corpia

GOVERNANÇA DE IDENTIDADE

GESTÃO DE PERFIL DE ACESSO

MINDSEC
SEGURANÇA E TECNOLOGIA

DINAMIO

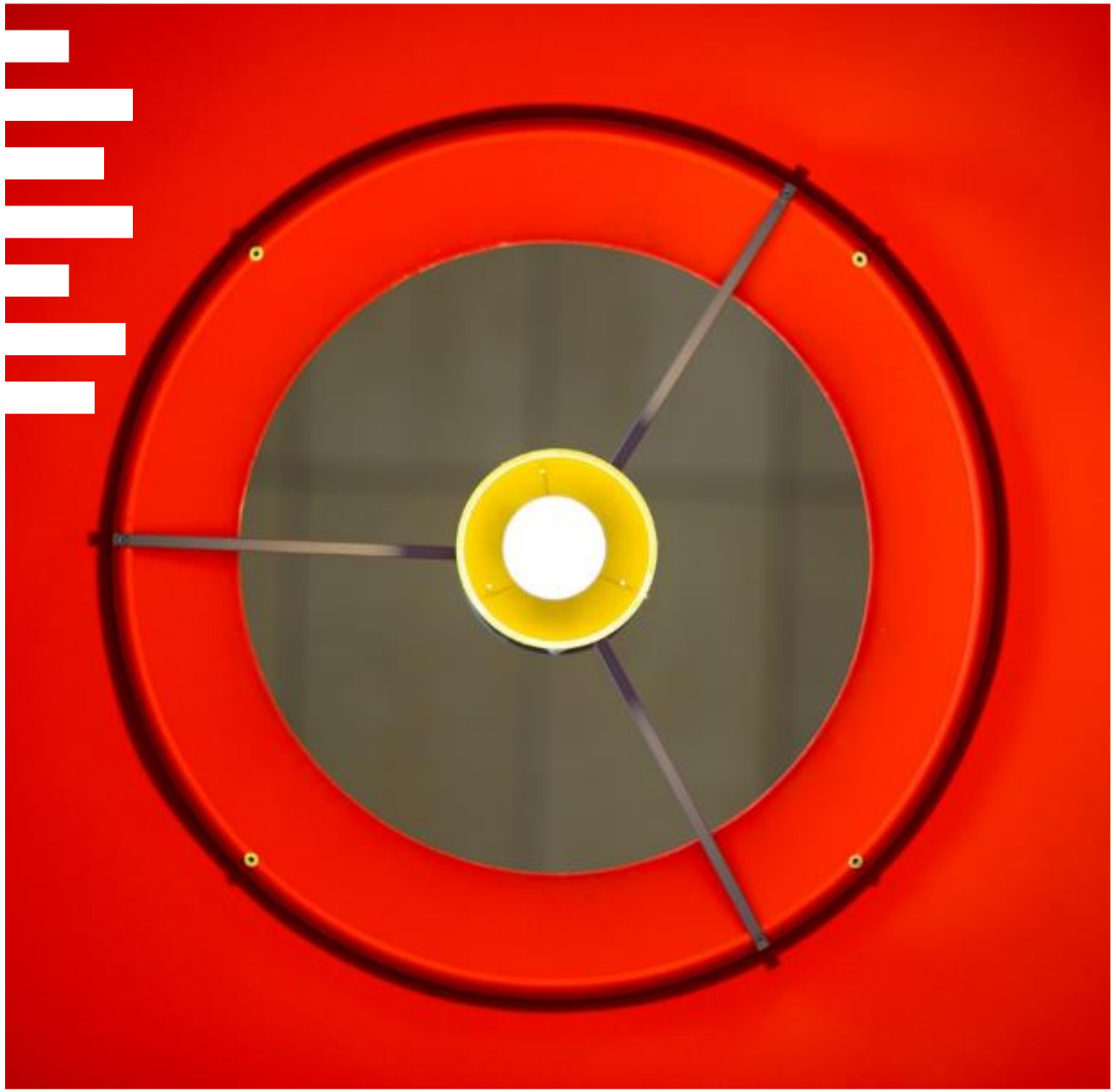
MINDSEC / DINAMIO

MINDSEC com 8 anos de mercado, possui experiência em serviços e consultorias para implementações de gestão de identidade e perfilamento de acessos, governança de SI, vCISO, LGPD, Pen Test, monitoração, treinamentos de conscientização e Mock Phishing. Além de oferecer a seus clientes solução de Corpia, CrowdStrike, Proofpoint, HSC, Comodo, Senhasegura

DINAMIO, com 23 anos de mercado, entrega para seus clientes tecnologias Corpia, Microsoft, Citrix, Kaspersky, Veeam e Forcepoint focadas em Segurança, Produtividade e Redução de custos. Possui serviços de Managed Services para operações e suporte ao ambiente de TI 24x7. Além de revender diversas outras marcas de softwares como Adobe, Corel, etc.

