INSTITUTO FEDERAL DE SANTA CATARINA

SAROM TORRES GAIER

Requisitos de segurança para arquitetura de um sistema de controle de acesso com cadeia de aprovação

São José - SC

abril/2024

RESUMO

O acesso a infraestruturas físicas em empresas é restrito e controlado por credenciais obtidas após rigorosos processos de aprovação. Em empresas com múltiplos Centros de Processamento de Dados (CPDs), cada unidade adota sistemas de autenticação próprios, o que torna complexa a concessão e revogação de acessos, especialmente quando há necessidade de acessos cruzados ou de terceiros. A descentralização desses processos pode levar a erros e aumentar os riscos de segurança, como vazamento de credenciais. Esse trabalho propõe estabelecer os requisitos mínimos de segurança para uma arquitetura centralizada para gestão de acessos, visando maior eficiência e segurança no controle e rastreamento de operações.

Palavras-chave: Controle de Acesso. Cadeia de aprovação. Centro de Processamento de Dados (CPDs).

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE CÓDIGOS

LISTA DE ABREVIATURAS E SIGLAS

ACL *Access Control List*.

CAD Controle de Acesso Discricionário.

CL *Capability List*.

CPD Centro de Processamento de Dados.

DAC *Discretionary Access Control*.

PIN *Personal Identification Number*.

PSI Política de Segurança da Informação.

RBAC *Role Based Access Control*.

SR Separação de Responsabilidades.

UML *Unified Modeling Language*.

SUMÁRIO

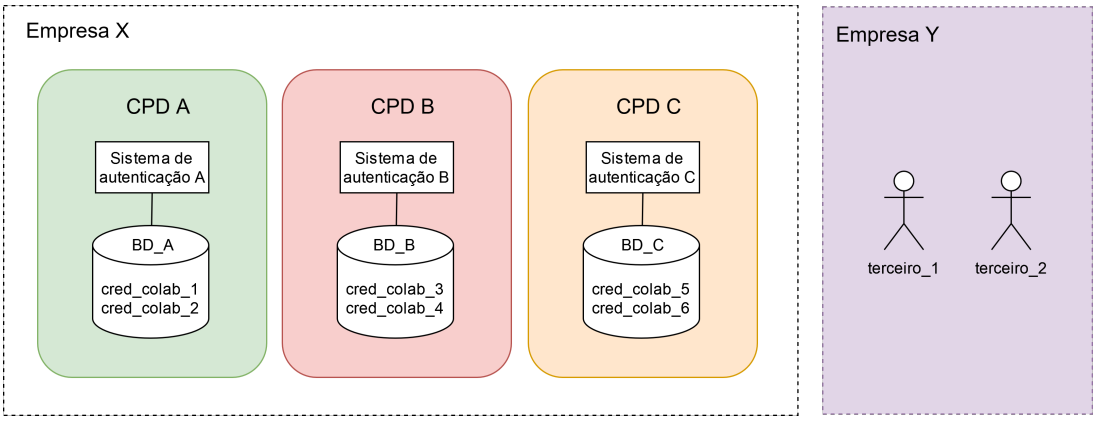
1 INTRODUÇÃO

Segundo NIST (2006), o controle de acesso visa proteger os recursos dos sistemas contra acessos não autorizados, assegurando a confidencialidade, integridade e disponibilidade dos dados. Além disso, previne atividades prejudiciais que poderiam comprometer o funcionamento dos sistemas e da infraestrutura. Colaboradores devem acessar apenas informações, sistemas e locais necessários para suas atividades, reduzindo riscos de fraudes e erros. O monitoramento contínuo é fundamental para detectar e responder rapidamente a atividades suspeitas.

Geralmente, o acesso às infraestruturas físicas de empresas e instituições é restrito a indivíduos específicos e controlado por credenciais obtidas após um rigoroso processo de aprovação. Em muitas instituições, há uma necessidade frequente de colaboradores de outras localidades da mesma empresa acessarem áreas diferentes das suas origens, o que exige concessões temporárias e pontuais de acesso. Além disso, fornecedores e prestadores de serviços também precisam solicitar e ter seus acessos aprovados, além de receberem as devidas credenciais de maneira segura.

A situação é ilustrada na Figura 1, que representa o cenário típico de múltiplos CPDs e uma mesma empresa, cada um com seu próprio sistema de autenticação conectados em suas bases individuais de credenciais para colaboradores autorizados.

Figura 1 – Cenário de múltiplos CPDs com gestão de acesso descentralizada



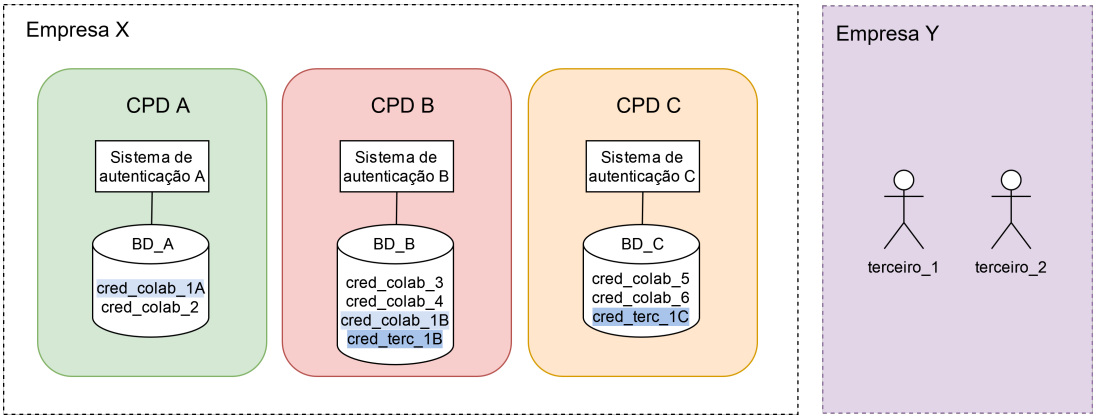
Fonte: Elaborada pelo autor.

