



CONTRÁLIA MANUAL DO UTILIZADOR V1.6

CONTEÚDO

0.	INTRODUÇÃO	3
1.	CRIAÇÃO DE CIRCUITOS	4
2.	TIPOLOGIAS DE INTERVENIENTES	6
3.	TIPOLOGIAS DE CIRCUITOS DE ASSINATURA	7
4.	CRIAÇÃO DO CIRCUITO DE ASSINATURA	8
5.	ASSINATURA DO CONTRATO PELO CLIENTE	10
6.	DOWNLOAD DE DOCUMENTOS ASSINADOS	13
7.	CANCELAMENTO DE CIRCUITOS	14
8.	MODELOS DE CIRCUITOS DE ASSINATURA	15
9.	TIMELINE	17
10.	PESQUISA DE CIRCUITOS	18
11.	LEMBRETES DE ASSINATURA	19
12.	HISTÓRICO DO ESTATUTO DE UM SIGNATÁRIO	20
14.	INSTALAÇÃO DE CERTIFICADO DIGITAL	21
15.	CAIXAS DE ASSINATURA	22
16.	REQUISITOS PARA ASSINATURA COM CERTIFICADO PRÓPRIO	22
16.1.	INSTALAÇÃO JAVA	22
16.2.	EXCEPÇÕES JAVA	22
16.3.	DESCARREGAMENTO E EXECUÇÃO DO COMPONENTE DESCARREGÁVEL	24
16.4.	ASSINATURA COM DNle	29
17.	ANEXOS	34
17.1.	ESPECIFICAÇÕES DE SEGURANÇA E INFRA-ESTRUTURA	34
17.1.1.	SEGURANÇA FÍSICA E AMBIENTAL	34
17.1.2.	SEGREGAÇÃO DA INFORMAÇÃO	34
17.1.3.	PROCESSO DE IDENTIFICAÇÃO E AUTENTICAÇÃO	34
17.1.4.	RESTRIÇÕES DE CONTROLO DE ACESSO	34
17.1.5.	PREVENÇÃO DE INTRUSÃO	35
17.1.6.	CYPHERING	¡Error! Marcador no definido.
17.1.7.	ARQUIVAMENTO DE CIRCUITOS CONTRALIA	35

0. INTRODUÇÃO

Contralia é um SaaS oferecido pela SERES para a assinatura online de documentos (aquilo a que chamamos circuito de assinatura).

Existem duas vias para lançar a assinatura de um documento, a primeira é carregar o próprio documento e um ficheiro de metadados para a conta SFTP que o cliente tiver configurado, a segunda é fazê-lo na plataforma SERES WEB CONNECT <https://webconnect.SERESnet.com/web/login>. Neste manual centrar-nos-emos na opção WEB.

1. CRIAÇÃO DE CIRCUITOS

Uma vez que o utilizador aceda com as suas credenciais, terá o seguinte menu:

Nombre	Fecha de envío	Estado	Documentos principales	Documentos adjuntos	Firmantes
CONTRATOS	26/09/2021 09:57:20	Totamente firmado	Contrato.pdf		JOSÉ DOMINGO BELLAH
Circuito WEB	24/09/2021 10:23:20	Totamente firmado	Contrato.pdf		Hicham OAHSSI
ROPD_01	18/09/2021 12:39:07	Expirado	ROPD_AEINCOOP.pdf		Carmen López
ROPD_01	17/09/2021 11:36:07	Expirado	ROPD_AEINCOOP.pdf		Carmen López
Test 1 16/09/2021	16/09/2021 16:40:07	Totamente firmado	Contrato.pdf	comunicado.pdf	Ramuel Torres Domínguez
Circuito WEB	16/09/2021 09:44:07	Cancelado	Contrato.pdf		Hicham OAHSSI

No separador Contralia estão listados todos os contratos lançados. Os campos apresentados são:

- Nome: nome do contrato que o próprio utilizador atribui quando o cria.
- Data de envio: data de lançamento do contrato.
- Situação: situação do contrato.
- Documentos principais: Documentos contratuais.
- Documentos anexos. É favor notar que os documentos anexos não estão sujeitos a assinatura, são meramente informativos.
- Signatários: signatários do contrato. Clicando num dos signatários, as suas informações aparecem numa janela pop-up:

Datos del firmante ✕

<p>Nombre: Hicham</p> <p>Teléfono: 0034687268785</p> <p>Estado: 24/06/2021 10:27:41 ✓ 24/06/2021 10:27:24 📄 24/06/2021 10:27:16 📧 24/06/2021 10:23:22 📧</p>	<p>Apellidos: QAISSI</p> <p>Email: hicham.qaissi@seres.es</p>
--	---

Os estados que um circuito de assinatura pode ter são os seguintes:

Estado	Descrição
Pedido de assinatura enviado aos signatários	Os signatários já receberam a notificação do pedido de assinatura.
Parcialmente assinado	Assinado por um dos signatários quando há mais do que um.
Expirado	O circuito atingiu o tempo máximo sem estar totalmente assinado.
Rejeitado por qualquer signatário	Alguns dos signatários recusaram-se a assinar.
Endereço de e-mail inválido	O e-mail de um dos signatários não é válido, bem porque a conta não existe ou porque a caixa de correio está cheia. O que acontece é que o servidor de correio electrónico do destinatário rejeitou o e-mail.
Cancelado	O transmissor cancelou o circuito.
Totalmente assinado	Assinado por todos os membros.

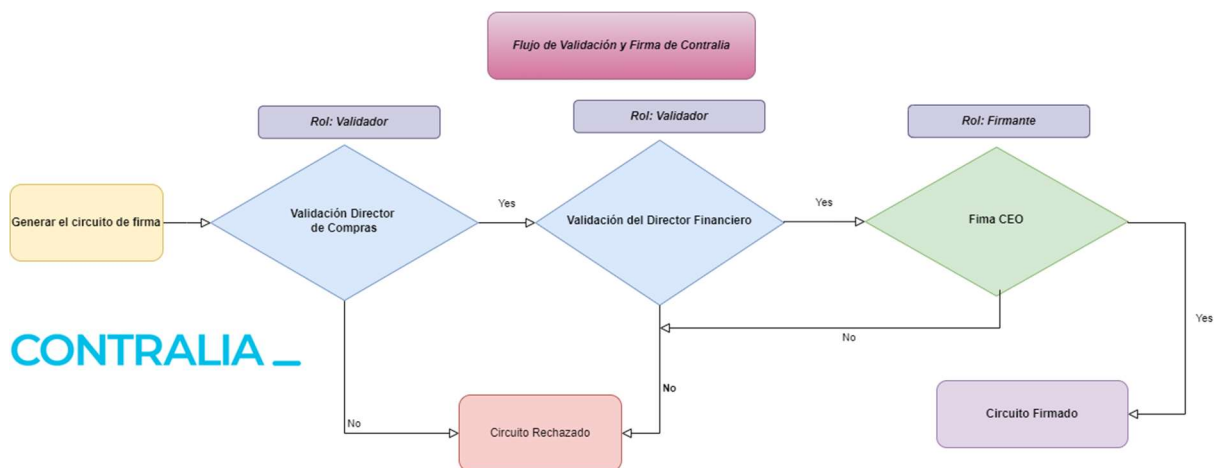
2. TIPOLOGIAS DE INTERVENIENTES

Os intervenientes podem ser ou Validador ou Signatário.

