

# Gestão de identidade e de acesso

SEG786203 – CST em Análise e Desenvolvimento de Sistemas

Prof. Emerson Ribeiro de Mello

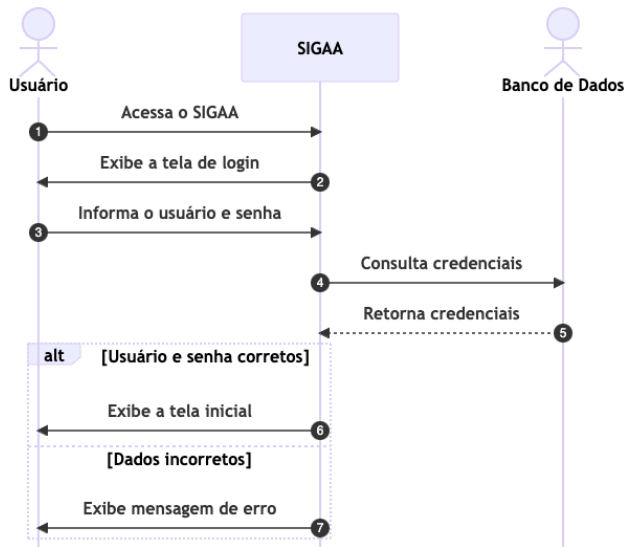
mello@ifsc.edu.br

# Licenciamento



Slides licenciados sob [Creative Commons "Atribuição 4.0 Internacional"](https://creativecommons.org/licenses/by/4.0/)

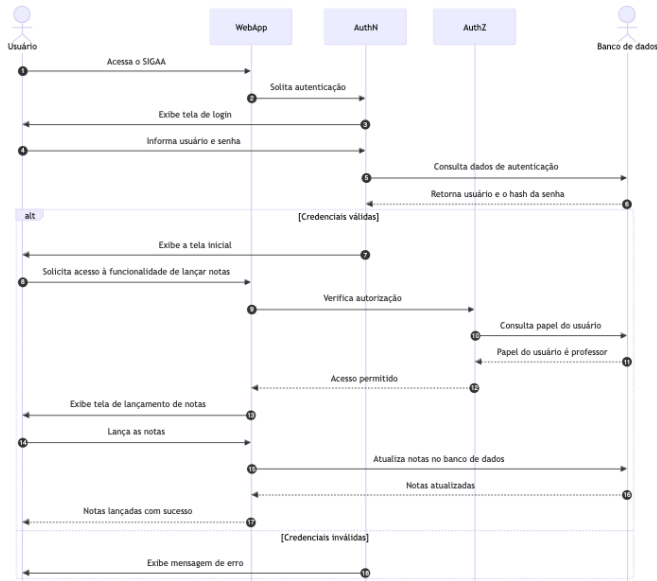
# Autenticação de usuário



- SIGAA responsável pela autenticação e autorização de usuários

# Autenticação e autorização de usuário

- Autenticação e autorização delegada para outro sistema



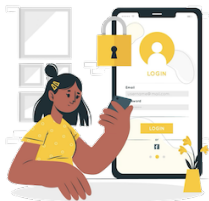
# Identidade digital

- **Identidade digital** é a representação de uma entidade para identificá-la em uma transação *online*
- **Autenticação digital** determina se um sujeito controla um ou mais **autenticadores** que estão associados a sua identidade
  - Senhas, chave privada, biometria
- **Prova de identidade** determina que um sujeito é quem ele diz ser
  - Tarefa desafiadora e sujeita a diversos ataques que objetivam a personificação

# Gestão de identidade e de acesso (GId)

*Identity and Access Management (IAM)*

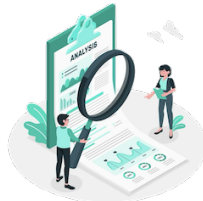
**Conjunto de processos e tecnologias** que visa garantir a **identidade digital** de uma entidade



**Autenticação**



**Autorização**



**Auditoria**

# Modelos de gestão de identidade

- Uma organização pode possuir diferentes sistemas de informação
- Cada sistema pode possuir diferentes formas de autenticação e autorização de usuários
- Tratar cada sistema de forma isolada pode ser ineficiente e inseguro

