PROGRAMA EDUCACIONAL EM SAÚDE DIGITAL DA UNIVERSIDADE FEDERAL DE GOIÁS

PÓS-GRADUAÇÃO LATO SENSU
EM SAÚDE DIGITAL

Certificado digital

Organizadores

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior
Taciana Novo Kudo
Ana Laura de Sene Amâncio Zara
Rejane Faria Ribeiro-Rotta
Renata Dutra Braga
Rita Goreti Amaral
Sheila Mara Pedrosa
Silvana de Lima Vieira dos Santos

2ª EDIÇÃO

Cegraf UFG

Comissão de Governança da Informação em Saúde (CGIS)

Silvana de Lima Vieira dos Santos

Centro de Inovação em Gestão da Educação e do Trabalho em Saúde (CIGETS) e Laboratório de Pesquisa em Empreendedorismo e Inovação (LAPEI)

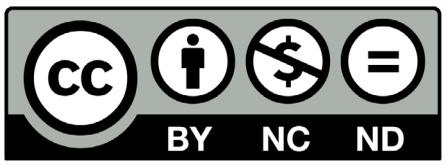
Cândido Vieira Borges Júnior

Ministério da Saúde / Secretaria Executiva / Departamento de Informática do Sistema Único de Saúde (DATASUS)

Merched Cheheb de Oliveira

Coordenação-Geral de Inovação e Informática em Saúde (CGIIS)

Adriano Santiago Dias dos Santos
Allan Nuno Alves de Sousa
André Gustavo Souza dos Santos
Andréia Cristina de Souza Santos
Blanda Helena de Mello
Elivan Silva Souza
Gabriella Nunes Neves
Josélio Emar de Araújo Queiroz
João Marquês Lopes Barbosa
Juliana Pereira de Souza Zinader
Juliana de Souza Santana
Kauara Ferreira
Kelly Neves Pinheiro Brito
Laís Bié Pinto Bandeira
Lara Liz Freire
Larissa Gonçalves Mangabeira da Silva
Lucas da Costa Roriz
Maria Cristina Ferreira de Abreu
Patrícia dos Santos Irigaray Rodrigues
Robson Willian de Melo Matos
Rodrigo André Cuevas Gaete
Silmara Vieira da Silva
Thais Lucena de Oliveira
Vanessa Lora
Vinicius Colonese Mrad
Vitor Rocha de Araújo



Certificado digital

Organizadores

Fábio Nogueira de Lucena

Plínio de Sá Leitão Júnior

Taciana Novo Kudo

Ana Laura de Sene Amâncio Zara

Rejane Faria Ribeiro-Rotta

Renata Dutra Braga

Rita Goreti Amaral

Sheila Mara Pedrosa

Silvana de Lima Vieira dos Santos

Cegraf UFG

2023

Revisão editorial
Ana Laura Sene Amâncio Zara

Revisão técnica
Andréia Cristina de Souza Santos (Ministério da Saúde)
Maria Cristina Ferreira de Abreu (Ministério da Saúde)

Capa
Iuri Vaz Miranda - graduando (UFG)

Editoração Eletrônica
Caio Barbosa Dias - graduando (UFG)
Layane Grazielle Souza Dias - graduanda (UFG)
Luma Wanderley de Oliveira - doutoranda (UFG)

1ª edição em 2022, pelo Cegraf UFG, ISBN: 978-85-495-0481-4,
DOI: https://doi.org/10.5216/CER.ebook.978-85-495-0481-4/2022

https://doi.org/10.5216/CER.ebook.978-85-495-0693-1/2023

Dados Internacionais de Catalogação na Publicação (CIP)
GPT/BC/UFG

C418 Certificado digital [E-book] / organizadores, Fábio Nogueira de Lucena ... [et al.]. - 2. ed. - Dados eletrônicos (1 arquivo : PDF) - Goiânia: Cegraf UFG, 2023.
il.

Inclui referências.
ISBN (E-book): 978-85-495-0693-1

1. Saúde - Estudo e ensino. 2. Certificado digital. 3. Assinaturas digitais. 4. Recursos eletrônicos da informação - Saúde digital. 5. Tecnologia médica. I. Lucena, Fábio Nogueira.

CDU: 614.39:004

Bibliotecária responsável: Joseane Pereira / CRB1: 2749

Certificado digital

Instituição responsável

Universidade Federal de Goiás (UFG)

- Comissão de Governança da Informação em Saúde da UFG (CGIS-UFG)
- Centro de Inovação em Gestão da Educação e do Trabalho em Saúde (CIGETS)
- Laboratório de Pesquisa em Empreendedorismo e Inovação da Universidade Federal de Goiás (LAPEI-UFG)

Instituição financiadora

Ministério da Saúde (MS)

- Secretaria Executiva (SE)
  - Departamento de Informática do Sistema Único de Saúde (DATASUS)
- Secretaria de Gestão do Trabalho e da Educação na Saúde (SGTES)

Apoio

Ministério da Saúde (MS)

- Secretaria de Atenção Primária à Saúde (SAPS)

SECRETARIA DE GESTÃO DO TRABALHO E DA EDUCAÇÃO NA SAÚDE | MINISTÉRIO DA SAÚDE | GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Abreviaturas e Siglas

AC	Autoridade Certificadora
AC-Raiz	Autoridade Certificadora Raiz
ANS	Agência Nacional de Saúde Suplementar
Anvisa	Agência Nacional de Vigilância Sanitária
AR	Autoridade de Registro
BPMN	*Business Process Model and Notation*
CAFe	Comunidade Acadêmica Federada
CF-e	Cupom Fiscal Eletrônico
CFF	Conselho Federal de Farmácia
CFM	Conselho Federal de Medicina
CFO	Conselho Federal de Odontologia
CGIS	Comissão de Governança da Informação em Saúde
CIGETS	Centro de Inovação em Gestão da Educação e do Trabalho em Saúde
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional de Pessoa Jurídica
CONFAZ	Conselho Nacional de Política Fazendária
CPF	Cadastro de Pessoa Física
CRM	Conselho Regional de Medicina
DARF	Documento de Arrecadação de Receitas Federais
DF	Distrito Federal
e-CPF	Certificado digital para pessoa física
e-CNPJ	Certificado digital para pessoa jurídica
GB	Gigabyte
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira

Inmetro	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ITI	Instituto Nacional de Tecnologia da Informação
Km/s	Quilômetro por segundo
LAPEI	Laboratório de Pesquisa em Empreendedorismo e Inovação
MB	Megabyte
MJ	Ministério da Justiça
NF-e	Nota Fiscal Eletrônica
NGS	Níveis de Garantia de Segurança
NGS-2	Segundo Nível de Garantia de Segurança
PDF	*Portable Document Format*
PEP	Prontuário Eletrônico do Paciente
PJ-e	Processo Judicial Eletrônico
RG	Registro Geral
RNDS	Rede Nacional de Dados em Saúde
SAPS	Secretaria de Atenção Primária à Saúde
SAT-CF-e	Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico
SBIS	Sociedade Brasileira de Informática em Saúde
SGTES	Secretaria de Gestão do Trabalho e da Educação na Saúde
SIS	Sistema de Informação em Saúde
S-RES	Sistema de Registro Eletrônico de Saúde
SSP	Secretaria de Segurança Pública
TISS	Troca de Informação de Saúde Suplementar
TSE	Tribunal Superior Eleitoral
UFG	Universidade Federal de Goiás
UNA-SUS	Universidade Aberta do Sistema Único de Saúde

Lista de Figuras, Tabelas e Vídeos

Sumário

Apresentação

Prezado(a) Participante,

Seja bem-vindo(a) ao Microcurso **Certificado Digital**!

A implementação da certificação digital no Brasil trouxe confiança e validade jurídica aos documentos e às transações em meio eletrônico. O Certificado Digital e a Assinatura Digital são elementos integrantes desse contexto, os quais são necessários para promover os benefícios da precisão de informações e da agilidade de serviços no ambiente digital.

A aplicação da certificação digital na área da saúde fomenta a efetividade esperada na Segurança da Informação em Saúde do Paciente, cenário em que os profissionais e gestores de saúde são capacitados e sensibilizados para utilizá-la adequadamente.

Este Microcurso faz parte do Programa Educacional em Saúde Digital da Universidade Federal de Goiás (UFG). A sua oferta foi motivada pela necessidade de identificar, univocamente, pessoas e estabelecimentos de saúde no contexto da integração com a Rede Nacional de Dados em Saúde (RNDS), de modo a promover a proteção às transações eletrônicas.

Este documento contém informações e referências importantes sobre a temática.

Bom estudo!!!

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 1

Conceitos e Histórico da Certificação Digital No Brasil

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 1: Conceitos e Histórico da Certificação Digital no Brasil

1.1 Documentos Digitais

Segundo o dicionário Priberam [1], documentos são declarações escritas que têm caráter comprovativo, prova, testemunho, confirmação. Documentos são parte da história humana e desempenham importante papel nas relações sociais, nas relações entre instituições e são amplamente utilizados no dia a dia.

No Brasil, pode-se especular que o primeiro documento de que se tem notícia foi a carta de Pero Vaz de Caminha [2], escrivão de Pedro Álvares Cabral, datada de primeiro de maio de 1500, informando acerca do descobrimento do Brasil alguns dias antes. Essa carta foi levada ao conhecimento do Rei de Portugal por Gaspar de Lemos. A carta expõe, logo no seu início, a humildade do autor e o esforço em retratar a "realidade":

> Posto que o Capitão-mor desta vossa frota, e assim os outros capitães escrevam a Vossa Alteza a nova do achamento desta vossa terra nova, que ora nesta navegação se achou, não deixarei também de dar disso minha conta a Vossa Alteza, assim como eu melhor puder, ainda que — para o bem contar e falar — o saiba pior que todos fazer. Tome Vossa Alteza, porém, minha ignorância por boa vontade, e creia bem por certo que, para aformosear nem afear, não porei aqui mais do que aquilo que vi e me pareceu.[2]

Ao longo dos anos, desenvolvemos mecanismos para lidar com documentos, visando a vários fins: expressar sua autoria, comprovar sua genuinidade, assegurar o acesso apenas ao destinatário, exprimir concordância com seus termos e/ou declarar que somos responsáveis por seu conteúdo, dentre outros. Independentemente da natureza (documento em papel ou eletrônico) e da categoria (certidão, declaração, resolução, etc.), os documentos estão sujeitos a confirmação de sua integridade e associados a pessoas – físicas ou jurídicas.

Em documentos manuscritos – aqueles documentos em papel – costumamos registrar nossa assinatura à caneta, aplicar selos e carimbos ou outra forma de nos identificar. Por exemplo, ao escrevermos nossa assinatura em um cheque de alguma instituição bancária, pretendemos declarar que somos o autor legítimo desse documento, ao mesmo tempo que concordamos com o conteúdo, por exemplo, o valor monetário em questão.

O constante processo de informatização que estamos presenciando, no qual sistemas computacionais são inseridos em praticamente todo e qualquer setor de atividade humana, promove a sociedade digital e, com ela, a digitalização, inclusive de documentos. Observe que, até há pouco tempo, um bem de valor estava restrito à sua existência e posse material. Hoje, o salário mensal recebido por um colaborador não necessariamente é materializado em cédulas e moedas. Esse colaborador, de fato, pode não tocar em nenhuma cédula e consumir todo ele por meio de operações digitais.

A digitalização resulta em conteúdos digitais, aqui denominados de documentos digitais. O conteúdo não está restrito a texto, também pode ser áudio, uma imagem, um vídeo ou uma combinação desses meios. Um documento digital é uma sequência de *bytes*, geralmente registrada em meio persistente como um disco de computador. A digitalização, em muitos casos, cria um documento digital correspondente à versão "material", por exemplo, uma nota fiscal eletrônica, que substitui a nota fiscal tradicional (impressa em papel). Noutros casos, como em um *email* que nunca foi impresso em papel, tem-se um documento digital cuja existência está restrita ao meio digital.

Um documento digital[1] tem vantagens sobre o equivalente "material". Por exemplo, uma prescrição eletrônica não depende de deslocamento físico do local onde é produzida até onde é consumida. Por outro lado, se registrada em papel, o trânsito é necessário, o que tem impacto em custos financeiros e tempo.

Em mais um exemplo, a Carta de Pero Vaz de Caminha[2], comentada acima, foi escrita nove dias após o descobrimento do Brasil e chegou ao conhecimento do Rei de Portugal, provavelmente, semanas após o "despacho". Hoje, um avião leva cerca de 9 horas para ir do Brasil a Portugal. Esse mesmo trajeto, realizado por um documento eletrônico, seria acessado instantaneamente para efeitos humanos. De fato, se fosse hoje, o Rei assistiria ao vivo a chegada, o que dispensaria a descrição do cuidadoso Pero Vaz de Caminha.

Observe a imagem a seguir (Figura 1). Ela é conhecida por "Bliss", produzida por Charles O'Rear, em 1996.[3] Em um mundo "material", ela teria pouca chance de ser a imagem, considerada por muitos, a mais visualizada de todos os tempos (considere os custos de produção e distribuição). Por outro lado, no mundo "virtual", se você usa computador há algum tempo, provavelmente já viu esta imagem inúmeras vezes, todas com a mesma nitidez, mesmo após vários anos, mas na tela do computador, nenhuma versão impressa.

Figura 1 – "Bliss", imagem produzida por Charles O'Rear

Fonte: Wikipedia.[3]

1 Usamos aqui os termos 'documento digital' e 'documento eletrônico' com o mesmo significado.
2 Disponível em: https://www.sohistoria.com.br/curiosidades/carta/.

Entre os vídeos mais vistos no Youtube®, o total de visualizações de cada um deles ultrapassa a quantidade de seres humanos no planeta. Quais seriam os custos de se obter tamanha visualização de um único desses vídeos, em um cenário onde devemos empregar meio material para divulgação? Seria viável produzir bilhões de cópias e distribuí-las? Documentos digitais, ao contrário dos equivalentes no mundo "material", tornam esses feitos possíveis.

1.2 Trânsito de Documentos Digitais

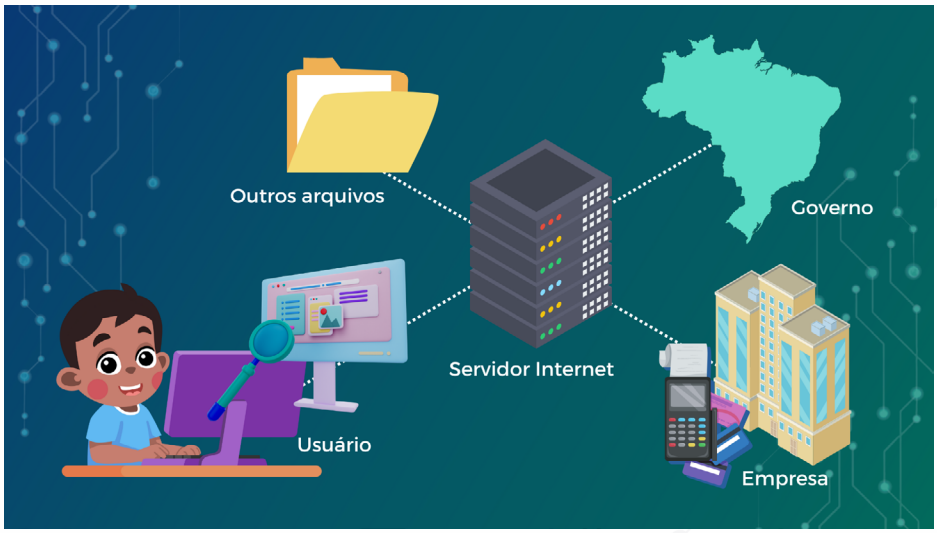
Os *bytes*[3] de um documento digital trafegam em uma velocidade medida em função da velocidade da luz, ou seja, a surpreendente 300.000 Km/s. Mesmo com a limitação da largura da banda, que é conhecida por *bandwidth*, redes de computadores atingem taxas de transferência (tráfego de dados) impressionantes. Redes de longa distância podem transferir mais de uma dezena de *gigabytes* (>10 GB) a cada segundo, o que significa transferir todo o conteúdo da Bíblia (10 MB) em um intervalo imperceptível para um ser humano.

Essa velocidade de transferência é um atrativo em um mundo cada vez mais veloz. Adicionalmente, há pontos de conexão em "todo" o Planeta, formando uma enorme rede conhecida como *Internet*.

Embora a comunicação para o trânsito de *bytes* possa ser invisível ao olho humano, boa parte da transferência de dados ocorre por conexões físicas (por exemplo, via fios). Essas conexões podem ser compreendidas como as "rodovias da Internet". A manutenção, a segurança e a expansão dessas rodovias é fundamental para a sociedade digital na qual vivemos hoje.

Na Figura 2, é ilustrado o cenário do tráfego de documentos digitais, em que entidades tais como indivíduos, empresas e governos, geram, enviam e recebem documentos pela *Internet*. Nesse contexto, a natureza (documento eletrônico) e o meio de comunicação (a *Internet*) agilizam o trâmite (envio e recebimento) de documentos digitais, bem como a geração, a validação e o acesso a informações sigilosas, o que confere economia e maior agilidade aos processos.

Figura 2 – Fluxo de documentos eletrônicos



Fonte: autoria própria.

