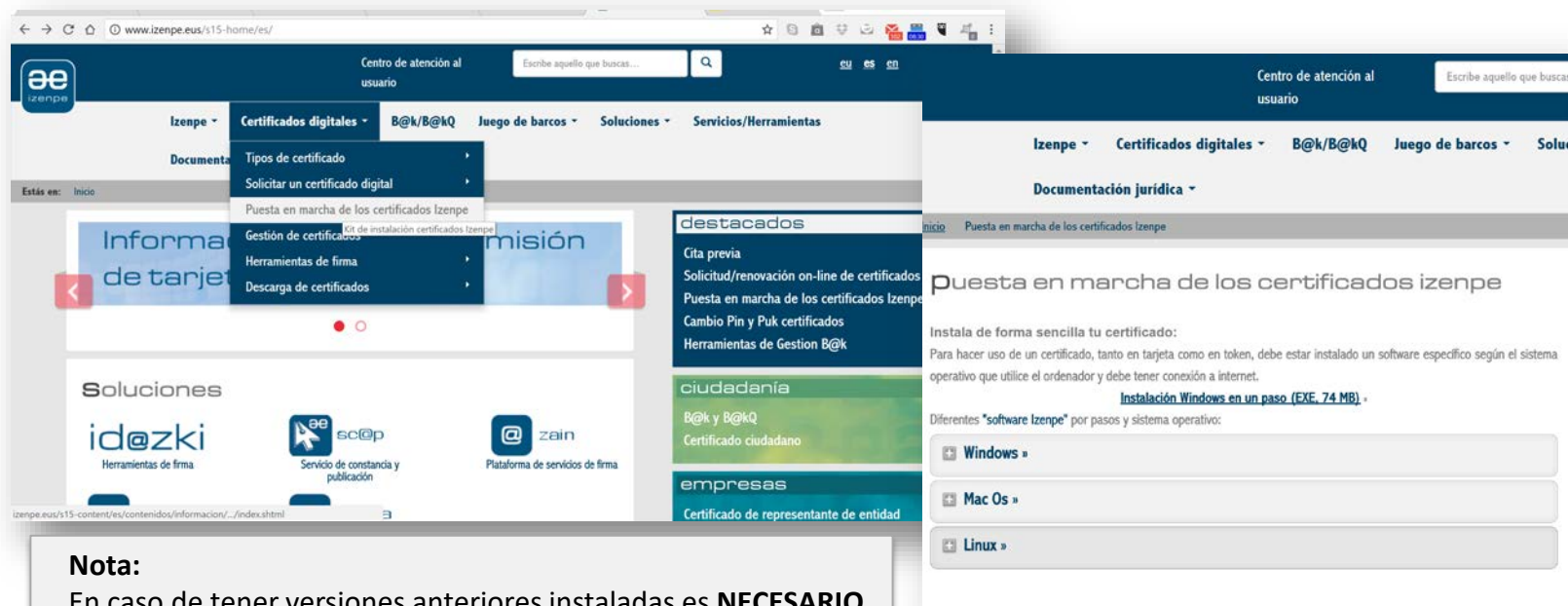
[@FIRMA – VALIDE](#)
[FNMT](#)

Tenemos certificado y...¿Ahora qué?

Puesta en marcha de los certificados

Una vez obtenida nuestra identificación digital debemos preparar nuestros equipos para poder hacer efectivas todas esas posibilidades de tramitación telemática que nos ofrece la E-administración.

Deberemos instalar en nuestros equipos siempre la última versión actualizada de los certificados que nuestro proveedor de servicios ofrezca en sus sitios web. En nuestro caso, Izenpe.



Centro de atención al usuario

Estás en: Inicio

Documentación

destacados

Cita previa

Solicitud/renovación on-line de certificados

Puesta en marcha de los certificados Izenpe

Cambio Pin y Puk certificados

Herramientas de Gestión B@k

ciudadanía

B@k y B@kQ

Certificado ciudadano

empresas

Certificado de representante de entidad

Puesta en marcha de los certificados Izenpe

Instala de forma sencilla tu certificado:

Para hacer uso de un certificado, tanto en tarjeta como en token, debe estar instalado un software específico según el sistema operativo que utilice el ordenador y debe tener conexión a internet.

