Como remover o Certificado Digital antigo

Se for usuário do navegador **Google Chrome** ou do **Microsoft Edge** e utilizar o Windows como sistema operacional do seu computador, ao acessar algumas páginas da UFU, você poderá se deparar com esta imagem ao entrar em um endereço de site da UFU:



Isso ocorre devido à dificuldade do Chrome e do Edge de atualizarem os certificados de segurança de navegação.

Para corrigir este inconveniente, ou seja, para exclusão de certificados vencidos, usaremos o **Gerenciador de Certificados do Windows**, da seguinte forma:

01 - Pressione a tecla do Windows no teclado (ao lado do ALT esquerdo) e a tecla da letra "R" simultaneamente.



02 - Você verá a janela "Executar". Digite o comando "**certmgr.msc**" e aperte e tecla "Enter" em seu teclado ou clique no botão "**OK**" com o cursor do mouse.

Executar				
	Digite o nome de um programa, pasta, documento ou recurso da Internet e o Windows o abrirá para você.			
<u>A</u> brir:	certmgr.msc	~		
	OK Cancelar <u>P</u> rocurar			

03 – Ao abrir o Gerenciador de Certificados, dê um duplo clique em "Autoridades de Certificação Intermediárias e, depois, um duplo clique em "Certificados".

Será necessário a exclusão de dois ou três certificados obsoletos.

Dois emitidos pela GlobalSin:

- Trusted Root CA SHA256 G2 e/ou
- Trusted Root TLS CA SHA256 G3
- E um emitido pela RNP:
- RNP ICPEdu OV SSL CA 2019

04 – Para excluir estes certificados, clique sobre o Certificado vencido (Trusted Root CA **SHA256 G2**) e, depois, no X vermelho no topo da tela. Se preferir, assim que marcar o certificado, pressione a tecla "Delete" do teclado.

🜇 certmgr - [Certificados - Usuário Atual\Autoridades de Certificação Intermediárias\Certificados]

Arquivo Ação Exibir Ajuda						
Certificados - Usuário Atual Excluir	^	Emitido para	Emitido por			
> 🦰 Pessoal		Sectigo RSA Organization Validation Secure Serv	USERTrust RSA C			
 Autoridades de Certificação Raiz Confiáveis Certificados Confiabilidade Corporativa Autoridades de Certificação Intermediárias Lista de Certificados Revogados Certificados Objeto de Usuário do Active Directory Fornecedores Confiáveis 		Soluti CA - OV	Trusted Root TLS			
		SSI Blindado 2	USERTrust RSA C			
		Starfield Services Root Certificate Authority - 62	Starfield Class 2			
		Symantec Class 3 SHA256 Code Signing CA	VeriSign Class 31			
		Thawte RSA CA 2018	DigiCert Global F			
		Trusted Root CA SHA256 G2	GlobalSign			
		Trusted Root TLS CA SHA256 G3	GlobalSign			
> 📔 Certificados Não Confiáveis		🔄 TrustSign BR Certification Authority (DV) 2	USERTrust RSA C			
> 📔 Autoridades de Certificação Raiz de Terceiros		SERTrust ECC Certification Authority	AddTrust Externa			
> 🦳 Pessoas Confiáveis		SERTrust RSA Certification Authority	AddTrust Externa			
> 🣔 Emissores de Autenticação de Cliente		Secure Server	USERTrust RSA C			
> 🧮 Outras Pessoas		🔄 Valid Certificadora Digital AlphaSSL CA 2018	Trusted Root CA			
> 🧮 Local NonRemovable Certificates		www.verisign.com/CPS Incorp.by Ref. LIABILITY	Class 3 Public Pr			
> 🧮 MSIEHistoryJournal		ZeroSSL RSA Domain Secure Site CA	USERTrust RSA C			
> Solicitações de Registro de Certificado						

Confirme a exclusão

•	Emitido para	Emitido por				
	🔄 Sectigo RSA Organization Validation Secure Serv	USERTrust RSA Certification Authority				
	🔄 Soluti CA - OV	Trusted Root TLS CA SHA256 G3				
	🔄 SSL Blindado 2	USERTrust RSA Certification Authority				
	🔄 Starfield Services Root Certificate Authority - G2	Starfield Class 2 Certification Authority				
	🔄 Symantec Class 3 SHA256 Code Signing CA	VeriSign Class 3 Public Primary Certification Authority				
	🔄 Thawte RSA CA 2018	DigiCert Global Root CA				
	Trusted Root CA SHA256 G2	GlobalSign				
	🔄 Trusted Root TLS CA SHA256 G3	GlobalSign				
	🔄 TrustSign BR Certification Authority (DV) 2	USERTrust RSA Certification Authority				
	SERTrust ECC Certification Authority	AddTrust External CA Root				
	Section Authority	AddTruct External CA Root				
	🔄 USERTrust RSA Domain 🖕 Certificados	\times				
	Valid Certificadora Digit					
	www.verisign.com/CPS	Os certificados emitidos por este CA ou qualquer CA de pível				
	🔄 ZeroSSL RSA Domain Se 🛛 📘 inferior já não	inferior já não serão confiáveis. Deseja excluir este certificado?				
	Deseja excluir e					
	-					
		Sim Não				

Exclua também o certificado **Trusted Root TLS CA SHA256 G3** e finalize com a exclusão do certificado **RNP ICPEdu OV SSL CA 2019**.



05 – Feche o navegador, abra novamente, acesse o endereço desejado que estará funcionando normalmente.