

Requerimentos de Segregação de Funções (SoD) & Soluções IAM: Melhor ficar atento às armadilhas

10.04.2024 - V 1.0
Auditório 1 Lado B



SAP® Recognized Services Provider
In Governance, Risk and Compliance

SAP® Recognized Expert (REx)
In Governance, Risk and Compliance

Estande

Área de Exposição

Estande 5



Aguardamos sua visita!

Zero Trust Security

SAP protegido, riscos eliminados!

Soluções para IAM, GRC, IdM, SSO

Riscos SoD & Controles

Redesenho de Perfis

Gestão de Licenças SAP

Suporte AMS especializado

Treinamentos personalizados

50" 4K DE VERDADE É SAMSUNG.

RISCOS SOD COMPLIANCE
IAM EXCELÊNCIA CYBER SECURITY
RISCOS ISO31000 GRC COSO IdM
GOVERNANÇA SUPORTE AMS
OPERADOR DE COMPLIANCE CVM ISO27000 SSO

in TrustSis consultoria

TrustSis

f TrustSis

TrustSis consultoria

CONHEÇA OS DIFERENCIAIS DE SER NOSSO PARCEIRO

Porttus compliance solutions

Folhetos de marketing

TrustSis consultoria

A Inteligência por trás dos controles compensatórios e riscos de segregação de funções (SoDs).

AI

TrustSis e o Poder da INTELIGÊNCIA ARTIFICIAL no Gestão de Riscos SoD

Matriz de Riscos SoD + Controles Compensatórios

A gestão de riscos de segregação de funções (SoD) é crucial para a segurança operacional das empresas, porém, definir controles compensatórios pode ser desafiador sem conhecimento técnico e funcional. A inteligência artificial emerge como solução, oferecendo suporte e agilidade na definição dos controles.

Diferenciais TrustSis

- Metodologia própria para revisão de matriz de Riscos SoD e definição de controles compensatórios.
- Solução sistêmica (GRC Design Studio - GDS) - arquitetura SAAS para facilitar o processo de revisão de matriz e proposta de controles compensatórios.
- Uso da Inteligência Artificial (AI) para revisão e proposta automatizada de controles compensatórios.
- Repertório benchmark [Out-of-the-box] de riscos e controles para ERP, SAP e não SAP.
- 60+ projetos realizados de definição e revisão de matriz de Riscos A, controles compensatórios, e Solução GRC [GRC Builder] para governança de acesso e monitoramento de Riscos SoDs.

Agende uma demonstração conosco agora mesmo e conheça os benefícios de seguir com a TrustSis nessa jornada!

WWW.TRUSTSIS.COM

Tel: (11) 2500-1644 | (11) 93079-1930 | vendas@trustsis.com | @trustsisconsultoria

TrustSis consultoria

Referência em Redesenho de Perfis & Aculturação Corporativa em GRC

Por quem faz da governança seu próprio negócio

Redesenho de Perfis

TrustSis University

O melhor modelo de perfil de acesso SAP para sua organização é aquele que nasce de forma transparente. É só isso, para problemas durante auditorias, é possível para incorporar melhorias contínuas de negócios e ações práticas, garantindo o cumprimento das boas práticas e regulamentações, como SOX e COX, evitando o custo de SoD e acesso indevidos.

Gestão de licenças SAP

Imagine como seria resolver os problemas de segregação de funções SoD em perfil e usuários SAP de maneira simples, rápida e eficiente. SAP tem soluções para identificar e reduzir de custos com licenças e garantir conformidade com auditorias. Agora não é possível, a TrustSis pode ajudar você!

Por que nos escolher?

- Metodologia própria para **redesenho de perfil de acesso**, reduzindo risco de redução de custos com licenças SAP.
- Solução sistêmica GRC Design Studio - GDS - arquitetura SAAS para facilitar o processo de redesenho de perfil.
- 100+ projetos realizados de redesenho de perfil para abrangência SOX, COX e etc.
- Solução GRC [GRC Builder] para governança de acesso e monitoramento de riscos SoD.
- Análise de **riscos SoD** em todos os níveis de acesso e gestão de perfil, durante o projeto.
- Repertório benchmark de perfil por atividade e função para análise e definição correta de perfil.

Entre em contato e saiba mais!

Tel: (11) 2500-1644 | Cel: (11) 93079-1930 | vendas@trustsis.com | trustsis.com

Rua Hilda Del Nero Bolognini, 102, sala 11A, Ed. The One, Jundiaí

Contate-nos e saiba mais! (11) 2500-1644 (11) 93079-1930 vendas@trustsis.com @trustsisconsultoria

Portus Compliance Solutions

DESAFIOS E REQUISITOS "IAM"

Desafios do ciclo de vida dos usuários de negócios

Contratação | **Logon de Acesso** | **Desligamento**

IAM

Autêntica, autoriza, gerencia, monitora e protege o acesso de usuários de sistemas de informação.

Metodologia

Com nossa metodologia Jump Start, podemos ajudar a otimizar a gestão sobre o processo de GRC, IAM, SOX, COX e etc.

A TrustSis é formada por uma equipe de profissionais qualificados e certificados por SAP, com alto nível de profissionalismo e comprometimento com os resultados efetivos de seus clientes.

Principais Funcionalidades

- Governança de acesso e identidades
- Automação da gestão de riscos SoD e controles compensatórios
- Conformidade com controles internos, auditoria, segurança, SOX, CVA, ISOC, LGPD, GDPR, etc.
- Fluxos de aprovação sob medida ao seu processo, através de parametrização
- Experiência de usuário (UX) redimensionada para o usuário

Vantagens:

- Resposta rápida para seus problemas
- Redução de custos com artigos de TI
- Adição simples e acelerada
- Maior valor agregado e resultados eficientes

FALE CONOSCO

(11) 2500-1644
(11) 93079-1930
vendas@portus.com
www.portus.com

Contate-nos e saiba mais! (11) 2500-1644 (11) 93079-1930 vendas@portus.com @trustsisconsultoria

Portus Compliance Solutions

GRC Builder

Gestão de acesso e monitoramento de Riscos SoD

Plataforma SAAS

Conheça a plataforma GRC mais inteligente e com rápida implementação do mercado!

Principais Funcionalidades

- Governança de acesso e identidades
- Automação da gestão de riscos SoD e controles compensatórios
- Conformidade com controles internos, auditoria, segurança, SOX, CVA, ISOC, LGPD, GDPR, etc.
- Fluxos de aprovação sob medida ao seu processo, através de parametrização
- Experiência de usuário (UX) redimensionada para o usuário

Vantagens:

- Resposta rápida para seus problemas
- Redução de custos com artigos de TI
- Adição simples e acelerada
- Maior valor agregado e resultados eficientes

FALE CONOSCO

(11) 2500-1644
(11) 93079-1930
vendas@portus.com
www.portus.com

Contate-nos e saiba mais! (11) 2500-1644 (11) 93079-1930 vendas@portus.com @trustsisconsultoria

TrustSis consultoria

ZERO TRUST SECURITY

SAP protegido, riscos eliminados.

bioLock

Como as capacidades de IAM do BioLock podem ser aplicadas para melhorar a segurança do SAP?

