

Coordenadoria de Gestão da Informação

# MANUAL NOVA BIOMETRIA (BioID)

DETRAN-PR  
2ª versão

## Sumário

1. Introdução.....	3
2. Funcionamento da nova solução de Biometria (BioID).....	3
3. Leitor biométrico .....	4
4. Coletor de assinatura .....	4
5. Webcam .....	4
6. Instalação do Componente AHS.....	4
7. Instalação do certificado AHS .....	6
7.1. Instalar o Certificado root no navegador GoogleChrome .....	6
7.2. Instalar o Certificado root no navegador Mozilla Firefox .....	11
8. Testar a solução de biometria .....	14
9. Cadastrar equipamento no sistema de Habilitação .....	14
10. Bloquear equipamento cadastrado no sistema de Habilitação .....	14
11. Limpeza de cache na verificação biométrica BioID .....	15
12. Revisão do Guia Rápido.....	16

**CURITIBA 2023**

**Coordenadoria de Gestão da Informação**

Av. Victor Ferreira do Amaral, 2940, Bloco A, térreo - Capão da Imbuia - Curitiba-PR

CEP: 82.800-900

Coordenador: Giolvane Ferreira

Elaboração do Manual: Dionísio Benedito

**MANUAL NOVA BIOMETRIA (BioID)**

2ª Versão

Revisão 01: 24/01/2023

## 1. Introdução

A nova solução de biometria (BiID) funciona através da instalação de um componente de integração biométrica chamado “Antheus Hardware Server” (AHS) e Certificado no navegador a ser utilizado.

Com essa nova solução não haverá mais biometria em situação de IH (Intervenção Humana). Após 03 tentativas de verificação biométrica, se não for possível a confirmação do candidato/conductor o sistema solicitará a validação facial. Para isso é necessário ter uma webcam (compatível com a solução) instalada no computador.

Características da nova solução de biometria:

1. Desenvolvido para uso em Sistema Operacional Microsoft Windows 10, 64 bits;
2. Utiliza leitores de digitais mais modernos, compatíveis com o Sistema Operacional Windows 10, que foram homologados pelo Detran/PR;
3. Utiliza coletores de assinatura mais modernos, compatíveis com o Sistema Operacional Windows 10, que foram homologados pelo Detran/PR; (uso exclusivo para função coleta biométrica)
4. Utiliza Webcam com resolução mínima de vídeo HD, 720p (desejável Full HD 1080p), compatível com DirectX.
5. Pode ser utilizado nos navegadores Google Chrome e Mozilla Firefox, nas versões mais atuais.

**OBSERVAÇÃO:** após realização de testes, foi constatado que a nova solução de biometria funciona normalmente no Sistema Operacional Windows 11, porém é importante verificar se os leitores de digitais, coletores de assinaturas e webcams que se pretende utilizar irão funcionar no Sistema Operacional, através de documentos do equipamento ou diretamente com o fabricante.

**IMPORTANTE:** Antes da compra de leitores de digitais, coletores de assinatura e webcam, verificar junto ao Detran/PR se os mesmos funcionam na nova solução de biometria e se deverão ser submetidos para testes.

## 2. Funcionamento da nova solução de Biometria (BiID)

Para uso da nova solução de biometria será necessário:

- Instalar leitor de digital;
- Instalar coletor de assinatura (apenas para função coleta biometria);
- Conectar Webcam;
- Instalar o Componente AHS (Antheus Hardware Server);
- Instalar o Certificado da Antheus no navegador que será usado para acesso ao sistema de habilitação.

### 3. Leitor biométrico

Conectar o leitor de digital e instalar o driver do equipamento. Verificar funcionamento conforme orientações do fabricante do equipamento.

### 4. Coletor de assinatura

Conectar o coletor de assinatura e instalar o driver do equipamento. Verificar funcionamento conforme orientações do fabricante do equipamento.

### 5. Webcam

Conectar a webcam que deverá ter resolução mínima de vídeo HD, 720p (desejável Full HD 1080p). Este equipamento deve ser compatível com DirectX.

Webcam com resolução inferior ao requisito mínimo inviabilizam a verificação facial.

Para a função de coleta biométrica, não serão aceitas fotos obtidas em câmeras com resolução inferior ao requisito mínimo.

## 6. Instalação do Componente AHS

**1º Passo** – Baixar o Componente AHS.

Acessar o link <https://www.detran.pr.gov.br/Pagina/NOVA-Biometria>, selecionar “**Instruções de uso**” e clicar em “**Componente AHS – Antheus Hardware Server**”.

**2º Passo** – Instalar o Componente AHS.

Localizar o arquivo Antheus Hardware Server baixado no computador.

**IMPORTANTE:** O arquivo baixado estará compactado, sendo necessário sua descompactação antes de iniciar a execução do instalador.

Após descompactar o arquivo, acessar a pasta descompactada e dar duplo clique no instalador do AHS.

Na janela do instalador do AHS, selecionar a opção “***I accept the terms in the License Agreement***” e clicar no botão **Install**.

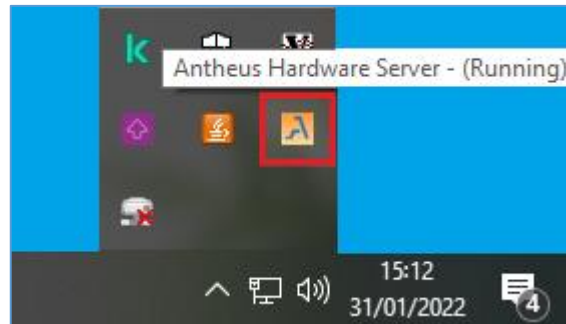
Após completada a instalação, clicar o botão **Finish**.

**3º Passo** – Verificar a versão do Componente AHS em execução.

Localizar o ícone AHS, na barra de tarefas do Windows, no canto inferior direito.

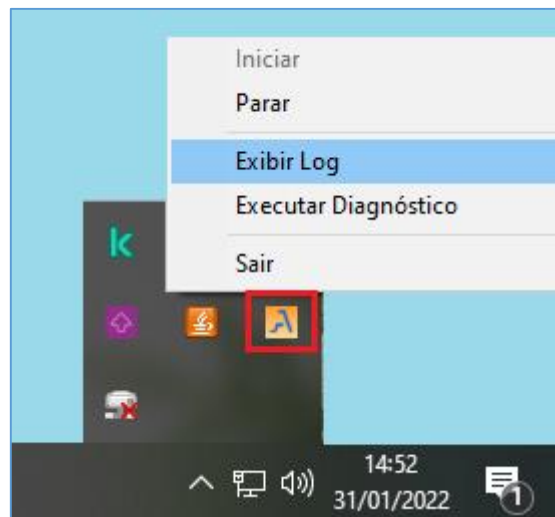
Geralmente o ícone do AHS fica nos ícones ocultos da barra de tarefa do Windows, conforme figura abaixo.