[Instalación Windows en un paso \(EXE, 74 MB\)](#)

Diferentes "software Izenpe" por pasos y sistema operativo:

- Windows »
- Mac Os »
- Linux »

Nota:

En caso de tener versiones anteriores instaladas es **NECESARIO DESINSTALARLAS.**

Tenemos certificado y...¿Ahora qué?

Puesta en marcha de los certificados

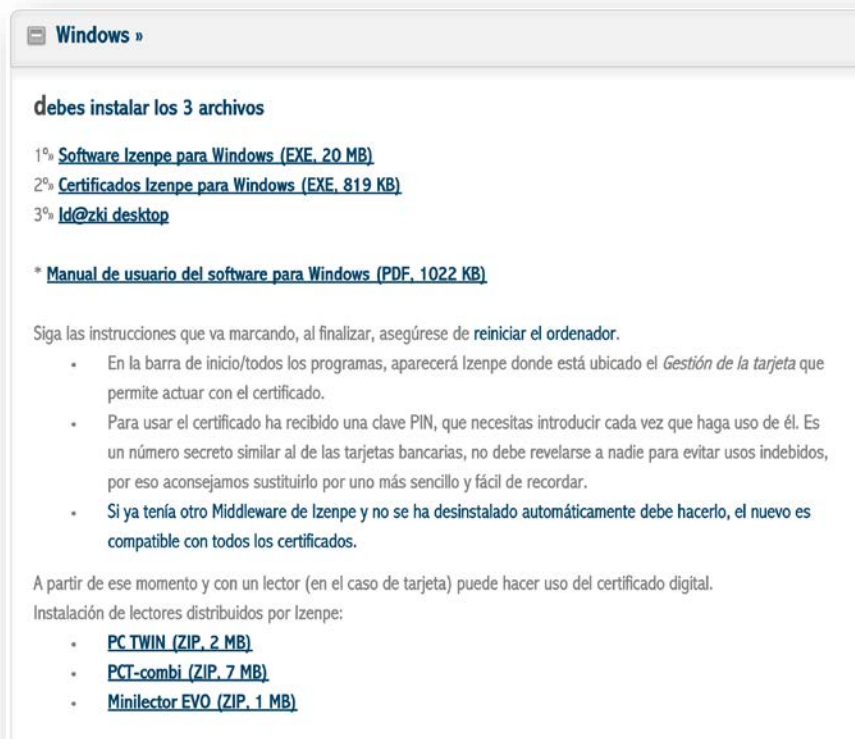
En la mayoría de los casos con hacer una instalación del paquete para “**Windows en un solo paso**” será suficiente. En él están contenidos los tres programas que se han de instalar.

Sólo en el caso de que nos de **error** o, porque necesitemos **actualizar** sólo **alguno de los componentes**, utilizaremos la instalación “**paso por paso**” y siempre siguiendo el orden de instalación en el que aparecen.

Notas a tener en cuenta:

.-Es importante tener **instalados y actualizado el sistema operativo y los navegadores ANTES** de instalar el **Middleware*** de Izenpe

-Es fundamental para que funcione todo bien **REINICIAR AL EQUIPO** tras la instalación



debes instalar los 3 archivos

- 1º [Software Izenpe para Windows \(EXE, 20 MB\)](#)
- 2º [Certificados Izenpe para Windows \(EXE, 819 KB\)](#)
- 3º [ld@zki desktop](#)

* [Manual de usuario del software para Windows \(PDF, 1022 KB\)](#)

Siga las instrucciones que va marcando, al finalizar, asegúrese de **reiniciar el ordenador**.