DESAFIOS

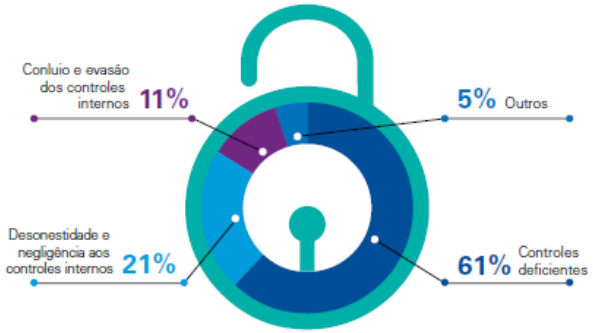
O QUE TE ESPERA ?



CONTROLE DE ACESSOS MANUAL

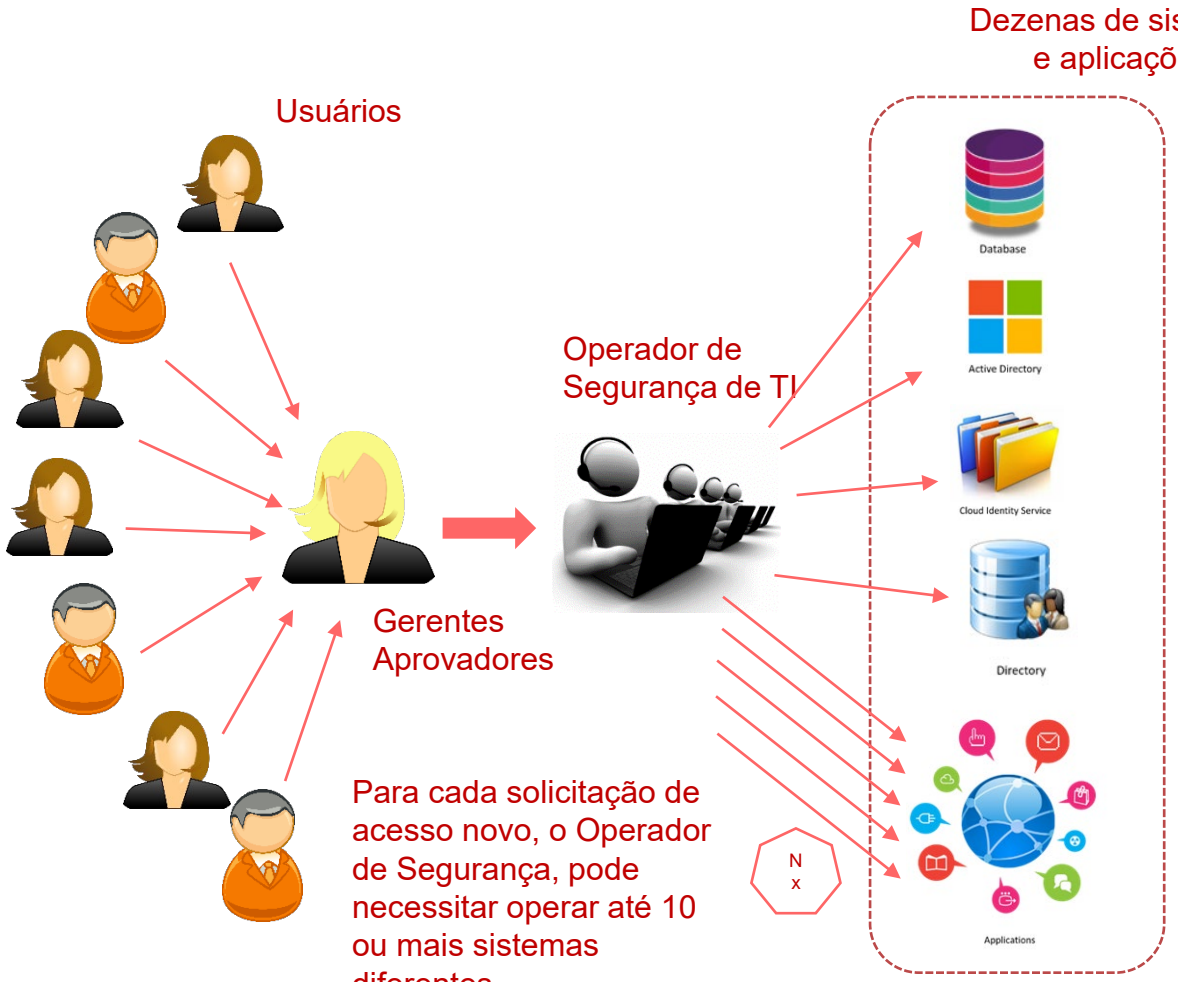
Devido ao processo manual e ao alto workload gerado pelo processo de gestão de identidade e acesso, estima-se que ***28% das empresas não adotam controles efetivos de gestão de acesso***