Passar o ponteiro do mouse em cima do ícone do AHS e verificar se o componente está rodando (Running).



**OBSERVAÇÃO:** Caso o AHS não esteja rodando, será necessário clicar com o botão direito do mouse no ícone do AHS e clicar em **Iniciar**.

Para verificar a versão que está rodando, clicar com o botão direito do mouse no ícone AHS e em seguida clicar em **Exibir Log**.

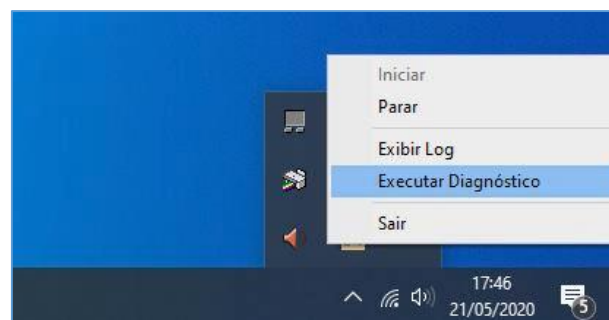


Irá abrir uma janela de logs do AHS.

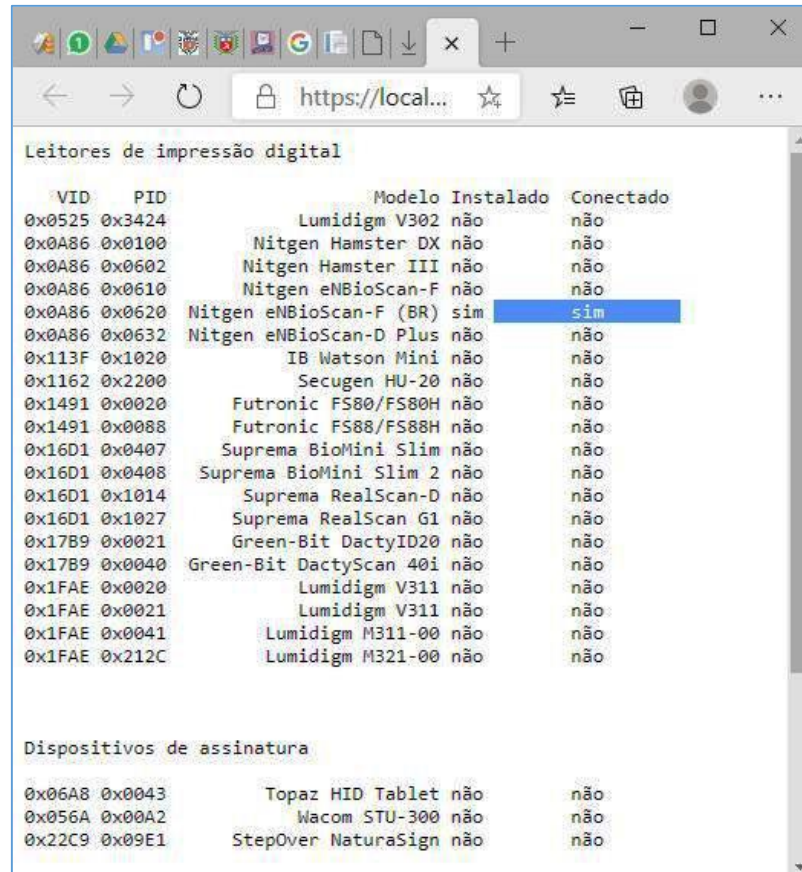
Na janela de logs do AHS, no começo do log, verificar a versão que está em execução.

**4º Passo** – Verificar se os equipamentos instalados foram identificados pelo AHS.

Clicar com o botão direito do mouse no ícone AHS e em seguida clicar em **Executar Diagnóstico**.



Uma tela de diagnóstico parecida com a imagem a seguir será aberta no browser. Verifique se os equipamentos necessários estão instalados e conectados.



Leitores de impressão digital				
VID	PID	Modelo	Instalado	Conectado
0x0525	0x3424	Lumidigm V302	não	não
0x0A86	0x0100	Nitgen Hamster DX	não	não
0x0A86	0x0602	Nitgen Hamster III	não	não
0x0A86	0x0610	Nitgen eNBioScan-F	não	não
0x0A86	0x0620	Nitgen eNBioScan-F (BR)	sim	sim
0x0A86	0x0632	Nitgen eNBioScan-D Plus	não	não
0x113F	0x1020	IB Watson Mini	não	não
0x1162	0x2200	Secugen HU-20	não	não
0x1491	0x0020	Futronic FS80/FS80H	não	não
0x1491	0x0088	Futronic FS88/FS88H	não	não
0x16D1	0x0407	Suprema BioMini Slim	não	não
0x16D1	0x0408	Suprema BioMini Slim 2	não	não
0x16D1	0x1014	Suprema RealScan-D	não	não
0x16D1	0x1027	Suprema RealScan G1	não	não
0x17B9	0x0021	Green-Bit DactyID20	não	não
0x17B9	0x0040	Green-Bit DactyScan 40i	não	não
0x1FAE	0x0020	Lumidigm V311	não	não
0x1FAE	0x0021	Lumidigm V311	não	não
0x1FAE	0x0041	Lumidigm M311-00	não	não
0x1FAE	0x212C	Lumidigm M321-00	não	não

Dispositivos de assinatura				
VID	PID	Modelo	Instalado	Conectado
0x06A8	0x0043	Topaz HID Tablet	não	não
0x056A	0x00A2	Wacom STU-300	não	não
0x22C9	0x09E1	StepOver NaturaSign	não	não

Se os dispositivos necessários não constarem como instalados e conectados, talvez seja o caso de trocar o equipamento de porta USB ou então reiniciar o computador e realizar novamente o diagnóstico. Se o problema persistir consulte um técnico especializado.

## 7. Instalação do certificado AHS

Mesmo se tratando de uma reinstalação do Componente AHS, recomenda-se verificar o Certificado de root da Antheus.

É imprescindível que o Certificado de root esteja instalado no navegador que será utilizado para o sistema da nova solução de biometria.