## Modelo de gestão de identidade

Define como a identidade digital de um usuário é criada, armazenada, compartilhada e utilizada nos sistemas de uma organização

# Principais papéis no modelo de GId

## ■ Usuário

- Entidade que participa de transações *online*

## ■ Provedor de identidade (IdP, *Identity Provider*)

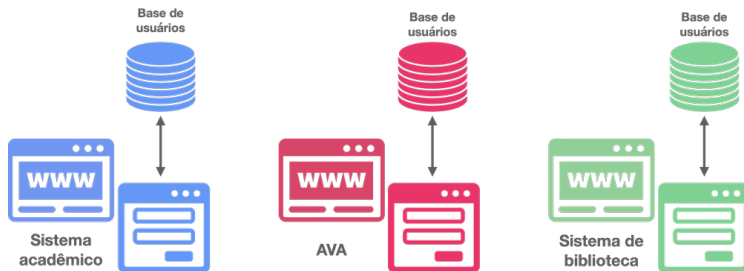
- Emite identidades digitais (conjunto de atributos) para seus usuários
- Implementa métodos próprios para comprovar que o usuário é detentor de tais atributos

## ■ Provedor de serviços (SP, *Service Provider*)

- Oferta serviços para usuários autorizados
- Possui relação de confiança com IdPs, pois delega a estes a tarefa de autenticar usuários



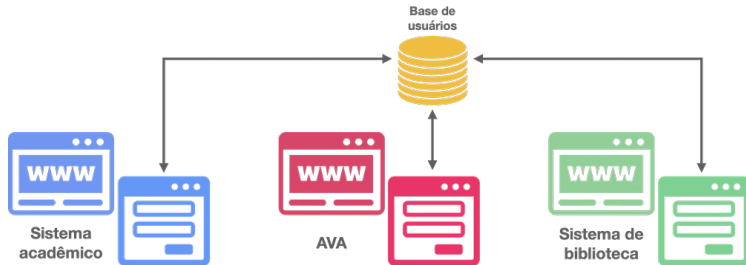
# Modelo baseado em silo ou tradicional



- Usuário terá múltiplas identidades digitais
- Usuário precisa passar pelo processo de autenticação em cada SP
- Diferentes interfaces de autenticação de usuário
- Aumenta superfície de ataque

# Modelo baseado em silo ou tradicional

## Diretório compartilhado



- Usuário terá uma única identidade digital
- Usuário precisa passar pelo processo de autenticação em cada SP
- Diferentes interfaces de autenticação de usuário
- Aumenta superfície de ataque

# Modelo baseado em silo ou tradicional

## Na prática

**Login**

Usuário:

Senha:

[Esqueceu ou deseja alterar sua senha?](#)

Sistema acadêmico

**Acessar Ambiente Virtual**

Identificação de usuário

Senha

[Esqueceu o seu usuário ou senha?](#)

AVA

**LOGIN no Pergamum**

Usuário:

Senha:

**ATENÇÃO**

Usuário: n. de matrícula (aluno) ou SIAPE (servidor)

Senha: Cadastrada na Biblioteca

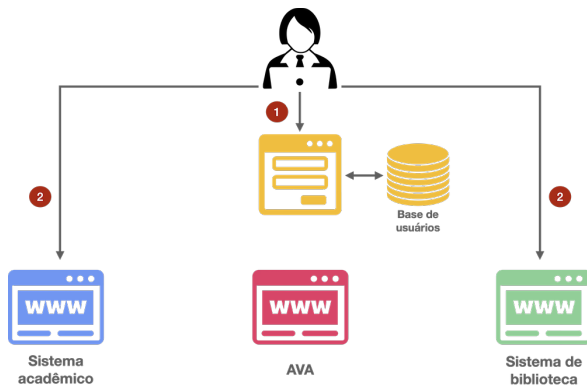
Mantenha seu e-mail atualizado no QAcadêmico.