- En la barra de inicio/todos los programas, aparecerá Izenpe donde está ubicado el *Gestión de la tarjeta* que permite actuar con el certificado.
- Para usar el certificado ha recibido una clave PIN, que necesitas introducir cada vez que haga uso de él. Es un número secreto similar al de las tarjetas bancarias, no debe revelarse a nadie para evitar usos indebidos, por eso aconsejamos sustituirlo por uno más sencillo y fácil de recordar.
- Si ya tenía otro Middleware de Izenpe y no se ha desinstalado automáticamente debe hacerlo, el nuevo es compatible con todos los certificados.

A partir de ese momento y con un lector (en el caso de tarjeta) puede hacer uso del certificado digital.

Instalación de lectores distribuidos por Izenpe:

- [PC TWIN \(ZIP, 2 MB\)](#)
- [PCT-combi \(ZIP, 7 MB\)](#)
- [Minilector EVO \(ZIP, 1 MB\)](#)

**Middleware*: programa o utilidad que permite la comunicación y el manejo de la propia tarjeta criptográfica a través del sistema operativo o del ordenador.

Tenemos certificado y...¿Ahora qué?

¿Nuestros equipos necesitan algo más?

JAVA

En algunas ocasiones, algunas de las webs a las que accederemos para tramitar necesitan que tengamos instalado **Java** (*software* gratuito de Oracle que se utiliza específicamente para la interacción en aplicaciones web desarrolladas en Java) para poder hacer uso del certificado en ellas. Aunque la tendencia es a desaparecer, aún es necesario tenerlo instalado y actualizado para determinados trámites.

Para que funcione el componente de firma Idazki, hay que tener instalada una versión 1.6 o superior de la máquina virtual de Java, con independencia de la actualización del componente de firma.

La mejor manera de actualizar java es visitando el sitio web www.java.com y descargándolo gratuitamente. Tras instalarlo debemos comprobar que se ejecuta correctamente (nos mostrará una opción para ello)

LECTOR DE TARJETAS

Es imprescindible que antes de probar los certificados tengamos instalado el lector de tarjetas criptográficas. Al conectarlo por primera vez es muy probable que el propio sistema reconozca que un nuevo hardware se ha conectado al ordenador e instale automáticamente el controlador del dispositivo (por eso es importante tener el sistema operativo actualizado). De no ser así, debe instalarse de forma manual el controlador o driver del dispositivo (se recomienda utilizar aquellos que facilitan o recomiendan las propias entidades certificadoras)



Proceso de firma electrónica con certificado

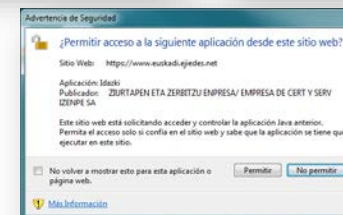
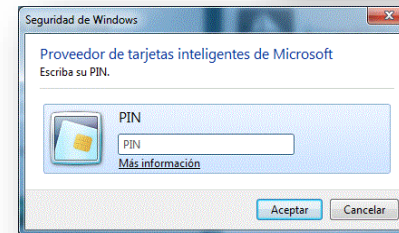
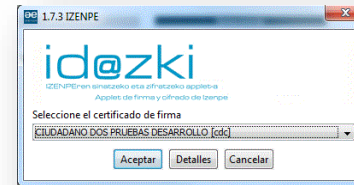
Si el navegador en el que se estamos tratando de firmar soporta los applets Java, se cargará el applet de Id@zki; en caso contrario, se mostrará la modalidad de firma con certificado mediante Idazki-desktop.

Utilizando el applet de firma de Id@zki

El **applet de Id@zki** es una aplicación Java en formato applet integrada en un navegador con funcionalidad de firma electrónica cifrada.

1. Seleccionar el certificado, en caso de tener más de uno.
2. Introducir el PIN asociado al certificado elegido (Es posible que el sistema le solicite el PIN en más de una ocasión y desde pantallas diferentes: por un lado lo solicitará Izenpe, y, por otro, el software que utiliza Windows para comprobar el certificado)
3. Permitir para que se ejecute el applet de Id@zki y poder así llevar a cabo la firma.