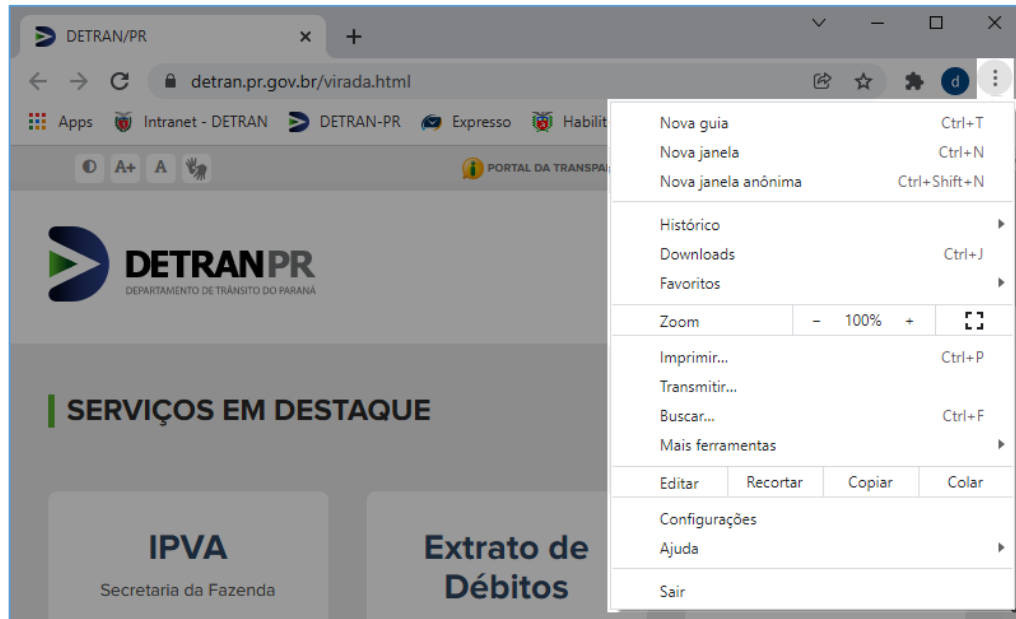
**OBSERVAÇÃO:** Recomenda-se utilizar o navegador GOOGLE CHROME, pois o novo sistema de Captura Biométrica, que foi desenvolvida para o sistema operacional Windows 10 pode apresentar falhas de funcionalidade, principalmente na captura de digitais, ao utilizar outros navegadores com no caso do Mozilla Firefox.

### 7.1. Instalar o Certificado root no navegador GoogleChrome

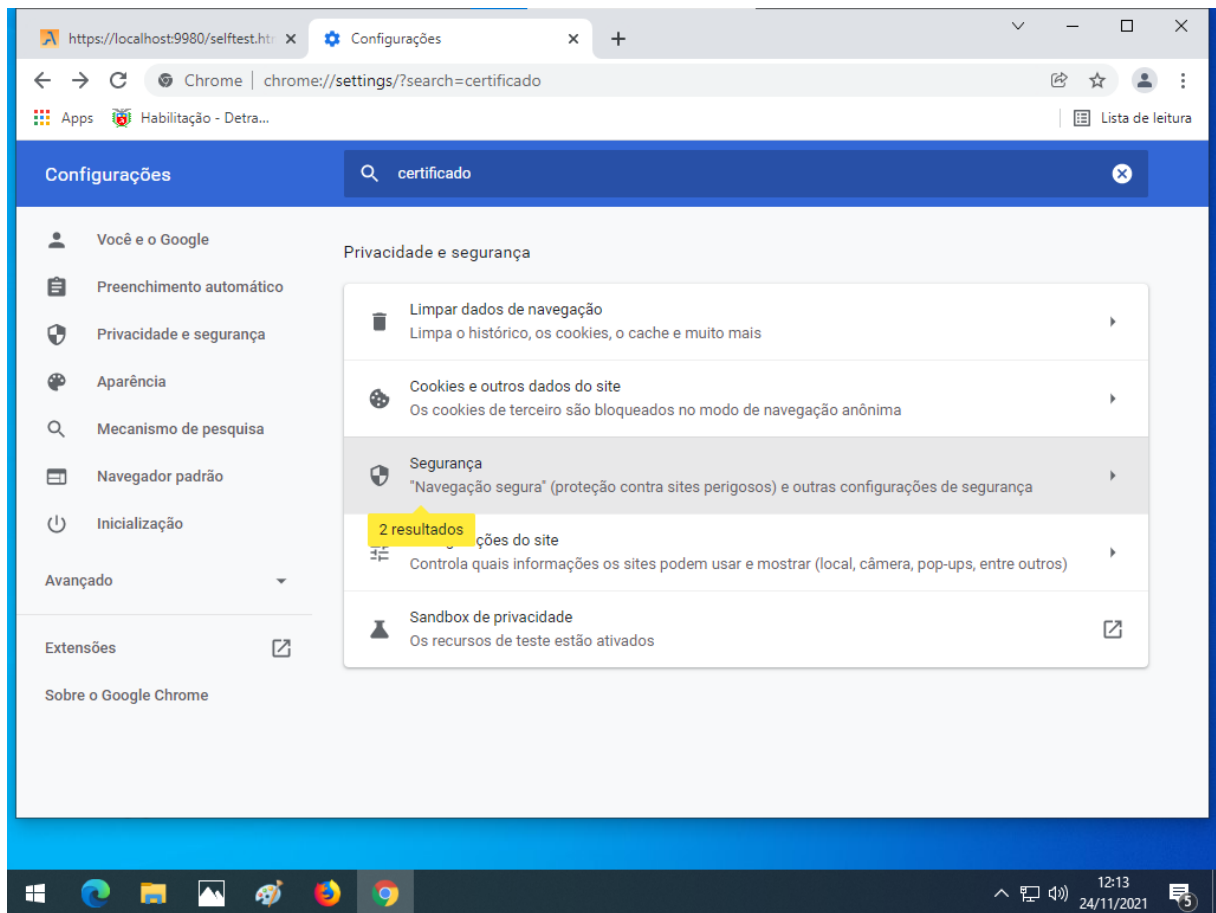
Será necessário acessar o gerenciamento de certificados do navegador.

Abriu o navegador GoogleChrome e clicar no painel de controle (ícone em forma de três pontos na vertical) que fica no canto superior direito da janela do navegador.

Selecionar a opção “Configuração”.