3 Disponível em: https://pt.wikipedia.org/wiki/Byte.

1.3 Documentos Digitais e Seus Desafios

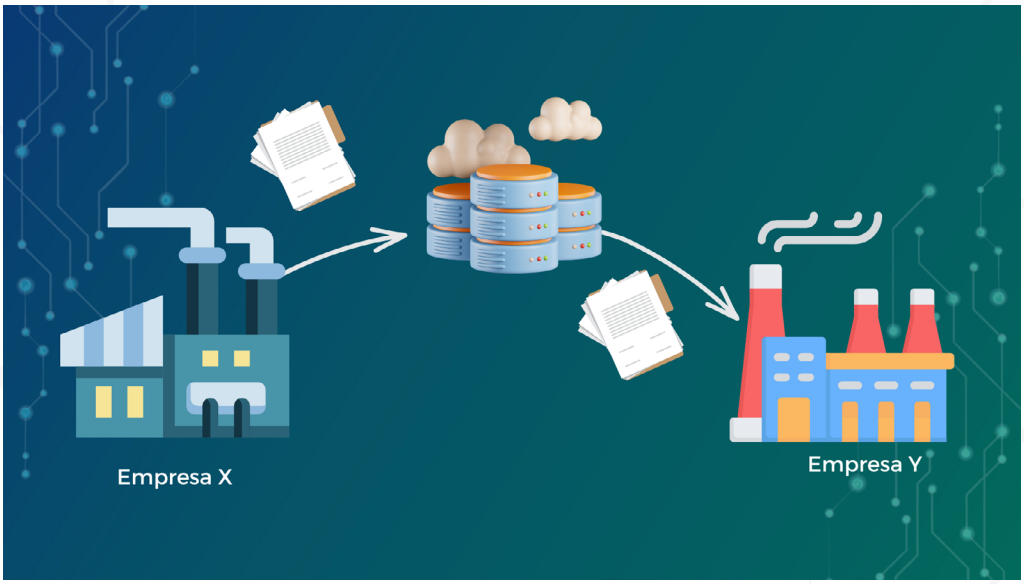
Um documento digital não apresenta “borrões” ou “rasuras” perceptíveis ao “olhar humano”, seja decorrente de uma remoção, substituição ou acréscimo de conteúdo.

Entre o ponto de origem até o destino, os *bytes* de um documento digital podem ser interceptados. Não há como evitar esse acesso. Em consequência, existe o risco do conteúdo ser acessado por pessoas não autorizadas (caso o conteúdo seja sigiloso) ou até ser alterado nesse trânsito, a partir da origem e antes de chegar ao destinatário, comprometendo a integridade do documento.

Para ilustrar esses desafios relacionados a documentos digitais, consideremos dois cenários típicos mostrados nas Figuras 3 e 4. Conforme breve descrição a seguir, tente ‘entender’ os elementos presentes em cada Figura.

Cenário 1: A Empresa X deseja enviar um importante documento para a Empresa Y, tal que o conteúdo original do documento seja preservado (o documento não deve ser modificado) e somente a Empresa Y tenha acesso ao conteúdo do documento.

Figura 3 – Exemplo de aplicação de documentos digitais: Cenário 1



Fonte: autoria própria.

Cenário 2: Um documento é assinado por Suse. Então, outras pessoas podem consultar quem são os signatários do documento, conforme o conteúdo fiel do mesmo, e o momento de cada uma das assinaturas (data e horário em que ocorreu a assinatura).

Figura 4 – Exemplo de aplicação de documentos digitais: Cenário 2

Fonte: autoria própria.

Conforme já antecipado, o uso de documentos digitais faz surgir várias questões:

- O conteúdo original do documento foi preservado ao longo do tempo (e do seu trajeto)?
- Os signatários legítimos do documento foram inequivocamente identificados?
- O documento é acessível somente às pessoas autorizadas?

As dúvidas sobre essas questões podem ser eliminadas. O conteúdo sigiloso pode ser protegido de tal forma que um interceptador tenha acesso apenas a um conteúdo criptografado (uma sequência ininteligível de *bytes*), uma sequência que só o destinatário pode decifrar. Adicionalmente, quando o destinatário recebe um documento digital, é possível assegurar que o seu conteúdo foi produzido por determinado autor, ou seja, a integridade do documento digital não foi comprometida. Isto é possível pelo emprego de certificação digital.

1.4 Processo Eletrônico e Certificação Digital

O termo "processo eletrônico" se refere ao uso de meio eletrônico para o armazenamento de documentos digitais (tais como arquivos armazenados em discos rígidos do computador) e à transmissão eletrônica por meio de comunicação a distância, com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores (a *Internet*).[5]

Por exemplo, quando um profissional de saúde cria uma prescrição eletrônica que estará acessível em uma farmácia, esse processo eletrônico deve envolver algumas propriedades, a saber:

Figura 5 - Carrossel propriedades do processo eletrônico

Autenticação:
se refere a estabelecer ou confirmar algo como legítimo. Por exemplo, a autenticação ou identificação segura de um usuário por meio de sua identidade digital. Nesse caso, tanto o profissional de saúde que prescreveu quanto aquele que irá consultar a prescrição eletrônica (documento digital).

A Certificação Digital é o instrumento empregado para lidar com as propriedades identificadas acima. Antes, contudo, é importante mencionar que há vários termos relacionados e que é pertinente conhecê-los e distingui-los entre si, tais como: Certificação Digital, Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), Certificado Digital e Assinatura Digital.[6]

1.5 Conceitos

No contexto da certificação de documentos - ou seja, a garantia da legitimidade - os conhecidos cartórios são os mecanismos tradicionais utilizados para os documentos em papel: reconhecimento de firma e autenticação de cópias de documentos, dentre outros serviços. No caso de documentos digitais, é necessária uma certificação própria aos documentos dessa natureza – a **Certificação Digital** – tal que a garantia da legitimidade seja similar (ou mesmo superior) a dos documentos em papel atestada por cartórios. A Certificação Digital visa a promover as propriedades comentadas acima, a saber: autenticação, privacidade, autorização, integridade e não-repúdio.

É natural que cada nação tenha um mecanismo adotado para tornar crível a certificação digital. Isso ocorre por meio de uma **infraestrutura de chaves públicas acreditada**, para que os documentos e as transações tenham amparo legal. Essa infraestrutura, usualmente, emprega uma hierarquia que representa a 'cadeia de confiança' para os documentos digitais e as transações digitais. A hierarquia em geral possui uma raiz comum - a Autoridade Certificadora Raiz (AC) - e vários entes subordinados, cada qual com papel bem definido.

Por exemplo, no Brasil, o Registro Geral (RG) (popularmente mencionado como documento de identidade) é um documento cuja raiz da hierarquia da cadeia de confiança é o Ministério da Justiça (MJ). A certificação e a emissão do RG podem ser realizadas pela Secretaria de Segurança Pública (SSP) de cada Unidade da Federação, tal que cada SSP está subordinada ao MJ, em hierarquia. Dessa forma, essa cadeia de confiança garante que um dado RG identifique inequivocamente um particular cidadão.

O Certificado Digital é a identidade eletrônica[4] de uma entidade (por exemplo, uma pessoa) que, para ser válido, necessita de uma AC, que faz parte de uma cadeia de confiança. No contexto de documentos eletrônicos, a AC associa uma entidade (pessoa física ou pessoa jurídica) a um par de chaves criptográficas – uma **chave pública** e uma **chave privada**.

A Infraestrutura de Chaves Públicas Brasileira (**ICP-Brasil**) define a estrutura e a organização necessárias para que a certificação digital tenha amparo legal no País. A AC raiz é o Instituto Nacional de Tecnologia da Informação, conhecido por ITI, cujo Cadastro Nacional de Pessoa Jurídica (CNPJ) é 04.039.532/0001-93 e está localizado em Brasília/DF.

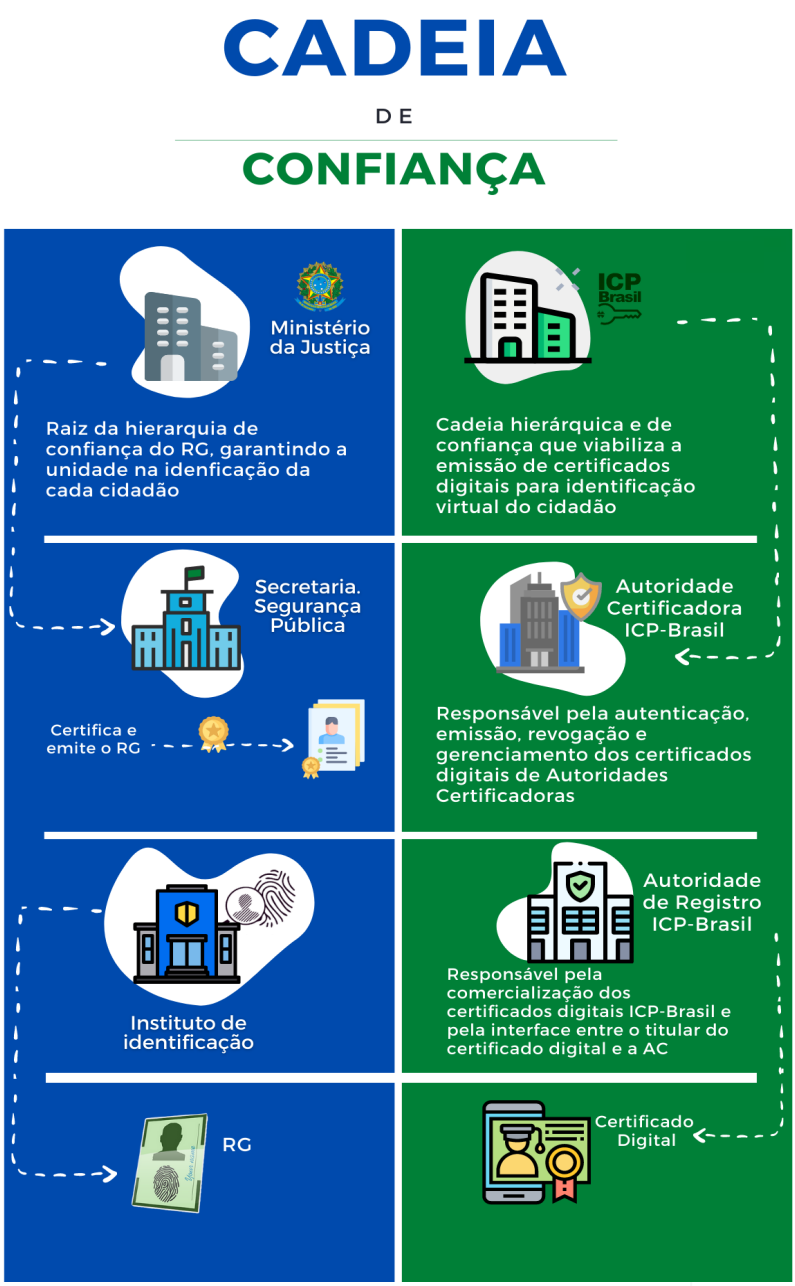
Convém esclarecer que a tecnologia necessária para a criação de certificados digitais encontra-se amplamente disponível e pode ser utilizada por qualquer pessoa. Contudo, para que tenha validade legal, uma 'cadeia de confiança', conforme esclarecido acima, necessariamente precisa ser obedecida. No Brasil, a 'cadeia de confiança' inicia pelo ITI (AC raiz) e se estende pelas AC de **primeiro nível**, daí para aquelas de **segundo nível**, até chegar às Autoridades de Registro (AR), aquelas que emitem os certificados digitais **válidos no território nacional.** Os Certificados Digitais emitidos por AR, por seguir a estrutura definida pela ICP-Brasil, também são denominados de **Certificados Digitais ICP-Brasil**.

Na Figura 5 é ilustrada, de forma sucinta, a analogia entre a cadeia de confiança para o RG (à esquerda) e a cadeia de confiança para o Certificado Digital (à direita). Na figura, a sigla AC denota Autoridade de Certificação e AR denota Autoridade de Registro, ambas são entidades acreditadas na estrutura do ICP-Brasil. Vale ressaltar que a ICP-Brasil é uma estrutura, uma especificação; quem é a AC raiz é o próprio ITI.[7]

Em resumo, o objetivo da ICP-Brasil é promover o uso de documentos digitais e transações digitais, com valor legal, a partir do processo de certificação digital, no território nacional. Por exemplo, a certificação digital atesta que, se uma pessoa utiliza o seu Certificado Digital (identidade digital) para assinar documentos digitais, as assinaturas digitais são não-repudiáveis.

4 Usamos os termos "identidade digital", "identidade eletrônica" e "identidade virtual" com o mesmo significado.

Figura 6 – Cadeia de confiança dos documentos: Registro Geral - RG (à esquerda) e Certificado Digital (à direita)



Fonte: adaptado de Machado (2010).[7]

1.6 Marcos da Certificação Digital no Brasil

O marco inicial da certificação digital em nosso País é a introdução da ICP-Brasil pela Medida Provisória Nº 2.200-2 de 24 de agosto de 2001.[8]

A finalidade primária da ICP-Brasil é ter uma infraestrutura para a autenticidade, integridade e validade jurídica de documentos em forma eletrônica. Essa Medida Provisória também criou o ITI, com o fim específico de ser a AC Raiz da ICP-Brasil. Outrossim, a ICP-Brasil foi estruturada na forma "conjunto de entidades",[9] cada qual com competência de atuação previamente delimitada, conforme descrito na Unidade 5.

Na Figura 6, em linha do tempo, são ilustrados alguns dos marcos pertinentes à história da certificação digital no Brasil. São evidenciados alguns dos instrumentos regulatórios que fortalecem o uso de certificados digitais no âmbito da ICP-Brasil.

Com respeito à área fiscal, a Nota Fiscal Eletrônica (NF-e) teve sua disposição inicial em 2003, com a Emenda Constitucional (EC) Nº 42,[10] que designa a prioridade de recursos ao compartilhamento de dados fiscais entre os entes da Federação. Para tornar possível esse compartilhamento, em 2005, um protocolo entre administradores tributários[11] foi estabelecido para a substituição das notas fiscais em papel por documento eletrônico. Esse marco dispôs sobre medidas e esforços para o desenvolvimento e padronização nacional da NF-e. Em 2006, Goiás e Rio Grande do Sul emitiram as primeiras NF-e com validade tributária.

Na área jurídica, a admissão de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais é alcançada pela Lei Nº 11.419,[5] de 19 de dezembro de 2006, que torna mandatória a aplicação de certificados digitais emitidos por AC credenciada. Especificamente, a lei dispõe sobre a informatização do processo judicial e estabelece, como uma das formas de assinatura eletrônica, a assinatura digital baseada no certificado ICP-Brasil.

Em relação à área de saúde, a Resolução do Conselho Federal de Medicina (CFM) Nº 1.821, de 11 de julho de 2007,[12] dispõe sobre a validade do Prontuário Eletrônico do Paciente (PEP). Essa Resolução aprova normas técnicas concernentes à digitalização e ao uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. A Resolução determina, ainda, que a eliminação de papel só é possível com a utilização do Certificado Digital padrão ICP-Brasil.

Figura 7 – Alguns dos primeiros marcos da Certificação Digital no Brasil

Fonte: autoria própria.

Com respeito à validade de documentos digitalizados, a Lei N° 12.682, de 9 de julho de 2012,[13] que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos, determina que o processo de digitalização que empregar o uso da certificação no padrão da ICP-Brasil terá garantia de integralidade, autenticidade e confidencialidade para documentos públicos e privados. Essa Lei atesta a validade de documentos digitalizados – obtidos a partir da conversão de um documento não digital, gerando uma fiel representação em código digital – e, por consequência, de documentos nato-digitais (criados originariamente em meio eletrônico), desde que seja aplicado Certificado Digital emitido no âmbito do ICP-Brasil.

Alguns outros marcos importantes são: em 2004, o Tribunal Superior Eleitoral (TSE) adotou certificação digital para a assinatura da conferência do *software* das urnas eletrônicas; em 2007, criado o processo de emissão de passaporte com Certificado Digital; em 2011, Processo Judicial Eletrônico (PJ-e); em 2012, Certificado Digital obrigatório para declaração de renda de pessoa física com renda superior a 10 milhões; em 2017, criação da Carteira Nacional de Habilitação 2 (CNH-2); dentre outros.

Por meio da Medida Provisória N° 2.200-2, de 24 de agosto de 2001,[8] a ICP-Brasil transformou o ITI em autarquia. Essa referência informa sobre a importância e a atenção com que o Estado Brasileiro trata o tema.

1.7 *Quiz*

Para testar os conhecimentos adquiridos até aqui, responda ao quiz no Ambiente Virtual.

- Autenticação, privacidade, autorização, integridade e não-repúdio são os pilares da certificação digital.
- A criação da ICP-Brasil em 2001 foi o passo inicial para que as pessoas físicas e jurídicas pudessem ter e usar certificados digitais no Brasil, em diversas ações de uso e validação de documentos digitais.
- Outros importantes marcos seguiram e continuarão a ocorrer, a partir de legislações que orientam e regulamentam a certificação digital em vários domínios e contextos da sociedade.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 2
Certificados Digitais – Tipos e Validade

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 2: Certificados Digitais - Tipos e Validade

O **Certificado Digital ICP-Brasil** é um documento de identidade eletrônico visando à identificação de seu titular (por exemplo, pessoa física ou jurídica) no mundo digital. Certificados digitais são empregados para assinar um documento digital. O efeito é similar àquele em que assinamos em papel e reconhecemos firma em um cartório, o cenário comum hoje em dia.

Doze tipos de certificados digitais ICP-Brasil foram inicialmente previstos: oito relacionados com assinatura digital e quatro relacionados com sigilo. Os tipos de Certificado Digital e algumas de suas características são apresentados na Tabela 1, na qual são observados dois propósitos principais:[14]

- certificados relacionados com **assinatura digital**; e
- certificados relacionados com **sigilo**.

Os **certificados relacionados com assinatura digital** buscam: (i) identificar quem assinou o documento (autenticidade); e (ii) confirmar a integridade do documento (permitir assegurar que o conteúdo não foi alterado após assinatura digital).