[Esqueci minha senha!](#)

Sistema de biblioteca

Fonte: Capturas de tela de sistemas de uma instituição federal de ensino – omitido para preservar a privacidade

# Modelo centralizado



- Uma única interface de autenticação de usuários
- Autenticação única (SSO, *Single Sign-On*)
- Autorização e auditoria centralizadas

# Modelo centralizado

## Soluções de código aberto e comerciais

### ■ Soluções de código aberto

- Keycloak

- CAS

### ■ Soluções comerciais

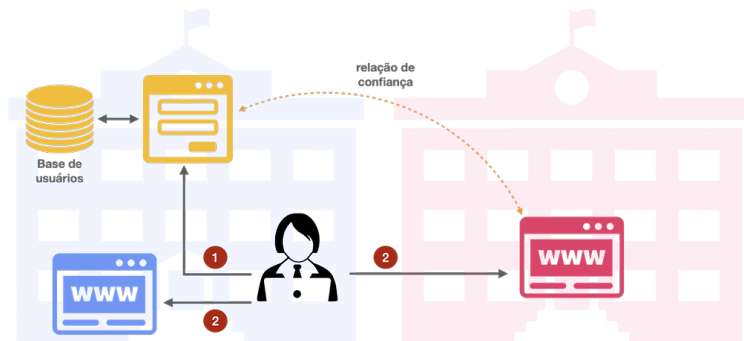
- Okta

- Microsoft Entra ID



Fonte: Logos baixados dos respectivos sites

# Modelo federado



- Uma única interface de autenticação de usuários
- Autenticação única (SSO, *Single Sign-On*)
- Autorização descentralizada

# Modelo federado

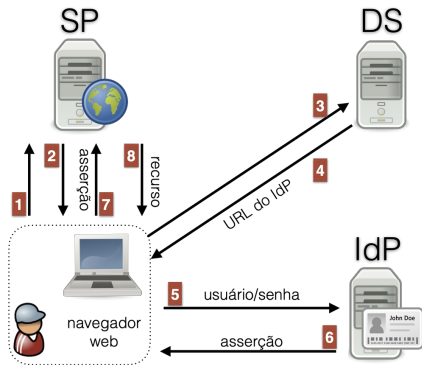
## Comunidade Acadêmica Federada (CAFe) da RNP

- Mais de 300 instituições de ensino e pesquisa
- Atributos do usuário compartilhados
  - Nome, CPF, e-mail, vínculo com a instituição, etc.
  - Há consentimento do usuário
- Fundamentada sobre o protocolo SAML2.0 e o *framework Shibboleth*
- Alguns SPs
  - <https://conferenciaweb.rnp.br>
  - <https://www.periodicos.capes.gov.br>
  - <https://filesender.rnp.br>



# Modelo federado

## Fluxo de autenticação federada



- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service* (DS)
- 3 DS redireciona para o IdP
- 4 IdP autentica o usuário
- 5 IdP redireciona para o SP

Fundamentada sobre redirecionamentos HTTP e o protocolo SAML2.0



# Modelo federado

## Fluxo de autenticação federada na CAFe

The screenshot displays the CAFe login page. On the left, a blue sidebar contains the text 'Acesso federado' and 'Já tenho uma conta' above an orange 'ENTRAR' button. Below this is the CAFe logo and the text 'comunidade acadêmica federada'. The main white area is titled 'Minha conta não é federada' with the subtitle 'Acessar usando uma conta local'. It features input fields for 'Email' (containing 'email@exemplo.com.br') and 'Senha' (with a link 'Esqueceu sua senha?'). Below these is another orange 'ENTRAR' button. At the bottom, it says 'ou acesse com' followed by buttons for Google and Facebook.

- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service* (DS)
- 3 DS redireciona para o IdP
- 4 IdP autentica o usuário
- 5 IdP redireciona para o SP


# Modelo federado

## Fluxo de autenticação federada na CAFe

Acessando serviço:  
ConferenciaWeb

**Encontre sua instituição**  
Faça login em sua instituição para acessar.

Federation  
Production



A CAFe não armazena suas informações. Mais informações nos [Termos de uso](#)

- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service (DS)*
- 3 DS redireciona para o IdP
- 4 IdP autentica o usuário
- 5 IdP redireciona para o SP

# Modelo federado

## Fluxo de autenticação federada na CAFe

Acessando serviço:  
ConferenciaWeb

### Encontre sua instituição

Faça login em sua instituição para acessar.