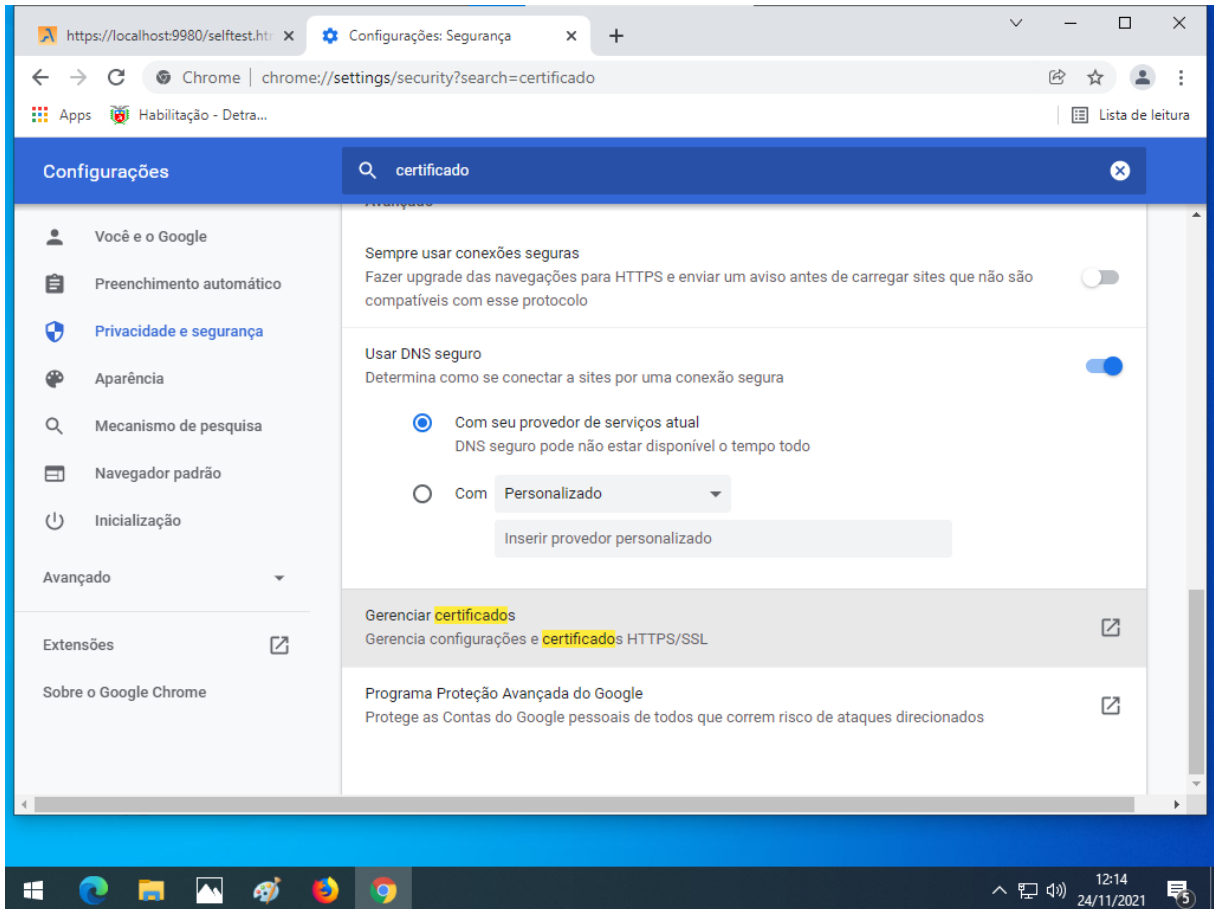


Na janela de configuração do GoogleChrome, selecionar a opção “**Segurança e privacidade**”.  
Dentro de Segurança e privacidade selecionar “**Segurança**”.



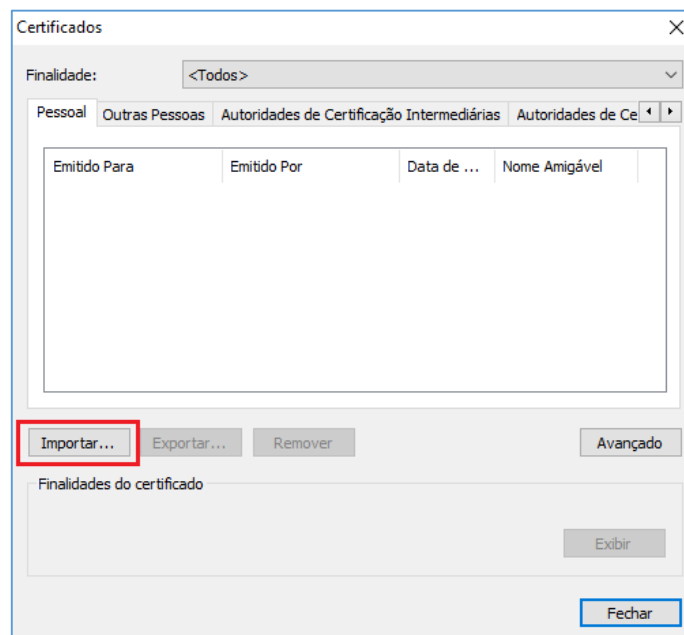
Em Segurança selecionar “**Gerenciar certificados**”.





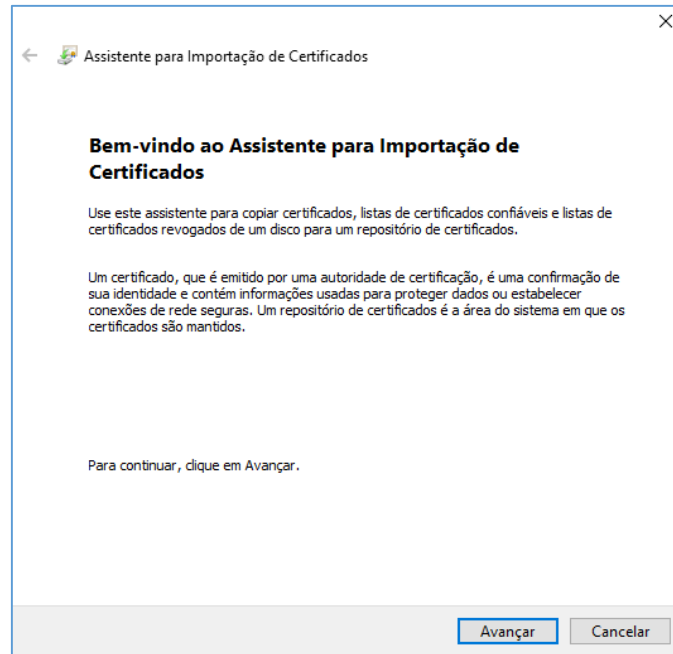
Após selecionar Gerenciar Certificados irá abrir uma janela de nome **Certificados**.