Verificação de ID para funcionários, fornecedores ou clientes.
Análise de comportamento de segurança baseada em dados de SAP.
Resposta rápida para seus problemas.
Redução de custos com artigos de TI.
Adição simples e acelerada.
Maior valor agregado e resultados eficientes.

Hackers não "INVADEM" - Hackers "ACESSAM" - Usando GenPass

5 Níveis Adicionais de Proteção no SAP

1. Proteção de acesso de login SAP
2. Monitoramento de transações (controle granular)
3. Verificação de ID na execução de transações (Branched/Unbranded)
4. Controle Digital (Identificação de Usuário e Contexto)
5. Monitoramento de todos os acessos de usuário

SOB O PRINCÍPIO DA CONFIANÇA ZERO, NENHUM USUÁRIO PODE SER CONFIADO SEM VERIFICAÇÃO!

Quer saber mais? Contate a TrustSis Consultoria!

TrustSis Consultoria | Rua Hilda Del Nero Bolognini, 102, sala 11A, Ed. The One, Jundiaí, Paraíba do Sul - RJ

Tel: (11) 2500-1644 | Cel: (11) 93079-1930 | vendas@trustsis.com | @trustsisconsultoria

TrustSis consultoria

Especializados em serviços de suporte: Célula de Acesso e Célula de Controle

SUPOORTE AMS TRUSTSIS

"MÉTODO OPERADOR DE COMPLIANCE"

OUTRAS EMPRESAS OFERECEM ATENDIMENTO A CHAMADOS, NÓS OFERECEMOS OPERADOR DE COMPLIANCE (GUARDIÃO DAS PRÁTICAS GRC).

DIFERENCIAIS

- Suportamos e consequentemente, conhecemos.
- Serviços sob medida
- Operação Especializada
- Conformidade Contínua

Serviços Oferecidos:

- Gestão de Acesso SAP / não SAP
- Gestão de Identidade IAM / IAM
- Gestão de Segurança (ISO, Zero Trust)
- Criação e manutenção de perfil
- Compliance Owner (Dono de perfil)
- Compliance Owner (Dono de Controles & Riscos)
- ABAP Security Check-point
- Administração e operação GRC

Contate-nos e saiba mais! (11) 2500-1644 (11) 93079-1930 vendas@trustsis.com @trustsisconsultoria

Palestrante



CEO

Claudio Rocha

Sócio fundador da TrustSis
Consultoria

25+ ANOS DE EXPERIÊNCIA EM GOVERNANÇA DE
ACESSO, SEGURANÇA, CONTROLES E RISCOS



FORMAÇÃO

- Bacharel em Análise de Sistemas – USF
- Pós-graduação em Análise de Sistemas - PUCCAMP
- Mestrado em Ciência da Computação (Tese em segurança) – UNICAMP

Esporte favorito



Introdução

Assim como as soluções de ERPs estão para a **gestão dos processos de negócios** (backoffice) de uma organização, as soluções de I&AM estão para a gestão do **ciclo de vida dos usuários de negócios**.

Conteúdo

- ✓ Nossa Empresa
- ✓ Conceitos IAM
- ✓ Desafios, contexto & cenário atual IAM
- ✓ Melhor ficar atento às armadilhas relacionados a requerimentos de Segregação de Funções (SoD) & Soluções IAM



PLATAFORMA IAM PARA
GESTÃO DO CICLO DE VIDA
DO USUÁRIO DE NEGÓCIO



Conteúdo

- ✓ Nossa Empresa

- ✓ Conceitos IAM

- ✓ Desafios, contexto & cenário atual IAM

- ✓ Melhor ficar atento às armadilhas relacionados a requerimentos de Segregação de Funções (SoD) & Soluções IAM

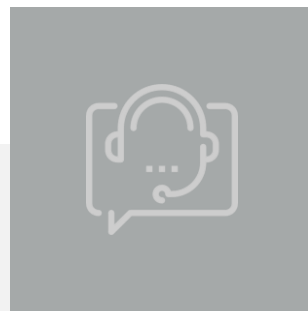
Nossa Empresa

Excelência em GRC e Segurança



Consultoria Implantação

Modelagem de
processos e
implantação de
soluções



Suporte AMS Outsourcing

Mão de obra
especializada
priorizando o retorno
sobre o investimento



TrustSis University

Escola de
conhecimento para o
acultramento
corporativo



Fábrica de Soluções

Resolvendo
problemas com
soluções inovadoras e
personalizadas

TRUSTSIS CONSULTORIA

Oferecemos serviços especializados em suporte, arquitetura, modelagem, gerenciamento, qualidade e projetos de implementação de processos e soluções GRC (Controle de Acesso, Controles Internos e Gestão de Riscos), Gestão de Auditoria, Gestão de Identidade, Single Sign-ON, Redesenho de Perfis e Security, nas áreas de Acesso, Identidade, Riscos, Controles, Auditoria, IAM, Segurança e Segurança Cibernética.



Conteúdo

- ✓ Nossa Empresa

- ✓ **Conceitos IAM**

- ✓ Desafios, contexto & cenário atual IAM

- ✓ Melhor ficar atento às armadilhas relacionados a requerimentos de Segregação de Funções (SoD) & Soluções IAM

Conceitos Diferentes



PRINCIPAIS FUNCIONALIDADES

IDM	IAM	IGA	PAM	CIAM	IDaaS	PIM
●	●	●	●	●	●	●
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○

- Autenticação**
- SSO - Single Sign ON
 - Gerenciamento de sessão
 - Serviço de senha
 - Autenticação forte

IDM	IAM	IGA	PAM	CIAM	IDaaS	PIM
●	●	●	●	●	●	●
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○

- Autorização**
- Baseado em função
 - Baseado em regras
 - Baseado em atributos
 - Autorização remota
 - SoD - Segregação de função

IDM	IAM	IGA	PAM	CIAM	IDaaS	PIM
●	●	●	●	●	●	●
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○

- Gerenciamento de usuários**
- Administração delegada
 - Gerenciamento de IDs e funções
 - Provisionamento
 - Gerenciamento de senhas
 - Self-service

IDM	IAM	IGA	PAM	CIAM	IDaaS	PIM
●	●	●	●	●	●	●
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○

- Repositório Central de Usuários**
- Diretório
 - Sincronização de dados
 - Metadiretório
 - Diretório virtual

IDM	IAM	IGA	PAM	CIAM	IDaaS	PIM
●	●	●	●	●	●	●
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○

- Integrações**
- Azure AD
 - IOT
 - Active Directory (AD)
 - Sistemas eSignature



Conteúdo

- ✓ Nossa Empresa

- ✓ Conceitos IAM

- ✓ **Desafios, contexto & cenário atual IAM**

- ✓ Melhor ficar atento às armadilhas relacionados a requerimentos de Segregação de Funções (SoD) & Soluções IAM