- Validador: Aprova o conteúdo do documento.
- Signatário: Assina o conteúdo do documento.

A cada participante é-lhe atribuído um papel na forma de criação do circuito:

Note-se que um circuito de assinatura pode ter tanto validadores como signatários. Abaixo está um exemplo de um fluxo de assinaturas contendo ambos os papéis.



3. TIPOLOGIAS DE CIRCUITOS DE ASSINATURA

As tipologias de circuitos de assinatura são marcadas pelo nível de segurança que cada uma apresentar. Na data da última versão deste documento, dispomos de 3 tipologias:

Tipologia 1.

- Assinatura do remetente com um certificado digital. Pode usar o seu próprio certificado digital ou a assinatura delegada.
- Assinatura do receptor com assinatura delegada de Seres. A assinatura do receptor é protegida com o código **OTP**¹.

Tipologia 2.

- Assinatura do remetente com um certificado digital. Pode usar o seu próprio certificado digital ou a assinatura delegada.
- Verificação da assinatura do receptor. é feita com uma verificação de aceitação via WEB. É assinado com o certificado SERES (assinatura delegada).

Tipologia 3.

- Assinatura do remetente com um certificado digital. Pode usar o seu próprio certificado digital ou assinatura delegada.
- Assinatura do receptor com certificado próprio emitido por uma Autoridade de Certificação (por exemplo, FNMT) ou DNle.

O cliente pode contratar pelo menos uma tipologia. No caso de ter apenas uma tipologia, esta última é tida em conta sem que o cliente tenha que fazer nada. No caso de ter mais do que uma, deve indicar qual utilizar no formulário de criação de circuitos (ponto seguinte).

¹ **OTP**: Palavra-passe única. Código numérico enviado ao signatário por SMS ou EMAIL para relacionar um número de telemóvel ou endereço de e-mail a uma pessoa e assinatura. Este tipo de assinatura é válido e reconhecido dentro da normativa [eIDAS](#).

4. CRIAÇÃO DE CIRCUITO DE ASSINATURA

Para criar um circuito de assinatura, clicar no botão de criação de circuitos:



NUEVO CIRCUITO ✕

* Campo obligatorio

Identificador circuito *:

Nombre circuito *:

E-mail del responsable :

Idioma *: Español ▼

Sello de tiempo : No Si

Tipo de Firma *: Firma con código OTP ▼

Añadir documentos

Sus documentos (max.1) *

Nombre	Tamaño
<input type="button" value="Añadir documento"/>	

Sus anexos (max.3)

Nombre	Tamaño
<input type="button" value="Añadir anexos"/>	
<input type="button" value="Eliminar anexos"/>	

Añadir destinatarios

Sus destinatarios (max.5)

Apellidos *	Nombre *	Rol *	Correo electrónico *	Teléfono * <small>(Debe comenzar con + ó 00)</small>	Enviar código por *	Teléfono Modificable
<input type="text"/>	<input type="text"/>	Firmante ▼	<input type="text"/>	<input type="text"/>	SMS ▼	<input type="checkbox"/>
<input type="button" value="Añadir destinatario"/>						

Receptores en copia (max.5)

Correo electrónico *
<input type="text"/>
<input type="button" value="Añadir receptor"/>

Plazo antes de expiración del circuito * (Pasado este plazo el circuito expirará y se anulará)

1 ▼ días

Recordar cada *

1 ▼ días

Cada um dos campos é detalhado abaixo:

Identificador do circuito: é o identificador interno do fornecedor se quiser integrar a rastreabilidade do circuito no CRM/ERP do emissor. Caso contrário, pode introduzir qualquer valor.

Nome do circuito: nome sob o qual o circuito de assinatura aparece. É muito útil ter os contratos ordenados e poder procurá-los pelo nome.

E-mail responsável: e-mail da pessoa a quem são enviadas todas as notificações de alteração de estado. Se não for indicado, o e-mail do fornecedor configurado em BDD será tido em conta.

Língua: língua em que o signatário é notificado. As línguas disponíveis são: espanhol, inglês, português e francês.

Nível de segurança: este parâmetro identificaria a tipologia do circuito a ser lançado. Para mais informações, ver o ponto [TIPOLOGIAS DE CIRCUITOS DE ASSINATURA](#). Se apenas tiver sido contratada uma tipologia, isto é tido em conta e este campo não aparecerá no formulário.

Os seus documentos: o próprio contrato.

Os seus anexos: os anexos. Como mencionado acima, os anexos não estão sujeitos a assinatura.

Destinatários:

- Apelido.
- Nome.
- Função: Validador ou Signatário.
- E-mail.
- Telefone. Deve sempre começar com "00" ou "+" e o código do país. Por exemplo, "0034" ou "+34".
- Enviar código OTP por: meios pelos quais o receptor pode receber o código de assinatura OTP. No caso de escolher a opção "Qualquer um", o cliente pode escolher entre SMS ou EMAIL.
- Telefone alterável: indica se o signatário pode alterar o número de telefone para a recepção do SMS de assinatura.

Destinatários em cópia: e-mails de pessoas que recebem uma cópia do documento final assinado.

Prazo antes da expiração do circuito: dias de expiração.

Relembrar a cada: a cada quantos dias quiser enviar um email de lembrete de assinatura para os signatários. No caso de multi-signatários, aqueles que já assinaram, não receberão o lembrete.

5. ASSINATURA DO CONTRATO PELO CLIENTE

O e-mail que o cliente recebe tem este aspecto:



ma, 29/06/2021 15:36
DEV SERES ESPAÑA <desacontralia@seresnet.com>
Solicitud de firma de documento

Para Hicham Qaissi

Estimado/a Hicham QAISSE,

DEV SERES ESPAÑA le invita a firmar un documento en línea. Por favor, haga clic en el siguiente enlace: [solicitud de firma](#).

Contexto de firma: Seguro Vehículo.
Código único de verificación: 986164946e204bc3b4298613e3b0aab8.
Fecha de vencimiento: 30/06/2021 15:36:29+02:00.

Un saludo cordial.

SERES
GRUPO DOCAPOSTE

Este mensaje ha sido generado de forma automática, por favor, no responda al mismo.

Clicando no link de assinatura, aparece o contrato propriamente dito e as opções para assinar ou rejeitar:



SERES
GRUPO DOCAPOSTE

Servicio de Firma Online de Documentos

El mecanismo de firma se ejecuta conforme a lo dispuesto en el Reglamento (UE) No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, por tanto al firmar usted acepta que dicho mecanismo es confiable y apropiado para los fines con los cuales se comunicó este mensaje y por tanto reconoce validez y efectos jurídicos a la firma electrónica generada. Al firmar acepta la documentación, la cual tendrá carácter contractual y registrará las relaciones entre las partes conforme a lo recogido en las condiciones contenidas en la misma.

He leído y acepto las [condiciones de la firma electrónica del Servicio Contralia](#).