Os **certificados relacionados com sigilo** são aplicados para criptografar o conteúdo do documento digital, visando a permitir o acesso ao conteúdo apenas a quem tiver autorização. Por exemplo, se o documento A for criptografado utilizando a **Chave Pública da Pessoa X**, então somente a **Chave Privada da Pessoa X** poderá descriptografar o documento A. Ou seja, o conteúdo do documento A, após ser criptografado, não poderá ser recuperado nem mesmo por quem o criptografou, o conteúdo só poderá ser revelado pela Pessoa X.

Tabela 1 – Tipos de Certificado Digital

Propósito	Tipo de certificado	Validade máxima	Chaves criptográficas	
			Tamanho (bits)	Mídia armazenadora
Assinatura digital	**A1**	1 ano	1.024 / 2.048	Instalado no disco do computador
	A2	2 anos	1.024 / 2.048	*Hardware* criptográfico, tal como cartão inteligente ou *token*
	A3	5 anos	1.024 / 2.048	*Hardware* criptográfico, tal como cartão inteligente, *token* ou nuvem
	A4	11 anos	2.048 / 4.096	*Hardware* criptográfico, tal como HSM** ou nuvem
	T3	5 anos	1.024 / 2.048	*Hardware* criptográfico, tal como cartão inteligente, *token* ou nuvem
	T4	11 anos	2.048 / 4.096	*Hardware* criptográfico, tal como HSM** ou nuvem
	A CF-e-SAT	5 anos	2.048	*Hardware* criptográfico
	OM-BR	10 anos	*	*Hardware* criptográfico

Sigilo	**S1**	1 ano	1.024 / 2.048	Instalado no disco do computador
	S2	2 anos	1.024 / 2.048	*Hardware* criptográfico, tal como cartão inteligente ou *token*
	S3	5 anos	1.024 / 2.048	*Hardware* criptográfico, tal como cartão inteligente, *token* ou nuvem
	S4	11 anos	2.048 / 4.096	*Hardware* criptográfico, tal como HSM** ou nuvem

(*) Regulamentado por instrução normativa. (**) HSM vem do inglês *Hardware Security Module*, ou Módulo de Segurança de *Hardware*, e se refere ao dispositivo que armazena o Certificado Digital na nuvem. Fonte: Brasil, Instituto Nacional de Tecnologia da Informação [s.d].[14]

Na segunda coluna da Tabela 1 – **Tipo de Certificado** – estão elencados os vários tipos conforme o propósito, a validade do certificado, o tamanho das chaves criptográficas e a mídia armazenadora da chave privada, a saber:

- Os certificados do **Tipo A** – A1, A2, A3 e A4 – são os mais comuns e utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.
- Os certificados do **Tipo T** – T3 e T4 – se referem ao Carimbo de Tempo (em inglês *timestamp*) e visam a garantir o instante de tempo em que o carimbo foi aplicado a um documento, conferindo integridade e temporalidade ao documento. Por exemplo, funciona como um "selo" que declara a data, hora, minuto e segundo em que um documento recebe uma assinatura digital.
- Os certificados do **Tipo S** – S1, S2, S3 e S4 – são utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo.
- Os certificados de **Tipo A CF-e-SAT** são utilizados exclusivamente em equipamentos para a assinatura de Cupom Fiscal Eletrônico (CF-e), por meio do Sistema de Autenticação e Transmissão de Cupom Fiscal Eletrônico (SAT-CF-e), seguindo a regulamentação do Conselho Nacional de Política Fazendária (CONFAZ).
- Os certificados do **Tipo OM-BR** são utilizados exclusivamente em equipamentos metrológicos regulados pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro).

Observe na Tabela 1 que alguns tipos de certificado são apresentados em níveis (escalas) de segurança: A (A1 a A4), S (S1 a S4) e T (T3 e T4). Por exemplo, os certificados do Tipo A4, S4 e T4 são mais rigorosos quanto à segurança em relação aos Certificados A1, S1 e T3, respectivamente. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho das chaves criptográficas, mídia armazenadora da chave, processo de geração do par de chaves, etc.

Atrelado a cada Certificado Digital, há duas chaves: uma **chave pública** e uma **chave privada**. A primeira é uma chave visível a todos e a segunda é restrita ao titular (dono) do certificado. Essas chaves são chamadas **chaves criptográficas**, pois são utilizadas para a criptografia (atos de encriptar e desencriptar) de informação acerca do conteúdo do documento eletrônico e das suas assinaturas digitais.

A chave privada do Certificado Digital deve ser de conhecimento e uso exclusivo do seu legítimo titular. Na prática, a chave privada não é 'memorizada' pelo seu titular, em vez disso é armazenada de forma criptografada em alguma mídia.

A mídia que armazena a chave privada (ver a Coluna **Mídia armazenadora das chaves criptográficas** na Tabela 1) é mais segura se em *hardware* criptográfico, com escalas de segurança em relação ao tipo de *hardware*.

Outrossim, o tamanho das chaves criptográficas (ver a Coluna **Tamanho das chaves criptográficas** na Tabela 1) impacta a segurança da certificação digital: quanto maior a chave, maior a segurança. Por exemplo, um certificado T4 é mais seguro que um T3, devido ao tamanho das chaves e o tipo de mídia armazenadora.

Em outro aspecto fundamental à certificação digital, todo Certificado Digital possui um período de validade. Nesse sentido, dois aspectos são proeminentes: (i) o ato de aplicar (associar) Certificados Digitais a documentos digitais para assinatura ou sigilo é restrito ao período de validade do certificado; (ii) o ato de checar a associação entre Certificados Digitais e documentos digitais pode ser realizada durante e após o período de validade dos certificados. Em geral, certificados mais seguros têm período de validade mais largo (ver a coluna **Validade máxima** na Tabela 1).

Na Figura 7, consta um exemplo de aplicação de Certificado do Tipo S (sigilo). Suse possui um Certificado Digital S1. Warllson precisa enviar, via *Web*, uma mensagem secreta para Suse. Se a mensagem for interceptada por outra pessoa, tal pessoa não poderá obter o conteúdo da mensagem:

1. Warllson utiliza a chave pública da Suse para encriptar a mensagem, para que, eventualmente, alguém que intercepte a mensagem encriptada não tenha acesso ao seu conteúdo.
2. A mensagem encriptada 'trafega' pela *Web* até alcançar a Suse (o destino da mensagem).
3. Suse utiliza sua chave privada para desencriptar a mensagem e, portanto, ter acesso ao conteúdo original da mensagem, pois, apenas o detentor da chave privada consegue decifrar e ler a mensagem (sem esse passo, a Suse também não conseguiria ter acesso ao conteúdo da mensagem).

Figura 8 – Exemplo de aplicação de Certificado Digital Tipo S (sigilo)

Fonte: autoria própria.

Por fim, o interessado em fazer uso de um Certificado Digital ICP-Brasil, pessoa física ou jurídica, usualmente deve adquiri-lo a partir de uma Autoridade Certificadora (AC) da estrutura hierárquica da ICP-Brasil. A Unidade **Processo de Aquisição e Uso**, presente neste *ebook*, esclarece a iniciação e a utilização de certificados digitais.

Sobre a aprovação dos Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil, a versão mais recente (e ampla) para os atributos de cada tipo de certificado é apresentada na Resolução Nº 179, de 20 de outubro de 2020,[15] que revoga outras resoluções anteriores.

2.1 *Quiz*

Para testar os conhecimentos adquiridos até aqui, responda ao quiz no Ambiente Virtual.

Os certificados digitais ICP-Brasil são classificados:

- quanto à natureza do uso: relacionados com assinatura digital e relacionados com sigilo;
- quanto à segurança: tamanho das chaves criptográficas, mídia armazenadora da chave privada, etc.;
- quanto à especificidade: assinatura em Cupom Fiscal Eletrônico, equipamentos metrológicos regulados pelo Inmetro, carimbo de tempo.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 3

Diferenças entre Assinatura Digital e Certificado Digital

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 3: Diferenças entre Assinatura Digital e Certificado Digital

O **Certificado Digital** é um documento de identificação, similar a um RG, Cadastro de Pessoa Física (CPF) ou CNPJ, cujo objetivo é estabelecer a identidade do seu titular no ambiente digital, principalmente, a *Internet*. Por exemplo, o Certificado Digital é usado para que um documento digital ou ação efetuada por um sujeito, por meio eletrônico, tal como o envio de uma mensagem (e-mail) ou uma transação bancária, seja identificada inequivocamente como sua, por meio de uma **Assinatura Digital**.

3.1 Certificado Digital

O Certificado Digital é um documento com validade limitada, cujo uso é protegido por um sistema de duas chaves criptográficas, uma pública e outra privada, as quais são únicas para a certificação no âmbito da ICP-Brasil.

Na Figura 8, constam algumas das informações em um Certificado Digital, que estão classificadas em grupos, conforme a seguir:

- **Certificado:** o número de série identifica o certificado; o período de validade representa o período no qual o certificado pode ser usado para sigilo ou assinatura digitais; e a chave pública se refere à chave criptográfica visível a todos.
- **Titular do certificado:** nesse grupo estão o nome completo e o e-mail do titular do certificado. Também constam os dados do documento de identificação do titular, tais como RG, CPF, CNPJ, documento de classe profissional (por exemplo, CRM – Conselho Regional de Medicina), etc.
- **Autoridade certificadora (AC):** o nome e a assinatura digital da AC que emitiu o certificado estão nesse grupo (por se tratar de um documento para o ambiente digital, o Certificado Digital também precisa ser assinado para ser válido).

Vale ressaltar que a chave privada não está presente na Figura 8, pois, conforme mencionado anteriormente, é armazenada de forma criptografada em alguma mídia, que deve ser acessível somente ao titular do certificado.

Convém, também, esclarecer que os dados pertinentes a um certificado são armazenados em um arquivo. Aqueles com a extensão **.p12** ou **.pfx**, por exemplo, empregam o formato PKCS #12 que pode, inclusive, incluir a chave privada. Há outros formatos como PEM, contudo estes e muitos outros detalhes tecnológicos estão além do escopo desta Unidade.

Figura 9 – Principais informações que constam no Certificado Digital

Fonte: autoria própria.

3.2 Assinatura Digital

Segundo a Wikipedia,[16] assinatura, ou firma, é uma marca ou escrito em algum documento que visa dar-lhe validade ou identificar a sua autoria; normalmente, costuma incluir todos ou parte dos nomes da pessoa por extenso e é representada por espécies de desenhos ou grafias específicas.

O termo **assinatura eletrônica** se refere a um valor que é associado a um documento eletrônico (ou transação eletrônica), para garantir sua autenticidade ou autoria, e pode ter diversas formas: biometria, login/senha, etc. Especificamente, a **assinatura digital** é um tipo de assinatura eletrônica, que emprega um par de chaves criptográficas (chave pública e chave privada), as quais estão associadas a um Certificado Digital.[6]

Para esclarecer o processo de assinatura digital no âmbito da Certificação ICP-Brasil, é necessário conhecer dois conceitos: **função de resumo** e **algoritmo criptográfico de chave pública**.

3.2.1 Função de Resumo

Uma **função de resumo** (também chamada **função *hash***) é uma função que recebe um conteúdo de entrada (por exemplo, um documento) e produz um valor de saída, a partir de um cálculo realizado sobre o conteúdo de entrada. Apesar de ser chamada 'função de resumo', a saída não produz informação resumida em relação ao documento original, mas um conteúdo cujo tamanho é tipicamente menor do que o do documento original. Existem várias funções de resumo e você pode experimentá-las do seu navegador.[17] Na Tabela 2, é ilustrada a aplicação de algumas funções de resumo aplicadas ao conteúdo de entrada igual a "certificação digital":[18]

Tabela 2 – Exemplos de aplicação de função de resumo com valores para a entrada "certificação digital".

Entrada	Função	Saída (sistema hexadecimal)
certificação digital	MD5	893C E27D 474A FA6E 204E A4B3 9925 7232
certificação digital	SHA1	F63F 932F 23DA AE19 D961 4EB6 E38C 5864 147A 0C7E
certificação digital	SHA256	0AAA A1E8 D95F 1994 CF0C 7DE8 F8A4 E039 5998 E3BA 8717 82F6 64A4 1BD4 7D80 2F42

Fonte: Dan's Tools [s. d.].[18]

Convém observar que não é possível obter o valor de entrada de uma função de resumo a partir da saída. Noutras palavras, a partir de uma sequência de saída conhecida (tal como "893C E27D 474A FA6E 204E A4B3 9925 7232" na Tabela 2), não é possível saber a sequência de entrada (ou seja, "certificação digital"), mesmo que se saiba que essa sequência é o resultado da função MD5, conforme na Tabela 2. É por esse motivo que sistemas, em geral, armazenam as senhas de seus usuários pelos valores de resumo (valores *hash*) correspondentes, em vez do valor original das senhas. Dessa forma, mesmo que o conteúdo dos valores de resumo tornem-se disponíveis, não é possível obter as senhas correspondentes.

Na Figura 9, consta uma função de resumo, cuja **entrada é um documento digital** (122 páginas se for impresso) e a **saída é um valor hexadecimal**[5], no caso o valor "56E2 9C21 A37B 00A2 8134 AB5C 8220 44AA". Observe que o tamanho do documento (122 páginas) é bem maior do que o valor hexadecimal de saída.

Figura 10 – Função *hash* aplicada a um documento digital

Fonte: autoria própria.

5 O sistema hexadecimal de numeração representa um valor por meio de uma sequência dos símbolos 0, 1, ..., 8, 9, A, B, ...E, F.

Por fim, uma função de resumo gera um valor de saída de tamanho fixo, independentemente do tamanho da entrada. Por exemplo, a função de resumo "SHA256" produz uma sequência hexadecimal de 64 caracteres hexadecimais, correspondentes aos 256 *bits*, tamanho fixo da saída produzida por essa função.

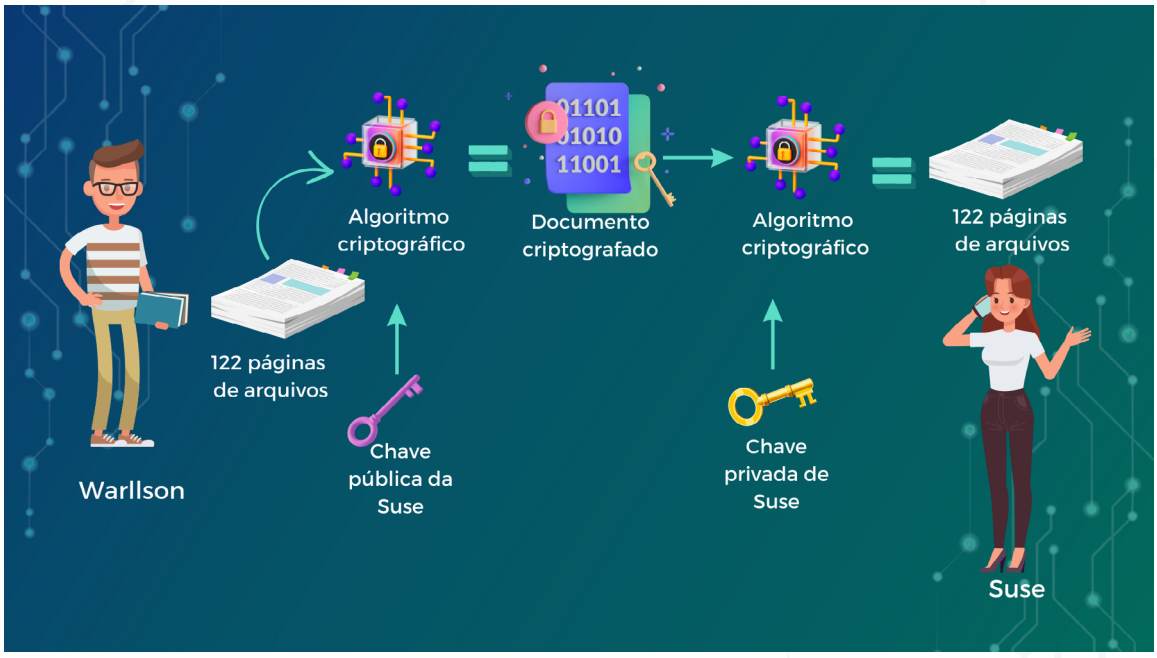
3.2.2 Algoritmo Criptográfico de Chave Pública

Um **algoritmo criptográfico de chave pública** faz uso de duas chaves, uma pública e outra privada. Nesse caso, ele usa uma das chaves criptográficas para encriptar (cifrar) um conteúdo de entrada e, portanto, produzir uma **versão criptografada do conteúdo**. O mesmo algoritmo criptográfico usa a outra chave criptografada para produzir o **conteúdo original** a partir da versão criptografada do conteúdo.

Observe que algoritmos de chave pública não exigem o compartilhamento de uma chave secreta (no caso, a chave privada). Ou seja, nenhum segredo precisa ser compartilhado (o que é mais seguro). De fato, a chave pública pode ser amplamente distribuída, enquanto a chave privada é mantida restrita ao seu proprietário. Adicionalmente, tendo em vista que tais algoritmos permitem que uma chave seja empregada para cifrar e a outra para realizar o processo inverso, vários usos são possíveis. Alguns deles são apresentados a seguir. Você pode experimentar, via navegador, o processo de uso de um algoritmo criptográfico de chave pública acessando o *link* https://www.md5hashgenerator.com/.[19]

Similarmente à Figura 7, na Figura 10, é ilustrado o uso de criptografia de chave pública: (i) um conteúdo é criptografado a partir de uma chave pública (a chave pública da Suse); (ii) uma chave privada (a chave privada da Suse) é aplicada à versão criptografada do conteúdo para produzir o conteúdo original.

Figura 11 - Aplicação de criptografia de chave pública



Fonte: autoria própria.