61% das ocorrências de Segurança são devidas a controles deficientes



Em empresa de grande porte, cada usuário pode chegar a ter 10 ou mais senhas diferentes

Ao longo dos anos, os usuários acumulam perfis com acessos desnecessários e conflituosos difíceis de serem identificados.



Para cada solicitação de acesso novo, o Operador de Segurança, pode necessitar operar até 10 ou mais sistemas diferentes.

DESAFIOS DA GESTÃO DE IDENTIDADE

A gestão de Identidade trás à área de Segurança diversos desafios.

1. **Alta quantidade de sistemas:** as empresas em geral possuem dezenas de sistemas, com bases de usuários e administração individualizados, que necessitam serem gerenciados simultaneamente. Poucos utilizam autenticação centralizada no Windows ou outro sistema de autenticação.

2. **Falta de visão unificada:** devido a não centralização e integração dos sistemas de autenticação de usuários, é praticamente impossível ter uma visão unificada que facilite gestão e de identidade e acessos, gerando alta demanda operacional e baixa efetividade de controles;

3. **Acumulo de acessos:** Com necessidade de gerenciamento de diversos sistemas de forma manual e a falta de processos de exclusão de acessos, ao longo do tempo, o usuário acumula acessos desnecessários à sua função atual, podendo gerar situações conflituosas de permissionamento;

4. **Falta de integração com RH:** o processo manual de gestão de identidade dificulta a integração com os processos de gestão de pessoas de RH, dificultando a concessão e exclusão de acessos quando da admissão, férias, transferência ou desligamento de funcionários;

5. **Registro e Monitoramento:** o processo manual de gestão de identidade torna quase impossível o gerenciamento de logs de registros de acessos e o monitoramento de acessos indevidos, causando grande risco operacional para as áreas de negócio;

6. **Compliance:** o processo manual de gestão de identidade dificulta a manutenção de controles efetivos de acesso, podendo expor a empresa à aderência de normas e regulamentações do setor e a boas práticas de proteção e sigilo da informação.

DESAFIOS DA GESTÃO DE IDENTIDADE

Para o processo de melhoria na gestão de Identidade é necessário:

1. **Tecnologia madura:** é necessário realizar estudo para certificar-se do uso das melhores tecnologias quem se adapte ao ambiente da empresa e não o contrário, como a integração e padronização dos diversos sistemas de autenticação de usuários;

2. **Processos bem mapeados:** é necessário levantar todos os processos de integração, aprovações, revogações, autoatendimento e demais fluxos necessários que suportem o processo de gestão de identidade;

3. **Implantação de uma cultura interna:** é necessário realização de fóruns de alinhamentos legais e de gestão e pessoas, treinamentos, envio de e-mails explicativos e ampla divulgação dos processos;

4. **Gestão de Perfis:** é recomendado que o mapeamento de perfis funcionais junto as políticas adotadas pelo RH e as áreas usuárias e alinhá-los processos de concessão de acessos;

5. **Exceções:** a implementação de processos de gestão de identidade e acessos deve ter seu processo de exceção mapeado e estabelecido, para atender às solicitações especiais ou que não requeiram ou não possam ser padronizadas;

6. **Terceiros:** é necessário ter processos integrados, definidos e claros para o tratamento de acessos de colaboradores terceirizados.