Os processos de aprovação para liberação das credenciais de acesso, geralmente seguem regras de segurança rigorosas, envolvendo uma ou mais pessoas responsáveis em cada localidade, podendo formar cadeias de aprovação complexas. Sem um mecanismo unificado, cada localidade pode adotar seus próprios processos e ferramentas de aprovação, resultando em complexidade na solicitação e autorização de acessos para colaboradores

e terceiros. Além disso, é crucial para a empresa garantir a segurança nos processos de revisão e revogação de acesso. Em um cenário descentralizado, cada unidade opera isoladamente, sem visão completa dos acessos como um todo, o que pode levar a erros na revogação ou até mesmo à falta dela.

No cenário descentralizado descrito, a necessidade de acesso cruzado entre diferentes CPDs dentro de uma empresa, bem como os acessos de fornecedores ou parceiros externos requer um rigoroso processo de autorização. Isso envolve várias etapas dentro de diferentes cadeias de aprovação, sujeição a diferentes políticas de segurança para cada credencial e compromete a observabilidade sobre quais domínios os colaboradores e a empresa terceira possui acesso. Além disso resulta na emissão de múltiplas credenciais de acesso o que pode aumentar os riscos de segurança, como vazamento de credenciais e falha na revogação de acesso após o período necessário.

Figura 2 – Múltiplos CPDs com gestão de acesso descentralizada, duplicidade de credenciais para colaboradores e terceiros.



Fonte: Elaborada pelo autor.

Tendo em vista a complexidade e sensibilidade dessas operações, é necessário que os sistemas de gerenciamento de acesso sejam não apenas seguros, mas também eficientes e fáceis de administrar. Este trabalho se propõe a estabelecer os critérios mínimos de segurança para uma arquitetura de um sistema centralizador de gestão de acessos a infraestruturas físicas como CPDs. De maneira que seja possível gerar solicitações de acesso, submetê-las a cadeias de aprovação e gerar rastreabilidade das operações realizadas no sistema.

1.1 Objetivos

1.1.1 Objetivo geral

O objetivo desse trabalho é estabelecer os critérios mínimos de segurança para uma arquitetura de um sistema centralizador de gestão de acessos a estruturas físicas tais

como CPDs.

1.1.2 Objetivos específicos

Os principais objetivos desse trabalho são:

- Elaborar os casos de usos mínimos necessários a serem atendidos para um sistema centralizador de gestão de acessos;
- Definir os requisitos mínimos de controles de acesso necessários para garantir a implantação de cadeias de autorização no sistema.
- Definir os requisitos mínimos de segurança para gerar rastros de auditoria que garantam a rastreabilidade das ações realizadas nos sistema.

1.2 Organização do texto

O texto está organizado da seguinte forma: No Capítulo 2 é apresentada uma fundamentação teórica dos conceitos e tecnologias que servirão de suporta para a implantação do projeto. O Capítulo 3 contém a metodologia a ser empregada no desenvolvimento do projeto, bem como o cronograma das atividades.

2 REVISÃO BIBLIOGRÁFICA

2.1 Autenticação, autorização e auditoria

Segundo Grassi, Fenton e Garcia (2017), o processo de autenticação visa estabelecer se um determinado sujeito que está tentando acessar um serviço é realmente quem alega ser. Essa validação ocorre por meio da verificação do sujeito ter controle de uma ou mais credenciais válidas que estão associadas a sua identidade digital.

No paradigma clássico, os autenticadores utilizados no processo de autenticação podem ser baseados em 3 tipos de fatores:

- Algo que você sabe (e.g. palavra-passe, *Personal Identification Number* (PIN));
- Algo que você possui (e.g. chave criptográfica);
- Algo que você é (e.g. dados biométricos);

A autorização consiste na atribuição de direitos (ITU, 1991) a um sujeito para acessar um determinado recurso. Isto é, a autorização determina quais ações ou recursos um usuário ou entidade está autorizado a realizar nos sistemas de informação.

A auditoria, por sua vez, tem como objetivo avaliar se os controles do sistema estão em conformidade com as políticas e procedimentos operacionais estabelecidos. Essa avaliação é realizada por meio de revisões independentes das trilhas de auditoria, que consistem em registros de atividades realizadas no sistema, considerando tanto os processos do sistema e os aplicativos quanto as ações realizadas pelos usuários nesses contextos (NIELES; DEMPSEY; PILLITTERI, 2017a).

Conforme Grassi, Fenton e Garcia (2017), a autenticação não determina as autorizações ou permissões de um usuário no sistema. Logo, validar e estabelecer corretamente a identidade do usuário é de responsabilidade do processo de autenticação e o controle de acesso assume que a autenticação do usuário foi realizada com sucesso previamente. Isto é, a eficácia do o controle de acesso depende de uma identificação adequada do usuário (SANDHU; SAMARATI, 1994).