Número de teléfono  España (34)

Contexto de firma: Seguro Vehículo
Nombre del firmante: Hicham QAISSE
Código único de verificación: 986164946e204bc3b4298613e3b0aab8
Fecha de vencimiento: 30/06/2021 15:36:29+02:00

1 of 2 Automatic Zoom

 **Concello de Lugo**
Seguro Automovil Completo

DATOS DE LA PERSONA SOLICITANTE

A partir de agora, o signatário tem duas opções:

- Iniciar o processo de assinatura. Quando o signatário aceita as condições do contrato e clica no botão "Iniciar processo de assinatura", receberá no seu telemóvel ou e-

Uma vez assinado ou rejeitado o circuito, este já não pode ser acedido:

SERES
GRUPO DOCAPOSTE

Servicio de Firma Online de Documentos


El mecanismo de firma se ejecuta conforme a lo dispuesto en el Reglamento (UE) No. 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, por tanto al firmar usted acepta que dicho mecanismo es confiable y apropiado para los fines con los cuales se comunicó este mensaje y por tanto reconoce validez y efectos jurídicos a la firma electrónica generada. Al firmar acepta la documentación, la cual tendrá carácter contractual y regirá las relaciones entre las partes conforme a lo recogido en las condiciones contenidas en la misma.

Este circuito de firma está cerrado ya que uno de los firmantes lo ha rechazado con fecha 29/06/2021 15:46:48+02:00.


Se a assinatura for rejeitada por um dos signatários, o circuito é atualizado com o estatuto "Rejeitado por um signatário". O signatário que rejeitou o circuito seria marcado com um X vermelho:

Nombre	Fecha de envío	Estado	Documentos principales	Documentos adjuntos
Seguro Vehículo	28/06/2021 15:36:29	Rechazado por algún firmante	Contrato.pdf	Michaen GAUSBI
CircuitoTest	28/06/2021 17:27:22	Rechazado por algún firmante	Contrato.pdf	Michaen GAUSBI

Se o circuito for totalmente assinado por todos os signatários, tanto o remetente como o receptor recebem um e-mail com um ZIP. Este ZIP contém tanto os documentos assinados como um certificado de prova da SERES como um terceiro de confiança, que resume todos os detalhes do circuito de assinatura, desde a sua criação até à sua assinatura completa.

 **DEV SERES ESPAÑA** <desacontralia@seresnet.com>
Documentos firmados. Circuito: CircuitoTest

Para

 6de06eecf4aa4205b4247bbaaa146325.zip
3 MB

Le adjuntamos los documentos firmados del circuito CircuitoTest con fecha 28/06/2021 17:31:31+02:00.

El circuito de firma queda cerrado.

SERES
GRUPO DOCAPOSTE

Este mensaje ha sido generado de forma automática, por favor, no responda al mismo.




Uma cópia do certificado de prova em PDF pode ser descarregada abaixo:



6de06eecf4aa4205b
4247bbaaa146325_e

6. DESCARREGAR DOCUMENTOS ASSINADOS

O emissor, através da sua conta Connect WEB, pode descarregar o ficheiro ZIP clicando no botão do certificado que aparece à direita do estado do circuito de assinatura.

Nombre	Fecha de envío	Estado
CircuitoTest	29/06/2021 15:53:28	Petición de firma notificada a los firmantes 
Seguro Vehículo	29/06/2021 15:36:29	Rechazado por algún firmante
CircuitoTest	28/06/2021 17:27:22	Totalmente firmado 
CircuitoTest	25/06/2021 12:39:23	Rechazado por algún firmante
Circuito Test Jorge	23/06/2021 16:43:24	Totalmente firmado 

Existe uma forma adicional de descarregar o ficheiro ZIP, quer digitalizando ou clicando no código QR incluído dentro do certificado de prova:

Estado del proceso

FIRMADO POR TODAS LAS PARTES

Fecha de Firma 24/11/2020 13:06:26+01:00

Firma e identificación de este CERTIFICADO

Código Registro Electrónico NOTARIAL 05beb43e610f418587ccdf9489080b

Descargar copia original de este certificado



Firma del Tercero de Confianza

Digitally signed by CERTIFICADO
TEST DESARROLLO
Date: 2020.11.24 13:07:18 CET
Reason: Contralia. SERES España

SERES
GRUPO DOCAPOSTE

O sistema solicitará um endereço de e-mail para o qual enviar o ficheiro ZIP. O e-mail deve ser de um dos membros do circuito: remetente ou receptor do circuito de assinatura.

SERES
GRUPO DOCAPOSTE

Servicio de Firma Online de Documentos

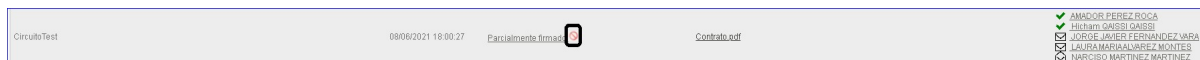
Descarga de certificado de evidencias para el circuito **cf2d864bfe6f4cd2ab4436d1752ded4b**

e-mail: Enviar certificado

O remetente pode também visualizar os documentos assinados clicando nos seus nomes.

7. CANCELAMENTO DO CIRCUITO

O remetente pode cancelar um circuito emitido desde que tenha um dos seguintes estatutos: "Notificado" ou "Parcialmente assinado". Para tal, clicar no botão de cancelamento.



Uma vez cancelado o circuito, os signatários já não têm acesso ao circuito.

8. MODELOS DE CIRCUITOS DE ASSINATURA

Por modelo de circuito de assinatura, entendemos a configuração de um fluxo de trabalho de validação e/ou assinatura com um conjunto de metadados, e estes fluxos de trabalho podem ser utilizados no formulário de criação do circuito sem necessidade de reler todos os parâmetros.

O menu de criação de modelos é semelhante ao menu de criação de circuitos:

Plantilla-Circuito
✕

* Campo obligatorio

Nombre plantilla *:

E-mail del responsable *:

Idioma : Español ▼

Sello de tiempo : No Si

Tipo de Firma : Firma con código OTP ▼

Añadir documentos

Sus documentos (max.1)

Nombre

+ Añadir documento

Sus anexos (max.3)

Nombre

+ Añadir anexos
- Eliminar anexos

Añadir destinatarios

Sus destinatarios (max.5)

Apellidos *	Nombre *	Rol *	Correo electrónico *	Teléfono <small>(Debe comenzar con + ó 00)</small>	Teléfono <small>Modificable</small>
+ Añadir destinatario					

Receptores en copia (max.5)

Correo electrónico

+ Añadir receptor

Plazo antes de expiración del circuito (Pasado este plazo el circuito expirará y se anulará)

1 ▼ días

Recordar cada

1 ▼ días

- Anular
+ Aceptar
+ Limpiar

Na lista de modelos, existe um menu para a sua utilização, edição, eliminação ou duplicação.

The screenshot shows the 'Contralia' interface with a table of templates. The table has three columns: 'Nombre Plantilla', 'Fecha Creación/Modificación', and 'Operación'. A context menu is open over the first row, showing options: 'Utilizar', 'Modificar', 'Eliminar', and 'Duplicar'.