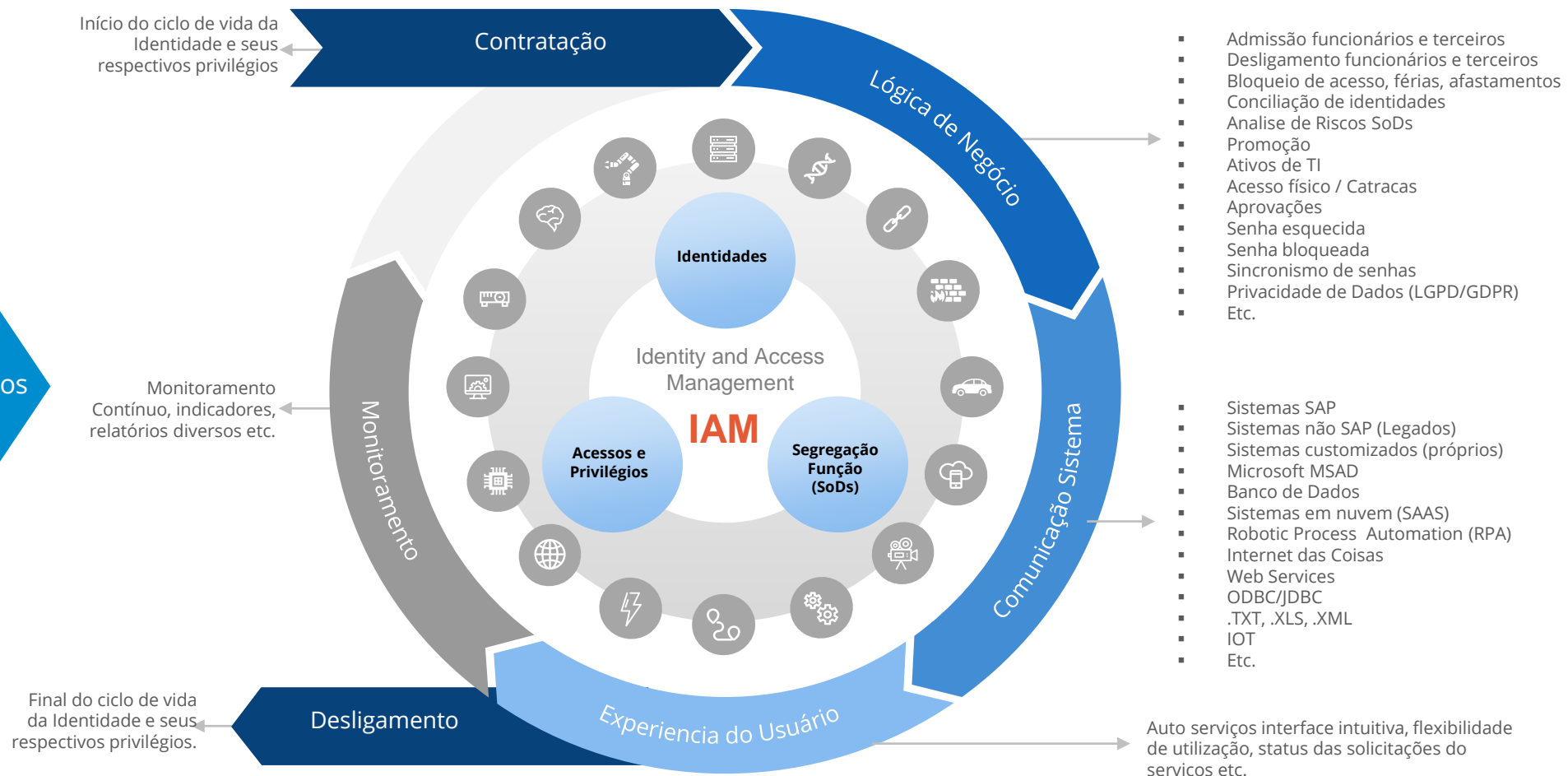
Quais desses conceitos incorporam a gestão da Segregação de Funções (SoD)?



Desafios

Requerimentos de Segregação de Funções (SoD) & Soluções IAM:

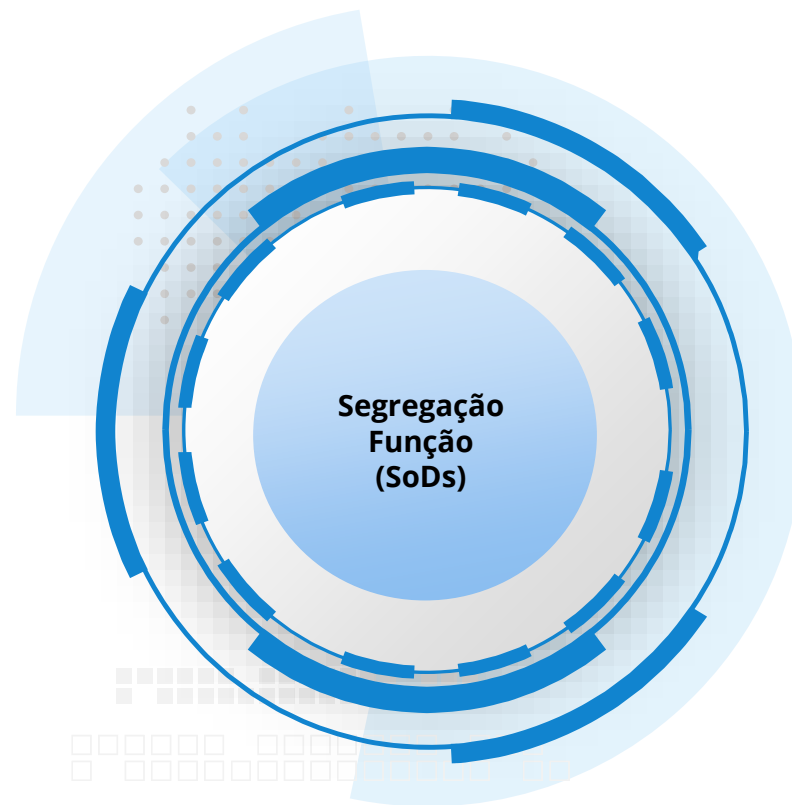
Melhor ficar atento às armadilhas

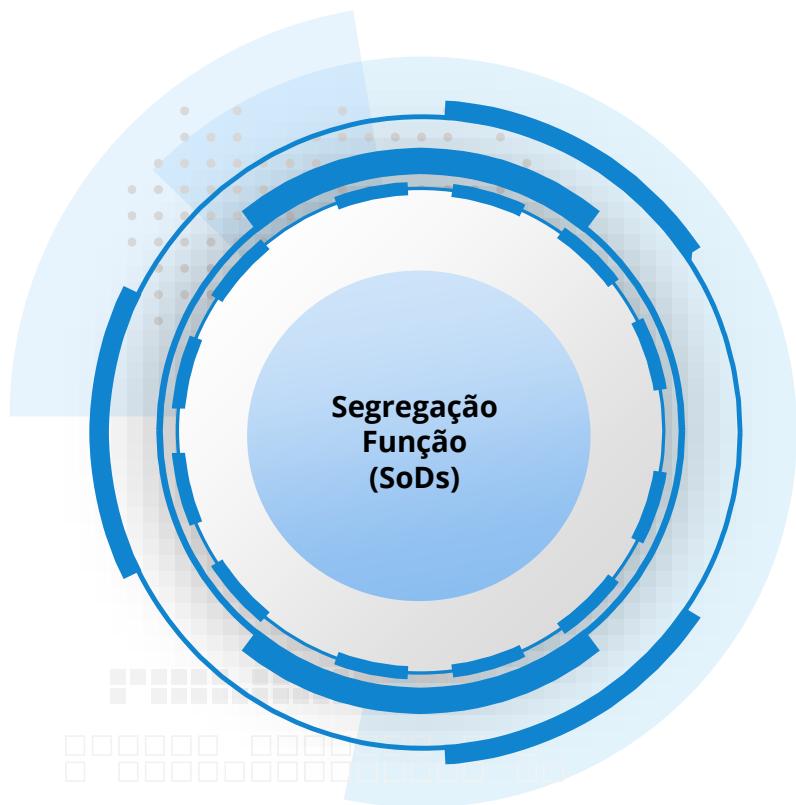


Desafios

Requerimentos de Segregação de Funções (SoD) & Soluções IAM:

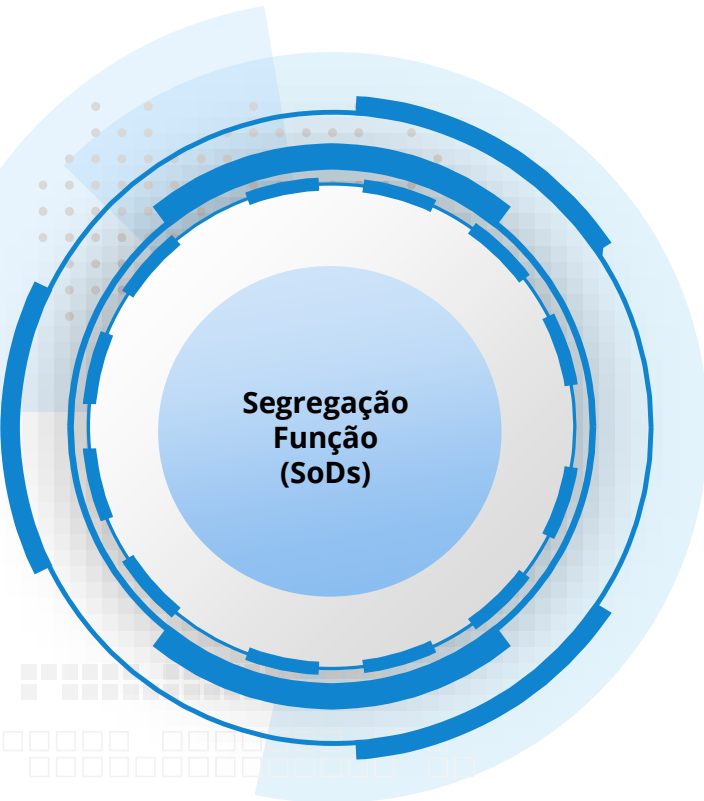
Melhor ficar atento às armadilhas





Definição:

A segregação de função, também conhecida como segregação de deveres ou segregação de funções, é um princípio de controle interno que visa reduzir o **risco de fraude, erro e má conduta** dentro de uma organização.



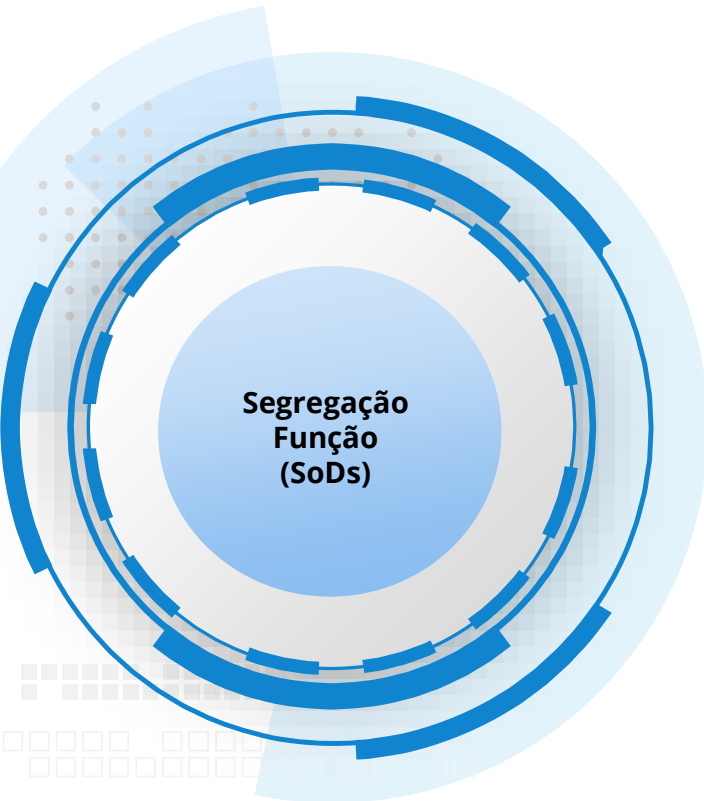
Segregação
Função
(SoDs)

Definição:

A segregação de função, também conhecida como segregação de deveres ou segregação de funções, é um princípio de controle interno que visa reduzir o **risco de fraude, erro e má conduta** dentro de uma organização.

Exemplos de combinações SoDs conflitantes:

- [Aprovação e autorização de transações financeiras com Registro] e [reconciliação de transações financeiras]
- [Recebimento de mercadorias e controle de estoque com Compras] e [seleção de fornecedores]
- [Gestão de caixa e conciliação bancária com Administração de sistemas] e [auditoria interna]



Segregação
Função
(SoDs)

Definição:

A segregação de função, também conhecida como segregação de deveres ou segregação de funções, é um princípio de controle interno que visa reduzir o **risco de fraude, erro e má conduta** dentro de uma organização.

Exemplos de combinações SoDs conflitantes:

- [Aprovação e autorização de transações financeiras com Registro] e [reconciliação de transações financeiras]
- [Recebimento de mercadorias e controle de estoque com Compras] e [seleção de fornecedores]
- [Gestão de caixa e conciliação bancária com Administração de sistemas] e [auditoria interna]

Por que se preocupar com a Segregação de Funções?

- a) Evitar risco de fraude, erro e má conduta
- b) Aplicar as melhores práticas de gestão de acesso
- c) Requerimento legal SOX, CVM
- d) Requisitos de controles internos
- e) Requisitos de segurança da informação
- f) Requisitos de auditoria Interna
- g) outros

Cenário atual

Gestão de Identidade & Gestão de Acesso (foco Riscos SoDs)

Fragmentação do processo

REQUISITOS

PRINCIPAIS REQUISITOS

- Governança de Identidades & acessos
- Melhores práticas de segurança
- Reduzir custo operacional

PRINCIPAIS REQUISITOS

- Governança de Riscos SoDs
- Regulamentação SOX, CVM
- Reduzir custo operacional

PLATAFORMA

Gestão de Identidade

Gestão de Acesso (foco Riscos SoDs)

PROCESSOS

PRINCIPAIS FUNCIONALIDADES

- Repositórios de perfis, grupos e privilégios
- Repositório de usuários vs perfis e grupos associados
- Criar / Bloquear / Desligar Identidade de empregados
- Criar / Bloquear / Desligar Identidade de terceiros
- Bloqueio da conta conforme período
- Bloqueio definitivamente conta e/ou remoção dos perfis de acesso
- Bloqueio imediato da conta
- Redefinir senha de usuário via interface autosserviço
- Acessos aos grupos de AD (pastas) via autosserviço
- Criar / Bloquear / Desligar Identidade de terceiros
- Fluxo de aprovação de solicitação de acesso adicional
- Fluxo de aprovação de solicitação acesso emergencial
- Provisionamento de acesso adicional / emergencial
- Revisão periódico de acesso
- Repositório de evidencias e log de auditoria
- Etc.