2.2 Controle de acesso

Segundo Chung, Ferraiolo e Kuhn (2006), o controle de acesso visa proteger os recursos do sistema contra acessos inapropriados ou indesejados, permitindo que apenas

usuários autorizados tenham acesso a eles. Do ponto de vista dos negócios, o controle de acesso tem como objetivo viabilizar o acesso das informações tanto para os usuários do sistema quanto para as aplicações, sendo que um controle de acesso bem gerenciado e efetivo deve facilitar esse compartilhamento.

Conforme Chung, Ferraiolo e Kuhn (2006) e Mello et al. (2022), algumas terminologias fundamentais utilizadas no controle de acesso são:

- **Objeto**: representação de um recurso que é acessado por um sujeito por meio de uma operação. São exemplos de objetos: registros, páginas, arquivos, diretórios, processos, programas, etc.
- **Sujeito**: é uma representação de uma entidade que deseja acessar o sistema ou recurso. Um sujeito pode ser uma pessoa, um processo ou um dispositivo.
- **Operação**: representa uma ação realizada pelo sujeito no objeto.
- **Permissão** (privilégio): autorização para realizar uma ação em um sistema. Geralmente, refere-se à combinação entre objeto e operação.
- **Atributos**: são características do sujeito, objeto ou condições relativas ao contexto.
- **Dono do recurso**: indivíduo que é responsável por determinada informação. Pode ser quem criou o recurso, o responsável pela organização ou qualquer pessoa ou papel que tenha sido designado como tal.
- **Guardião do recurso**: quem efetivamente gerencia e monitora o recurso, garantindo a aplicação das políticas de controle de acesso e a disponibilidade dos recursos aos usuários autorizados.

2.2.1 Políticas, Modelos e Mecanismos

O controle de acesso pode ser abstraído em três diferentes níveis: políticas, modelos e mecanismos de controle de acesso. Segundo Chung, Ferraiolo e Kuhn (2006) a política de controle de acesso são os requisitos e diretrizes de alto nível que determinam como o acesso é gerenciado. É por meio da política de controle de acesso que é definido quais indivíduos - sujeitos - podem acessar quais informações - objetos - e em quais circunstâncias. Essas definições devem cobrir todas as possibilidades de acesso que possam ocorrer no sistema e devem ser consistentes, isto é, não podem existir diretrizes que sejam conflitantes entre si.

De acordo com Windley (2005) o controle de acesso é, antes de tudo, uma questão de política e, ainda que possa ser considerada em um contexto específico de uma aplicação, a política é um reflexo os objetivos de negócio e de segurança que foram acordados com

outras políticas organizacionais. Além disso, as políticas podem se referir aos recursos de uma unidade organizacional ou entre diferentes unidades ou podem ser baseadas em fatores como necessidade, competência, autoridade, obrigação ou conflito de interesses (CHUNG; FERRAIOLO; KUHN, 2006).

É importante levar em consideração que nem todos os sistemas requerem o mesmo nível de proteção, visto que alguns ambientes podem exigir políticas extremamente restritas e granulares enquanto outros podem demandar maior flexibilidade. De maneira geral, não existe uma política que possa ser considerada melhor que outra, existem políticas que garantem mais proteção que outras e que estão mais adequadas ao ambiente para o qual foram idealizadas (SANDHU; SAMARATI, 1994).

Por sua vez, um modelo de controle de acesso é o nível intermediário e visa prover uma representação formal da política de controle de acesso e seu funcionamento. É útil para provar teoricamente as limitações que possam existir em um sistema e opera como uma ponte entre as políticas e os mecanismos de controle de acesso (CHUNG; FERRAIOLO; KUHN, 2006).

Já os mecanismos de controle de acesso são o nível mais baixo da abstração e implementam as políticas garantindo que todos os acessos estão de acordo com o que foi determinado nela. É possível existirem diferentes mecanismos que aplicam a mesma política, isso facilita alterar a política e apenas adaptar o mecanismo para implementá-la (JAJODIA; SAMARATI; SUBRAHMANIAN, 1997).

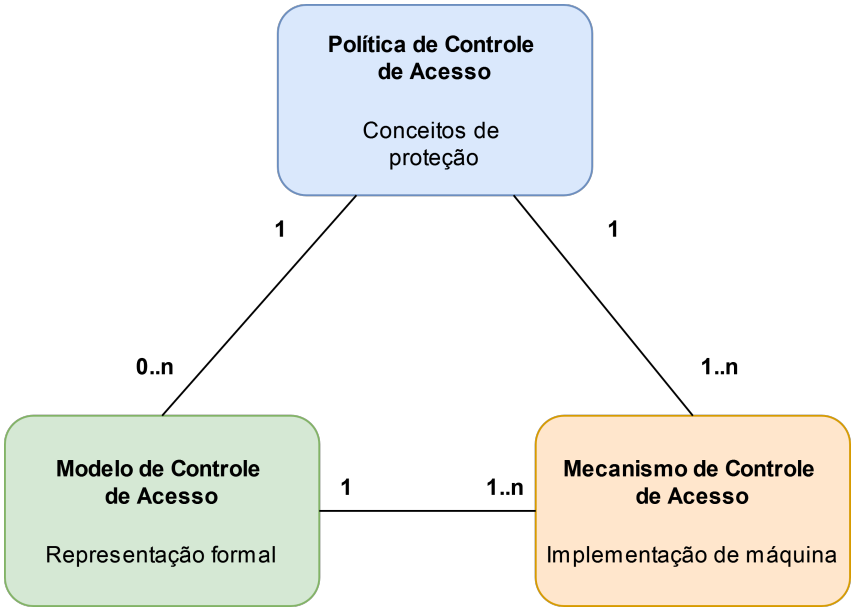
Os conceitos de política, modelo e mecanismo de controle de acesso são frequentemente utilizados de maneira equivocada e seus sentidos acabam sendo intercambiáveis através da literatura. Sendo assim, a Figura 3 apresenta um mapeamento desses conceitos sua inter relação.