Nombre Plantilla	Fecha Creación/Modificación	Operación
Plantilla contrato-tipo-compra-venta-vehiculos.pdf (AU)Suma Banca	09/09/2022 06:59:25	----- Utilizar Modificar Eliminar Duplicar
Nueva plantilla de prueba en PFE Contrato.edf (AU)Suma Banca	20/07/2022 13:04:39	
Firma Contrator Limp Contrato.edf (AU)Nombre Validador: (F)Nombre Firmante	19/07/2022 09:49:58	
Plantilla 18072022 Contrato.edf (AU)Hichem DASSI	18/07/2022 19:26:31	-----

9. TIMELINE

Uma vez assinado o circuito por todos os membros, é disponibilizada ao transmissor uma tabela de sequência de estados com datas e horas:

FIRMA POLÍTICA DE REGISTRO DE JORNADA José Antonio De la Torre De la Fuente	14/06/2021 11:26:40	Totalmente firmado		Aceptacion_entrega_politica_de_tiempo_de_trabajo.pdf		José Antonio De la Torre De la Fuente
FIRMA POLÍTICA DE REGISTRO DE JORNADA José Antonio De la Torre De la Fuente	11/06/2021 09:59:12	Totalmente firmado		Aceptacion_entrega_politica_de_tiempo_de_trabajo.pdf		José Antonio De la Torre De la Fuente
FIRMA POLÍTICA DE REGISTRO DE JORNADA José Antonio De la Torre De la Fuente	11/06/2021 09:52:16	Totalmente firmado		Aceptacion_entrega_politica_de_tiempo_de_trabajo.pdf		José Antonio De la Torre De la Fuente
FIRMA POLÍTICA DE REGISTRO DE JORNADA	09/06/2021 11:25:38	Totalmente firmado		Aceptacion_entrega_politica_de_tiempo_de_trabajo.pdf		Mariano Martínez
FIRMA POLÍTICA DE REGISTRO DE JORNADA	09/06/2021 11:17:36	Totalmente firmado		Aceptacion_entrega_politica_de_tiempo_de_trabajo.pdf		Mariano Martínez



As datas e horas são exibidas no fuso horário do país do utilizador ligado (configurado quando um cliente se regista).

10. PESQUISA DE CIRCUITO

Está disponível um formulário de pesquisa de circuitos:

The screenshot shows a web interface for searching circuits. At the top, there are three buttons: 'Nuevo circuito de firma' (with a checkmark), 'Buscar' (with a magnifying glass icon), and 'Certificado digital' (with a star icon). Below these is a table with a header 'Circuitos adjuntos' and several empty rows. To the right of the table is a search form with the following fields: 'Nombre' (text input), 'Fecha de envío' (date range with 'a' separator), 'Estado' (dropdown menu), 'Firmante' (text input), 'Documento principal' (text input), and 'Documento adjunto' (text input). At the bottom of the form, there are three buttons: 'Descargar CSV' (with a download icon), 'Buscar' (with a magnifying glass icon), and 'Limpiar' (with an 'x' icon). The 'Buscar' button at the top and the 'Descargar CSV' button at the bottom are highlighted with black boxes.

As pesquisas podem ser descarregadas em formato CVS para análise no futuro.

11. LEMBRETES DE ASSINATURA

Para além dos lembretes automáticos de assinatura (se o remetente assim tiver indicado no formulário de criação do circuito), o remetente pode enviar lembretes de assinatura a destinatários específicos, desde que estes últimos não tenham assinado e que o circuito tenha o estatuto "Notificado" ou "Parcialmente Assinado". Para tal, clicar no nome do signatário e na janela pop-up clicar em "Enviar lembrete de assinatura". O destinatário recebe um e-mail idêntico ao primeiro, recordando-lhe a assinatura.

Datos del firmante ✕

Nombre: Hicham	Apellidos: QAISSI QAISSI
Teléfono: 0034639736914	Email: hicham.qaissi@seres.es
Estado: 29/06/2021 15:53:30 	<input type="button" value="✓ Enviar recordatorio de firma"/>

12. HISTÓRICO DO ESTATUTO DE UM SIGNATÁRIO

A qualquer momento, o emissor pode saber como tem decorrido o seu contrato. Pode saber o estado e as datas de cada signatário. Para tal, clique no nome do signatário.

Datos del firmante ✕

Nombre: Hicham	Apellidos: QAISSI 1
Teléfono: 0034639736914	Email: hicham.qaissi@seres.es
Estado: 28/06/2021 17:31:29	
28/06/2021 17:31:13	
28/06/2021 17:27:56	Código OTP solicitado y enviado por SMS al 0034687268785
28/06/2021 17:27:25	

14. INSTALAÇÃO DE CERTIFICADOS DIGITAIS

Como mencionado acima, o emissor pode utilizar o seu próprio certificado digital para a assinatura. Para o fazer, o certificado deve ser instalado na loja de certificados Connect.



Se o emissor não tiver certificado, é utilizada a assinatura delegada com o certificado SERES.

15. CAIXAS DE ASSINATURA

Por defeito, as caixas de assinatura do terceiro de confiança (SERES), do emissor do contrato e do cliente receptor aparecem numa página adicional que é adicionada ao contrato PDF.

Se o remetente quiser mostrar apenas algumas das caixas, mostrando-as numa página específica e numa posição específica no documento, deve notificar o seu representante de vendas para armazenar esta configuração na base de dados. Se um emissor tiver tal configuração na base de dados, esta será utilizada, por isso, tenha cuidado ao colocar as caixas em áreas do documento onde haja informação sensível, uma vez que estas caixas esconderiam o conteúdo.

É aconselhável utilizar sempre as configurações padrão.

16. REQUISITOS PARA ASSINATURA COM CERTIFICADO PRÓPRIO.

16.1. INSTALAÇÃO JAVA

A componente de assinatura local Contralia Seres é um JNLP descarregável que pode ser executado em Java. Para isso, a máquina local deve ter Java (versão 8) instalado.

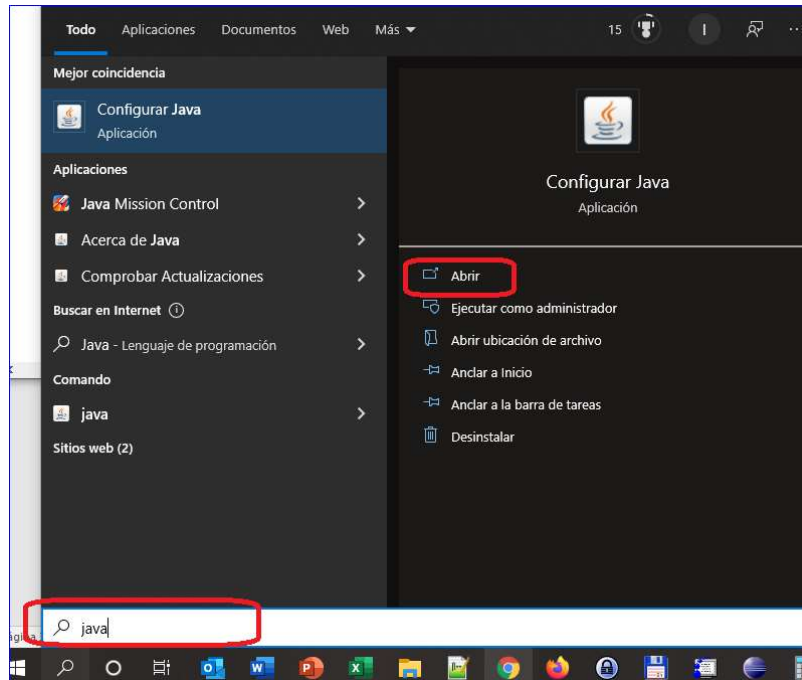
Se não tiver o Java JRE 8 instalado, pode descarregá-lo e instalá-lo clicando no seguinte [link](#).