Na janela Certificados clicar no botão **Importar**.

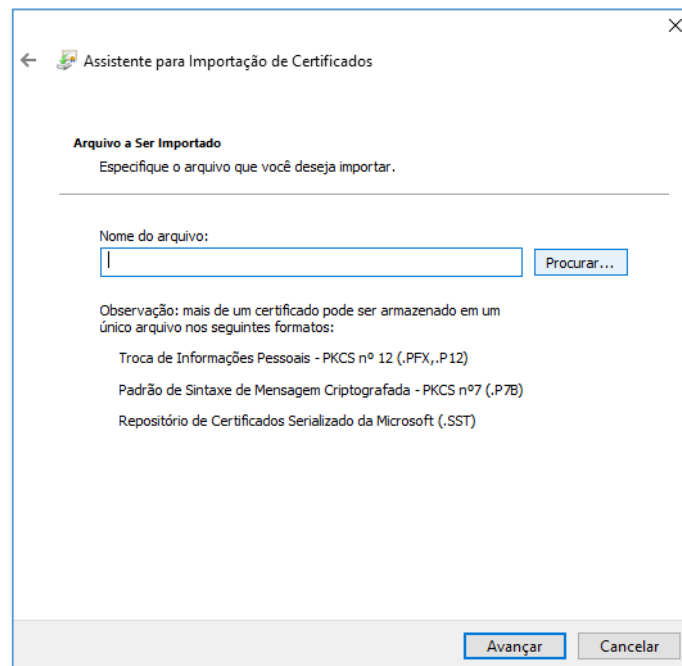


Írá abrir uma tela de assistência de importação de certificado.

Clicar no botão **Avançar**.




Em seguida, clicar no botão **Procurar**.



Localizar e selecionar o arquivo **"Antheus\_root\_ca"**, localizado na pasta Antheus Hardware Server.

Caminho da pasta: Disco Local (C:) > Arquivos e Programas > Antheus Hardware Server.

Na janela do Assistente de Certificado avançar até aparecer a opção concluir.

←  Assistente para Importação de Certificados


**Arquivo a Ser Importado**  
Especifique o arquivo que você deseja importar.

---

Nome do arquivo:

Observação: mais de um certificado pode ser armazenado em um único arquivo nos seguintes formatos:

- Troca de Informações Pessoais - PKCS n° 12 (.PFX,.P12)
- Padrão de Sintaxe de Mensagem Criptografada - PKCS n°7 (.P7B)
- Repositório de Certificados Serializado da Microsoft (.SST)

←  Assistente para Importação de Certificados

**Repositório de Certificados**  
Repositórios de certificados são áreas do sistema onde os certificados são guardados.

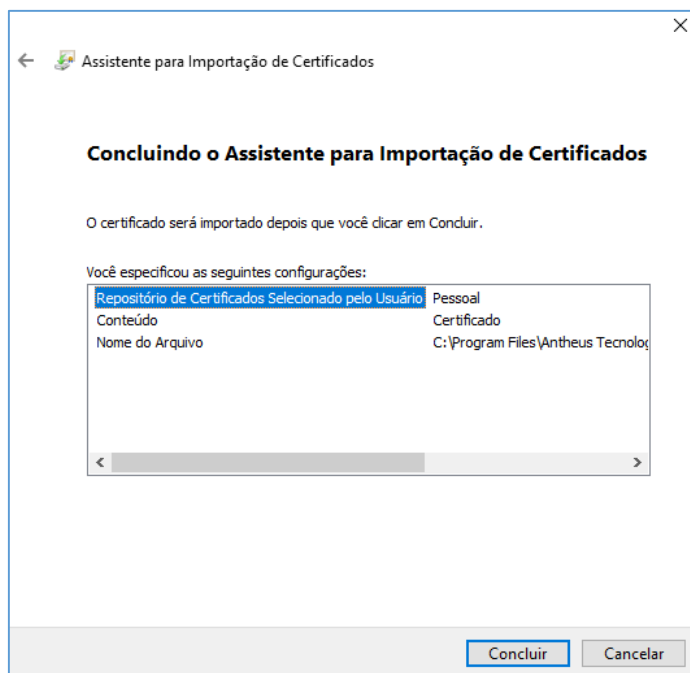
---

O Windows pode selecionar automaticamente um repositório de certificados ou você pode especificar um local para o certificado.

Selecionar automaticamente o repositório de certificados conforme o tipo de certificado

Colocar todos os certificados no repositório a seguir

Repositório de Certificados:



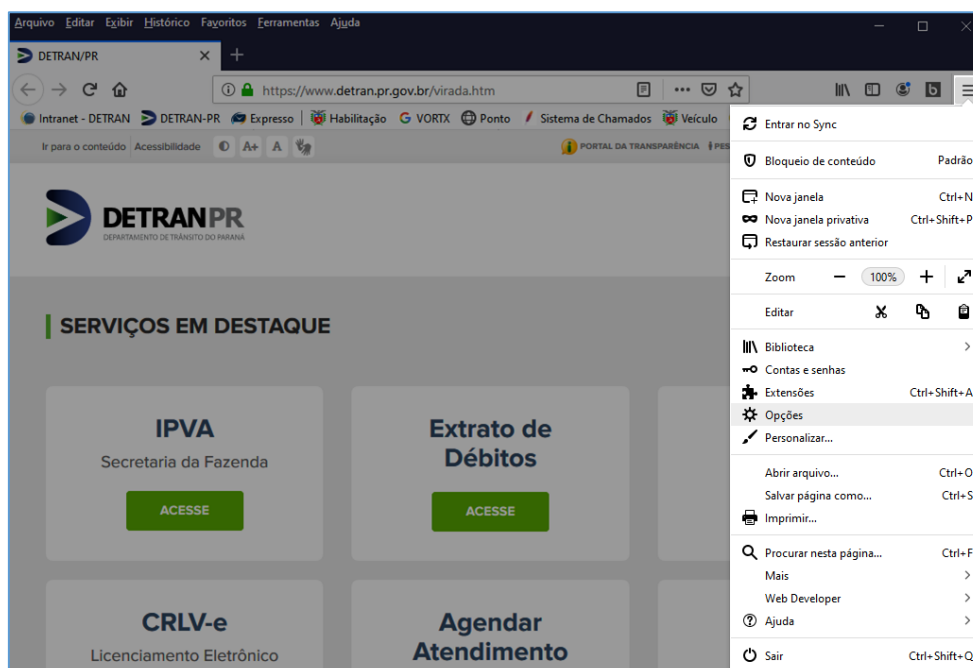
**OBSERVAÇÃO:** Dependendo da versão do navegador Google Chrome, o caminho para importação de Certificados pode divergir desta presente instrução. A versão utilizada nesta instrução é o Chrome 97.0.4692.99.