3.2.3 Uso de Assinatura Digital

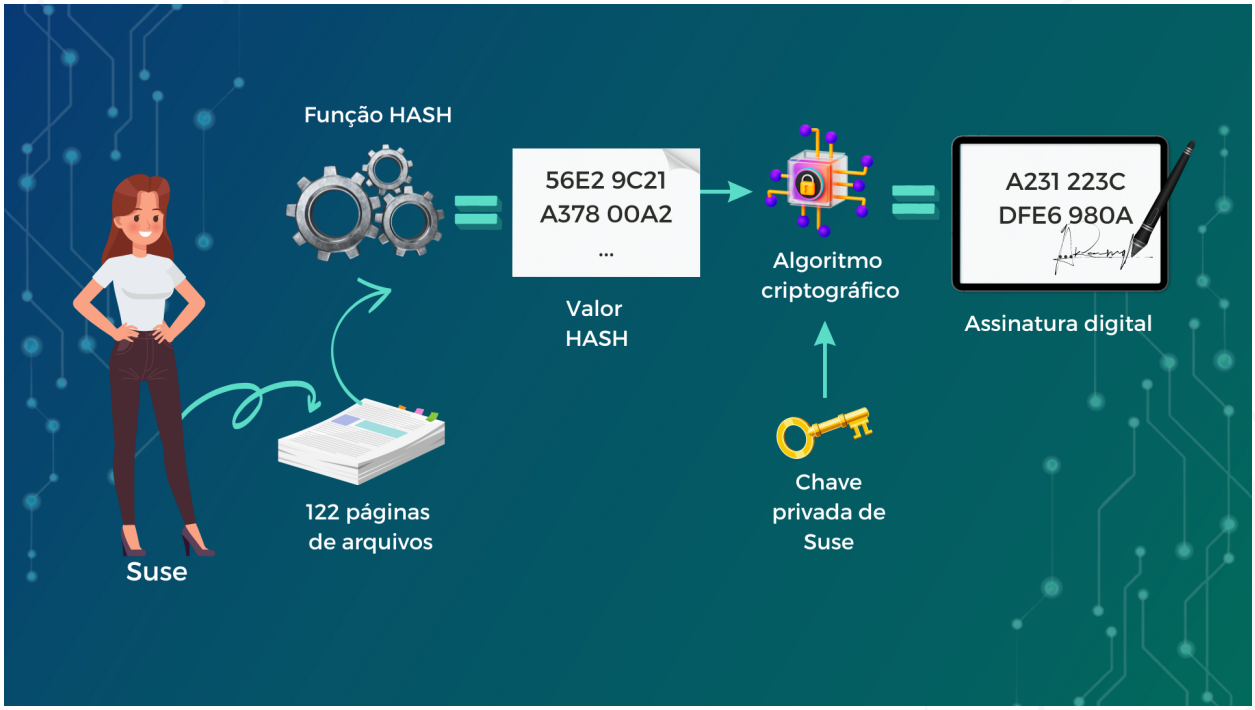
O emprego da **assinatura digital** no âmbito da Certificação ICP-Brasil ocorre em dois momentos: (i) geração de assinatura digital; e (ii) checagem de assinatura digital.

Na **geração da assinatura digital**, é produzido um valor de saída (uma sequência de dados) a partir de dois conteúdos, a saber: (i) o documento sendo assinado; e (ii) a chave privada do Certificado Digital de quem está assinando. O valor produzido (a sequência de dados) é a assinatura digital em si. Na Figura 11, é ilustrada a geração de uma assinatura digital, que é composta dos seguintes passos:

1. Uma função de resumo é aplicada ao documento original para produzir um **valor de resumo do documento,** representado na Figura 11 pelo valor hexadecimal "56E2 9C21 A37B 00A2 8134 AB5C 8220 44AA".
2. O algoritmo criptográfico de chave pública usa o valor de resumo do documento e a chave privada do assinante para produzir o **valor referente à assinatura digital**, representado na Figura 11 pelo valor hexadecimal "A231 223C DFE6 980A FFEA AB99 E129 E9A7".

Em resumo, a assinatura digital é um valor (sequência de *bytes*) obtido a partir do documento sendo assinado e da chave privada do seu assinante.

Figura 12– Geração de assinatura digital

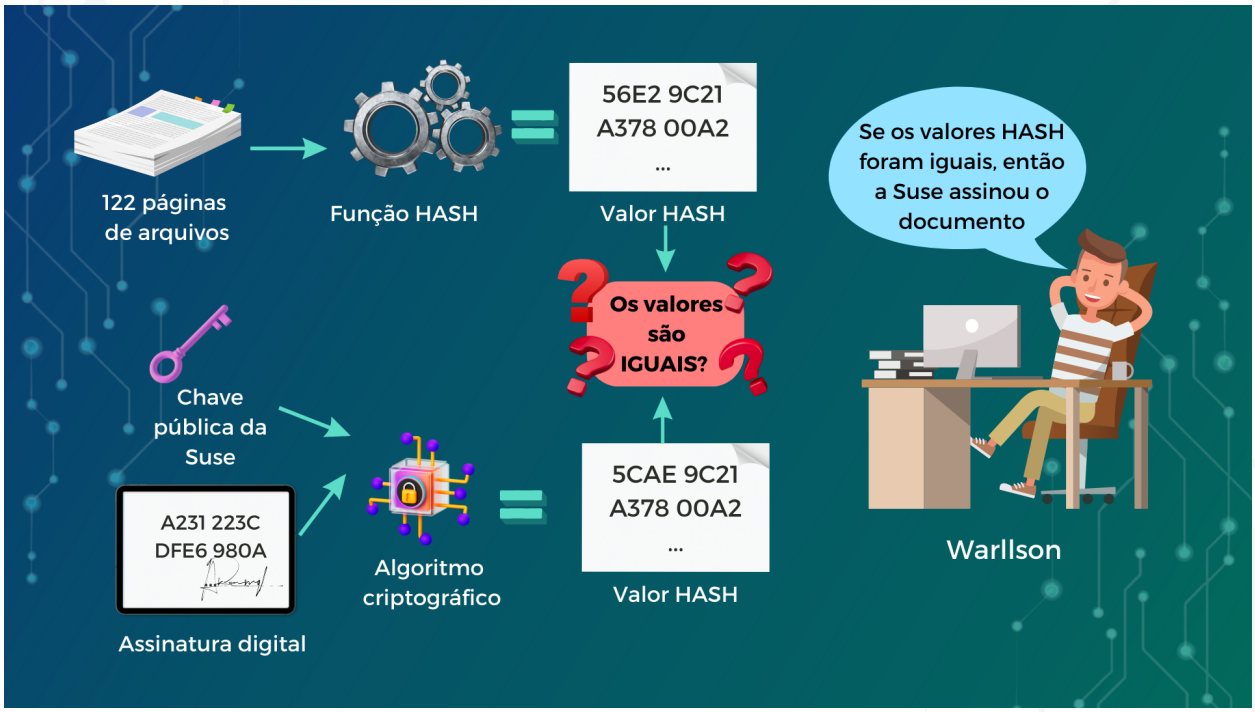


Fonte: autoria própria.

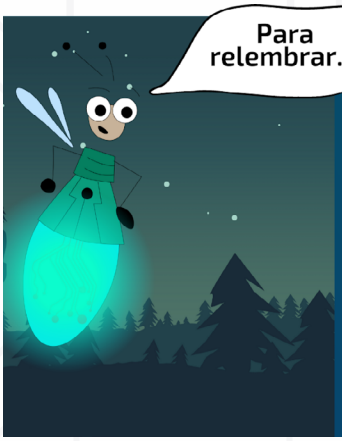
Uma vez que documentos eletrônicos estão assinados digitalmente, é pertinente comprovar por meio da **checagem da assinatura digital** para, por exemplo, responder a pergunta "fulano assinou este documento?". Na Figura 12, é ilustrada a checagem da assinatura digital, que é composta dos seguintes passos:

1. Uma função de resumo é aplicada ao *documento original* para produzir um **valor de resumo do documento**, representado na Figura 12 pelo valor hexadecimal “56E2 9C21 A37B 00A2 8134 AB5C 8220 44AA”. Naturalmente, deve ser aplicada a mesma função de resumo utilizada para assinar o documento.
2. O algoritmo criptográfico de chave pública, utilizado para produzir a assinatura digital, recebe como entrada o **valor de assinatura digital** (na Figura 12, o valor “A231 223C DFE6 980A FFEA AB99 E129 E9A7”) e a **chave pública do assinante** para produzir um **valor que representa a assinatura digital desencriptada**, representado na Figura 12 pelo valor hexadecimal “56E2 9C21 A37B 00A2 8134 AB5C 8220 44AA”.
3. Os valores produzidos nos Passos 1 e 2 são comparados: (i) se forem idênticos, fica comprovado que o documento recebeu a assinatura digital do titular da chave pública usada no Passo 2; (ii) se forem distintos, a assinatura está incorreta. Ou seja, pode-se assegurar que o documento empregado no Passo 1 não foi assinado com a chave privada do suposto assinante.

Figura 13 – Checagem de assinatura digital



Fonte: autoria própria.



- Certificado Digital é um documento de identificação no ambiente digital.
- Assinatura Digital é uma assinatura aplicada a um documento eletrônico, cuja autenticidade pode ser checada a partir do Certificado Digital do autor da assinatura.
- O processo de assinatura digital gera assinaturas digitais válidas juridicamente, se forem empregados certificados digitais no âmbito da ICP-Brasil.

3.3 Faça você mesmo: Certificado Digital e Assinatura Digital

Para ilustrar o uso do certificado digital e da assinatura digital, considere ter o seu certificado digital pessoal (um certificado para pessoa física). Como os certificados ICP-Brasil não são gratuitos, então vamos empregar o certificado da cadeia **ICPEdu**.

ICPEdu é uma plataforma de emissão de certificados digitais pessoais para membros de instituições que fazem parte da Comunidade Acadêmica Federada, como é o caso da Universidade Federal de Goiás. Não é raro que tais instituições utilizem o Certificado Digital **ICPEdu**, visto que são gratuitos, mas sua validade é restrita ao sistema acadêmico e de pesquisa brasileiros, podendo ser usado por alunos, professores e servidores.

3.3.1 Emissão do Certificado ICPEdu

Para a emissão do seu certificado ICPEdu, considere as instruções abaixo:

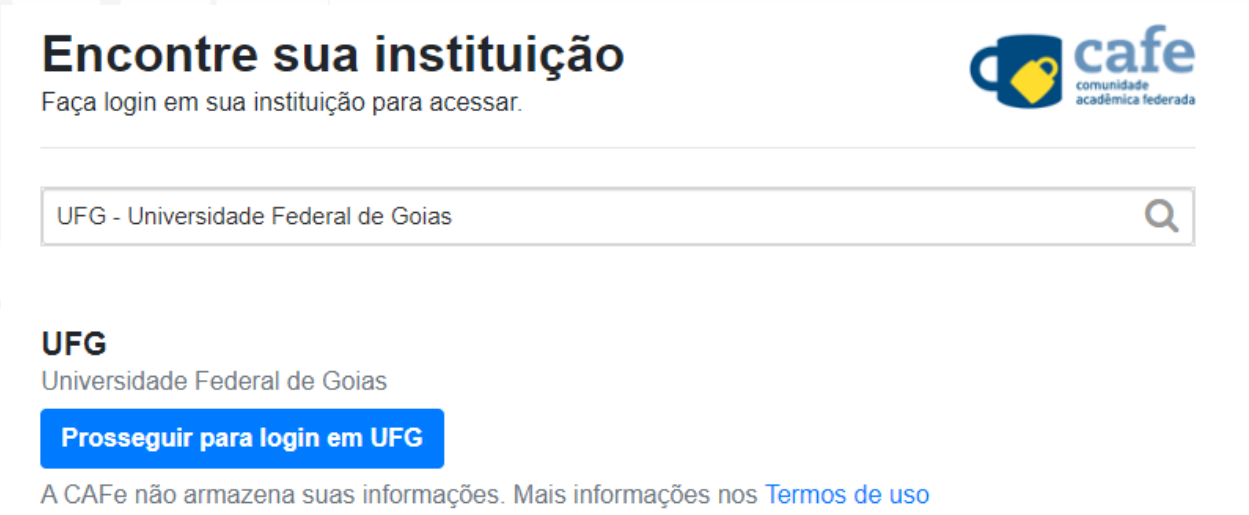
1) Entre no site https://pessoal.icpedu.rnp.br/home e veja o conteúdo da Figura 13.

Figura 14 – Interface ICPEdu

Fonte: Rede Nacional de Ensino e Pesquisa.

2) Clique em “Emitir Certificado Pessoal”.
3) Para ter direito ao certificado, a instituição deve fazer parte da Comunidade Acadêmica Federada (CAFe). Selecione a instituição “Universidade Federal de Goiás”, conforme a Figura 14 (afinal, você é aluno e possui e-mail com o domínio ufg.br; por exemplo, *meunome*@discente.ufg.br), e clique em “Prosseguir” para ter acesso como membro CAFe pela UFG. O certificado será do Tipo **A1** e a emissão será feita pela Autoridade Certificadora AC PESSOAS, Instituição UFG - Universidade Federal de Goiás.

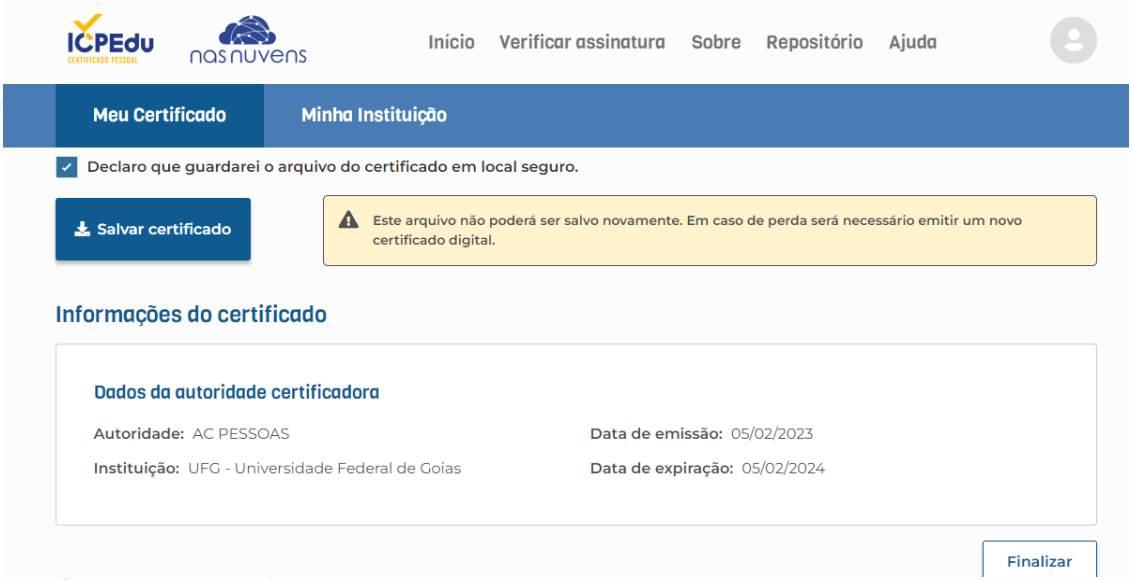
Figura 15 – Interface para a instituição da Comunidade Acadêmica Federada (CAFe)



Fonte: Rede Nacional de Ensino e Pesquisa.

4) Você será direcionado para o serviço de *login* CAFe, então forneça seu e-mail e a senha do seu e-mail (o e-mail pessoal como aluno da UFG, tal como *meunome*@discente.ufg.br).
5) Uma vez que você identificou-se como aluno da UFG, clique em “Emitir Certificado Pessoal”, e receberá a mensagem “Você não possui certificado ativo no momento”. Então, clique novamente em “Emitir Certificado Pessoal”.
6) Confira os seus dados pessoais que foram exibidos, a saber: nome, CPF, e-mail e data de nascimento. Então, clique em “Confirmar dados”.
7) Para concluir a emissão será necessário fornecer pertinentes ao certificado: (i) uma nova senha, que será a senha para acesso à chave privada do certificado; e (ii) um lembrete dessa senha (para o caso de você esquecer a senha). Note que, para utilizar o certificado em suas assinaturas digitais, você deverá fornecer a senha de acesso à chave privada do certificado, então é mandatório não esquecer tal senha. Marque “Estou ciente de que minha senha não pode ser recuperada”, e clique em “Emitir novo certificado”.
8) Uma tela similar ao conteúdo da Figura 15 será exibida. Marque “Declaro que guardarei o arquivo do certificado em local seguro” e clique em “Salvar certificado”. O arquivo do certificado será então copiado para o seu computador (confira se o arquivo foi copiado para o diretório “*Downloads*”, caso este diretório esteja configurado no seu computador para “baixar arquivos”).

Figura 16 – Interface para “salvar certificado”



Fonte: Rede Nacional de Ensino e Pesquisa.

9) Para concluir, clique em “Finalizar” e verá um resumo do seu certificado, com dados tais como: detentor do certificado (você), CPF, e-mail, nascimento, autoridade certificadora, data de emissão e data de expiração.