16.2. EXCEPÇÕES JAVA

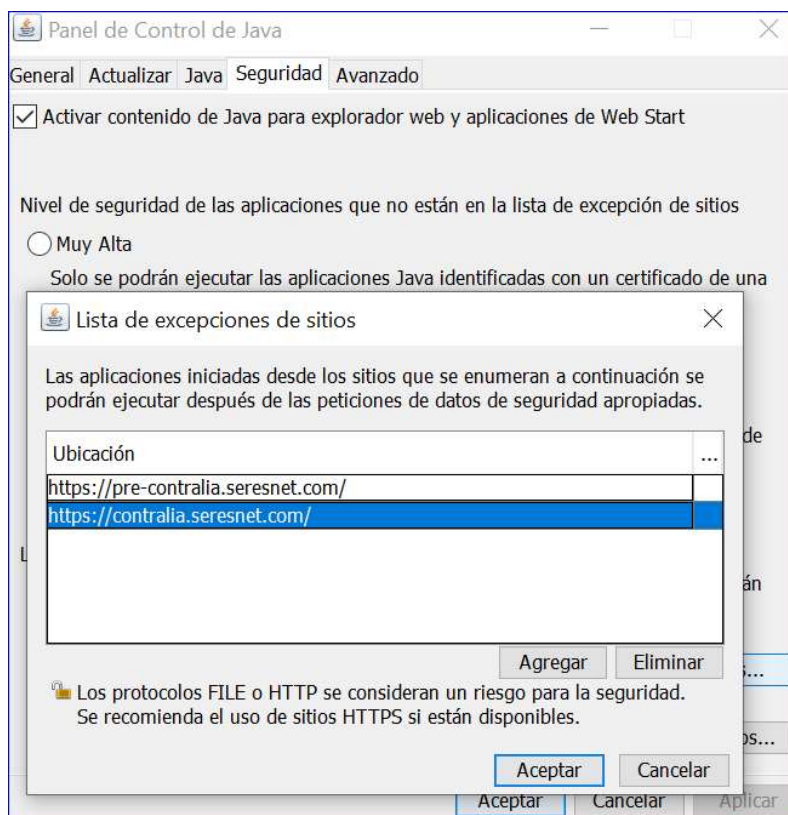
Por razões de segurança, Java bloqueia a maioria dos endereços da execução de programas de terceiros na sua máquina local.

Para o fazer, os URLs de execução teriam de ser adicionados às exceções Java.

1. Abrir o painel de controlo Java



2. Adicionar o URL de execução da componente de assinatura no separador de segurança:

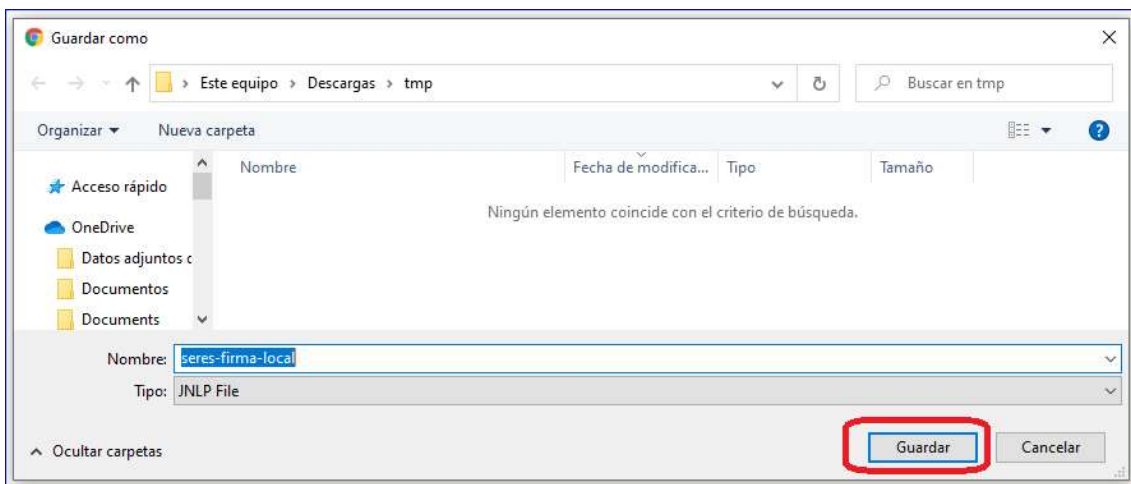


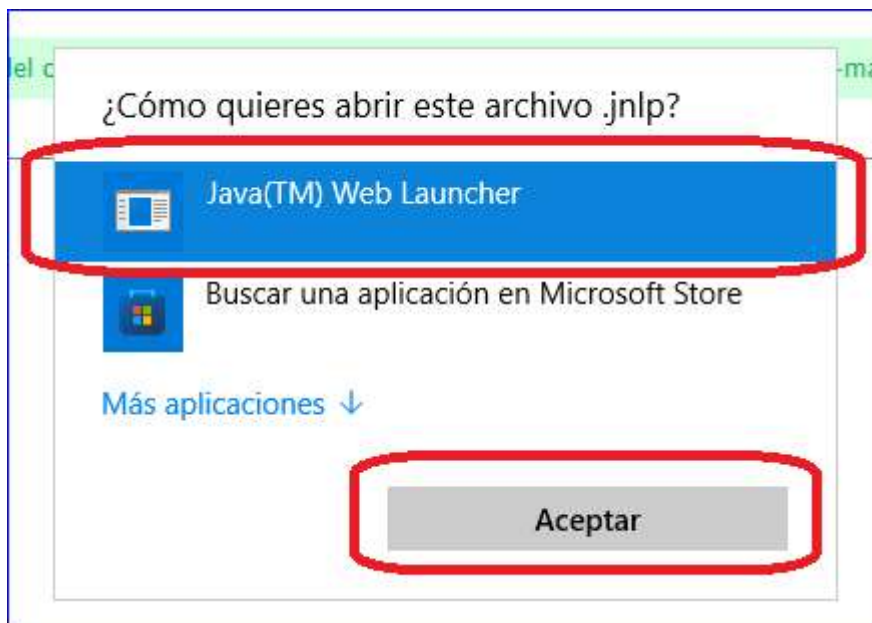
Ambiente TESTE: <https://pre-contralia.seresnet.com>