PRINCIPAIS FUNCIONALIDADES

- **Repositórios e Riscos SoDs**
- **Repositórios de controles compensatórios**
- Repositórios de perfis, grupos e privilégios
- Repositório de usuários vs perfis e grupos associados
- **Análise de riscos SoDs ad-hoc**
- **Análise de riscos SoDs para solicitações de acessos**
- **Análise de riscos SoDs para manutenção de perfis**
- Fluxo de aprovação de solicitação de acesso adicional
- Fluxo de aprovação de solicitação acesso emergencial
- Provisionamento de acesso adicional / emergencial
- Revisão periódico de acesso “potencial foco em riscos SoDs”
- **Repositório de riscos mitigados (usuários vs. Riscos)**
- **Relatórios analíticos de riscos de usuários**
- **Relatórios analíticos de riscos de perfis**
- Repositório de evidencias e log de auditoria
- Etc.

CONECTORES

PRINCIPAIS SISTEMAS ATENDIDOS

- MS AD , Azure
- ERPs SAP, não SAP
- Sistemas diversos

PRINCIPAIS SISTEMAS ATENDIDOS

- ERPs SAP, não SAP
- Sistemas diversos

DONOS

PRINCIPAIS GERENCIADORES

- Gerente de TI (Acesso, governança, segurança, infraestrutura)

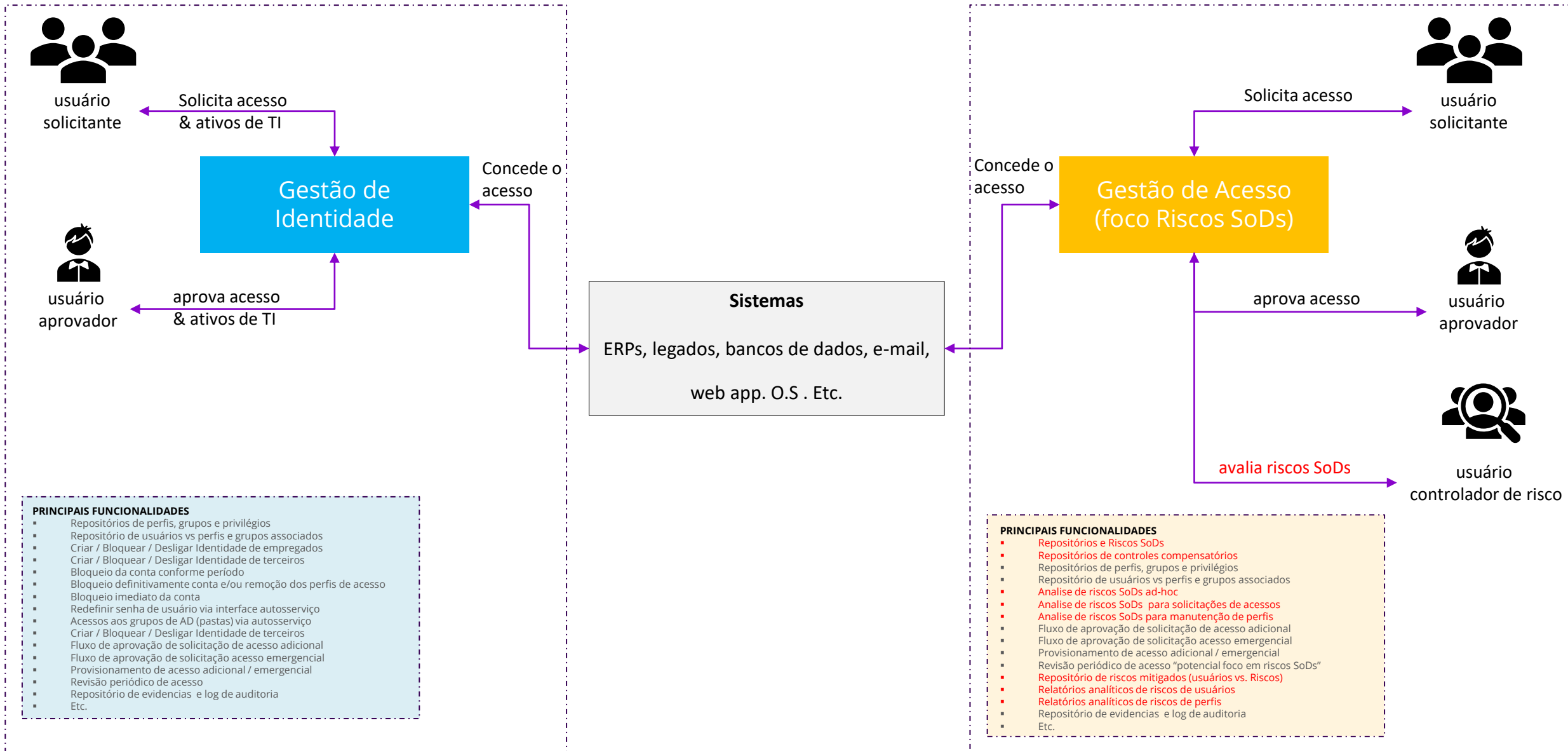
PRINCIPAIS GERENCIADORES

- Gerente de Sistemas (corporativos)

Cenário atual

Gestão de Identidade & Gestão de Acesso (foco Riscos SoDs)

Fragmentação do processo, na prática



PRINCIPAIS FUNCIONALIDADES

- Repositórios de perfis, grupos e privilégios
- Repositório de usuários vs perfis e grupos associados
- Criar / Bloquear / Desligar Identidade de empregados
- Criar / Bloquear / Desligar Identidade de terceiros
- Bloqueio da conta conforme período
- Bloqueio definitivamente conta e/ou remoção dos perfis de acesso
- Bloqueio imediato da conta
- Redefinir senha de usuário via interface autosserviço
- Acessos aos grupos de AD (pastas) via autosserviço
- Criar / Bloquear / Desligar Identidade de terceiros
- Fluxo de aprovação de solicitação de acesso adicional
- Fluxo de aprovação de solicitação acesso emergencial
- Provisionamento de acesso adicional / emergencial
- Revisão periódica de acesso
- Repositório de evidências e log de auditoria
- Etc.

PRINCIPAIS FUNCIONALIDADES

- Repositórios e Riscos SoDs
- Repositórios de controles compensatórios
- Repositórios de perfis, grupos e privilégios
- Repositório de usuários vs perfis e grupos associados
- Análise de riscos SoDs ad-hoc
- Análise de riscos SoDs para solicitações de acessos
- Análise de riscos SoDs para manutenção de perfis
- Fluxo de aprovação de solicitação de acesso adicional
- Fluxo de aprovação de solicitação acesso emergencial
- Provisionamento de acesso adicional / emergencial
- Revisão periódica de acesso "potencial foco em riscos SoDs"
- Repositório de riscos mitigados (usuários vs. Riscos)
- Relatórios analíticos de riscos de usuários
- Relatórios analíticos de riscos de perfis
- Repositório de evidências e log de auditoria
- Etc.