Error "No hay certificados disponibles para la firma electrónica": Este error puede tener relación con la **configuración del middleware**, por no tenerlo instalado o por estar utilizando una versión antigua. Ocurre a pesar de estar identificadas/os correctamente en la Sede electrónica.



Proceso de firma electrónica con certificado

Utilizando Id@zki desktop

Id@zki-desktop es una **aplicación de escritorio que debe descargar e instalarse una única vez**, antes de firmar y **con permisos de administrador**.

La firma mediante Id@zki-desktop es la modalidad de firma que se selecciona de forma automática cuando se detecta que el navegador en el que se va a firmar no soporta los *applets* Java.

A partir de este punto el proceso es el mismo que cuando firmamos con el applet de java. Primero nos identificamos ante la seguridad de Windows y seguido ante el Middleware de Izenpe.



BIZKAIA B

A partir de este momento está trabajando sobre una **conexión segura**. Toda la información que envíe o reciba, será automáticamente cifrada para su seguridad.

Para acceder al **Servicio de BizkaiaBai con Firma Electrónica basada en Certificado Reconocido**, puede consultar los Certificados admitidos en el siguiente enlace:

[Acceso al listado de Certificados de Firma electrónica admitidos en la Oficina Virtual de Hacienda y Finanzas - BizkaiaBai](#)

Para más información sobre el Certificado de Izenpe pulse [aquí](#).

Inserte su tarjeta de identificación en el lector de su equipo. A continuación se le requerirá el número **PIN** de la misma y se validará la información contenida en el **Certificado** que deberá ser **Reconocido**.

Es imprescindible para poder firmar con certificado descargar la última versión de **Idazki desktop** en la página de [Izenpe](#). En caso de tener instalada una versión más antigua de Idazki desktop deberá desinstalarla de su equipo antes de instalar la nueva versión.

Para acceder al Servicio BizkaiaBai pulse el botón aceptar:

Proceso de firma electrónica con juego de barcos

Es una **herramienta de firma electrónica de persona física (no representante)** que combina los juegos de barcos con una contraseña y la gestión por parte de Izenpe, como tercero de confianza, de la firma que permite a la persona usuaria autenticarse y realizar firma electrónica avanzada.

La casilla del número de referencia aparecerá cargada con el número que hemos introducido al identificarnos (normalmente DNI). Debemos introducir la contraseña (entregada junto a las claves PIN y PUK del certificado electrónico) y las coordenadas del juego de barcos.

Ventajas

- Consideración de Firma Electrónica Avanzada.
- No necesita Software.
- Elimina la necesidad de lector.
- Verificación por parte de Izenpe (PSC).
- PIN asociado.
- Posibilidad de pérdida y recuperación de PIN.



»Español »Euskara

identificarse de manera segura

Acceda mediante **juego de barcos**

» Juegos de barcos admitidos
» Preguntas frecuentes

Nº de referencia

Contraseña

¿Olvidó su contraseña?

Coordenadas

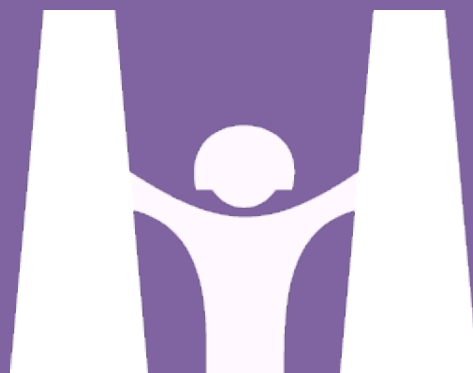
Borrar datos

O M K

3	1	5	4	7
9	8	2	0	6

continuar

* Obligatorio
* Obligatorio
* Mínimo 8 caracteres



EMAKUNDE

EMAKUMEAREN EUSKAL ERAKUNDE
INSTITUTO VASCO DE LA MUJER