## 7.2. Instalar o Certificado root no navegador Mozilla Firefox

Será necessário acessar o gerenciamento de certificados do navegador.

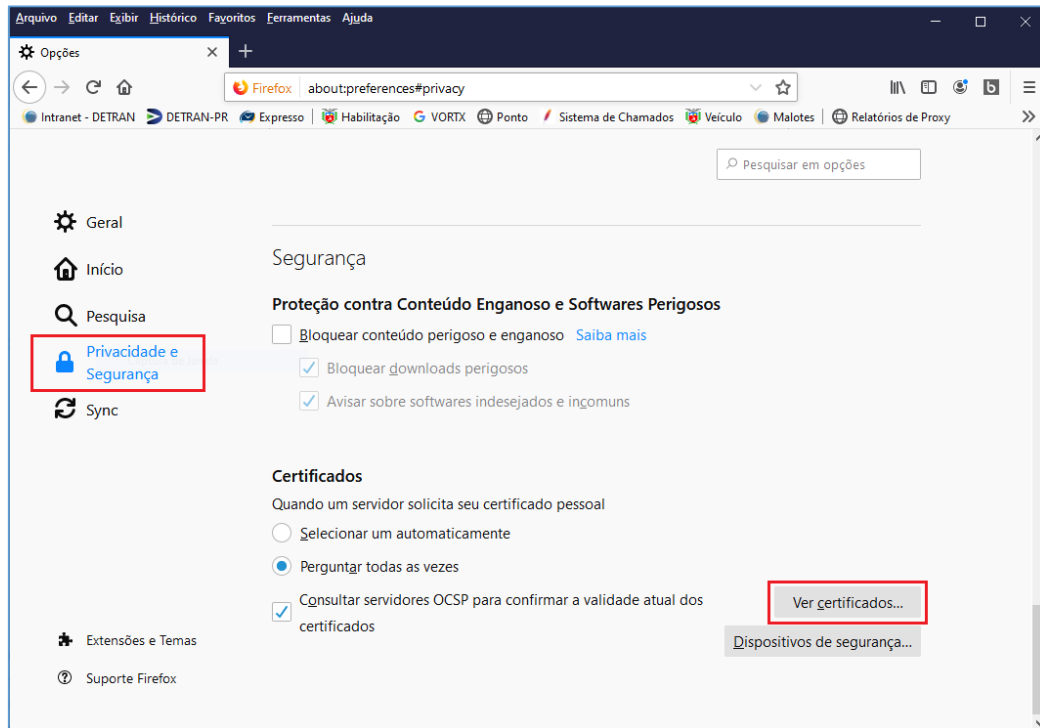
Abrir o navegador Mozilla Firefox e clicar no painel de controle (ícone em forma de três barras horizontais) que fica no canto superior direito da janela do navegador.

Selecionar a opção “Opções”.



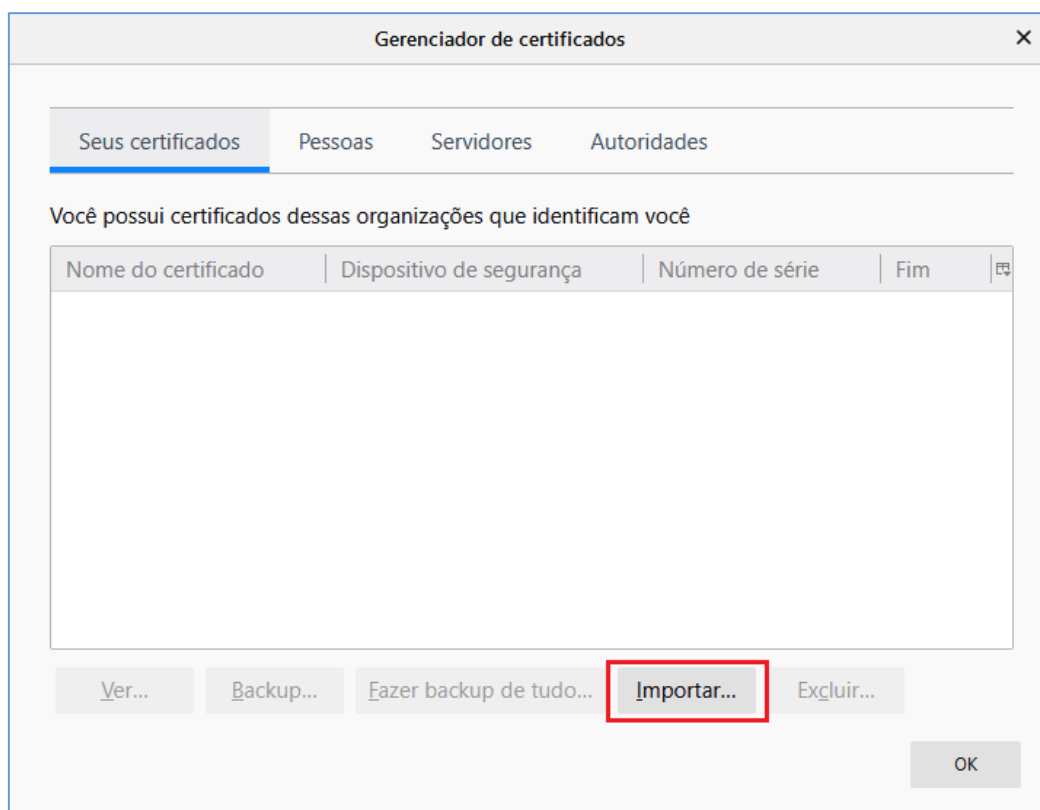
Na janela de configuração do Mozilla Firefox, selecionar a opção “**Privacidade e Segurança**”.

Dentro de Privacidade e Segurança, selecionar “**Ver certificados**”.