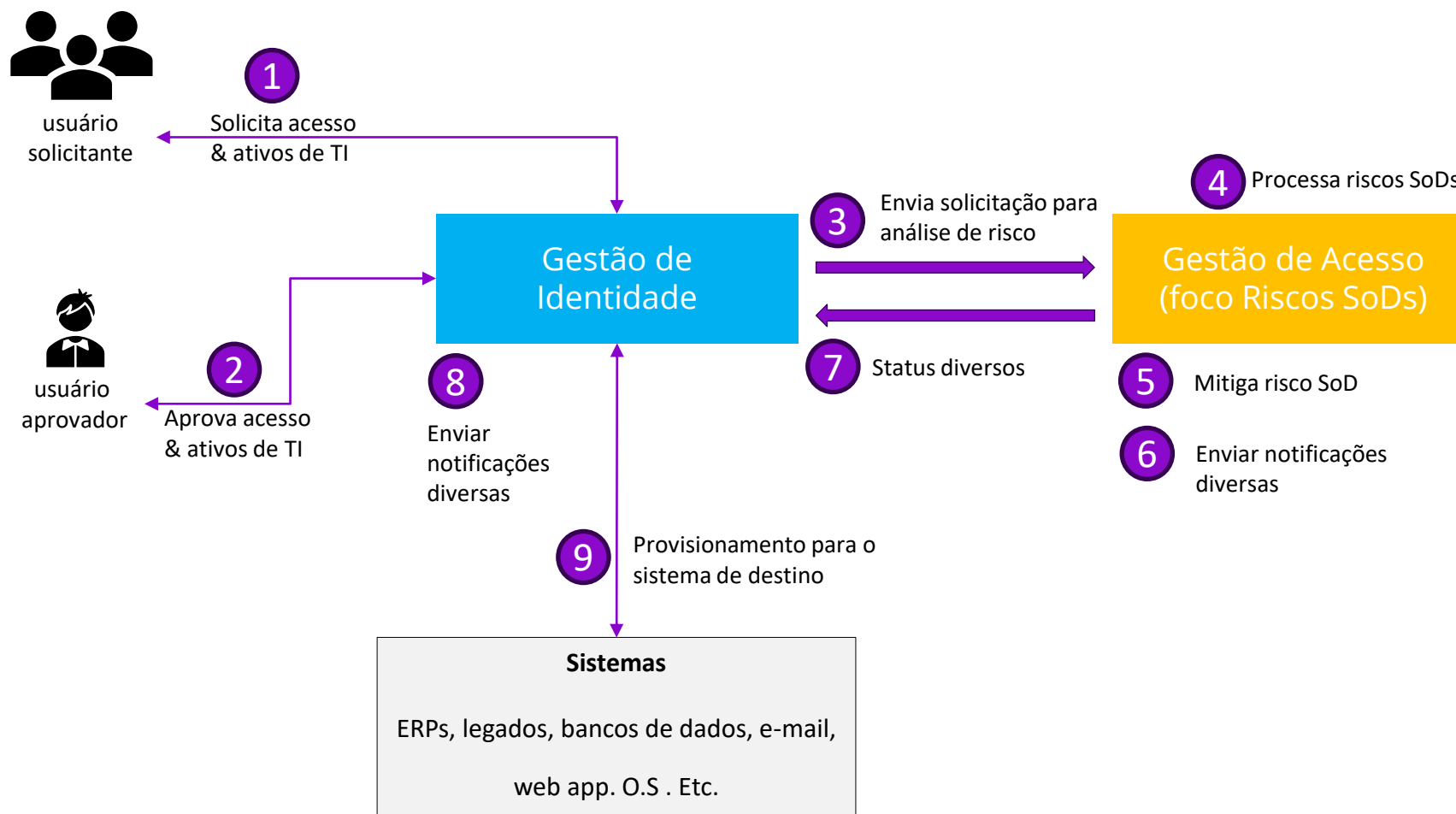
Cenário desejado

Gestão de Identidade & Gestão de Acesso (foco Riscos SoDs)

Melhores práticas - Processos

IAM

Identity and Access Management



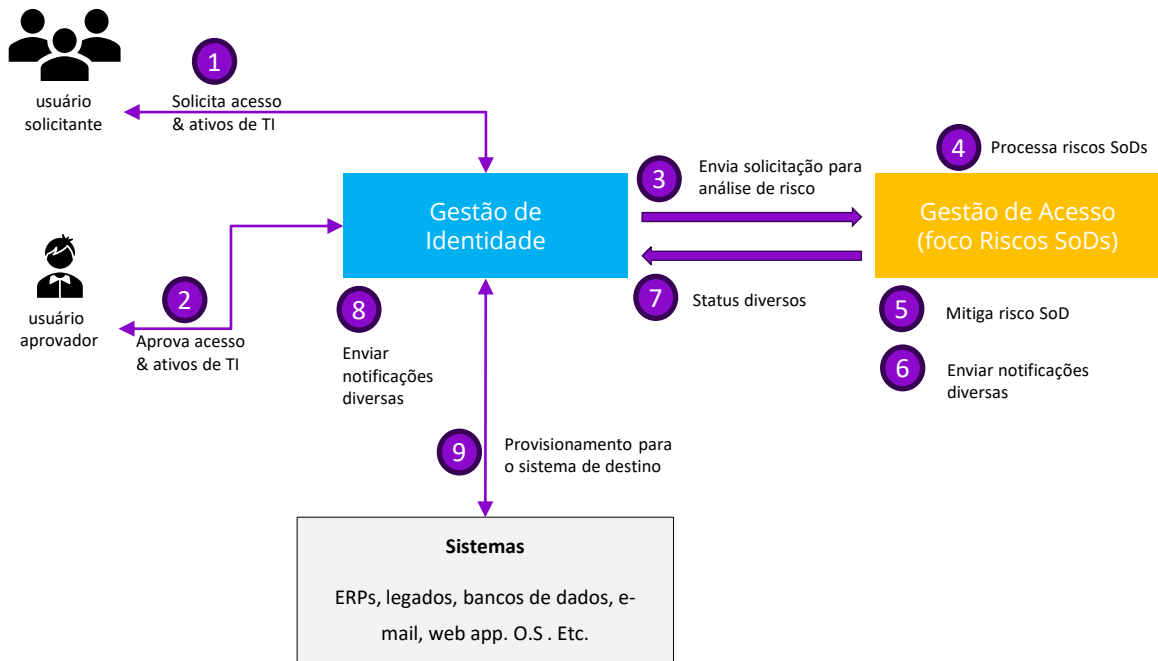
Cenário desejado

Gestão de Identidade & Gestão de Acesso (foco Riscos SoDs)

Melhores práticas - Processos

IAM

Identity and Access Management



5 Considerações importantes

- 1. Não é obrigatório** ter funcionalidades de SoD em soluções de IdM. **Obs.** É possível ter soluções e fornecedores diferentes.
- 2. Evitar o uso de soluções de ITSM** para fornecer funcionalidades de identidade, principalmente relacionadas aos riscos SoDs
- 3. Evitar integrações e replicação de conteúdo de riscos SoDs** quando possível. **Obs.** Unificar a interface nem sempre proporciona a melhor experiência para o usuário.
- 4. Buscar maximizar a integração de notificações e status** para reduzir custos operacionais, garantir rastreabilidade e melhorar a experiência do usuário.
- 5. Obter o melhor resultado na análise de riscos SoDs**, que verdadeiramente representa a exposição do negócio aos riscos.