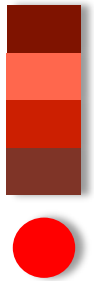
7. **Registros de Logs e Monitoração:** para uma implementação efetiva de gestão de identidade é necessário avaliar e considerar as implementações de registros de operações e alertas automáticos para monitoração e comportamentos anômalos.

EXISTE SOLUÇÃO

Projeto de Perfil de Acesso *é um dos projetos mais importantes no processo de gestão de identidade e que dá suporte operacional tanto para o processo Manual como para o processo Automatizado de gestão de identidade.*

No processo de concessão de acesso baseado em perfil, o usuário ganha ou perde acesso de acordo com a necessidade de sua função na área onde se encontra alocado.

O processo de perfil integra a gestão de pessoas realizadas pela área de RH com a gestão de acesso de recursos necessário para a função exercida pelo colaborador.

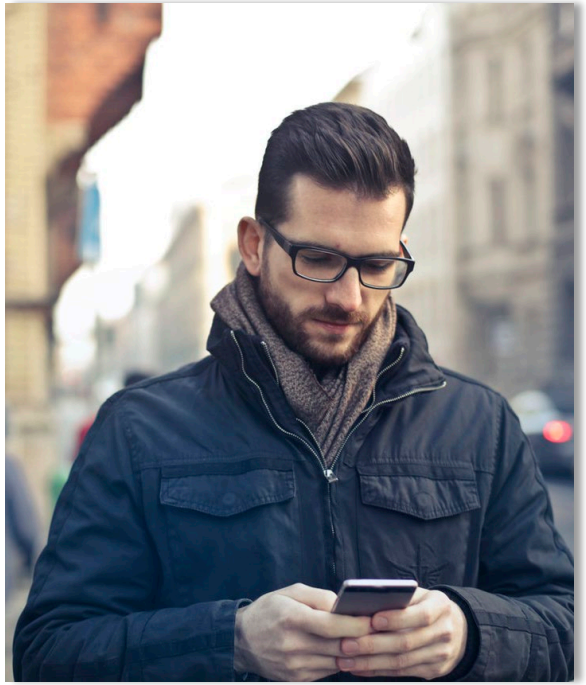


PERFIL ACESSO

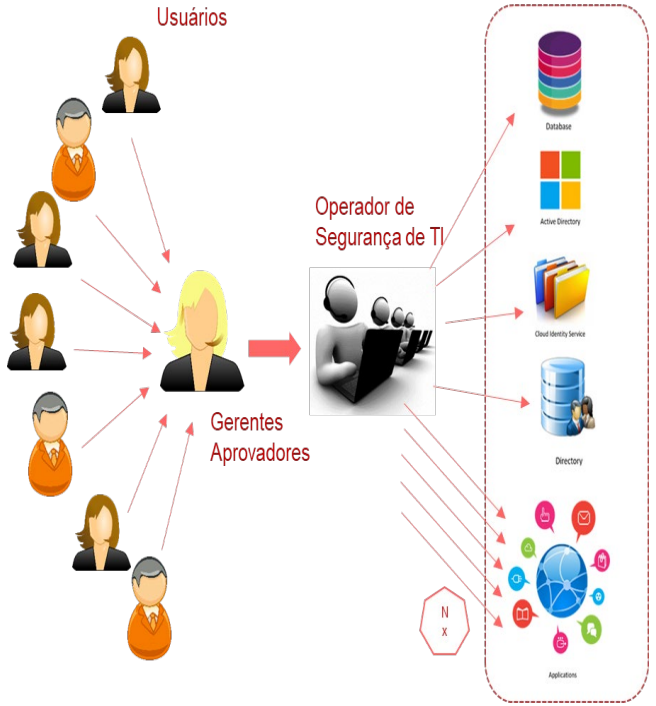
Estruturação da Gestão de Acesso baseado no Perfil
Funcional (ou Cargo) e área/local do colaborador !