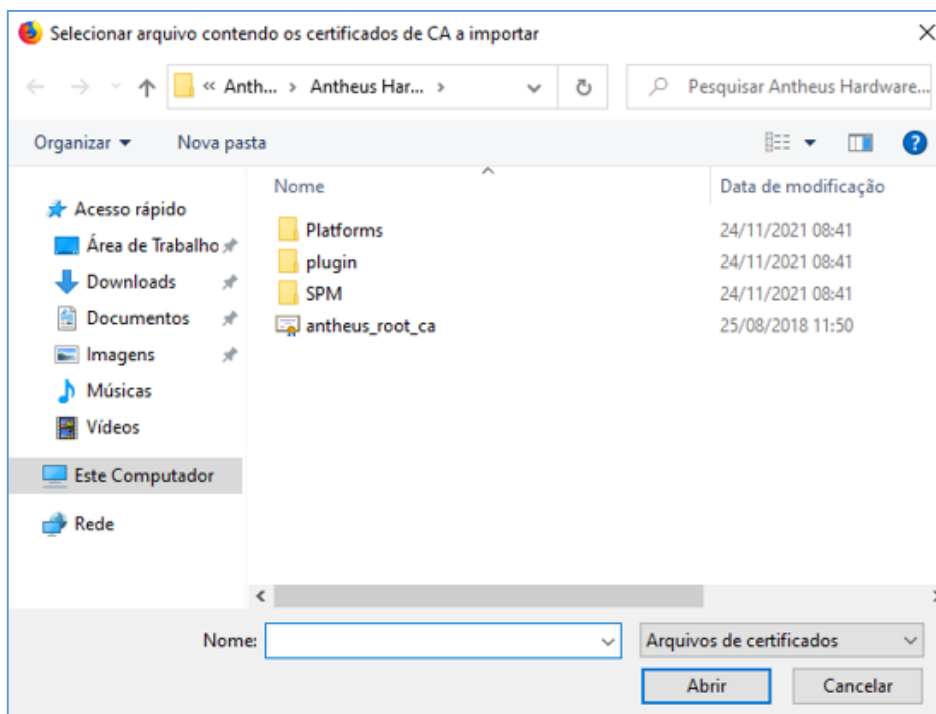
Após selecionar Ver Certificados, irá abrir uma janela de nome “**Gerenciador de Certificados**”.

Na janela Gerenciador de Certificados, clicar no botão **Importar**.



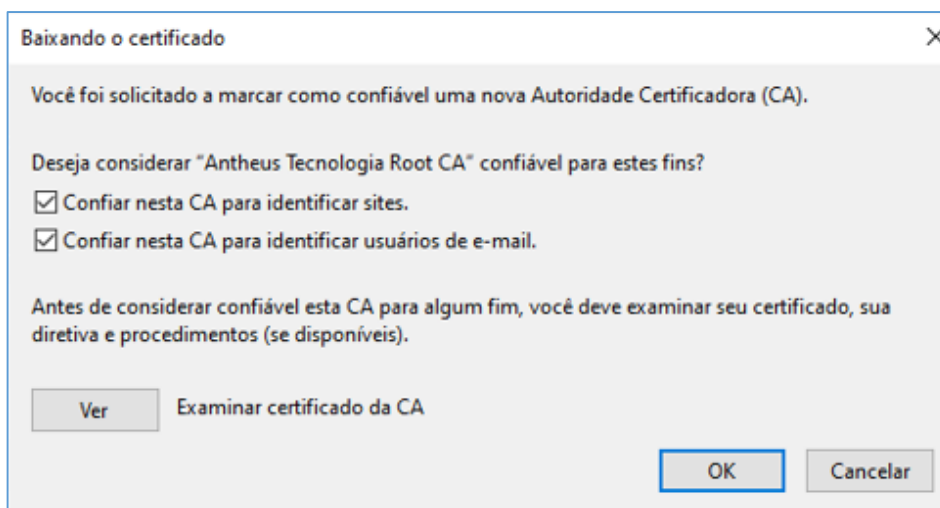
Localizar e selecionar o arquivo “**Antheus\_root\_ca**”, localizado na pasta Antheus Hardware Server.

Caminho da pasta: Disco Local (C:) > Arquivos e Programas > Antheus Hardware Server.



Após selecionado o arquivo “**Antheus\_root\_ca**” (Selecionar e clicar no botão Abrir), irá abrir uma janela de nome “**Baixando o certificado**”.

Manter marcadas as opções “**Confiar nesta CA para identificar sites**” e “**Confiar nesta CA para identificar usuários de e-mail**” e clicar no botão **OK**.



Na janela do Gerenciador de Certificados clicar no botão **OK**.

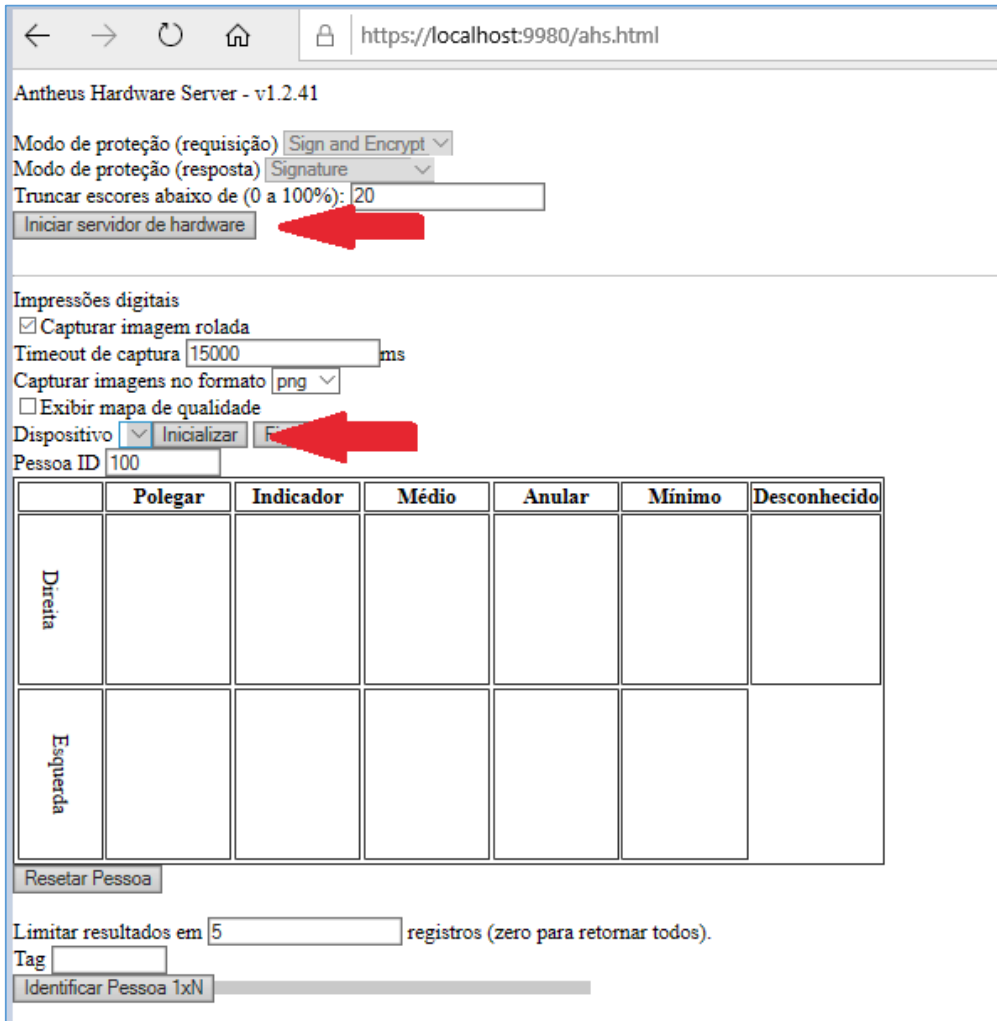
**OBSERVAÇÃO:** Dependendo da versão do navegador Mozilla Firefox, o caminho para importação de Certificados pode divergir desta presente instrução. A versão utilizada nesta instrução é o Firefox 68.0.1.