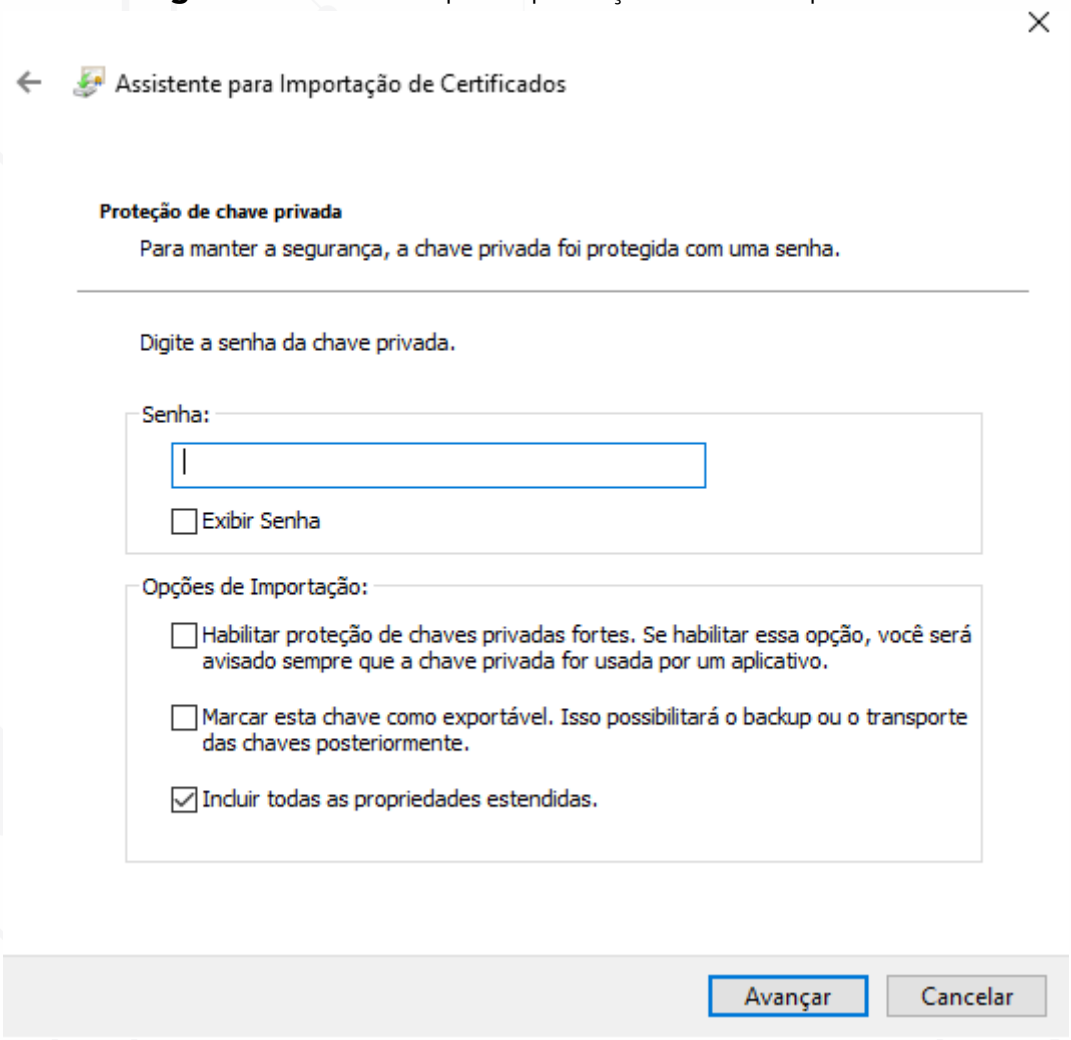
Pronto! O certificado foi emitido e o arquivo com o conteúdo do certificado foi salvo em seu computador.

3.3.2 Instalação do Certificado ICPEdu no Windows

Após a emissão do certificado, é necessário “instalar” o certificado no seu computador (veremos, aqui, como instalar no Windows®). Então, favor observar os seguintes passos:

1) Encontre o arquivo do certificado digital que foi copiado para o seu computador, conforme instruções na Seção 3.3.1. Possivelmente, o arquivo foi copiado para o diretório “*Downloads*”, mas lembre-se de guardar o arquivo em local seguro:
Em geral, a identificação do arquivo possui o nome e o CPF do seu detentor, tal como o padrão: “nome_e_cpf_do_usuario-certificate.p12”.
2) Após localizar o arquivo, clique duas vezes no arquivo (clique duplo).
3) Uma janela é então aberta para questionar se a instalação será na “Máquina atual” ou no “Usuário atual”. Recomenda-se instalar no “Usuário atual” para impedir que outros usuários do mesmo computador possam usar o seu certificado. Marque “Usuário atual” e clique em “Avançar”.
4) O nome do arquivo é exibido. Então, clique em “Avançar” novamente.
5) Uma tela similar ao conteúdo da Figura 16 é exibida. Marque “Incluir todas as propriedades estendidas” e digite a senha de acesso à chave privada do seu certificado (a mesma senha que você informou ao criar o certificado).

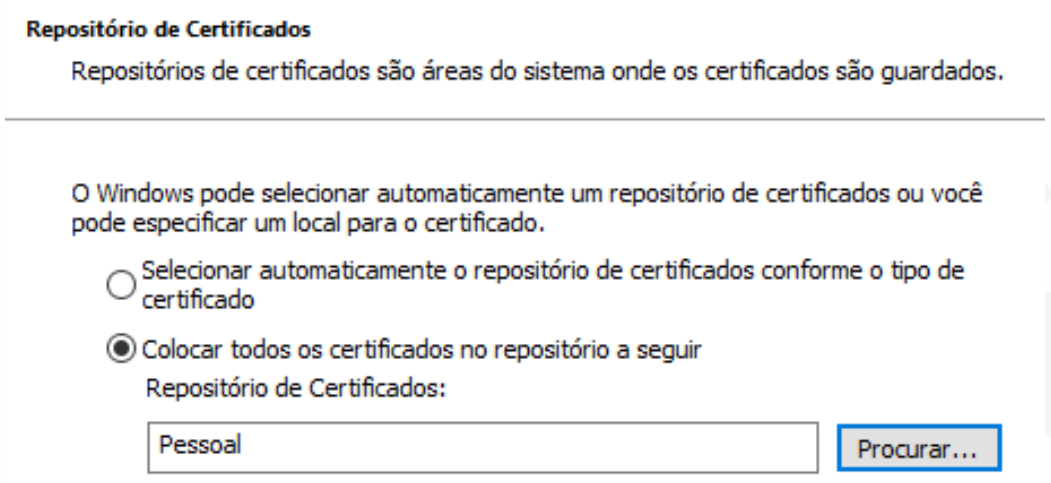
Figura 17 - Interface para “proteção de chave privada”



Fonte: autoria própria.

6) Uma tela para a “seleção de repositório de certificado” (Figura 17) é exibida. Marque “Colocar todos os certificados no repositório a seguir” e, para fins de simplicidade, clique em “Procurar”, em seguida, selecione a pasta “Pessoal”. Então, clique em “Avançar”.

Figura 18 – Interface para “repositório de certificado”



Fonte: autoria própria.

7) Para finalizar, uma tela é exibida para sua conferência, contendo as configurações que você selecionou. Então, clique em “Concluir”. Pronto! O certificado está instalado.

3.3.3 Obter os Certificados dos Entes da Cadeia de Confiança

Vimos, na Unidade 1, que há uma “cadeia de confiança” na forma de uma hierarquia, a qual é empregada aos documentos digitais e às transações digitais. Para tal, cada ente da “cadeia de confiança” precisa ser reconhecido como “acreditado” (confiável) por meio do seu próprio certificado digital. No caso do Certificado ICPEdu, esses entes são AC RAIZ e AC PESSOA.

Para obter (copiar para o computador) o certificado digital dos entes da “cadeia de confiança”:

1) Acesse a página https://pessoal.icpedu.rnp.br/public/repositorio, conforme a Figura 18.

Figura 19 – Interface para “certificados AC”

Fonte: autoria própria.

2) Selecione “Certificados AC”, clique em “Certificado AC Raiz” e clique em “Certificado AC Pessoa”, para copiar para o seu computador os arquivos dos certificados dos entes AC RAIZ e AC PESSOA, respectivamente. Ambos os arquivos (ac-raiz-v3.cer e ac-pessoa.cer), possivelmente, foram copiados para o diretório “*Downloads*”.

3.3.4 Instalar os Certificados dos Entes da Cadeia de Confiança

Utilizaremos o *software Adobe Acrobat Reader®*, com o intuito de fazer assinaturas digitais com o uso do nosso Certificado **ICPEdu**, especificamente, a assinatura digital para documentos em arquivos do Tipo *Portable Document Format* (PDF).

O *software Adobe Acrobat Reader®* é amplamente utilizado para a visualização (leitura) de documentos PDF. Caso não o tenha instalado no seu computador, o uso desse *software* é gratuito e ele pode ser obtido aqui.

Para instalar os certificados dos entes da cadeia de confiança, cujos arquivos foram copiados para o seu computador conforme a Seção 3.3.3, favor seguir os passos:

1) Inicie a execução do *Adobe Acrobat Reader®*.

2) No menu “Editar” do *Adobe Acrobat Reader®*, selecione a opção “Preferências” (em geral, é a última opção do menu “Editar”).

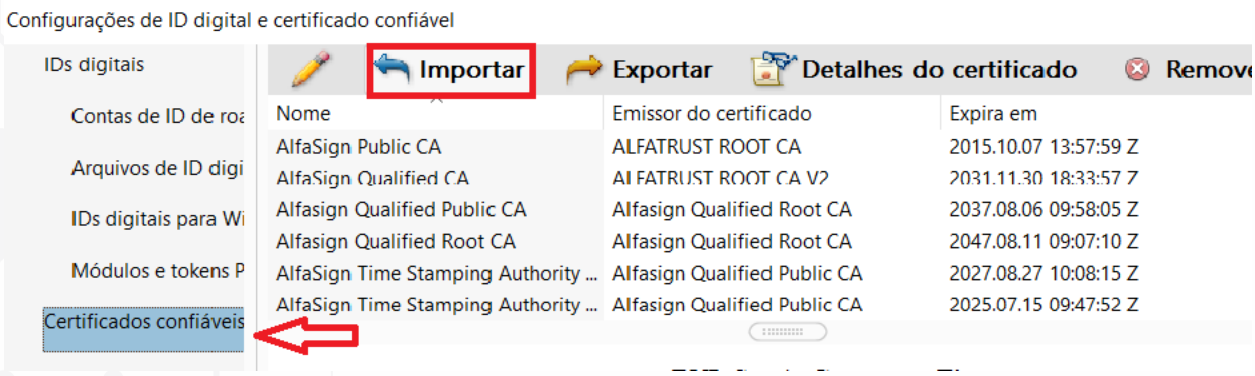
3) Conforme a Figura 19, selecione a categoria “Assinaturas” e clique no botão “Mais...” do grupo “Certificados confiáveis e de identidade”.

Figura 20 – Interface para “certificados confiáveis e de identidade”

Fonte: autoria própria.

4) Conforme a Figura 20, selecione a categoria “Certificados confiáveis” e clique no botão “Importar”.

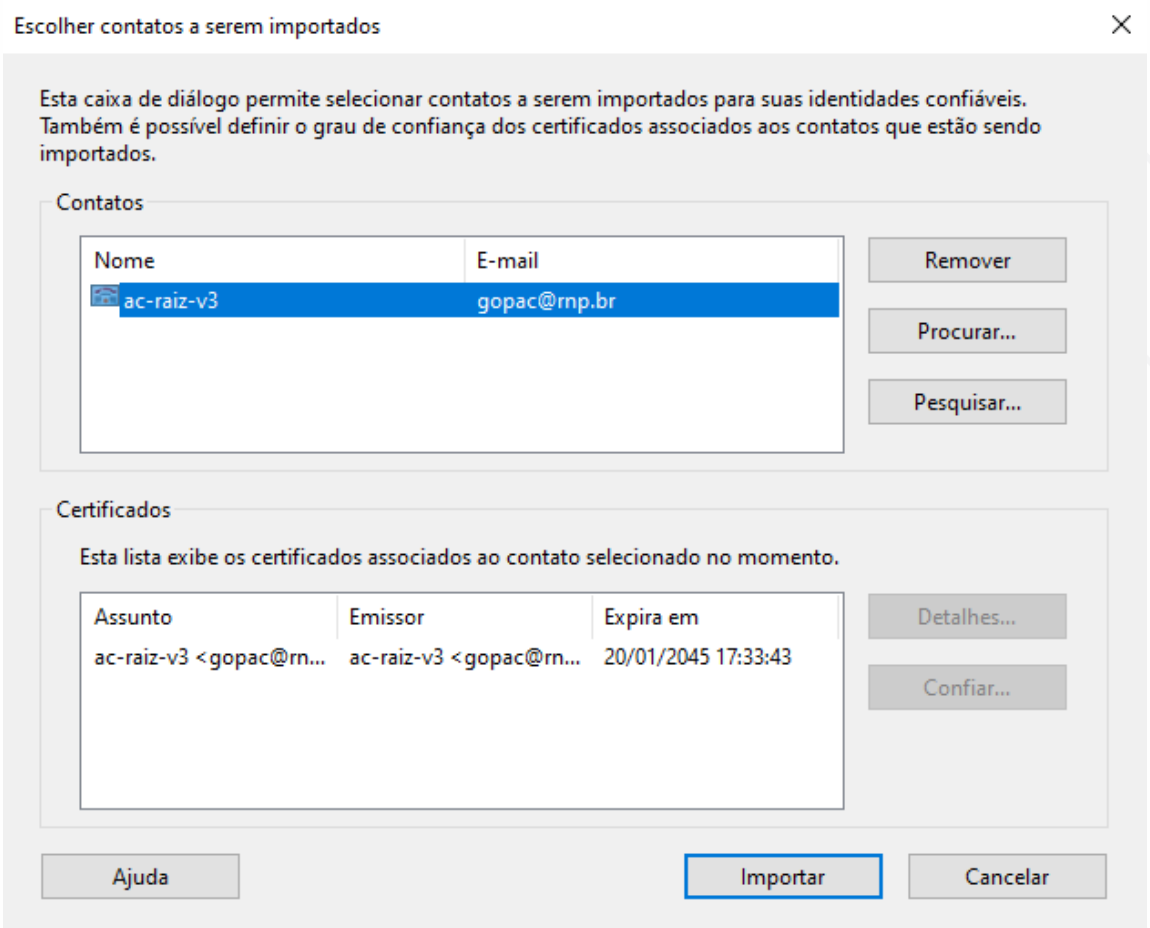
Figura 21 – Interface para “Configurações de ID digital e certificado confiável”



Fonte: autoria própria.

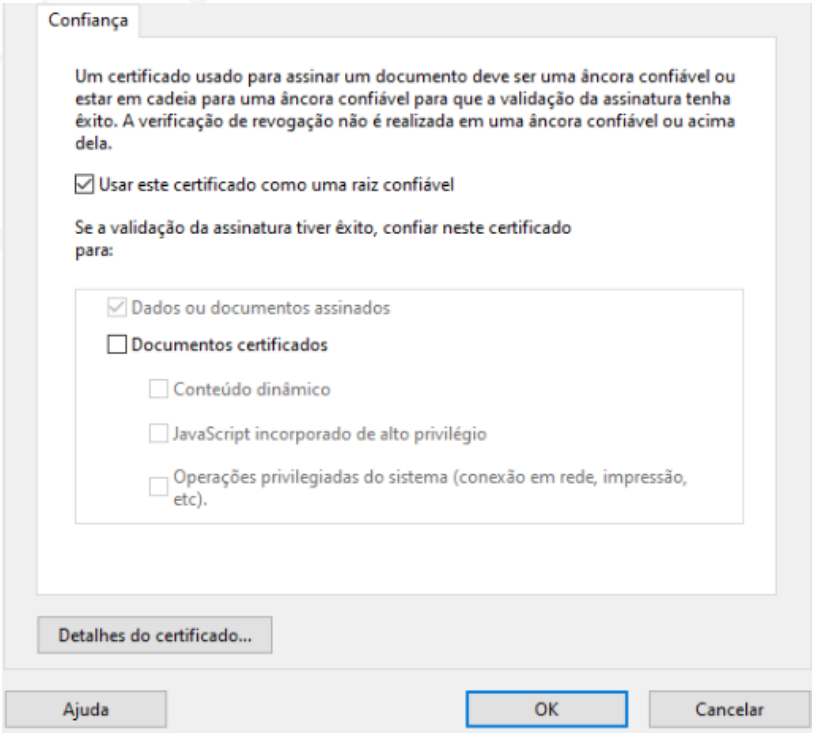
5) Conforme a Figura 21, clique em “Procurar ...” e selecione o arquivo “ac-raiz-v3.cer” (referente ao certificado digital do ente AC RAIZ) que você copiou para o seu computador, conforme as instruções na Seção 3.3.3. Em seguida, clique no Contato “ac-raiz-v3” para ver abaixo o certificado “ac-raiz-v3”. Para finalizar esse passo, selecione esse certificado e clique em “Confiar ...”:
Uma tela similar à Figura 23 será exibida. Então, marque “Usar este certificado como uma raiz confiável” e clique em “OK”. Pronto! O certificado da AC RAIZ foi instalado como uma identidade confiável (acreditada).

Figura 22 – Interface para “importar identidades confiáveis”



Fonte: autoria própria.

Figura 23 – Interface para “confirmar identidades confiáveis”



Fonte: autoria própria.

6) Repita o Passo 5, com respeito ao arquivo “ac-pessoa.cer”, para que o certificado da AC PESSOA seja instalado como uma identidade confiável (acreditada).
7) Após os Passos 5 e 6, clique em “Importar” para finalizar a instalação dos Certificados dos entes da cadeia de confiança do seu Certificado **ICPEdu**.