**IFSC**  
Instituto Federal de Santa Catarina  
[Prosseguir para login em IFSC](#)  
A CAFe não armazena suas informações. Mais informações nos [Termos de uso](#)

Federacion  
Production

- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service (DS)*
- 3 DS redireciona para o IdP
- 4 IdP autentica o usuário
- 5 IdP redireciona para o SP

# Modelo federado

## Fluxo de autenticação federada na CAFe

Acesso pela instituição:



**INSTITUTO FEDERAL**  
Santa Catarina

Usuário

Senha

☐ Salvar meu login

**Entrar**

[Painel de Segurança](#) 

- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service* (DS)
- 3 **DS redireciona para o IdP**
- 4 IdP autentica o usuário
- 5 IdP redireciona para o SP

# Modelo federado

## Fluxo de autenticação federada na CAFe

Acesso pela instituição:



**INSTITUTO FEDERAL**  
Santa Catarina

Usuário

Senha

☐ Salvar meu login

**Entrar**

[Painel de Segurança](#) 

- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service* (DS)
- 3 DS redireciona para o IdP
- 4 **IdP autentica o usuário**
- 5 IdP redireciona para o SP

# Modelo federado

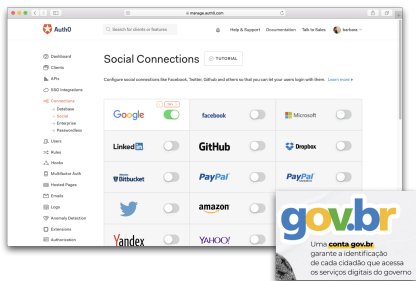
## Fluxo de autenticação federada na CAFé



- 1 Usuário acessa o SP
- 2 SP redireciona para o *Discovery Service* (DS)
- 3 DS redireciona para o IdP
- 4 IdP autentica o usuário
- 5 IdP redireciona para o SP

# Modelo federado

## Login social










- Estabelecimento de confiança entre SPs e IdPs de forma bilateral
  - SP tem que se registrar previamente no IdP
- Autorização para compartilhamento de atributos
  - Consentimento do usuário indica quais atributos serão compartilhados
- Fundamentada sobre os protocolos OAuth2.0 e OpenID Connect (OIDC)
  - Temos redirecionamentos HTTP e troca de tokens

# Modelo federado

## Login social

### Signup Form

	Continue with Google	×
	Continue with Facebook	×
	Continue with Spotify	×
	Continue with Microsoft	×
	Continue with Dribbble	×
	Continue with Github	×
	Continue with LinkedIn	×

Fonte: <https://webflow.com>

- Estabelecimento de confiança entre SPs e IdPs de forma bilateral
  - SP tem que se registrar previamente no IdP
- Autorização para compartilhamento de atributos
  - Consentimento do usuário indica quais atributos serão compartilhados
- Fundamentada sobre os protocolos OAuth2.0 e OpenID Connect (OIDC)
  - Temos redirecionamentos HTTP e troca de tokens



# Modelo federado

Login social, fluxo de autenticação

## DETRAN DIGITAL

### Para acessar faça seu login

Com o cadastro no DETRAN DIGITAL, você poderá visualizar seus dados, documentos e solicitações encaminhadas ao órgão. Abra suas solicitações pela internet e evite filas.

Pessoa Jurídica? ⓘ

Não está cadastrado?

**CADASTRAR VIA GOV.BR**

Fazer login como:

**ACESSAR O PORTAL VIA GOV.BR**

UTILIZAR LOGIN ANTIGO    ESQUECI A SENHA

# Modelo federado

## Login social, fluxo de autenticação



### Autorização de uso de dados pessoais

**Serviço: Acesso - SC**

Este serviço precisa utilizar as seguintes informações pessoais do seu cadastro:

- Identidade gov.br
- Nome e foto
- Endereço de e-mail
- Número de telefone celular
- Dados de vinculação de empresas do gov.br
- Confiabilidades de sua conta

A partir da sua aprovação, a aplicação acima mencionada e a plataforma gov.br utilizarão as informações listadas acima, respeitando [os termos de uso e o aviso de privacidade](#).