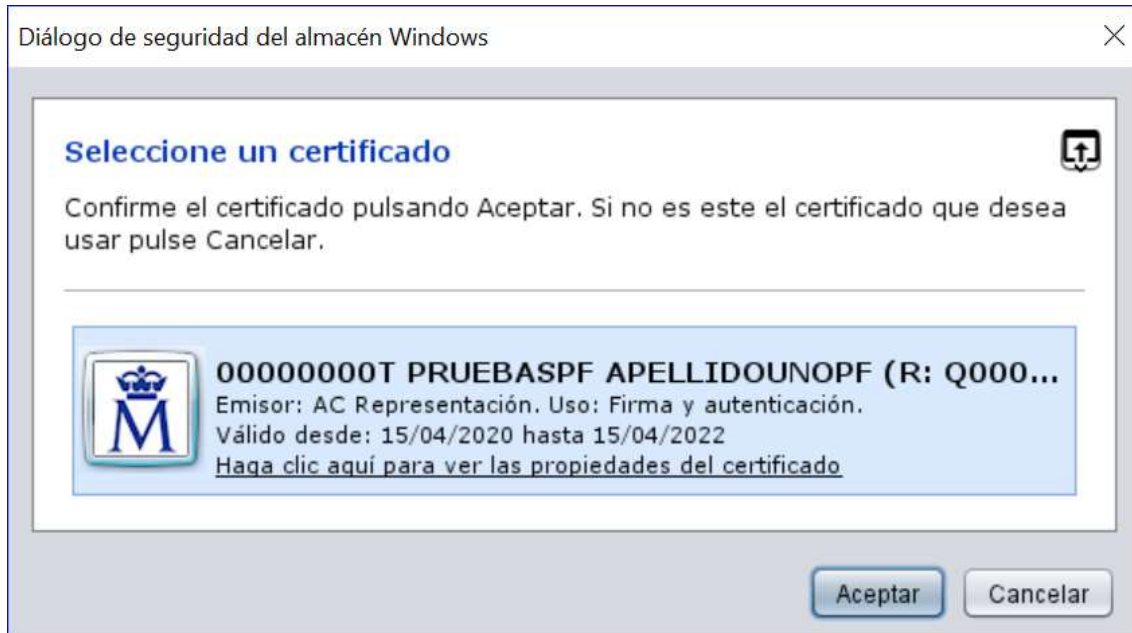
Ambiente PROD: <https://contralia.seresnet.com>

16.3. DOWNLOAD E EXECUÇÃO DE COMPONENTE DESCARREGÁVEL

Os ecrãs seguintes mostram os passos a seguir para descarregar e executar a componente de assinatura do nosso documento:



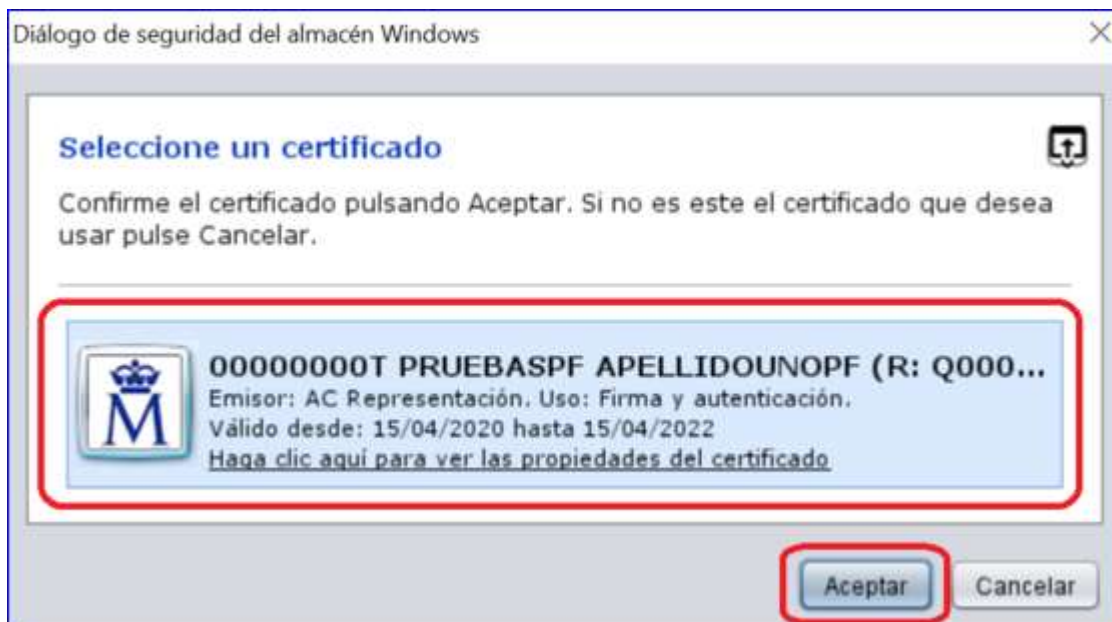




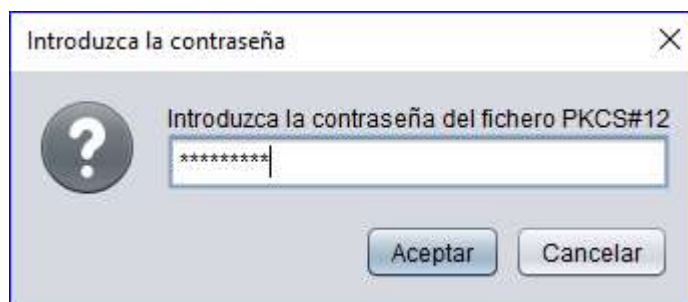
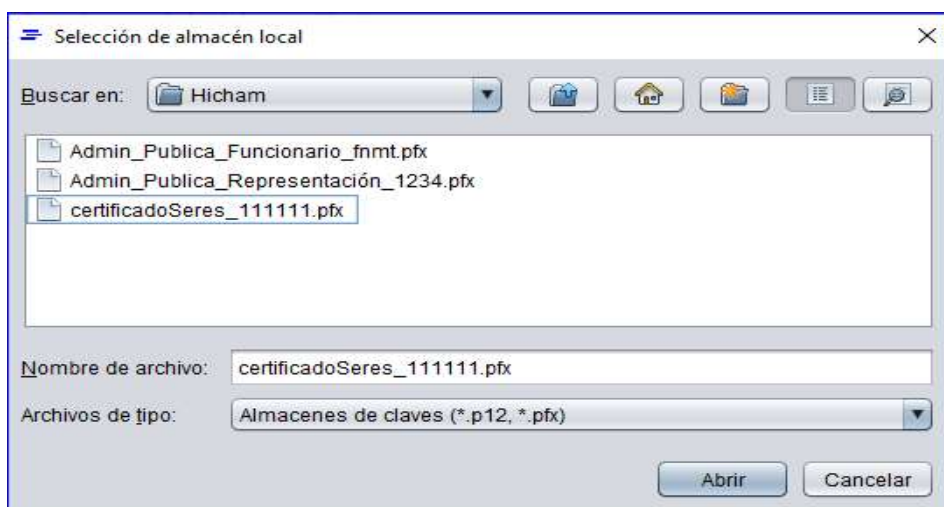
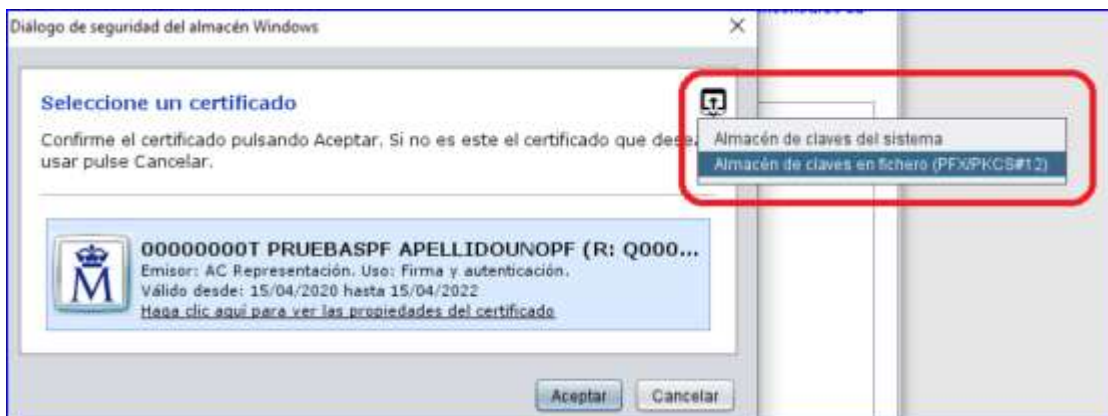
A partir deste ponto, temos duas opções:

Assinar com um dos certificados que temos instalados no nosso armazém de certificados ou utilize um certificado acessível (ficheiro binário).