Nas próximas subseções serão apresentados as principais políticas e modelos de controle de acessos. Na subseção 2.2.2 será apresentado o Controle de Acesso Discricionário, na subseção 2.2.3 será discutido o Controle de Acesso Obrigatório e na subseção 2.2.4 e subseção 2.2.5 serão apresentados o Controle de Acesso Baseada em Papéis e o Controle de Acesso Baseada em Atributos, respectivamente.

2.2.2 Controle de Acesso Discricionário - CAD

No Controle de Acesso Discricionário (CAD), as decisões de acesso são estabelecidas com base na identidade dos solicitantes - sujeitos - e em regras explícitas que determinam quem tem permissão para realizar ações específicas em recursos específicos - objetos (JAYANT.D et al., 2014). Por exemplo, se utilizado em cenários de controle de acesso de arquivos, apenas os usuários que foram explicitamente autorizados pelo proprietário do arquivo poderão acessá-lo e de acordo com as permissões específicas para cada

Figura 3 – Mapeamento da relação entre política, modelo e mecanismo de controle de acessos.



Fonte: Adaptado de Hu e Scarfone (2012)

usuário e para cada arquivo.

As políticas discricionárias apresentam uma série de desvantagens, tais como:

- Os privilégios de acesso são decididos pelo dono do recurso dificultando garantir a consistência de uma política global de acessos (JAYANT.D et al., 2014).
- Não possui controle do fluxo de informações. Uma informação pode ser copiada de um objeto para outro e ser disponibilizada a outros usuários sem a permissão de seu dono (CHUNG; FERRAIOLO; KUHN, 2006).
- É vulnerável a ataques de programas maliciosos (JAYANT.D et al., 2014) como o *Trojan Horse*. Programas executados em um sistema herdam a identidade de quem os executa (CHUNG; FERRAIOLO; KUHN, 2006), portanto podem explorar as permissões de um determinado usuário a fim de ter acesso e/ou comprometer informações.

Diversos modelos podem representar a política discricionária, entre eles estão a matriz de controle de acesso (subseção 2.2.2.1), a lista de controle de acesso e a lista de capacidades (subseção 2.2.2.2).

2.2.2.1 Matriz de Controle de Acesso

A matriz de controle de acesso é modelo baseado na política *Discretionary Access Control* (DAC) e consiste em uma tabela em que as linhas representam os sujeitos, as

colunas representam os objetos e as entradas consistem nos permissões de acesso que cada sujeito possui sobre cada objeto.

Tabela 1 – Exemplo de matriz de acessos contendo conjunto de autorizações.

	Arquivo A	Arquivo B	Programa A	Programa B
Usuário 1	*read* *write* *delete* *owner*	*read* *write*	*execute*	*write*
Usuário 2	*read* *write*	*read* *write* *delete* *owner*	*read* *execute*	
Usuário 3	*read*	*write*	*read* *write* *execute*	*read* *execute*

Fonte: Elaborada pelo autor.

A Tabela 1 contém um exemplo de matriz de controle de acesso em forma de tabela de autorizações, em que cada usuário possui um conjunto de permissões para cada recurso mapeado. A matriz de controle de acesso também pode ser representada por uma lista de triplas contendo <Sujeito, Objeto, Permissão>.

2.2.2.2 Lista de controle de acessos e Lista de Capacidades

Comumente a matriz de controle de acesso é subdividida por colunas ou linhas. Quando obtidas apenas as colunas denomina-se Lista de Controle de Acesso (ACL) na qual determina para um objeto específico uma lista completa de todos os sujeitos e suas respectivas permissões. Pode ser representada como uma lista de tuplas <Sujeito, Permissão>, conforme Código 2.1

Código 2.1 – Exemplo de uma Lista de controle de acesso

```
1  ACL(Arquivo A) = { Usuário 1 : (read; write; delete; owner);
2                     Usuário 2 : (read; write);
3                     Usuário 3 : (read) }
4
5  ACL(Arquivo B) = { Usuário 1 : (read; write);
6                     Usuário 2 : (read; write; delete; owner);
7                     Usuário 3 : (write) }
8
9  ACL(Programa A) = { Usuário 1 : (execute);
10                     Usuário 2 : (read; execute);
11                     Usuário 3 : (read; write; execute) }
12
13 ACL(Programa B) = { Usuário 1 : (write);
```

```
14                    Usuário 3 : (read;execute) }
```

Quando a matriz é subdividida em linhas dá resulta na Lista de Capacidades (CL) na qual é possível definir para um determinado sujeito todos os objetos e permissões ele possui. Também pode ser representada como uma lista de tupla <Objeto, Permissão>, conforme Código 2.2 (CHUNG; FERRAIOLO; KUHN, 2006).