CONCESSÃO ATUAL

Esforço Operacional



- ✓ **Coordenador de Segurança Lógica** = Tem que autorizar o acesso a vários sistemas/perfis por Usuário;
- ✓ **Proprietário** = Tem que aprovar as solicitações para cada novo usuário que vai acessar o Sistema/Perfil de sua responsabilidade;
- ✓ **Gestor** = Tem que enviar o "De acordo" por e-mail para cada perfil solicitado;
- ✓ **Segurança da Informação** = tem que validar todos os acessos;
- ✓ **Há dificuldade no controle e na Revisão** (Recertificação) dos acessos.



PERFIL DE ACESSO

Usuários

AGRUPAMENTOS POR **FUNÇÃO**

ATENDENTE

OPERADOR

AGRUPAMENTOS POR **LOCAL**

FINANCEIRO

CONTAS A PAGAR

PERFIL

ATENDENTE FINANCEIRO	Sistema 1 Sistema 2 Sistema 3 Sistema 4
ATENDENTE CONTAS A PAGAR	Sistema 1 Sistema 2 ~~Sistema 3~~ ~~Sistema 4~~
OPERADOR FINANCEIRO	Sistema 1 ~~Sistema 2~~ ~~Sistema 3~~ Sistema 4
OPERADOR CONTAS A PAGAR	~~Sistema 1~~ ~~Sistema 2~~ Sistema 3 Sistema 4

CONCESSÃO

VISÃO PROCESSUAL

CONSTRUÇÃO PERFIL

Para a construção do Perfil de Acesso, o Gestor e Dono do Recurso aprova previamente a concessão para quem estiver no local e função definida.

Para as solicitações manuais, os pedidos são imediatamente enviados para aprovações do Gestor da Área e Dono do Recurso

SOLICITAÇÃO PERFIL

Quando automatizado, ao ser cadastrado do sistema de RH, será concedido automaticamente os perfis pre-definidos

Usuário ou seu Gestor pode solicitar o Perfil de Acesso baseado na função e local onde estará locado

AUTOMATIZAÇÃO

O Sistema de IDM conecta-se a todos os sistemas que necessitam ter acessos gerenciados através de APIs de conexão, a ter um perfil aprovado por processo automático ou por fluxo de concessão o IDM conecta-se ao sistema e concede ou exclui o acesso

ALTERAÇÃO DE ACESSOS

Quando o usuário muda de uma localidade para outra ou de uma função para outra, o IDM automaticamente recebe esta Informação do sistema de RH, exclui os acessos antigos e concede os novos acessos requeridos à nova função e local.

Tratamento de exceção é feito via Solicitação avulsa e aprovado pelo Gestor e Dono do Recurso

VISÃO DO ADMISTRADOR

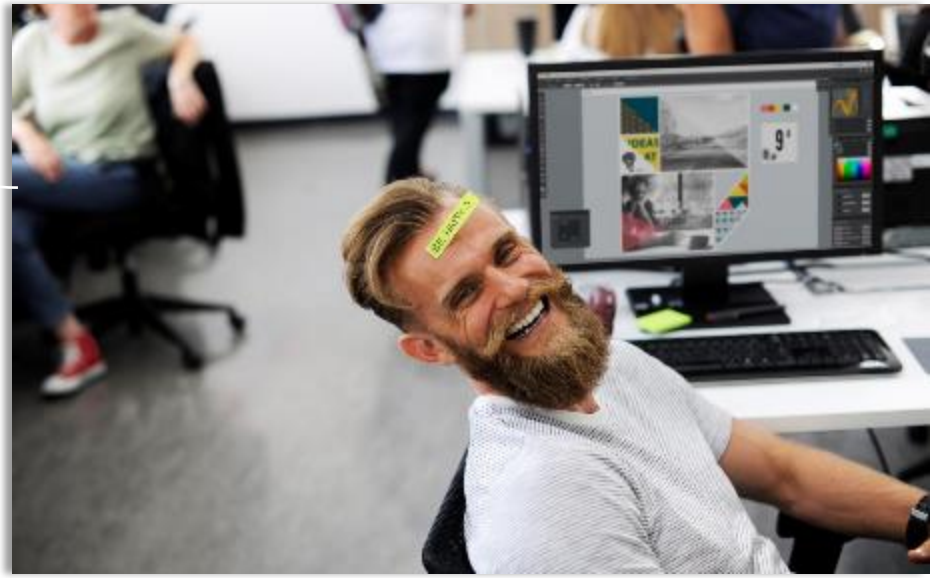
Como o usuário passa a ver a gestão de acesso