## 8. Testar a solução de biometria

Para testar se a solução verificação biométrica está operando sem problemas acesse:


<https://localhost:9980/ahs.html>

Será exibida a tela abaixo, clique em “Iniciar Servidor de hardware”, depois em “Inicializar”. Depois coloque sua digital no leitor, se ela aparecer na tela é porque está operando normalmente.




Browser address bar: <https://localhost:9980/ahs.html>

Antheus Hardware Server - v1.2.41

Modo de proteção (requisição)    
Modo de proteção (resposta)    
Truncar escores abaixo de (0 a 100%):   
 

Impressões digitais

Capturar imagem rolada  
Timeout de captura  ms  
Capturar imagens no formato    
 Exibir mapa de qualidade  
Dispositivo      
Pessoa ID

	Polegar	Indicador	Médio	Anular	Mínimo	Desconhecido
Direita						
Esquerda						

Limitar resultados em  registros (zero para retornar todos).  
Tag

## 9. Cadastrar equipamento no sistema de Habilitação

Após instalação do componente, do leitor biométrico e realização do diagnóstico, o passo seguinte será efetuar o cadastramento do equipamento no sistema de Habilitação. Para tanto, acesse “Outros > Segurança > Cadastro de Equipamentos BioID”.

## 10. Bloquear equipamento cadastrado no sistema de Habilitação

Para realizar o bloqueio do equipamento, basta selecionar a função “Cadastro de equipamentos BioID, aguardar a identificação do equipamento cadastrado e clicar no botão “Bloquear”. Para tanto, acesse “Outros > Segurança > Cadastro de Equipamentos BioID”.

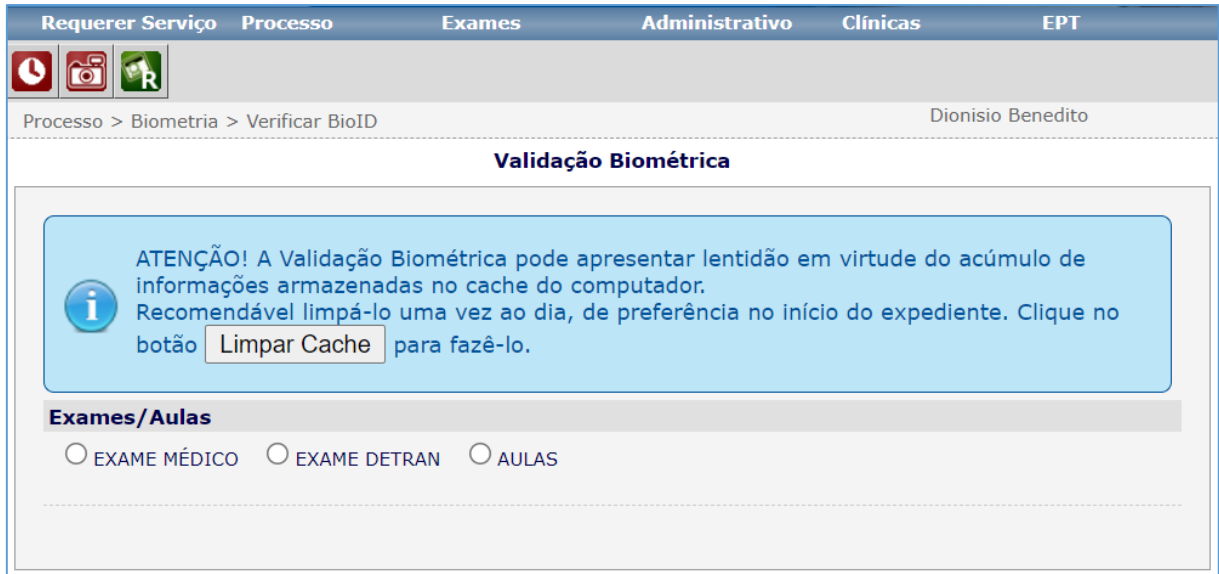
Uma vez bloqueado, será possível realizar novo cadastro de equipamento.

## 11.Limpeza de cache na verificação biométrica BioID

**IMPORTANTE:** Sempre limpar o cache antes de carregar a turma para verificação biométrica.

Falta de limpeza do cache acarreta na demora na verificação.

Ao abrir a tela de serviço **Verificar BioID**, clicar no botão **Limpar Cache**.



Requerer Serviço   Processo   Exames   Administrativo   Clínicas   EPT

Processo > Biometria > Verificar BioID Dionisio Benedito


**Validação Biométrica**

**ATENÇÃO!** A Validação Biométrica pode apresentar lentidão em virtude do acúmulo de informações armazenadas no cache do computador. Recomendável limpá-lo uma vez ao dia, de preferência no início do expediente. Clique no botão **Limpar Cache** para fazê-lo.

**Exames/Aulas**

EXAME MÉDICO    EXAME DETRAN    AULAS

Após clicar no botão de limpeza de cache, irá abrir uma página conforme figura abaixo.



Sistema **DETRAN/PR**   Módulo de Habilitação

Processo > Biometria > Limpar Cache BioID

**Limpar Cache - BioID**

**Antheus Hardware Server**

**Cache para verificação biométrica limpo!!!**

**Esta página fechará automaticamente em 6 segundos**

Será necessário aguardar a conclusão da limpeza.

Após concluída a limpeza, a página fechará automaticamente, voltando para a tela do sistema de Habilitação.



## 12.Revisão do Guia Rápido

<b>Nº Revisão</b>	<b>Data</b>	<b>Alteração</b>
00		1ª versão do Manual.
01	24/01/2023	Atualização do Manual.