Código 2.2 – Exemplo de uma Lista de Capacidades

```
1  CL(Usuário 1) = { Arquivo A : (read; write; delete; owner);
2                    Arquivo B : (read; write);
3                    Programa A: (execute);
4                    Programa B: (write) }
5
6  CL(Usuário 2) = { Arquivo A : (read; write);
7                    Arquivo B : (read; write; delete; owner);
8                    Programa A: (read, execute) }
9
10 CL(Usuário 3) = { Arquivo A : (read);
11                   Arquivo B : (write);
12                   Programa A: (read; write, execute);
13                   Programa B: (read; execute) }
```

2.2.3 Controle de Acesso Obrigatório

No Controle de Acesso Obrigatório as decisões de acesso são realizadas por uma autoridade central (CHUNG; FERRAIOLO; KUHN, 2006). Nesse caso, as diretrizes definidas independem da identidade dos sujeitos ou objetos, além disso os usuários e administradores do sistema não possuem autoridade sobre as regras de autorização tampouco podem modificar ou delegar permissões de acesso (MAZIERO, 2020).

As políticas obrigatórias podem ser do tipo multinível ou multilateral. A política multinível categoriza os recursos e os sujeitos em diferentes níveis de acordo com a sensibilidade das informações - e.g *confidencial*, *secret*, *top secret* - e com confiabilidade de cada usuário, a partir dessa classificação é que as autorizações serão concedidas ou negadas.

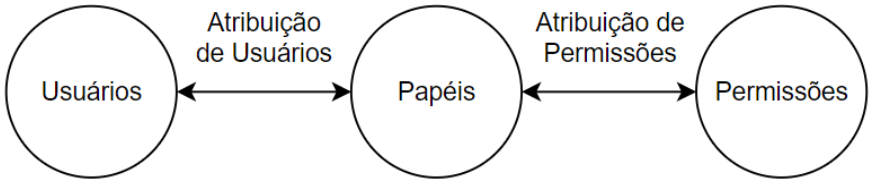
2.2.4 Controle de Acesso Baseada em Papéis (*Role-Based Access Control* - RBAC)

Historicamente, as políticas discricionárias (subseção 2.2.2) e as políticas mandatórias (subseção 2.2.3) surgiram devido às demandas dos setores acadêmicos e militares, respectivamente. Dessa maneira, nenhuma delas satisfez completamente as demandas das organizações comerciais (SANDHU; SAMARATI, 1994). Nesse contexto emergiu a

política baseada em papéis em que as decisões de acesso são definidas conforme o papel que cada usuário performa como parte de uma organização.

No modelo *Role Based Access Control* (RBAC) básico as permissões de acesso são agrupadas por papéis e o uso dos recursos são restritos aos usuários que estão autorizados a serem associados a esses determinados papéis (CHUNG; FERRAIOLO; KUHN, 2006). Conforme Figura 4, as relações entre usuários-papéis e entre papéis-permissões são do tipo muitos para muitos, isto é, vários usuários podem estar associados a vários papéis, da mesma maneira que várias permissões podem ser associadas a vários papéis (FERRAIOLO et al., 2001).

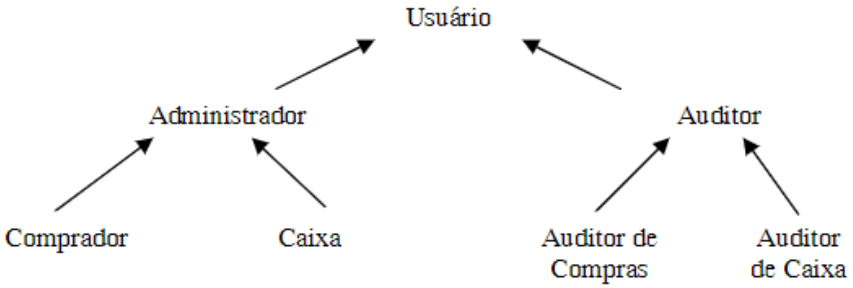
Figura 4 – RBAC básico.



Fonte: Adaptado de Sandhu, Ferraiolo e Kuhn (2000)

Além disso, o modelo RBAC possui algumas outras extensões, tais como: o modelo RBAC hierárquico e o modelo RBAC restrito. O modelo hierárquico viabiliza que um papel possa herdar as permissões associadas a outro papel estabelecendo uma ordem parcial que define uma relação de responsabilidades entre os papéis (FIGUEIREDO; MOTTA, 2007). No exemplo da Figura 5, o papel de *Comprador* possui, no mínimo, todas as permissões do papel *Administrador*, além daquelas específicas do seu papel.

Figura 5 – Exemplo de uma hierarquia de papéis.



Fonte: (FIGUEIREDO; MOTTA, 2007)

Por sua vez, o modelo restrito adiciona ao modelo hierárquico a Separação de Responsabilidades (SR). A Separação de Responsabilidades (SR) baseia-se no princípio de que nenhum usuário deve possuir privilégios suficientes para fazer uso indevido do sistema (CHUNG; FERRAIOLO; KUHN, 2006). Em outras palavras, tem como objetivo

assegurar que fraudes ou danos acidentais não ocorram como resultado de uma excessiva concentração de poder em um único indivíduo. Por exemplo, um usuário autorizado a realizar compras em um sistema não pode ser o mesmo responsável por auditar essas compras, pois isso criaria um conflito de interesses (FIGUEIREDO; MOTTA, 2007). Portanto, essas autorizações devem ser particionadas a fim de não viabilizarem a oportunidade de prejuízos e fraudes.

A Separação de Responsabilidades (SR) pode ser estática ou dinâmica. Na SR estática um usuário que está associado a um papel esse não pode ser associado a outro simultaneamente que cause conflito de interesse. Já na SR dinâmica o usuário pode possui dois papéis conflitantes associados desde que esses papéis não sejam ativados durante a mesma sessão (MELLO et al., 2022).