ADMINISTRADOR

- ✓ PLANEJAMENTO DOS ACESSOS UMA ÚNICA VEZ, FACILITANDO O CONTROLE E A GESTÃO;
- ✓ OS ACESSOS JÁ FICAM DISPONÍVEIS AUTOMATICAMENTE;
- ✓ TODOS OS ACESSOS SÃO REMOVIDOS NO CASO DE TRANSFERÊNCIA DE ÁREA
- ✓ REALIZA REVISÃO DE PERFIL ANUALMENTE
- ✓ BLOQUEIO AUTOMÁTICO

PERFIL DE ACESSO

- ✓ Agrupamento de acessos pré-definidos, baseados em local x função.
- ✓ São alterados quando necessário
- ✓ São sujeitos a revisão Anual



VISÃO DO USUÁRIO

Como o usuário passa a ver a gestão de acesso

USUÁRIO

- ✓ AO CHEGAR EM SEU POSTO DE TRABALHO JÁ POSSUI OS ACESSOS NECESSÁRIOS
- ✓ SOLICITA NOVO PERFIL OU ACESSO DE EXCEÇÃO
- ✓ AGUARDA APROVAÇÃO E CONCESSÃO DOS ACESSOS
- ✓ UTILIZA NOVOS ACESSOS

PERFIL DE ACESSO

- ✓ Agrupamento de acessos, baseados em local x função, necessário para exercer sua função.
- ✓ Exceções são solicitadas a parte

SEGREGAÇÃO DE ACESSOS

SEGREGAÇÃO DE FUNÇÕES

O objetivo da separação de responsabilidades / segregação de funções é garantir que não haja quebra de segurança na organização ou processos fraudulentos

CARGO ou FUNÇÃO

LOCAL X CARGO ou LOCAL X FUNÇÃO

Cada opção tem o seu benefício, deve ser utilizado de acordo com o perfil da empresa

Local x Cargo

- ✓ Locais diferentes podem ter o mesmo cargo
- ✓ Mesmo cargo não pode requerer acessos diferentes dentro da mesma área
- ✓ Cargos diferentes podem requerer o mesmo acesso
- ✓ *Recomendado para empresas onde cada exerce uma função distinta*

Local x Função

- ✓ Mesmo local pode ter diversas Funções
- ✓ Mesma Função pode ser concedida a mais de um local
- ✓ Função pode conter cargos diferentes
- ✓ Função é independente do Cargo
- ✓ *Recomendado para empresas onde existam diferentes cargos exercendo a mesma Função*

BENEFÍCIOS

Planejamento dos acessos uma única vez, facilitando o controle e a gestão;

Os acessos já ficam disponíveis para cada grupo automaticamente;

Todos os acessos são removidos no caso de Transferência de área;

Agilidade na concessão e revogação de acesso;

Possibilidade e automatização do processo de gestão de acessos;

Maior qualidade e controle sobre os acessos existentes na organização;

PROJECT PHASES

MAPEAMENTO

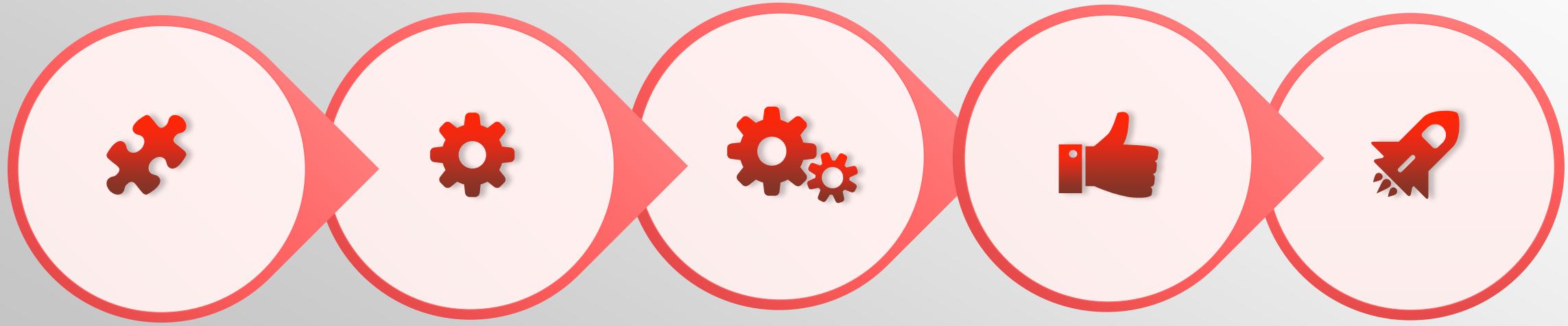
Realização de entrevistas e verificações sistêmicas para o mapeamento de grupos de acesso existentes e necessários. O Objetivo é identificar nas especificações de atribuição funcional as informações necessárias para a definição do *Perfil Funcional*..