Negar

Autorizar

# Quais as vantagens com o login social?

## ■ Para o usuário

- Autenticação única (SSO)
- Não precisa lembrar de múltiplas senhas
- Pode compartilhar atributos de forma seletiva (consentimento) e revogar o consentimento a qualquer momento
- Facilidade de uso em dispositivos móveis, quando combinado com gerenciadores de senhas ou *passkeys*

## ■ Para o provedor de serviços

- Redução de custos com autenticação
- Redução de custos com suporte ao usuário
- Melhora a experiência do usuário

# Quais as desvantagens com o login social?

## ■ Para o usuário

- Perda de privacidade, pois o IdP pode rastrear a navegação do usuário
- Perda de controle sobre seus dados pessoais
- Perda de acesso a serviços, caso o IdP bloqueie a conta
- Perda de acesso a serviços, caso o IdP seja descontinuado

## ■ Para o provedor de serviços

- Perda de controle sobre a autenticação do usuário
- Perda de controle sobre a experiência do usuário
- Perda de controle sobre a disponibilidade do serviço

# Quais as desvantagens com o login social?

## ■ Para o usuário

- Perda de privacidade, pois o IdP pode rastrear a navegação do usuário

■ Perda de

■ Perda de

■ Perda de

## ■ Para o provedor

■ Perda de

■ Perda de

■ Perda de



1

---

<sup>1</sup> <https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html>

# Quais as desvantagens com o login social?

The New York Times

21/08/2022

## ***A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.***

Google has an automated tool to detect abusive images of children. But the system can get it wrong, and the consequences are serious.

- Perdeu acesso aos emails, contatos, documentos e fotos
- Perdeu sua conta Google Fi (seu número de telefone celular)
- Sem celular e sem email, não pode ter acesso as senhas de uso único (OTP) necessárias para acessar suas contas em outros provedores de serviço

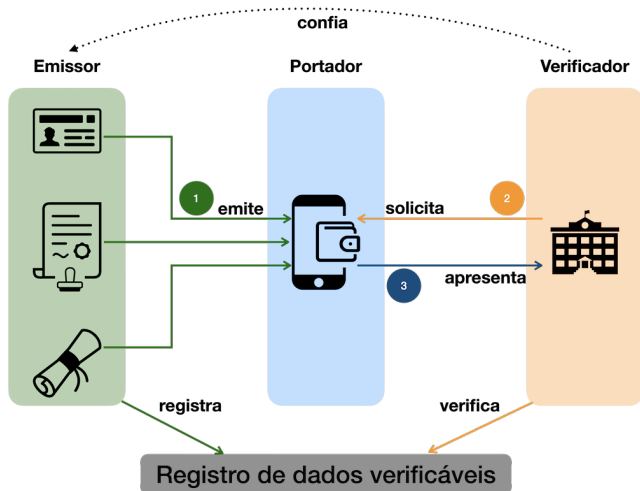
# Identidade digital descentralizada (IDD) I

## *Digital Identity Decentralized (DID)*

- **O usuário é o detentor de sua identidade digital**
  - IdP não é mais o detentor da identidade digital do usuário
- **Atributos são atestados criptograficamente e armazenados em uma carteira digital**
  - IdP não participa mais do processo de autenticação do usuário
- **O usuário compartilha atributos com SPs de forma seletiva**
  - Prova de conhecimento zero (*zero-knowledge proof*)
- **Fundamentada sobre os padrões W3C**
  - *Verifiable Credentials (VCs)* e *Decentralized Identifiers (DIDs)*

# Identidade digital descentralizada (IDD) II

*Digital Identity Decentralized (DID)*





# Identidade digital descentralizada (IDD)

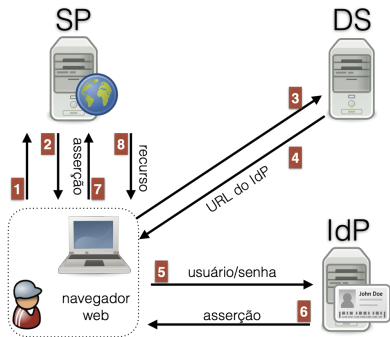
## Caso de uso

- **Processo de matrícula pode exigir documentos que comprovem**
  - Identidade civil
  - Local de residência
  - Certificados de conclusão de cursos anteriores
- **Como receber e confiar em tais documentos se isso for feito de forma *online*?**
  - **IDD** pode ser uma solução
  - Credenciais emitidas por entidades confiáveis
  - Credenciais são atestadas criptograficamente
  - Credenciais são armazenadas na carteira digital do usuário