2.2.5 Controle de Acesso Baseada em Atributos (*Attribute-Based Access Control* - ABAC)

Segundo Chung et al. (2019), em que as decisões de acesso são baseadas em atributos do sujeito a qual solicita o acesso, do objeto a ser acessado ou das condições ambientais em que a requisição foi realizada. Alguns atributos que podem ser considerados ao estabelecer a política são hora do dia, dia da semana, localização geográfica, entre outros (MELLO et al., 2022).

De certa maneira, as *Access Control List* (ACL) e o RBAC podem ser considerados casos particulares de ABAC tendo em vista que nesses modelos são utilizados as atributos de identidade e papéis do sujeito, respectivamente, para as decisões de autorização.

Em cenários empresariais, o conjunto de componentes necessários para implementar o ABAC pode se tornar complexo conforme o aumento da escala exigindo capacidades de gestão complexas as quais garantam a distribuição e consistência das políticas e atributos, bem como o emprego eficaz do mecanismo de controle de acesso em toda a organização (CHUNG et al., 2019).

2.3 Política de Segurança da Informação

Segundo Nieles, Dempsey e Pillitteri (2017b), a segurança da informação consiste na proteção da informação e dos sistemas de informação contra acessos, usos, divulgação, interrupção, modificação ou destruição não autorizados. A segurança da informação é alcançada por meio da implementação de um conjunto adequado de controles, incluindo políticas, regras, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware* (ABNT, 2022b). Conforme Hintzbergen et al. (2018), os princípios fundamentais da segurança da informação são a confidencialidade, a integridade e a disponibilidade

e podem ser definidos da seguinte maneira:

- **Confidencialidade**: se refere ao nível necessário de sigilo a ser aplicado em cada informação com o objetivo de que apenas sujeitos autorizados possam acessá-la.
- **Integridade**: se refere à precisão e consistência com o estado ou informação pretendida. A modificação não autorizada de dados é uma violação à sua integridade. Além disso, a informação pode ser incorreta ou não autentica, mas possuir integridade, ou ser correta e autêntica, mas faltar integridade, visto que esse atributo não está relacionado com a veracidade dos dados, mas sim com sua exatidão do seu estado.
- **Disponibilidade**: se refere à capacidade de assegurar que os usuários autorizados tenham acesso à informação e aos ativos correspondentes sempre que forem requeridos. As características principais da disponibilidade são:
  - **Oportunidade**: a informação está disponível quando necessário.
  - **Continuidade**: a equipe consegue continuar trabalhando no caso de falha.
  - **Robustez**: existe capacidade suficiente para permitir que toda a equipe trabalhe no sistema.

O propósito da Política de Segurança da Informação (PSI) é definir as normas e procedimentos adequados a fim de assegurar a segurança das informações e estabelecer as responsabilidades e estruturas organizacionais relativas à segurança dos ativos das organizações. Portanto, a PSI deve estar alinhada com as ações da empresa, ser clara e concisa de maneira a promover uma fácil compreensão, bem como estar acessível ao público alvo e ser revisada regularmente. (SANTOS, 2014). Além disso, tem como finalidade preservar a confidencialidade, integridade e disponibilidade das informações, descrevendo a conduta adequada para seu manuseio, controle, proteção e descarte.

Em ABNT (2022b) é recomendado que as organizações definam, em mais alto nível, uma PSI que estabeleça a abordagem da organização para gerenciar sua segurança da informação, levando em consideração:

- A estratégia e requisitos de negócios;
- Regulamentações, legislações e contratos;
- Riscos e ameaças atuais e projetados para a segurança da informação.

Além disso, em ABNT (2022b) é orientado que, em um nível mais baixo, a PSI seja apoiada por políticas específicas por tema visando atender às necessidades de determinados grupos-alvo dentro da organização. Como exemplo de possíveis temas de

políticas específicas estão: controle de acesso, gestão de ativos, classificação e tratamento de informações, entre outros.

Existem diversas normas e padrões de segurança que auxiliam na orientação de quais controles podem ser considerados na criação e atualização de uma PSI. Dentre esses padrões destacam-se a ABNT (2022a) e a ABNT (2022b), as quais descrevem requisitos abrangentes para definição, implementação, manutenção e aprimoramento contínuo de Sistemas de Gestão da Segurança da Informação. Além disso, o NIST (2022) fornece diretrizes e controles de segurança da informação que são amplamente reconhecidos e podem ser adaptados ao contexto organizacional e ser utilizado como uma valiosa fonte de orientações e boas-práticas na construção da PSI.

3 PROPOSTA

Este trabalho tem como objetivo definir os critérios mínimos de segurança para arquitetura de um sistema centralizador de gestão de acessos a CPDs em diferentes localidades. Os critérios de segurança devem garantir que as seguintes premissas sejam atendidas:

- Apenas pessoas autorizadas tenham suas credenciais de acesso liberada;
- Deve ser possível a implantação de cadeias de aprovação de acesso com diversos níveis de autorização;
- Deve ser existir separação de responsabilidade entre os solicitantes e aprovadores de acesso.
- Os acessos devem ser concedidos prevendo o tempo a qual estarão disponíveis;
- Os acessos possam ser revogados a qualquer momento;
- Deve permitir observabilidade quanto aos usuários registrados, liberações de acessos e cadeias de aprovação das instalações;
- Deve ser possível auditar as ações de solicitação, gestão de acessos e autorizações;