Conteúdo

- ✓ Nossa Empresa

- ✓ Conceitos IAM

- ✓ Desafios, contexto & cenário atual IAM

- ✓ Melhor ficar atento às armadilhas relacionados a requerimentos de Segregação de Funções (SoD) & Soluções IAM

Obter o melhor resultado na análise de riscos SoDs, que verdadeiramente representa a exposição do negócio aos riscos.

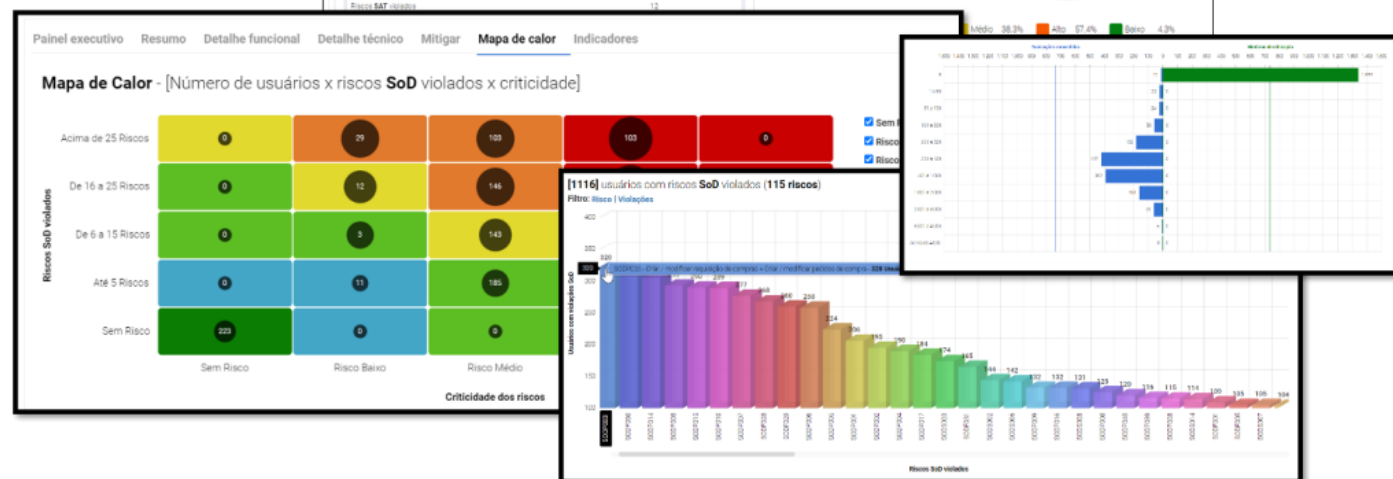
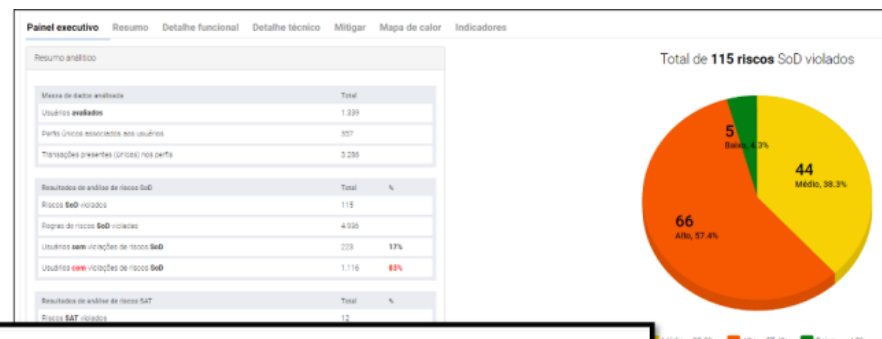
8 Considerações importantes

1. Evitar a construção da matriz de riscos SoDs com base apenas na **combinação de perfis críticos**.
2. Construir a matriz de riscos SoDs observando a arquitetura de segurança e privilégios de cada sistema monitorado
3. **Não desativar riscos** SoDs simplesmente porque não foram violados.
4. Incluir os **desenvolvimentos e personalizações** dos sistemas na matriz de riscos.
5. Garantir que todos os **módulos funcionais** estejam representados na matriz de riscos.
6. **Revisar periodicamente** a matriz de riscos SoDs para adequar sua estrutura ao negócio.
7. Garantir que a matriz de riscos abranja todos os módulos funcionais do sistema monitorado.
8. Estabelecer um processo de conformidade contínua para mantê-la atualizada.



GRC Builder: Uma Abordagem Descomplicada

O GRC Builder é uma solução de arquitetura SAAS com licenciamento por subscrição, moderna e intuitiva que facilita a análise, governança de acesso, gerenciamento e monitoramento de conflitos de segregação de funções (riscos SoDs).



8 Considerações importantes: [GRC Builder já atende as considerações importantes](#)

1. Evitar a construção da matriz de riscos SoDs com base apenas na combinação de perfis críticos.
2. Construir a matriz de riscos SoDs observando a arquitetura de segurança e privilégios de cada sistema monitorado
3. Não desativar riscos SoDs simplesmente porque não foram violados.
4. Incluir os desenvolvimentos e personalizações dos sistemas na matriz de riscos.
5. Garantir que todos os módulos funcionais estejam representados na matriz de riscos.
6. Revisar periodicamente a matriz de riscos SoDs para adequar sua estrutura ao negócio.
7. Garantir que a matriz de riscos abranja todos os módulos funcionais do sistema monitorado.
8. Estabelecer um processo de conformidade contínua para mantê-la atualizada.