3.3.5 Assinar um Documento PDF

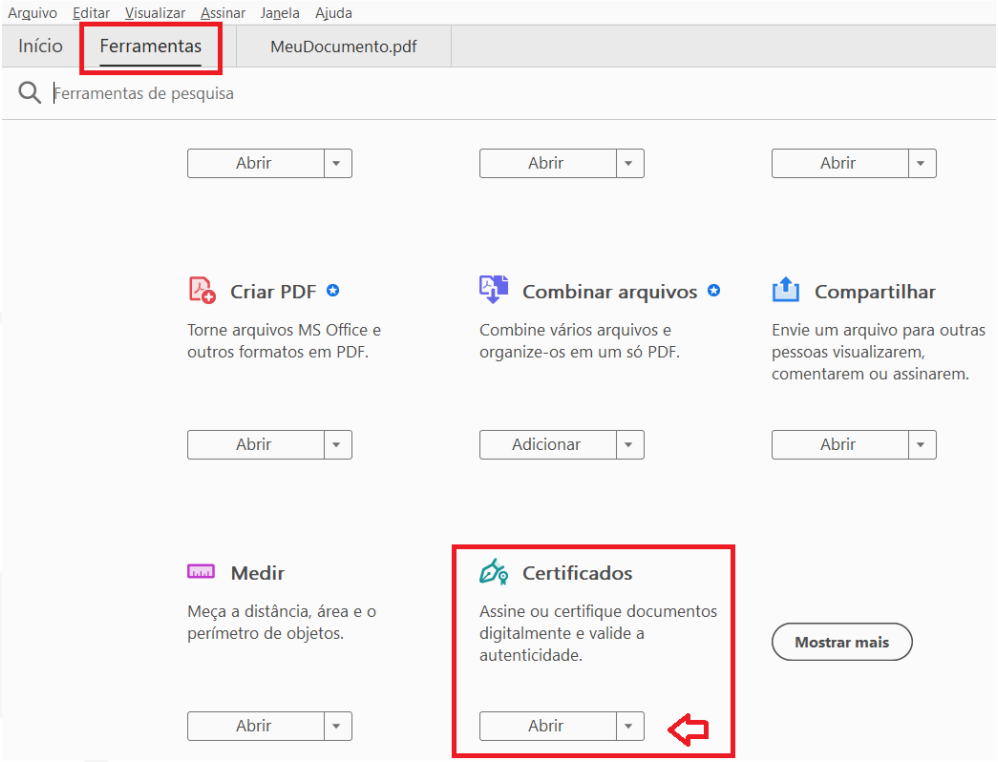
Vamos utilizar o Certificado **ICPEdu** para aplicar uma Assinatura Digital em um Documento.

A seguir, é ilustrado o processo de assinatura usando o *Adobe Acrobat Reader*®. Contudo, em um estabelecimento de saúde, provavelmente, o processo será outro, empregando o Sistema de Informação em Saúde (SIS) usado pelo estabelecimento, com um conjunto “menor” de passos e “maior” simplicidade.

Selecione um documento no formato PDF e o renomeie para “MeuDocumento.pdf”. Abra esse arquivo usando o *software Adobe Acrobat Reader*® e siga os passos:

1) Conforme a Figura 23, selecione o menu “Ferramentas” e clique no botão “Abrir” da Ferramenta “Certificados”.

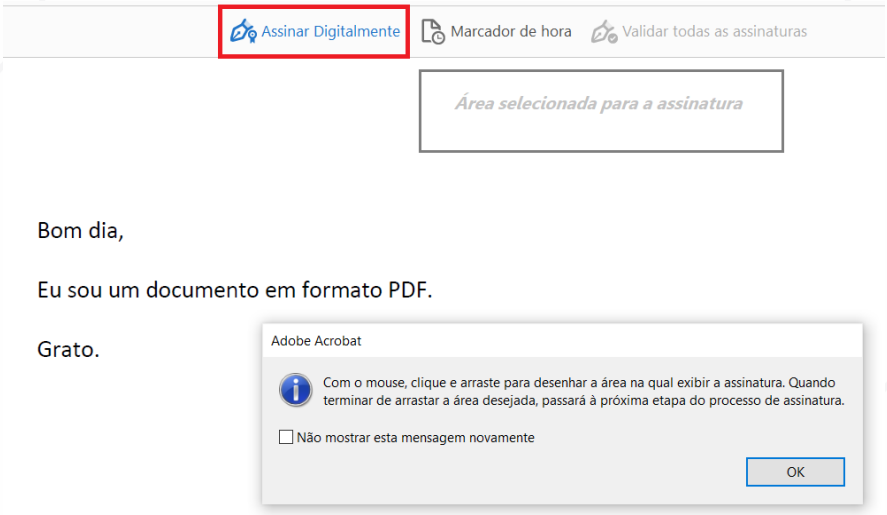
Figura 24 – Interface para “ferramenta de certificados”



Fonte: autoria própria.

2) Clique em “Assinar Digitalmente” e “com o *mouse*, clique e arraste para desenhar a área na qual exibir a assinatura” (Figura 24).

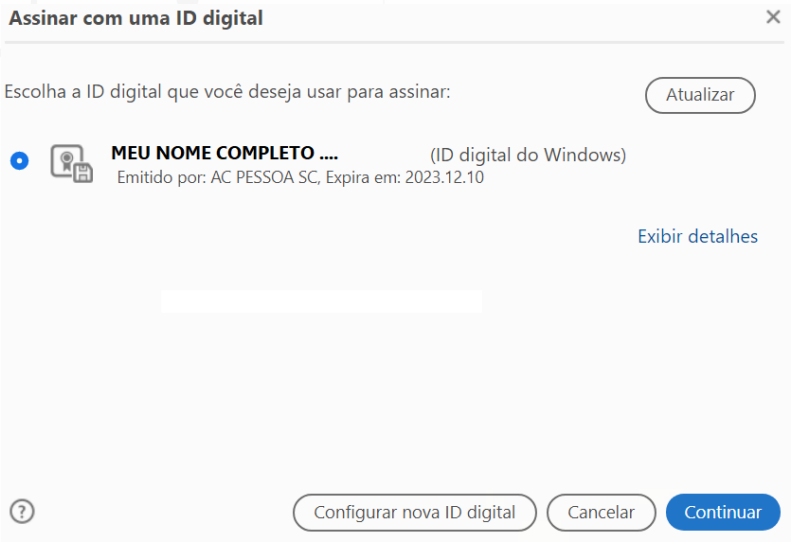
Figura 25 – Interface para “seleção da área para exibir a assinatura”



Fonte: autoria própria.

3) Escolha a identificação digital, dentre as várias identificações instaladas no seu computador. Você poderá selecionar a identificação do seu Certificado **ICPEdu** (Figura 25). Então, clique em “Continuar”.

Figura 26 – Interface para “seleção de identificação digital”



Fonte: autoria própria.

4) Revise se o conteúdo do documento pode interferir na assinatura e clique em “Assinar”:

5) Selecione um nome para o arquivo do documento assinado. Utilize “MeuDocumentoAssinado.pdf”, que é a versão assinada digitalmente para o documento no arquivo “MeuDocumento.pdf”.

Neste momento, você poderá ver a marca da assinatura digital no local que você selecionou no Passo 2. Também, o *software Adobe Acrobat Reader®* exibe a mensagem “Assinado e todas as assinaturas são válidas”.

3.3.6 Validar a Assinatura Digital

O software *Adobe Acrobat Reader®*, ao exibir a mensagem “Assinado e todas as assinaturas são válidas”, atestou que o documento possui assinatura digital de um certificado digital com cadeia de confiança acreditada (confiável).

Adicionalmente, utilizaremos o serviço de validação disponível neste *link* https://pessoal.icpedu.rnp.br/public/verificar-assinatura, que é dedicado à validação de assiaturas digitais feitas a partir de Certificados **ICPEdu**:

1) Clique em “Enviar arquivo” para selecionar o arquivo “MeuDocumentoAssinado.pdf” (Figura 26), que é a versão assinada documento do arquivo “MeuDocumento.pdf”.

Figura 27 – Interface para “validação de assinatura digital”

Fonte: autoria própria.

2) Clicar em “Verificar Assinatura” para iniciar o processo de validação da assinatura digital. Ao final, é exibido um resumo que inclui: se a assinatura é válida, se a cadeia do certificado é válida e se o documento foi alterado após a assinatura, tal como exibido na Figura 27.

Concluímos o processo de emissão e instalação do certificado e a assinatura de documento com o certificado emitido.

Figura 28 – Interface para “resultado de validação de assinatura digital”

Fonte: autoria própria.

3.4 *Quiz*

Para testar os conhecimentos adquiridos até aqui, responda ao quiz no Ambiente Virtual.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 4

Benefícios e Aplicações de Certificado Digital na Saúde Digital

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 4: Benefícios e Aplicações de CertificadoDigital na Saúde Digital

A Saúde Digital promove o uso de registros eletrônicos de saúde. E tais registros devem ser assinados digitalmente para atribuir a autoria deles a um determinado profissional de saúde. Nesse sentido, algumas das iniciativas para regulamentar o uso da certificação digital na área da saúde são apresentadas a seguir.

4.1 Saúde Suplementar

A Agência Nacional de Saúde Suplementar (ANS) e o Ministério da Saúde estabeleceram normas para a Troca de Informação de Saúde Suplementar (TISS).[20] Essas normas estabelecem o uso da certificação digital na área da saúde suplementar, e trazem padrões para garantir a interoperabilidade das informações trocadas entre clínicas, hospitais e outros prestadores de serviços de saúde e os operadores dos planos. Ou seja, os agentes da saúde suplementar passam a 'falar a mesma língua' (pela adoção de padrões) e a usar a assinatura digital para os dados de saúde. A adoção de padrões traz benefícios tais como: a melhoria na obtenção de informações para estudos epidemiológicos, o aperfeiçoamento na comunicação entre os atores do setor da saúde, a redução de custos administrativos e, sobretudo, o acréscimo de qualidade da assistência ao usuário.

4.2 Sistemas de Informação em Saúde Eletrônico

Um sistema de informação em saúde é utilizado pelos usuários, por exemplo, profissionais de saúde, para auxiliar na assistência aos pacientes. É necessário que o acesso seja seguro e confiável. Convém ressaltar que o sistema de Prontuário Eletrônico do Paciente (PEP) é usado vinculado a um estabelecimento de saúde ou uma rede de estabelecimentos do mesmo mantenedor. Entretanto, um Sistema de Registro Eletrônico em Saúde (S-RES) é transversal aos distintos prestadores de serviços, sendo longitudinal pela vida do paciente. Em geral, provido por governos ou operadoras de planos de saúde. Em tese, o S-RES recebe os dados coletados por meio dos PEP.

A Sociedade Brasileira de Informática em Saúde (SBIS) e o CFM têm trabalhado em conjunto na elaboração de normas para padronizar o uso da certificação digital na área da saúde. A Resolução CFM Nº 1.821/2007[12] estabeleceu dois Níveis de Garantia de Segurança (NGS)[6]. O segundo nível (NGS-2) é o nível requerido para a eliminação de registros em papel, cujas principais exigências são:

- o uso de Certificado Digital padrão ICP-Brasil;
- a assinatura digital de todos os documentos de saúde; e
- o uso de carimbo do tempo nos registros de saúde.

6 A Resolução CFM 1821/2007 foi modificada pela Resolução CFM 2218/2018.

Abaixo, segue excerto do documento "Requisitos para certificação de Sistemas de Registro Eletrônico em Saúde", especificamente o requisito NGS2.01.01, relevante para a presente contexto, no qual se lê:

> O S-RES deve permitir que certificados digitais ICP-Brasil possam ser utilizados por profissionais de saúde para o processo de assinatura digital de documentos do prontuário do paciente, atendendo às normas de uso definidas pela ICP-Brasil na utilização desses certificados.[21]

4.3 Laudos de Análises Clínicas

Em 2015, a Agência Nacional de Vigilância Sanitária (Anvisa) publicou uma alteração no Regulamento Técnico para Funcionamento de Laboratórios,[22] que torna obrigatório o uso de certificação digital na área da saúde para laudos eletrônicos emitidos por laboratórios de análises clínicas. Noutras palavras, para garantir a autenticidade e a integridade do laudo eletrônico emitido, o laboratório clínico e o posto de coleta laboratorial devem empregar a assinatura digital do profissional que liberou o laudo, segundo Certificado Digital padrão ICP-Brasil.

Por meio dessa Resolução, a Anvisa definiu as diretrizes que garantem a segurança de laudos digitais que dispensam o uso de papel para o laudo de análise clínicas.

4.4 Rede Nacional de Dados em Saúde

Na perspectiva de um estabelecimento de saúde, a Rede Nacional de Dados em Saúde (RNDS) é uma iniciativa recente, que oferece serviços para a interoperabilidade em saúde no território nacional. No Brasil, é por meio da RNDS que um estabelecimento em saúde disponibiliza informação que será consumida por outro.

Quando um estabelecimento de saúde se integra à RNDS, cria-se a possibilidade dele contribuir com informações em saúde pertinentes aos usuários que assiste, bem como consumir informações geradas por outros estabelecimentos.

Os serviços oferecidos pela RNDS para interoperabilidade requerem o uso de certificados digitais dos estabelecimentos de saúde, tal que os mesmos possam agregar e usufruir da interoperabilidade entre sistemas. A cooperação entre sistemas e estabelecimentos de saúde será estendida ao longo do tempo, para viabilizar as necessidades de troca de informação em saúde no Brasil.

Convém mencionar que a RNDS não será um repositório que replica exaustivamente todo o conteúdo armazenado em sistemas de PEP nos estabelecimentos de saúde. Na RNDS são armazenados documentos clínicos, padronizados, de forma a serem guardados eventos clínicos que ocorreram na vida do cidadão, tais como vacinações, internações hospitalares, etc.

Por fim, o uso de certificados digitais na saúde promove a migração de prontuários e processos físicos para o mundo digital e, consequentemente, conduz a benefícios e desafios. O horizonte aponta para a interoperabilidade completa entre os sistemas de informação em saúde no território nacional, nos vários níveis de atenção à saúde e nas várias esferas de competência, desde entre municipais e regionais até entes federais, o que inclui todos os ramos alcançados pelo SUS.

Em adição, a certificação digital na área da saúde fomenta a segurança da atenção à saúde, pois assegura a autenticidade de um registro de saúde assinado por um dado profissional de saúde. Essa possibilidade também promove a eficiência operacional de suas unidades, pois a rápida transferência de registros eletrônicos torna-se, adicionalmente, segura.

A adesão de estabelecimentos de saúde à RNDS é alcançada por meio do uso de certificados digitais, conforme descrito no Guia da RNDS.[23]

Adicionalmente, a SBIS certifica sistemas de informação em saúde. As exigências a serem satisfeitas, em geral, estão agrupadas pelo tipo de sistema a ser avaliado: consultório individual, ambulatório, teleconsulta e receita digital são alguns deles. Quando não há categoria específica, o sistema deve atender os "Requisitos para Segurança da Informação". Os vários documentos estão disponíveis aqui[24] e uma consulta simples a eles revela que o emprego de Certificado Digital e Assinatura Digital estão presentes em todos eles.

4.5 Storyboard

Percorra a animação no *storyboard* e entenda os benefícios e a importância da certificação digital aplicada ao PEP para assinatura digital dos registros de saúde.

4.6 Quiz

Para testar os conhecimentos adquiridos até aqui, responda ao quiz no Ambiente Virtual.

Registros de saúde no Prontuário Eletrônico do Paciente (PEP) devem ser assinados com Certificados Digitais padrão ICP-Brasil (Tipo A), além de receber Carimbo de Tempo a partir de Certificados Digitais padrão ICP-Brasil (Tipo T).

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 5

Organização da ICP-Brasil

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 5: Organização da ICP-Brasil

A ICP-Brasil é o sistema nacional brasileiro de certificação digital. Esse é o órgão público brasileiro de infraestrutura de chaves públicas (em inglês, *public key infrastructure*), criado pela Medida Provisória Nº 2.200-2 de 2001:

> Fica instituída a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a **autenticidade**, a **integridade** e a **validade jurídica** de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.[8]

Dessa forma, a certificação digital no âmbito da ICP-Brasil busca promover legalidade e segurança às transações e aos documentos que trafegam no mundo digital. A ICP-Brasil representa uma cadeia de confiança para processos, pessoas e tecnologias empregadas, para viabilizar a validade jurídica para a mudança do mundo físico para o virtual. A Medida Provisória Nº 2.200-2[8] também estabelece os entes da ICP-Brasil:

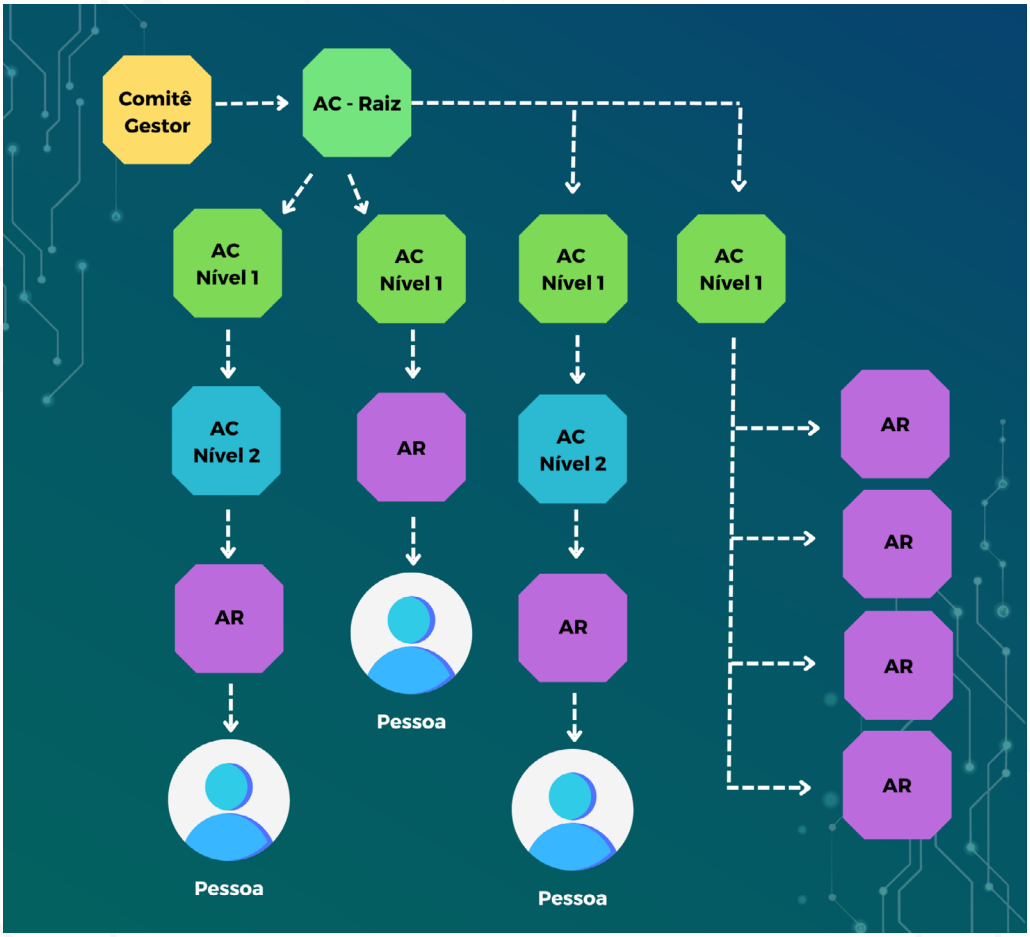
> A ICP-Brasil será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz (AC-Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR).[8]

A estrutura da ICP-Brasil é apresentada na Figura 14:

- AC-Raiz denota Autoridade Certificadora Raiz;
- AC Nível 1 denota Autoridade Certificadora de Nível 1;
- AC Nível 2 denota Autoridade Certificadora de Nível 2; e
- AR denota Autoridade de Registro.