# Modelo de gestão de identidade federada

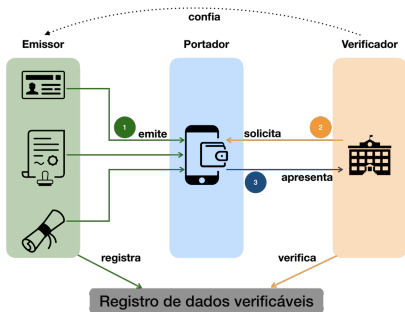
## Fluxo de autenticação



- **Autenticação intermediada por IdP**
  - IdP participa de toda interação do usuário
- **Atualmente amparada em primitivas da navegação web**
  - Redirecionamentos de URL
  - Parâmetros de URL e cookies
- **Federated Credential Management API**
  - Primitivas para autenticação federada
  - Sem redirecionamentos e sem cookies

# Identidade Digital Descentralizada

## Fluxo de autenticação



### ■ Autenticação sem intermediários

- Usuário autentica diretamente com SP
- Não há redirecionamentos

### ■ Carteira do usuário em evidência

- Escolha da credencial para autenticação
- Assina requisições de autenticação

### ■ Registro de dados verificáveis

- Consultado por SPs para verificar credenciais

# Estabelecimento de confiança

## Modelo de gestão de identidade federada

### ■ Usuários confiam no IdP

- Pode ser um IdP de sua escolha
- Ou pode ser imposto (e.g. da universidade, do governo)

### ■ Confiança mútua entre IdP e SP

- Por meio de acordos bilaterais
- Ou por meio de federações (conjunto comum de políticas e padrões)

#### **Nota**

**Do ponto de vista do usuário**, a confiança no IdP é transferida para os SPs. O usuário confia que o **IdP não irá compartilhar informações** além do necessário com os SPs e que o **IdP não tem interesse em monitorar** suas atividades

# Estabelecimento de confiança

## Identidade Digital Descentralizada

### ■ Usuários confiam em suas carteiras

- Pode ser uma carteira de sua escolha (idealmente)
- Verificadores e emissores podem exigir que a carteira atenda requisitos mínimos

### ■ Confiança entre Emissores e Validadores

- Confiança é estabelecida por meio de acordos bilaterais (descentralizada)
- Fundamentada em DIDs, VCs e Registro de Dados Verificáveis

#### **Nota**

*Frameworks* e padrões de governança ajudam a garantir que os emissores sejam reconhecidos e confiáveis, criando uma rede de confiança para os validadores

# Controle dos dados do usuário

## ■ Modelo de gestão de identidade federada

- Dados do usuário mantidos no IdP e compartilhados com SPs
- Termo de consentimento apresentado ao usuário no momento da autenticação
- ZKP não é nativo nos protocolos comumente usados

## ■ Identidade Digital Descentralizada

- Dados do usuário mantidos na carteira do usuário
- ZKP podem ser usadas para provar propriedades dos dados sem revelá-los

### Nota

É importante **considerar a assimetria de poder** entre o usuário e o SP. Termo de consentimento e ZKP são mecanismos para empoderar o usuário, mas dependem do SP para serem efetivos

# Resumo das diferenças

## Modelo federado e Identidade Digital Descentralizada

Característica	Federado	IDD
Modelo de confiança	Acordos formais bilaterais	Não exige acordos
Controle dos dados	Dados no IdP	Dados na carteira do usuário
Fluxo de Autenticação	IdP intermediário	Direta com SP
Autenticação	SAML, OIDC	Assinaturas DIDs/VCs
Autorização	SAML, OIDC	Atributos VCs/VPs

# Aula baseada em



MELLO, Emerson Ribeiro de *et al.* Autenticação e Autorização: antigas demandas, novos desafios e tecnologias emergentes. *In*: MINICURSOS do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg). Porto Alegre, RS, set. 2022. DOI: <https://doi.org/10.5753/sbc.10710.3.1>.