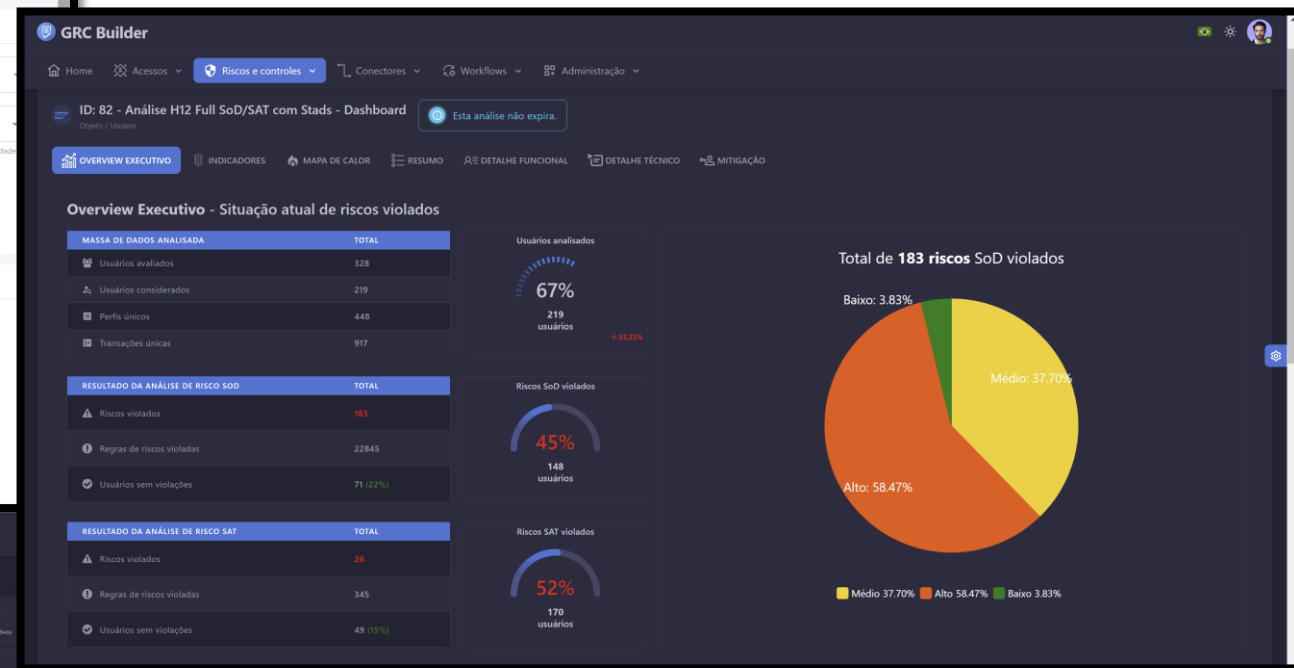
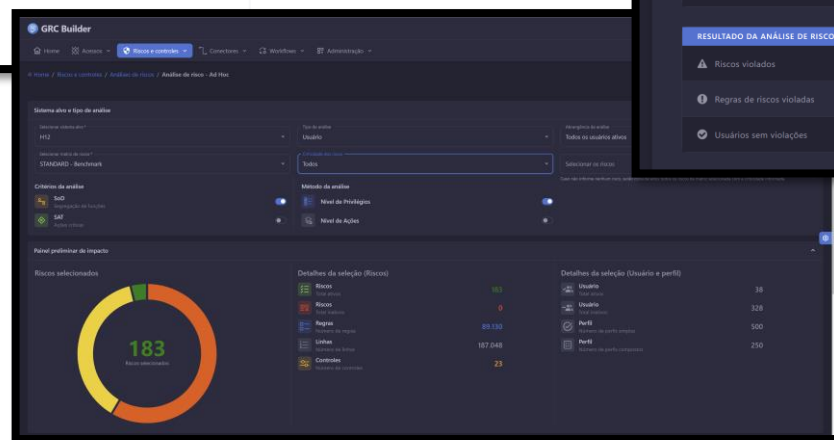
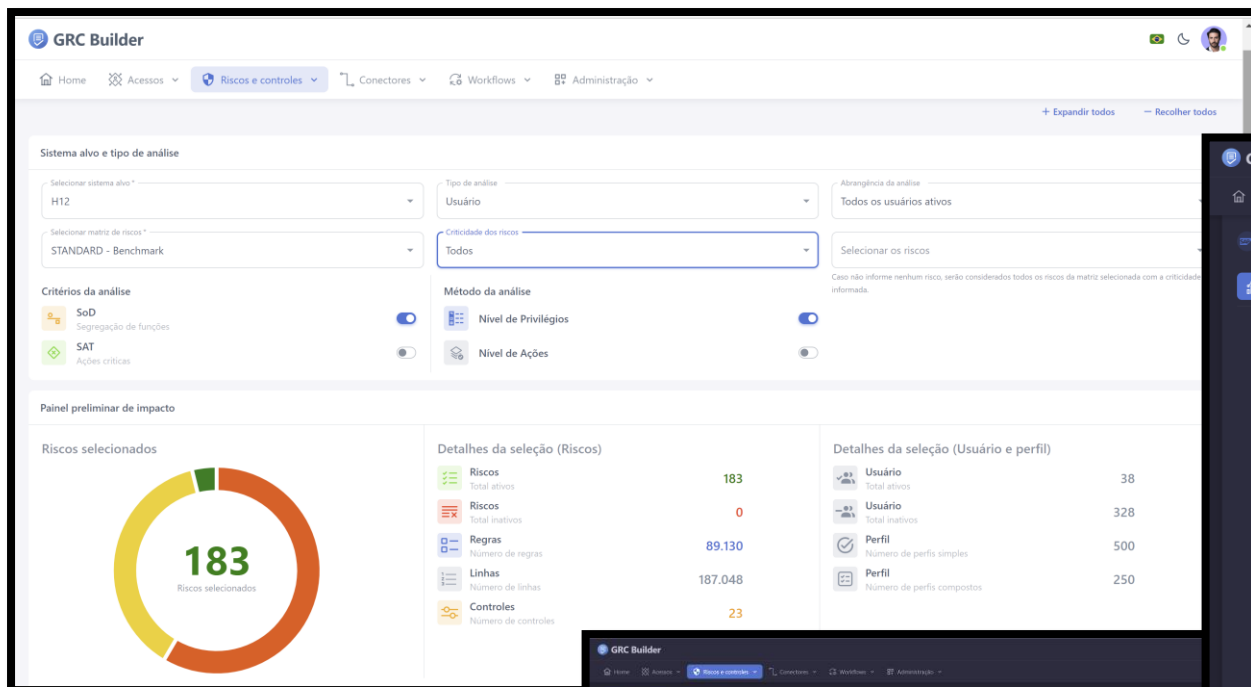
Solução



GRC Builder

Gestão de Acesso e monitoramento de Riscos SoDs

Exemplos de interface modo escuro



Estande

Área de Exposição

Estande 5



Aguardamos sua visita!

Zero Trust Security

SAP protegido, riscos eliminados!

TrustSis consultoria

Soluções para IAM, GRC, IdM, SSO

Riscos SoD & Controles

Redesenho de Perfis

Gestão de Licenças SAP

Suporte AMS especializado

Treinamentos personalizados

RISCOS SOD COMPLIANCE
IAM EXCELÊNCIA CYBER SECURITY
RISCOS ISO31000 GRC COSO IdM
GOVERNANÇA SUPORTE AMS
OPERADOR DE COMPLIANCE CVM ISO27000 SSO

TrustSis consultoria TrustSis consultoria TrustSis

TrustSis consultoria

CONHEÇA OS DIFERENCIAIS DE SER NOSSO PARCEIRO

Porttus compliance solutions

Obrigado

Endereço

Edifício The One Office Tower
Rua Hilda Del Nero Bisquolo, 102, Conj.
1114 e 1116 – Anhangabaú Jundiaí – SP.
CEP: 13208-703

Telefone & e-Mail

Claudio Rocha
Sócio Diretor
Claudio.rocha@trustsis.com
+55 11 98962-1019 / +55 11 2500-1646



Mídias Sociais

www.trustsis.com

www.linkedin.com/company/trustsis

Youtube.com/trustsisconsultoria

Facebook.com/trustsis