Observe que há uma hierarquia entre os entes (na Figura 28, a hierarquia é de cima para baixo), na forma de uma cadeia de confiança, para garantir que um Certificado Digital seja emitido de forma correta, segundo um criterioso processo de identificação, tornando-o um documento eletrônico confiável.

Figura 29 – Estrutura simplificada da ICP-Brasil



Fonte: adaptada de Brasil, Instituto Nacional de Tecnologia da Informação [s.d.].[9]

O **Comitê Gestor** é a entidade máxima da arquitetura da ICP-Brasil, que tem por finalidade atuar na formulação e controle da execução das políticas públicas relacionadas à ICP-Brasil, o que inclui normatização e procedimentos administrativos, técnicos, jurídicos e de segurança. Segundo a Medida Provisória Nº 2.200-2,[8] compete ao Comitê Gestor:

> I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
>
> II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;
>
> III - estabelecer a política de certificação e as regras operacionais da AC Raiz;
>
> IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
>
> V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação; dentre outras.[8]

O Instituto Nacional de Tecnologia da Informação (ITI) é uma autarquia federal com sede em Brasília-DF, criado com o fim específico de ser a **AC-Raiz** da ICP Brasil, pela Medida Provisória N° 2.200-2.[8] A **AC-Raiz** é a executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, para:

> emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.[8]

A **AC-Raiz** tem o certificado de nível mais alto na ICP-Brasil, que possui a chave pública correspondente à chave privada usada para assinar o seu próprio certificado e os certificados das AC de nível subsequente.

As **AC** são entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, para:

> emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.[8]

Na Figura 13 são observadas AC de Níveis 1 e 2, pois, há requisitos mínimos no desempenho de atribuições de cada nível. A AC de único nível desempenha as responsabilidades de Níveis 1 e 2.

As **AR** são entidades vinculadas em termos operacionais à determinada AC, para "identificar e cadastrar usuários, encaminhar solicitações de certificados às ACs e manter registros de suas operações".[8]

A identificação do usuário é feita de forma presencial, mediante comparecimento pessoal do usuário, ou por outra forma que garanta nível de segurança equivalente, observadas as normas técnicas da ICP-Brasil.

Por fim, observa-se na estrutura ICP-Brasil que há ACs dos setores público e privado.

Os entes correntes da estrutura ICP-Brasil podem ser vistos em tempo real. Observe as empresas participantes, bem como a hierarquia entre elas no escopo da certificação digital, conforme descrito aqui.[9]

A seguir, no Vídeo 1, veja a entrevista com Ruy Cesar Ramos Filho para entender melhor sobre o papel do Instituto Nacional de Tecnologia da Informação (ITI) e sobre os marcos e desafios da certificação digital do Brasil.

Vídeo 1 - Entrevista com Ruy Cesar Ramos Filho, membro do Instituto Nacional de Tecnologia da Informação (ITI), sobre a Certificação Digital do Brasil

Fonte: autoria própria.

5.1 *Quiz*

Para testar os conhecimentos adquiridos até aqui, responda ao quiz no Ambiente Virtual.

- O modelo brasileiro é o de certificação com raiz única.
- A AC-Raiz é a primeira autoridade da cadeia de certificação.
- Na ICP-Brasil, a AC-Raiz é o ITI, que executa as políticas de certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 6

Processo de Aquisição e Uso

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 6: Processo de Aquisição e Uso

Sobre a adoção e o uso de Certificados Digitais, em geral, certificados são pagos e adquiridos a partir de uma AC, que é uma entidade presente na hierarquia da ICP-Brasil. A escolha de um Certificado Digital deve levar em conta o propósito (assinatura ou sigilo) e o nível de segurança previsto para o tipo do certificado.

Usualmente, uma AC comercializa um subconjunto dos tipos de certificado. Os mais comuns são A1 e A3, cada um deles pode ser para pessoa física ou pessoa jurídica (usualmente, rotulados como e-CPF e e-CNPJ, respectivamente).

São ainda observados períodos de validade diversos para o mesmo tipo de certificado; por exemplo, são comercializados certificados do tipo A3 com períodos de validade de 12 meses e 36 meses, cujas mídias armazenadoras são nuvem e cartão inteligente, respectivamente.

Há ainda os certificados dos tipos A1 e A3 (e-CPF) que evidenciam a identificação baseada em conselhos de classe profissional, tais como conselhos dos profissionais médicos, contadores e advogados.

Os passos a seguir representam um processo genérico (processo clássico) para a aquisição de um Certificado Digital:

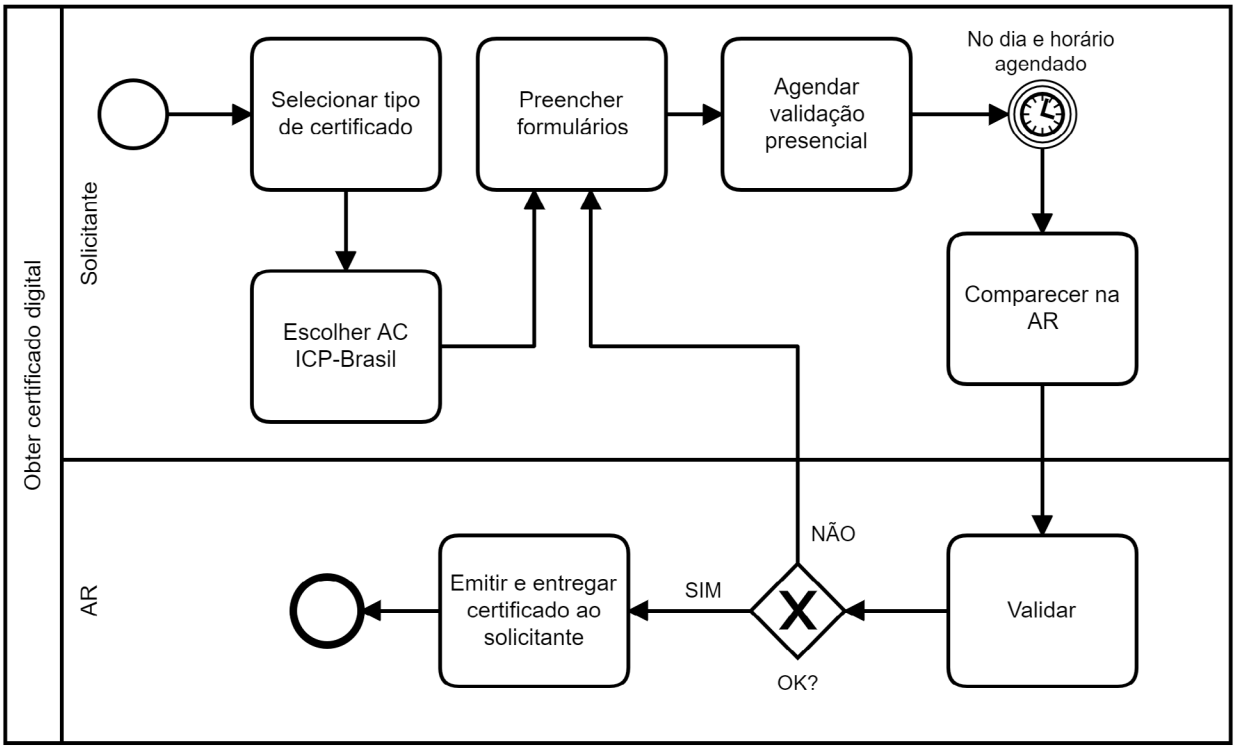
1. A aquisição de um Certificado Digital inicia com a escolha de uma das AC da ICP-Brasil.
2. No site da AC escolhida, o solicitante seleciona o tipo de Certificado Digital de pessoa física ou jurídica, conforme a sua necessidade. Os tipos mais comercializados são:
   - **A1**: validade de um ano, armazenado no computador;
   - **A3**: validade de até cinco anos, armazenado em cartão ou token criptográfico;
   - Os tipos T e S também são opções comuns.
3. A AC então informará ao solicitante sobre os custos do certificado, as formas de pagamento, os equipamentos necessários e a documentação obrigatória para emissão.
4. O solicitante preenche os formulários de solicitação e efetua o pagamento.
5. O solicitante faz agendamento (dia e horário) para a validação presencial, diretamente em uma das Autoridades de Registro (ARs) subordinadas à AC escolhida, ocasião em que a AR instruirá o solicitante sobre todo o processo.
6. O solicitante comparece à AR para levar os documentos obrigatórios, conferir os formulários preenchidos e passar pelo processo de identificação - por exemplo, por meio do cadastramento biométrico, com a coleta da biografia facial (foto) e das digitais.
   - A legislação prevê casos em validação remota. Por exemplo, para residentes no exterior, a validação pode ser por videoconferência. Nesse caso, se o solicitante possuir biometria cadastrada na ICP-Brasil ele poderá emitir um certificado com validade de até cinco anos, caso contrário, a emissão do certificado é restrita a um ano.

- Em adição, pela Instrução Normativa ITI N° 5, de 22 de fevereiro de 2021 [25], é possível o emprego de videoconferência para a identificação biométrica e a validação do requerente de Certificado Digital.

7. O Certificado Digital é emitido e entregue ao solicitante, conforme o tipo de certificado e mídia escolhidos.

Essas atividades estão ilustradas no fluxo apresentado na Figura 29, por meio da notação BPMN (*Business Process Model and Notation*), que se destina à modelagem de processos de negócios.

Figura 30 - Processo genérico para a aquisição de Certificado Digital



Fonte: autoria própria.

6.1 Orientações sobre Manuseio

O uso indevido do Certificado Digital pode resultar em danos ao seu titular. Alguns cuidados são apresentados a seguir:

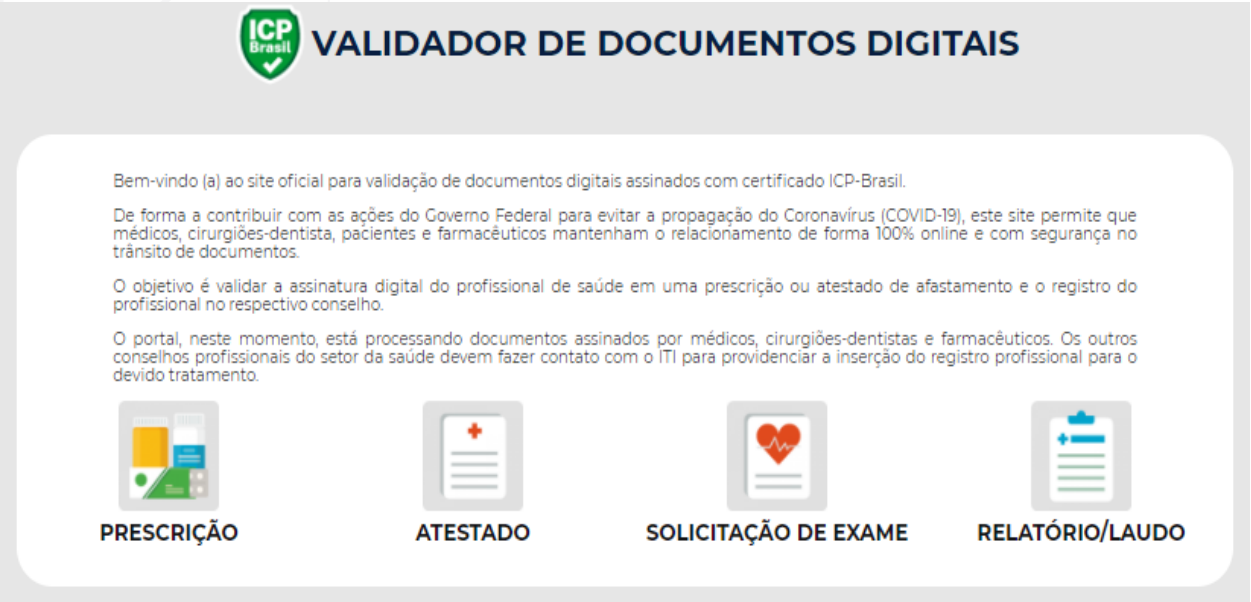
- A senha de acesso à chave privada deve ser restrita ao titular.
- O acesso à própria chave privada deve ser restrita ao titular.
- A senha de acesso à chave privada deve ser longa, possuir números e letras intercaladas, evitar dados pessoais (tais como data de aniversário e nome de parentes) e ser memorizada em vez de anotada.
- Se a chave privada for armazenada no disco rígido de algum computador (por exemplo, Certificado Digital Tipo A1), esse computador deve possuir protetor de tela com senha, não deve ser compartilhado e deve ser mantido em lugar seguro. Caso contrário, é preferível o armazenamento da chave privada em cartão inteligente ou *token* (por exemplo, Certificado Digital Tipo A3).

6.2 Validação de Documentos Clínicos

Motivado pelo contexto da propagação do novo coronavírus, foi disponibilizado pelo Governo Federal a médicos, cirurgiões-dentistas, pacientes e farmacêuticos, um serviço (imagem do *site* na Figura 30) para a validação de assinaturas digitais do profissional de saúde, disponível aqui.[26]

Basicamente, é necessário o envio (*upload*) do arquivo em formato PDF (prescrição, atestado, solicitação de exame, relatório, laudo). Então, a validade da assinatura digital e o número do registro profissional serão consultados pelo conselho profissional (CFF, CFM, CFO, etc.), conforme indicados no formulário. O resultado da pesquisa informará se o documento é assinado e se não sofreu qualquer tipo de alteração após a sua assinatura e, ainda, confirmará os dados referentes ao prescritor que assinou o documento digital.

Figura 31 – Validador de documentos digitais



Fonte: Brasil, Instituto Nacional de Tecnologia da Informação.[26]

O conteúdo desse Portal informa claramente:

1. Se refere ao site oficial para validação de documentos digitais assinados com certificado ICP-Brasil. A validação é restrita a certificados ICP-Brasil, ou seja, somente certificados criados por uma AR, que faz parte da cadeia de confiança, cuja raiz é o ITI, poderão ser validados; todos os demais não serão validados.
2. Alguns exemplos: validar a assinatura digital do profissional de saúde em uma prescrição ou atestado de afastamento e validar o registro do profissional no respectivo Conselho. Efetivamente, a validação verifica que, de fato, a assinatura digital pertence a um profissional de saúde com registro no respectivo Conselho.

Conforme mencionado, o Portal, neste momento, está processando documentos assinados por médicos, cirurgiões-dentistas e farmacêuticos. Os outros Conselhos Profissionais do setor da saúde devem fazer contato com o ITI para providenciar a inserção do registro profissional para o devido tratamento.

6.3 Visão das Possibilidades de Uso

O seu cenário de interesse já emprega a certificação digital para a agilidade e segurança de serviços? Na Tabela 3, constam exemplos de aplicação de certificação digital em vários cenários, considerando as perspectivas pessoal, institucional e empresarial.

Tabela 3 – Exemplos de aplicação de certificação digital

Contexto	Alguns exemplos
Administração pública	Receber informações contábeis, financeiras e fiscais vindas de municípios, estados, o Distrito Federal e a União.
Classes profissionais	Advogados: consultar processos, enviar petição, ajuizar nova demanda, receber intimações, controlar prazos.
	Contadores: emitir certidão negativa de débitos, dar baixa de inscrição estadual, consultar pendências.
	Médicos: acessar sistemas de Prontuário Eletrônico do Paciente (PEP), prescrever medicamentos.
Economia	Entregar, retificar, gerar Documento de Arrecadação de Receitas Federais (DARF) e demais atos de declarações do Imposto sobre a Renda da Pessoa Física.
	Comunicar operações financeiras ao Ministério da Economia.
Educação	Assinar e registrar digitalmente diplomas de graduação, com integridade e interoperabilidade dos dados.
Informação e comunicação	Efetuar publicações de atos no Diário Oficial da União, tramitar atos pelo Sistema de Envio Eletrônico de Matérias.
Justiça	Acompanhar processos judiciais, na Justiça Federal, dos Estados, Militar dos Estados e na Justiça do Trabalho.
	Interligar a justiça ao Banco Central e às instituições bancárias, para agilizar o envio de informações e ordens judiciais.
Notariado	Lavrar escrituras públicas.
Relações trabalhistas	Comunicar ao Governo, as informações relativas aos trabalhadores, como vínculos, contribuições previdenciárias.
Saúde	Usar Cédula de Identidade de Médico – CRM Digital com *chip* criptográfico para certificação digital, para assinar registros de saúde.
Trânsito	Aquisição e uso de Carteira Nacional de Habilitação (CNH) em formato eletrônico.