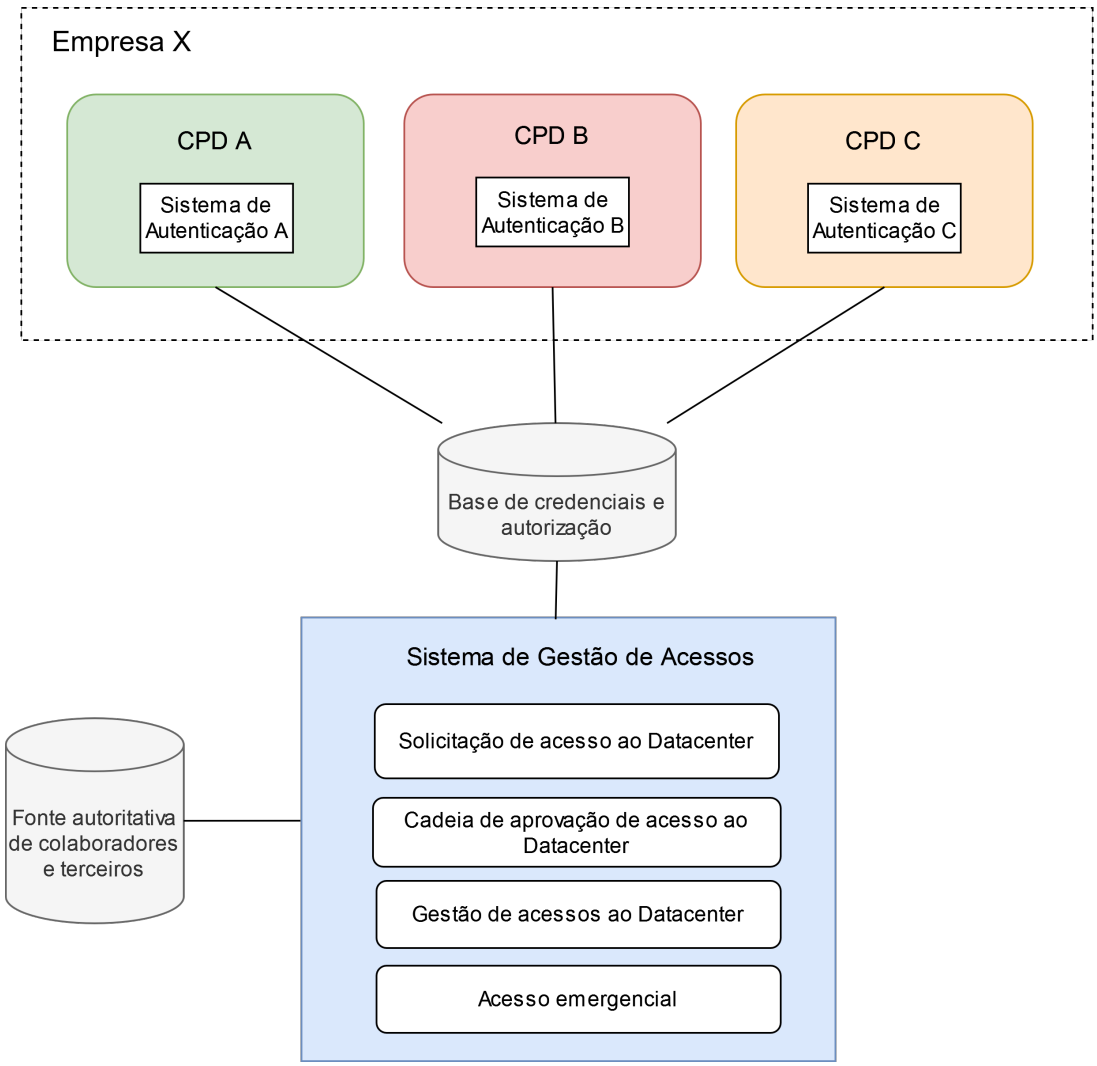
A Figura 6 contém um diagrama com o esquemático de um sistema centralizador que permite a gestão de acessos. Nesse cenário as credenciais de acesso são unificadas em uma base e disponibilizadas para os sistemas de autenticação de cada CPD. Além disso ele deve viabilizar a solicitação de acessos, suportar a gestão das cadeias de aprovação e permitir que acessos emergenciais com tempo de expiração sejam concedidos. Esse sistema estará conectado à fonte autoritativa das identidades dos colaboradores e terceiro.

Os critérios de segurança que serão definidos nesse trabalho devem suportar a criação de sistemas de gestão de controle de acesso de maneira que esteja de acordo com as boas práticas de segurança elencadas nas principais publicações sobre controle de acesso. A próxima seção contém a metodologia que será utilizada nesse projeto.

3.1 Metodologia

Nas seguintes seções estão detalhadas as etapas essenciais para atingir os objetivos definidos, tais como os casos de uso do sistema, o modelo de controle de acesso a ser utilizado, o estabelecimento das cadeias de aprovação, os requisitos de persistência de dados, bem como a trilha de auditoria a ser gerada pelo sistema.

Figura 6 – Arquitetura para solução centralizadora de concessão de acessos e credenciais de CPDs.



Fonte: Elaborado pelo autor

3.1.1 Casos de Uso

Serão criados casos de uso relativos às principais funcionalidades específicas do sistema autorização. Isso permitirá identificar as operações críticas em que são necessárias ações de aprovação hierárquica e etapas extras de segurança. Nesse caso, poderão ser utilizados diagramas *Unified Modeling Language* (UML) ou descrições dos elementos estruturais a fim de representar cada cenário.

3.1.2 Modelo de controle de acesso

Será definido um modelo de controle de acesso que permita a separação de responsabilidades e que evidencie quais atributos são necessários para a execução das operação no sistema.