PERFIL FUNCIONAL

Planilhamento dos perfis x funcionalidades requeridas, definindo assim o Perfil por “ator”

IMPLANTAÇÃO

Rollout de implantação dos perfis funcionais



REQUISITOS FUNCIONAIS

Identificar os requisitos funcionais de cada posição e área, relacionando as funcionalidades a cada “ator” no processo

TESTES FUNCIONAIS

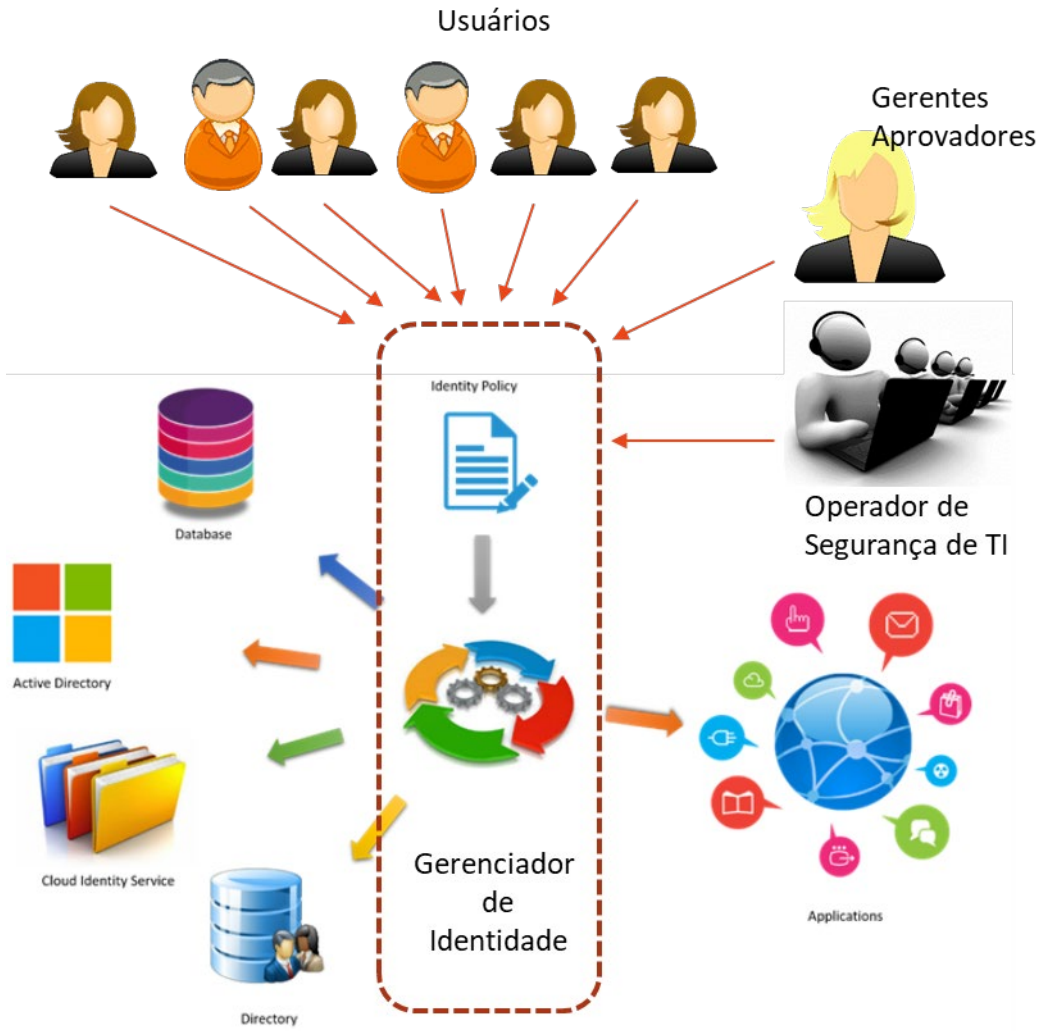
Planejamento e realização de testes de validação dos perfis funcionais definidos na etapa anterior