Fonte: autoria própria.

Acesse o *site* https://aquitemcd.iti.gov.br/[27] para conhecer serviços, aplicações, sistemas e processos que aceitam o uso do seu Certificado Digital no padrão da ICP- Brasil. A página está em constante atualização e você pode contribuir!

Por fim, o cidadão pode acessar os dados dos seus certificados digitais ou checar se há Certificado Digital em seu nome, por meio de um serviço desenvolvido pelo ITI para consultar certificados digitais emitidos pela ICP-Brasil, conforme o Portal https://meucertificado.iti.gov.br/login.[25]

Ao longo dos anos, há um aumento da adoção de certificados digitais em vários cenários. A expansão dos serviços digitais na sociedade tem sido alcançada e representa uma tendência à difusão do uso e dos benefícios da certificação digital no Brasil.

EDUCAÇÃO E CAPACITAÇÃO
DE RECURSOS HUMANOS
EM SAÚDE DIGITAL

Certificado digital

Unidade 7

Encerramento do Microcurso

Fábio Nogueira de Lucena
Plínio de Sá Leitão Júnior

Unidade 7: Encerramento do Microcurso

Certificado digital, ou seja, a identidade de uma pessoa física ou jurídica, no mundo virtual, é uma ferramenta indispensável à Saúde Digital, na qual muitas atividades são realizadas por intermédio de computadores, como o compartilhamento de informações.

Profissionais de saúde, ao interagirem com SIS, serão identificados de forma segura por meio do certificado correspondente, por exemplo. De fato, de forma bem mais segura que o comum emprego de usuário e senha. Esse uso também significa segurança para o consumidor, que saberá exatamente quem foi o autor da informação consumida e que a mesma não foi adulterada, quando é assinada digitalmente. De forma similar, em uma prescrição eletrônica, o farmacêutico não terá dúvidas sobre o conteúdo da prescrição nem sobre o autor após a validação da assinatura digital em questão.

Esses benefícios, para serem usufruídos, demandam ajustes em SIS existentes, a aquisição de certificados digitais por usuários e o uso deles.

No Brasil, assim como há órgãos específicos para a emissão da Carteira de Identidade, há o ITI, responsável por gerir a ICP-Brasil, que regula a emissão de certificados digitais válidos legalmente no País.

Dessa forma, esse *ebook* oferece acesso a informações relevantes sobre Certificado Digital, assinatura digital, onde obter um certificado e orientações sobre o seu uso, o que é necessário para a implementação da Estratégia de Saúde Digital do Brasil.

Referências

1. PRIBERAM DICIONÁRIO. **Definição de documento.** Disponível em: https://dicionario.priberam.org/documento. Acesso em: 22 jan. 2023.

2. MINISTÉRIO DA CULTURA. Fundação Biblioteca Nacional. Departamento Nacional do Livro. **A carta de Pero Vaz de Caminha.** p. 1. Disponível em: http://objdigital.bn.br/Acervo_Digital/Livros_eletronicos/carta.pdf. Acesso em: 22 jan. 2023.

3. WIKIPEDIA. **Bliss (imagem).** Disponível em: https://pt.wikipedia.org/wiki/Bliss_(imagem). Acesso em: 22 jan. 2023.

4. TELEGEOGRAPH. **Submarine cable map**. Disponível em: https://www.submarinecablemap.com/. Acesso em: 22 jan. 2023.

5. BRASIL. **Lei Nº 11.419, 19 de dezembro de 2006.** Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 22 jan. 2023.

6. BRASIL. **Lei Nº 14.063, de 23 de setembro de 2020.** Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931. Acesso em: 22 jan. 2023.

7. MACHADO, R. C. **Certificação Digital ICP-Brasil:** os caminhos do documento eletrônico no Brasil. Módulo Usuário. Niterói: Editora Impetus. 243 pp.

8. BRASIL. **Medida Provisória Nº 2.200-2/2001, de 24 de agosto de 2001.** Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm. Acesso em: 22 jan. 2023.

9. BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Estrutura.** Disponível em: https://estrutura.iti.gov.br/. Acesso em: 22 jan. 2023.

10. BRASIL. **Emenda Constitucional Nº 42, de 19 de dezembro de 2003.** Dispõe sobre recursos prioritários das administrações tributárias da União, dos Estados, do Distrito Federal e dos Municípios, para o compartilhamento de cadastros e de informações fiscais, na forma da lei ou convênio. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc42.htm. Acesso em: 22 jan. 2023.

11. ENCONTRO NACIONAL DE ADMINISTRADORES TRIBUTÁRIOS (ENAT). **Protocolo de Cooperação 03/2005 – II ENAT, de 27 de agosto de 2005.** Protocolo para a implantação da Nota Fiscal Eletrônica, integrante do Sistema Público de Escrituração Digital. Dispõe sobre medidas e esforços para o desenvolvimento e padronização nacional da NF-e, com o intuito da substituição das notas fiscais em papel por documento eletrônico. Disponível em: https://www.fazenda.sp.gov.br/nfe/legislacao/legislacao_protocolo_ENAT_03_2005.pdf. Acesso em: 22 jan. 2023.

12. CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CFM Nº 1.821/2007, 23 de novembro de 2007.** Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821. Acesso em: 22 jan. 2023.

13. BRASIL. **Lei Nº 12.682, de 9 de julho de 2012.** Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm. Acesso em: 22 jan. 2023.

14. BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Certificado digital: saiba mais.** Disponível em: https://aquitemcd.iti.gov.br/certificado-digital/. Acesso em: 22 jan. 2023.

15. BRASIL. **Resolução CG ICP-BRASIL Nº 179, de 20 de outubro de 2020.** Aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Políticas de Certificados na ICP-Brasil - DOC-ICP-04. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cg-icp-brasil-no-179-de-20-de-outubro-de-2020-284449391. Acesso em: 22 jan. 2023.

16. WIKIPEDIA. **Assinatura.** Disponível em: https://pt.wikipedia.org/wiki/Assinatura. Acesso em: 22 jan. 2023.

17. ONLINE TOOLS. **Função de resumo SHA256.** Disponível em: https://emn178.github.io/online-tools/sha256.html. Acesso em: 22 jan. 2023.

18. DAN'S TOOLS. **MD5 Hash Generator.** Disponível em: https://www.md5hashgenerator.com/. Acesso em: 22 jan. 2023.

19. JAVAINUSE. **Online RSA Encryption, Decryption And Key Generator Tool.** Disponível em: https://www.javainuse.com/rsagenerator. Acesso em: 22 jan. 2023.

20. AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (ANS). **Resolução Normativa ANS Nº 153, de 28 de maio de 2007.** Estabelece padrão obrigatório para a troca de informações entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde sobre os eventos de saúde. Disponível em: https://www.legisweb.com.br/legislacao/?id=106748. Acesso em: 22 jan. 2023.

21. MIRANDA, C. F.; MARQUES, E. P.; KIATAKE, L. G. G.; VIRGINIO JÚNIOR, L. A.; SILVA, M. L.; SANZOVO, O. A. C. *et al*.. **Requisitos para certificação de Sistemas de Registro Eletrônico em Saúde:** segurança da informação. Versão 5.1. Sociedade Brasileira de Informática em Saúde (SBIS) [internet]. 2021. 42 pp. Disponível em: http://sbis.org.br/certificacao/Requisitos_Certificacao_SBIS_Seguranca_V5.1.pdf. Acesso em: 22 jan. 2023.

22. AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). **Resolução da Diretoria Colegiada RDC Nº 30, de 24 de julho de 2015.** Altera a Resolução – RDC n.º 302, de 13 de outubro de 2005, que dispõe sobre o Regulamento Técnico para funcionamento de Laboratórios Clínicos. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/anvisa/2015/rdc0030_24_07_2015.pdf. Acesso em: 22 jan. 2023.

23. MINISTÉRIO DA SAÚDE. **Guia da Rede Nacional de Dados em Saúde (RNDS):** público-alvo. Disponível em: https://rnds-guia.saude.gov.br/docs/publico-alvo/gestor/certificado. Acesso em: 22 jan. 2023.

24. SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE (SBIS). **Manuais e listas de requisitos.** Disponível em: http://sbis.org.br/documentos-e-manuais/. Acesso em: 22 jan. 2023.

25. BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Instrução Normativa ITI Nº 5/2021, 22 de fevereiro de 2021.** Aprova a versão 4.0 do DOC-ICP-05.02, aprova a versão 2.0 do DOC-ICP-05.05 e altera o DOC-ICP-05.03 para prever a emissão de certificados digitais por videoconferência. Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-iti-n-5-de-22-de-fevereiro-de-2021-304617035. Acesso em: 22 jan. 2023.

26. BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Validador de assinaturas eletrônicas em documentos digitais de saúde.** Disponível em: https://assinatura-digital.iti.gov.br/. Acesso em: 22 jan. 2023.

27. BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Aplicações com certificado digital ICP-Brasil.** Disponível em: https://aquitemcd.iti.gov.br/. Acesso em: 22 jan. 2023.

28. BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Meu certificado.** Disponível em: https://meucertificado.iti.gov.br/login. Acesso em: 22 jan. 2023.

Referências Complementares

BRASIL. **Decreto Nº 10.543, 13 de novembro de 2020.** Dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10543.htm. Acesso em: 22 jan. 2023.

BRASIL. **Lei Nº 14.063, 23 de setembro de 2020.** Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.063-de-23-de-setembro-de-2020-279185931. Acesso em: 22 jan. 2023.

CONSELHO FEDERAL DE MEDICINA (CFM). **Resolução CFM Nº 2.218, 29 de novembro de 2018.** Revoga o artigo 10º da Resolução CFM nº 1.821/2007, de 23 de novembro de 2007, que aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2018/2218. Acesso em: 22 jan. 2023.

COORDENADOR DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA. **Resolução CG ICP-Brasil Nº 182, 18 de fevereiro de 2021.** Aprova a versão revisada e consolidada do documento Visão Geral sobre Assinaturas Digitais na ICP-Brasil - DOC-ICP-15. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/resolucoes/Resoluo_CGICPBrasil_182Dec10139Etapa3DOC15_assinada.pdf. Acesso em: 22 jan. 2023.

Minibiografias

Organizadores

Fábio Nogueira de Lucena é graduado em Ciência da Computação (UFG), mestre e doutor em Ciência da Computação (UNICAMP), especialista em Informática em Saúde (UNIFESP), Project Management Professional (PMI) e Certified Software Development Professional (IEEE), além de possuir outras certificações da indústria de software. É professor titular do curso de Engenharia de Software do Instituto de Informática da UFG.

Github: https://github.com/kyriosdata

E-mail: kyriosdata@ufg.br

Plínio de Sá Leitão Júnior é Engenheiro Eletricista, com mestrado e doutorado pela Universidade Estadual de Campinas (UNICAMP) na área de Engenharia de Software, e Especialização em Informática em Saúde pela Universidade Federal de São Paulo (UNIFESP). É Professor Associado no Instituto de Informática da Universidade Federal de Goiás (UFG), com atuação na graduação e na pós-graduação. Desenvolve pesquisas nos temas Teste de Software, Banco de Dados, Inteligência Computacional e Persistência de Registros Clínicos.

E-mail: plinio.sa.leitao.junior@ufg.br

Taciana Novo Kudo é professora adjunta do Instituto de Informática da Universidade Federal de Goiás (UFG). É mestre e doutora em Ciência da Computação pelo Departamento de Computação (UFSCar) e graduada em Ciência da Computação (UNIMAR). Possui experiência profissional na área de Engenharia de Software, especificamente em Engenharia de Requisitos e Gerência de Projetos, em institutos de pesquisa e empresas de São Paulo e Goiás. Como pesquisadora, atua em projetos voltados para Engenharia de Software, Engenharia de Requisitos e Informática aplicada à Educação e à Saúde.

E-mail: taciana@ufg.br

Ana Laura de Sene Amâncio Zara é graduada em Farmácia e em Análises Clínicas (UFMT), especialista em Avaliação de Tecnologias em Saúde (UFRGS) e em Docência do Ensino Superior (UCDB). Possui mestrado e doutorado em Epidemiologia pelo Programa de Pós-Graduação em Medicina Tropical e Saúde Pública (UFG) e pós-doutorado pelo Programa de Pós-graduação de Odontologia da Faculdade de Odontologia (UFG). Atualmente, é professora do Departamento de Saúde Coletiva da UFG. Ensina, pesquisa e orienta nas áreas de Epidemiologia, Saúde Coletiva, Metodologia e Editoração Científicas, Economia da Saúde, Bioestatística, Informática em Saúde e Revisões Sistemáticas.

E-mail: analauraufg@gmail.com

Rejane Faria Ribeiro-Rotta é graduada em Odontologia (UFG), especialista em Radiologia Bucomaxilofacial e Estomatologia, mestre e doutora em Odontologia (Diagnóstico Bucal) (USP-Bauru), com experiência em colaborações internacionais em pesquisa e intercâmbios, e na gestão institucional do ensino superior. Professora titular da Faculdade de Odontologia da UFG. Fundadora do Centro Goiano de Doenças da Boca da Faculdade de Odontologia da UFG (CGDB-FO-UFG) e da Comissão de Governança da Informação em Saúde da UFG. Principais temáticas de pesquisa: Diagnóstico de lesões da região bucomaxilofacial / Câncer de boca; Dores crônicas orofaciais; Diagnóstico por imagem da região bucomaxilofacial; Prática baseada em evidência, Informação e Informática em saúde.

E-mail: rejanefrr@ufg.br

Renata Dutra Braga é professora adjunta do Instituto de Informática da Universidade Federal de Goiás (UFG). É mestre e doutora em Ciências da Saúde pela Faculdade de Medicina da UFG, pós-graduada em Informática em Saúde (UNIFESP) e em Qualidade e Gestão de Software (PUC-GO) e é graduada em Sistemas de Informação (UniEvangélica). É atualmente vice-coordenadora da Comissão de Governança da Informação em Saúde (CGIS-UFG). Ensina, pesquisa, orienta e desenvolve projetos de extensão na área de saúde digital, com interesse, principalmente em modelagem de processo de negócios, engenharia de requisitos, modelos de informação, terminologias clínicas e padrões para a troca da informação em saúde.

E-mail: renatadbraga@ufg.br

Rita Goreti Amaral é professora titular da Faculdade de Farmácia da Universidade Federal de Goiás (UFG), com atuação na graduação e pós-graduação. Graduada em Farmácia e Bioquímica e especialista em Citologia Clínica (UFG). Mestre em Biologia Celular e Molecular (USP) e Doutora em tocoginecologia pela Faculdade de Ciências Médicas (UNICAMP). Coordenadora do Laboratório de Monitoramento Externa da Qualidade da Faculdade de Farmácia (UFG). Desenvolve projetos de pesquisa e extensão na área de Citologia Clínica e Saúde Pública, atuando nos seguintes temas: controle da qualidade em citopatologia do colo do útero, prevenção, detecção precoce de doenças, aperfeiçoamento de métodos diagnósticos, desenvolvimento e validação de práticas de cuidado do paciente nas doenças crônicas transmissíveis e não transmissíveis, informática em saúde e assistência farmacêutica.

E-mail: rita@ufg.br

Sheila Mara Pedrosa é graduada e mestre em Enfermagem pela Faculdade de Enfermagem (UFG), especialista em Saúde Coletiva e Regulação em Saúde no SUS (IEP/HSL) e doutora em Ciências da Saúde pela Faculdade de Medicina (UFG). Atualmente é professora adjunta do Centro Universitário de Anápolis e desenvolve pesquisa e extensão no âmbito das violências e vulnerabilidade social. É membro da Comissão de Governança da Informação em Saúde (CGIS-UFG) e participa de projetos voltados à saúde digital.

E-mail: sheilaenf@gmail.com

Silvana de Lima Vieira dos Santos - é enfermeira, mestre e doutora em Ciências da Saúde (UFG), Especialista em Enfermagem em Infectologia (USP) e em Informática em Saúde (UNIFESP). É professora associada da Faculdade de Enfermagem (UFG). Vice líder do Núcleo de Estudos e Pesquisa de Enfermagem em Prevenção e Controle de Infecção Relacionada à Assistência à Saúde (NEPIH), vinculado ao CNPq. Experiência na área de prevenção e controle de infecções relacionadas à assistência à saúde, epidemiologia e informática em saúde. Coordenadora da Comissão de Governança da Informação em Saúde (CGIS-UFG).

E-mail: silvanalvsantos@ufg.br

PROGRAMA EDUCACIONAL EM SAÚDE DIGITAL DA UNIVERSIDADE FEDERAL DE GOIÁS

CGIS UFG Comissão de Governança da Informação em Saúde

CIGETS CENTRO DE INOVAÇÃO EM GESTÃO DA EDUCAÇÃO E DO TRABALHO EM SAÚDE

MINISTÉRIO DA SAÚDE

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

SOBRE O E-BOOK

Tipografia: Montserrat

Publicação: Cegraf UFG
Câmpus Samambaia, Goiânia - Goiás. Brasil. CEP 74690-900
Fone: (62) 3521-1358
https://cegraf.ufg.br