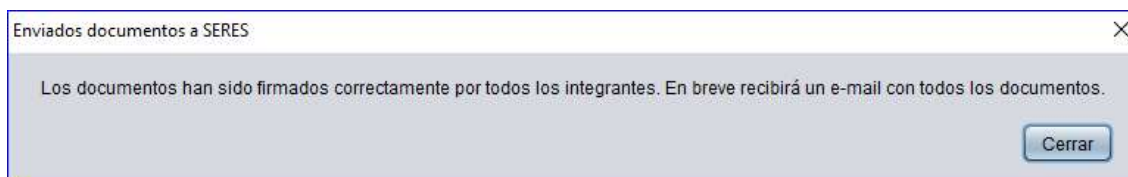
1. Assine com um dos certificados instalados no nosso armazém de certificados:



2. Assinar com um ficheiro de certificado localizado num caminho acessível:



Uma vez que assinarmos com uma das duas opções acima, recebemos uma mensagem de confirmação:



A partir deste momento, o documento está completamente assinado. Numa questão de segundos, receberá um e-mail com todos os documentos.

16.4. ASSINATURA COM DNIE

Com a componente de assinatura com certificado local, também o podemos fazer com o certificado de assinatura digital incluído no Documento Nacional de Identidade (DNIE).

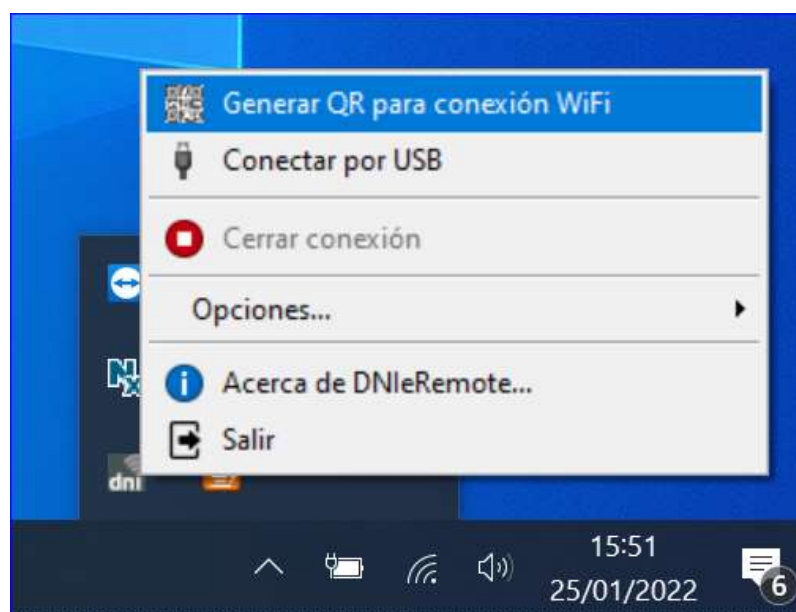
Há duas maneiras de assinar com o nosso DNIE:

1. Com um leitor DNIE:

Com qualquer leitor DNIE disponível no mercado, ligar o leitor à porta USB e inserir o DNIE no leitor. Ao abrir o link de assinatura que recebemos por e-mail, na lista de certificados incluída no nosso armazém de certificados, o certificado electrónico aparecerá e podemos assinar com ele como se fosse um certificado fisicamente instalado na nossa máquina.

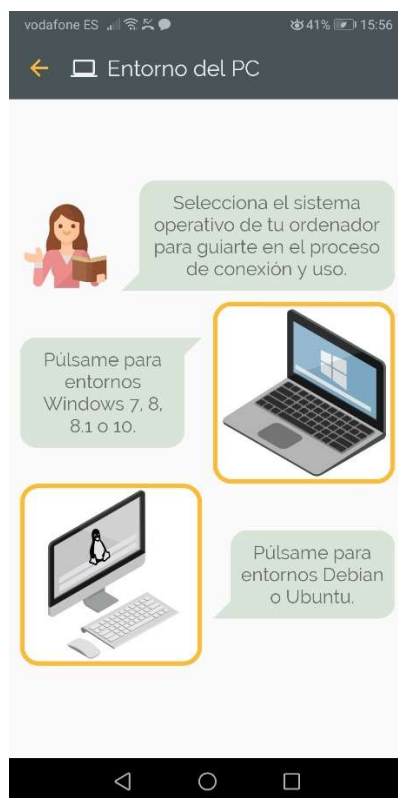
2. Com o nosso smartphone:

- Esta assinatura é feita através do NFC. Para tal, precisamos de instalar um par de componentes no nosso PC e smartphone:
- No seu PC, descarregue a aplicação DNIERemote a partir da Polícia Nacional no seguinte link.
- No seu smartphone, descarregue a aplicação DNIESmartConnect a partir da Fábrica Nacional de Moneda y Timbre (FNMT) no seguinte link.
- Executamos ambas as aplicações no nosso PC (DNIERemote) e smartphone (DNIESmartConnect).
- Modo de ligação WiFi:
 - Ligue o seu PC e smartphone à mesma rede WIFI.
 - No nosso PC, no menu de opções do DNIERemote, na barra de notificação, seleccionar Generate QR for WiFi connection:





- No nosso smartphone, na aplicação DNIeSmartConnect, seleccionamos o sistema operativo do nosso computador:



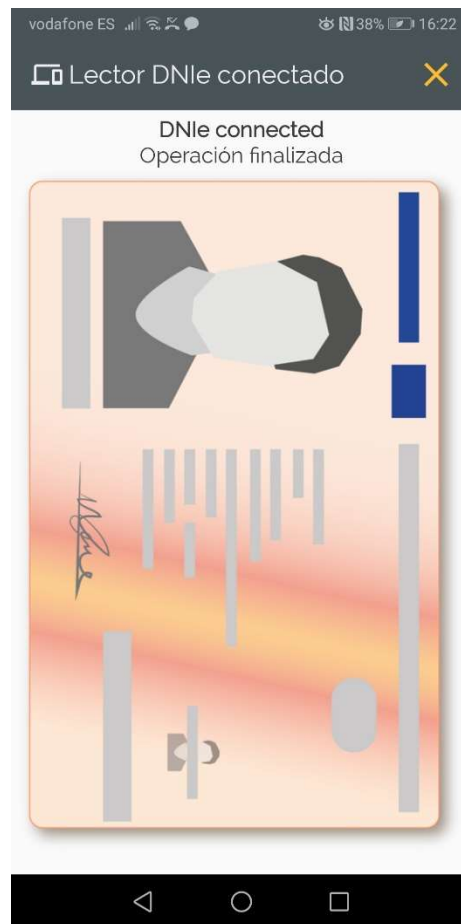
- Seleccionar o tipo de ligação WiFi:

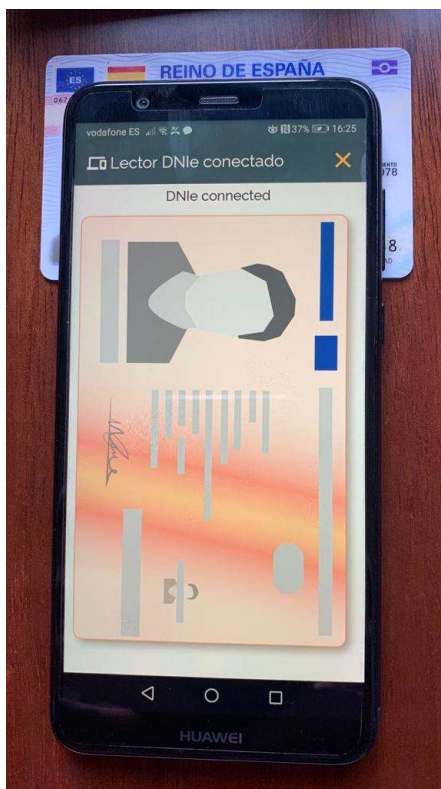


- A partir do smartphone, digitalizar o QR gerado no PC. A partir deste momento, o DNleRemote detecta o nosso smartphone.



- O DNleRemote irá pedir-nos para aproximarmos o nosso DNle do dispositivo:





- A partir deste momento, ao assinar com Contralia, o nosso DNle aparecerá como um dos certificados do armazém de certificados.
- Modo de ligação USB:

O procedimento é muito semelhante ao da ligação WiFi, excepto que neste caso temos de ligar o smartphone ao PC com um cabo USB.

17. ANEXOS

17.1. ESPECIFICAÇÕES DE SEGURANÇA E INFRA-ESTRUTURAS

17.1.1. SEGURANÇA FÍSICA E AMBIENTAL

Os Centros de Processamento de Dados SERES (DPCs) estão equipados com controlos para impedir o acesso não autorizado, perda, roubo, danificação ou comprometimento de instalações e bens de informação. Foram implementados:

- Controlos de acesso físico: guardas, câmaras, controlo de acesso biométrico, etc.
- Controlos ambientais, por exemplo: sistemas de detecção e extinção de incêndios, Sistema de Alimentação Ininterrupta Redundante de electricidade (SAIs), Sistema de Ar Condicionado Redundante e Controlo de Humidade, etc.
- Protecções perimetrais: CCTV, detecção de movimento, construção com protecção contra incêndios com factores entre RF120 e RF240, etc.

17.1.2. SEGREGAÇÃO DA INFORMAÇÃO

SERES segrega logicamente tanto o processamento como o armazenamento da informação da empresa cliente por meio de diferentes mecanismos de controlo.

Os acessos necessários para fornecer apoio aos utilizadores, o acesso à base de dados pelo pessoal especializado e quaisquer outros métodos de acesso não normalizados são identificados e restringidos.

17.1.3. PROCESSO DE IDENTIFICAÇÃO E AUTENTICAÇÃO

A SERES assegura que todos os utilizadores internos com acesso à sua infra-estrutura disponham de identificadores únicos e mecanismos de autenticação apropriados para justificar a identidade destes utilizadores. Estes mecanismos incluem os seguintes controlos:

- Os utilizadores inactivos são desactivados após 30 dias e apagados após 90 dias.
- As palavras-passe iniciais fornecidas ao utilizador devem ser alteradas após o primeiro login.
- As senhas devem ser alteradas a intervalos definidos (90 dias).
- É necessário um comprimento mínimo de senha de 8 caracteres.
- As palavras-passe devem ser complexas, tal como definidas pelas normas da indústria.
- A identidade do utilizador final é validada antes de a palavra-passe ser redefinida.
- As senhas de instalação predefinidas são alteradas durante a instalação do software.
- As palavras-passe dos utilizadores finais e administradores nunca são guardadas na sua forma original (sem hash) e nunca são transmitidas por correio electrónico.
- As senhas não são transmitidas em texto claro em redes internas ou externas.

17.1.4. RESTRIÇÕES DE CONTROLO DE ACESSO

A SERES controla o acesso aos sistemas de processamento, armazenamento e comunicação de dados para impedir o acesso não autorizado aos sistemas de informação por utilizadores internos e finais. Entre os controlos implementados, encontram-se os seguintes:

- O acesso aos sistemas e redes é restrito àqueles que o requerem para as suas responsabilidades de trabalho.
- O acesso é desactivado imediatamente após já não ser necessário.
- As comunicações de dados são protegidas para impedir o acesso não autorizado.
- Os pedidos de acesso são devidamente aprovados antes de serem deferidos.

17.1.5. PREVENÇÃO DE INTRUSÃO

A SERES possui ferramentas de prevenção de intrusão, detecção, inspecção de conteúdos e monitorização para ajudar a prevenir e detectar o uso indevido de sistemas de informação no âmbito de aplicação. Estas ferramentas incluem:

- Implementação de soluções anti-malware.
- Criptografia de palavras-passe relacionadas com ligações a sistemas.
- São efectuados testes de penetração e vulnerabilidade pré-produção para todas as aplicações acessíveis ao público através da Internet.
- Sistema de Detecção de Intrusão / Sistema de Prevenção de Intrusão (IDS / IPS).
- Um Sistema de Gestão de Informação e Eventos de Segurança (SIEM) é utilizado para recolher, agregar, correlacionar e fornecer notificação de eventos de segurança.

17.1.6. ENCRIPTAÇÃO

A SERES implementa diferentes mecanismos de encriptação de acordo com as melhores práticas da indústria, a fim de garantir a confidencialidade da informação, entre elas:

- Encriptação (hashing) de palavras-passe relacionadas com ligações a sistemas.
- Capacidade de encriptar dados em trânsito pela Internet utilizando protocolos de comunicação seguros (sFTP, HTTPS, etc.).
- O sistema fornece encriptação de dados em repouso em bases de dados, utilizando o esquema de encriptação por blocos AES-192, de acordo com a sensibilidade da informação armazenada.

17.1.7. ARQUIVAMENTO DE CIRCUITOS CONTRALIA

A SERES armazena os circuitos de assinatura do Contralia durante os anos exigidos pelos regulamentos de cada país do cliente, podendo aumentar estes anos se o cliente necessitar. O acesso a estes circuitos é garantido 24x7, podendo utilizar o formulário de pesquisa para localizar os circuitos de acordo com o seu nome, nomes dos signatários ou e-mails, estado e data. Por Circuito, entendemos os documentos de assinatura em PDF e a rastreabilidade das alterações do seu estado.

A SERES disponibiliza aos seus clientes a possibilidade de descarregar relatórios de circuitos de assinatura em formato CSV.