IDENTITY MANAGEMENT

GERENCIADOR DE IDENTIDADE E ACESSOS IDM

Através do sistema de Gestão de Identidade e Acesso:

- Automatiza-se o processo de concessão e revogação de acessos;
- Automatiza-se as solicitações de acessos;
- Gerencia-se através de políticas e relatórios todas as concessões pertencentes a cada usuário;
- Automatiza-se o processo de reset de senhas;
- Centraliza todas as requisições e workflow de autorização de acessos;
- Agiliza o processo de concessão e revogação de acessos.



CHARLES
CLAUDIA

PONTOS IMPORTANTES

PROJETO IDM

Para uma boa implementação de IDM é necessário uma excelente estratégia de integração ao negócio

1. **Tecnologia madura:** é necessário realizar estudo para certificar-se da melhor tecnologia que se adapte ao ambiente da empresa e não o contrário, bem como sua integração com os diversos sistemas da empresa;

2. **Processos bem mapeados:** é necessário levantar todos os processos de integração, aprovações, revogações, autoatendimento e demais fluxos necessários que devem ser customizados na ferramenta, para não alterar demasiadamente os processos atuais da empresa;

3. **Implantação de uma cultura interna:** é necessário realização de fóruns de alinhamentos legais e de gestão e pessoas, treinamentos, envio de e-mails explicativos e ampla divulgação dos novos processos;

4. **Gestão de Perfis:** é necessário realizar mapeamento de perfis funcionais junto as políticas adotadas pelo RH e as áreas usuárias e alinhá-los aos acessos que deverão ser concedidos;

5. **Exceções:** a implementação de processos de gestão de identidade e acessos deve ter seu processo de exceção mapeado e estabelecido, para atender às solicitações especiais ou que não requeiram ou não possam ser padronizadas;

6. **Terceiros:** é necessário ter processos integrados, definidos e claros para o tratamento de acessos de colaboradores terceirizados.

7. **Registros de Logs e Monitoração:** para uma implementação efetiva de IDM é necessário avaliar e considerar as implementações de registros de operações e alertas automáticos para monitoração e prevenção de falhas.

Muitas empresas não obtém sucesso com a implementação de IDM devido:

1. **Planejamento longo, com demora nas primeiras entregas do projeto:** devido as características do projeto, a implementação de IDM pode levar 2 ou mais anos e na realidade pode nunca acabar. Por isto experiência e um bom planejamento são fundamentais para o sucesso do projeto.

2. **Falha na fase de análise e desenho:** boa parte das empresas falham no projeto de IDM devido a falhas durante o planejamento e desenho de implementação. Nesta fase é necessário muito mais que a visão técnica da tecnologia para a implementação, é necessário conhecer os processos e a cultura de empresa para que o projeto torne-se viável;

3. **Não usar as funcionalidade nativas do produto:** boa parte das dificuldades técnicas da implementação do IDM deve-se ao desejo de adaptar o produto ao máximo para não mudar o processo da empresa, isto traz riscos adicionais devido ao excesso de customização;

4. **Não prever o futuro:** o projeto de IDM é implantação que dificilmente será substituída o futuro, por isto uma boa escolha do produto, um bom planejamento e uma boa implementação são fundamentais para suportar ao máximo as direções futuras tecnológicas da empresa;

5. **Não envolver as área de negócios no projeto:** o projeto de gestão de identidade e acesso não se faz sozinha dentro de IT, é necessário o envolvimento das áreas de negócios, recursos humanos, *compliance* e jurídico. Também é importante ter um *Sponsor* executivo fora da área de tecnologia a fim de facilitar e priorizar a condução do projeto.

DÚVIDAS ???

ESTAMOS À DISPOSIÇÃO

MINDSEC
DINAMIO

corpia

Kleber Melo
kleber.melo@mindsec.com.br
mindsec.com.br
(11) 9 9494-4324 (11) 4010-3388

Charles Bauer
charles@dinamio.com.br
dinamio.com.br
(11) 9 5215-1187 I (47) 9 9125-6666 I
(11) 3185-6975