3.1.3 Fluxo de Cadeia de Aprovação

Será definido um fluxo de cadeia de aprovação estabelecendo quais atores são responsáveis por delegar e autorizar determinada concessão de acesso. Além disso serão definidas ações de solicitação de acesso e definições de novas cadeias de aprovação. Serão utilizados fluxogramas e/ou matrizes de cadeia de aprovação a qual permitam identificar quem são os donos dos recursos e quem são as partes interessadas.

3.1.4 Persistência de dados e mensageirias

Serão definidos os requisitos de segurança para persistência das identidades, credenciais e informações de acesso, tais como serviços de diretórios e/ou base de dados. Além disso, serão estabelecidos os canais de comunicação e notificação dos eventos a serem disparados pelo sistema.

3.1.5 Rastreabilidade e auditoria

Serão definidos critérios e padrões de atributos e ações a fim de gerar rastros de auditoria de maneira que todas as ações críticas possam ser auditadas inequivocamente.

3.2 Cronograma

O desenvolvimento das etapas definidas na seção 3.1 seguirá o seguinte cronograma, conforme Tabela 2

- A1: Elaboração dos casos de uso;
- A2: Definição do Modelo de controle de acesso e persistência de dados e mensageirias;
- A3: Elaboração do Fluxo da Cadeia de Aprovação.
- A4: Definição dos critérios de rastreabilidade e auditoria.

Atividade	Ago.	Set.	Out.	Nov.	Dez.	Jan.
A1	✓	✓				
A2			✓	✓		
A3				✓	✓	
A4					✓	✓

Tabela 2 – Cronograma de atividades

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO IEC 27001*: Segurança da informação, segurança cibernética e proteção à privacidade - sistemas de gestão da segurança da informação - requisitos. [S.l.], 2022. 29 p. 19

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO IEC 27002*: Segurança da informação, segurança cibernética e proteção à privacidade - controles de segurança da informação. [S.l.], 2022. 203 p. 17, 18, 19

CHUNG; FERRAIOLO, D.; KUHN, D. *Assessment of Access Control Systems*. [S.l.]: NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2006. 10, 11, 12, 13, 15, 16

CHUNG et al. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. [S.l.]: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2019. 17

FERRAIOLO, D. F. et al. Proposed nist standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, Association for Computing Machinery, New York, NY, USA, v. 4, n. 3, p. 224–274, aug 2001. ISSN 1094-9224. Disponível em: https://doi.org/10.1145/501978.501980. 16

FIGUEIREDO, B. C.; MOTTA, G. H. Um modelo pragmático de separação de responsabilidades para o controle de acesso baseado em papéis. In: SBC. *Anais do VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. [S.l.], 2007. p. 191–204. 16, 17

GRASSI, P.; FENTON, J.; GARCIA, M. *Digital Identity Guidelines [including updates as of 12-01-2017]*. [S.l.]: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2017. 10

HINTZBERGEN, J. et al. *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018. 17

HU, V.; SCARFONE, K. *NIST Interagency Report 7874, Guidelines for Access Control System Evaluation Metrics*. 2012. 13

ITU. *Security architecture for Open Systems Interconnection for CCITT applications*. 1991. Recommendation X.800. Disponível em: https://www.itu.int/rec/T-REC-X.800-199103-I/en. 10

JAJODIA, S.; SAMARATI, P.; SUBRAHMANIAN, V. A logical language for expressing authorizations. In: *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*. [S.l.: s.n.], 1997. p. 31–42. 12

JAYANT.D, B. et al. Analysis of dac mac rbac access control based models for security. *International Journal of Computer Applications*, v. 104, p. 6–13, 10 2014. 12, 13

MAZIERO, C. *Sistemas Operacionais: Conceitos e Mecanismos*. [S.l.: s.n.], 2020. ISBN 978-85-7335-340-2. 15

MELLO, E. R. 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: Sociedade Brasileira de Computação, 2022. p. 1–50. ISBN 978-85-7669-510-3. Disponível em: https://www.researchgate.net/publication/363644432_Autenticacao_e_Autorizacao_antigas_demandas_no-_vos_desafios_e_tecnologias_emergentes. 11, 17

NIELES, M.; DEMPSEY, K.; PILLITTERI, V. *An Introduction to Information Security*. [S.l.]: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2017. 10

NIELES, M.; DEMPSEY, K.; PILLITTERI, V. *An Introduction to Information Security*. [S.l.]: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2017. 17

NIST, J. T. F. T. I. I. W. G. *Security and Privacy Controls for Information Systems and Organizations*. Gaithersburg, MD, 2022. 19

SANDHU, R.; FERRAIOLO, D.; KUHN, D. The nist model for role-based access control: Towards a unified standard. In: . Proceedings of the Fifth ACM Workshop on Role-Based Access Control (RBAC '00), Berlin, DE, 2000. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916402. 16

SANDHU, R.; SAMARATI, P. Access control: principle and practice. *IEEE Communications Magazine*, v. 32, n. 9, p. 40–48, 1994. 10, 12, 15

SANTOS, E. P. dos. Segurança da informação: Como garantir a integridade, a confidencialidade e a disponibilidade das informações em uma organização educacional privada de teresina/information security: How to ensure integrity, confidentiality and availability of the infor. *Revista FSA (Centro Universitário Santo Agostinho)*, v. 7, n. 1, 2014. 18

WINDLEY, P. J. *Digital Identity: Unmasking identity management architecture (IMA)*. [S.l.]: "O'Reilly Media, Inc.", 2005. 11