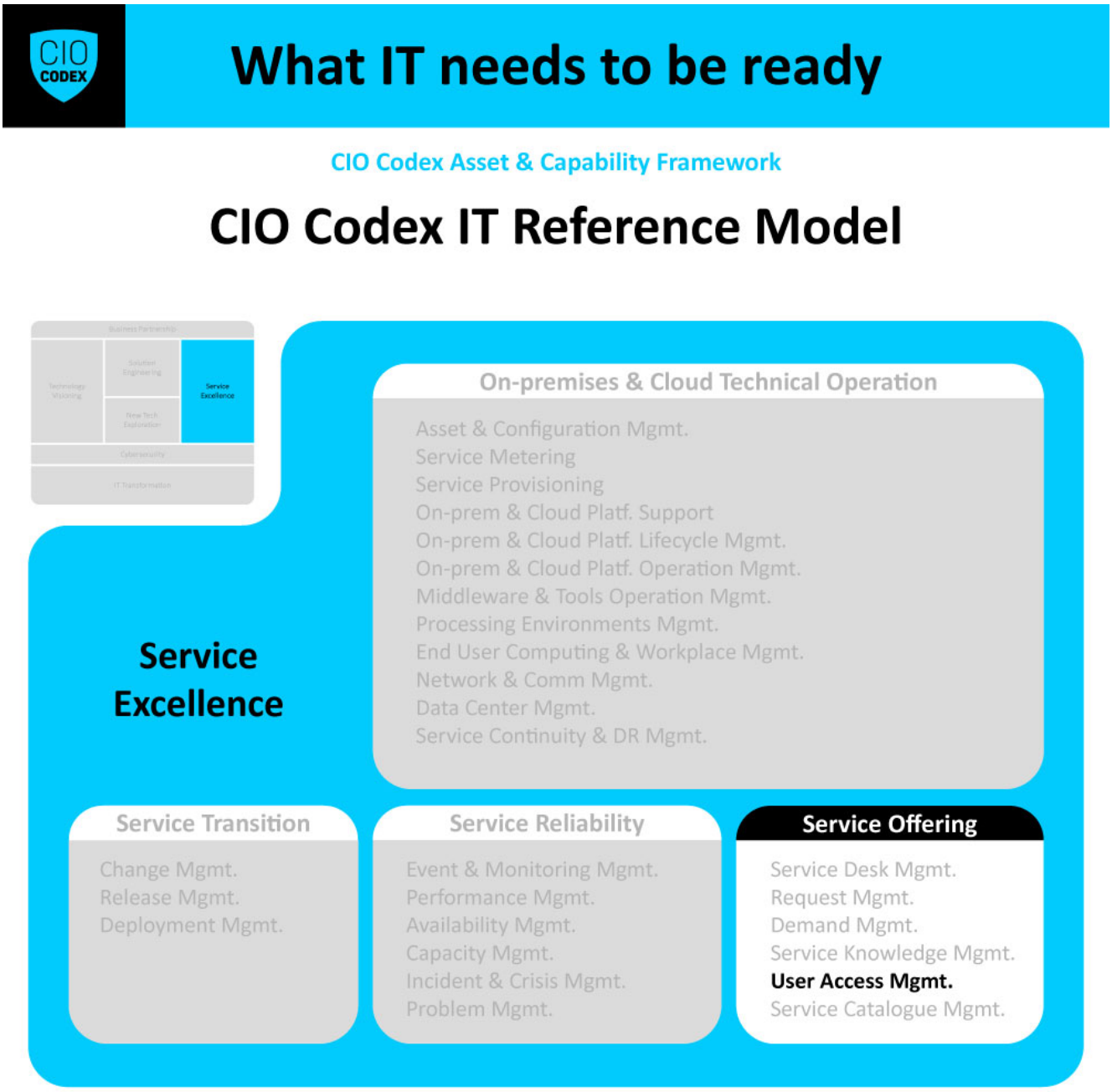

A User Access Request Management, inserida na macro capability de Service Offering e alinhada com a camada de Service Excellence do CIO Codex Capability Framework, desempenha um papel vital na gestão de acessos de usuários aos sistemas e serviços de TI.

Seu objetivo é garantir a integridade dos sistemas de TI, a segurança dos dados e o cumprimento de regulamentações, ao mesmo tempo em que proporciona uma experiência de usuário eficiente e segura.

Essa capability é fundamentada em conceitos essenciais.

A Gestão de Pedidos de Acesso é o ponto central, englobando o processo de

solicitação, revisão, aprovação e concessão de direitos de acesso aos recursos de TI.

As Políticas de Segurança e Conformidade estabelecem diretrizes e regras para garantir a segurança da informação e o cumprimento de regulamentações, alinhando todos os acessos a esses padrões.

A Revisão de Acessos é uma prática contínua que envolve a avaliação regular dos direitos de acesso dos usuários para garantir que permaneçam apropriados e necessários.

A Automatização de Processos é essencial, pois utiliza ferramentas e sistemas para agilizar e automatizar o fluxo de trabalho de gerenciamento de solicitações de acesso.

As características distintivas da User Access Request Management são notáveis.

Ela aprimora a segurança, garantindo que todos os acessos estejam em conformidade com as políticas de segurança, reduzindo os riscos de violações de dados e ameaças cibernéticas.

Contribui para a conformidade regulatória, o que é crucial em setores altamente regulados, como o financeiro e o de saúde.

A eficiência operacional é um dos seus pontos fortes, pois automatiza processos, reduzindo a carga de trabalho manual e melhorando a eficiência no gerenciamento de acessos.

Além disso, proporciona auditoria e rastreabilidade ao manter registros detalhados de todas as solicitações e aprovações de acesso, garantindo conformidade com regulamentações.

A User Access Request Management permite uma resposta rápida às mudanças, possibilitando ajustar rapidamente os direitos de acesso conforme as mudanças nas necessidades dos usuários e na estrutura organizacional.

Essa capability tem um propósito fundamental: garantir que todos os acessos sejam concedidos de acordo com as políticas de segurança e conformidade estabelecidas, ao mesmo tempo em que permite que os direitos de acesso sejam revisados e ajustados conforme necessário.

Ela afeta diretamente a segurança da informação, a eficiência operacional e a conformidade regulatória.

Dentro do contexto do CIO Codex Capability Framework, os objetivos da User Access Request Management são claros e estratégicos.

Ela busca promover a Eficiência Operacional ao simplificar e agilizar o processo de solicitação e concessão de acesso, reduzindo o tempo gasto pelos usuários e pela

equipe de TI.

Além disso, seu objetivo é impulsionar a Inovação, garantindo que os direitos de acesso sejam concedidos de forma precisa e eficaz, permitindo que os colaboradores tenham acesso às ferramentas e recursos necessários para impulsionar a inovação e a produtividade.

A contribuição para a Vantagem Competitiva é uma meta relevante, assegurando que a organização cumpra os requisitos de conformidade, proteja seus ativos de informação e mantenha a confiança dos clientes.

Garantir que a infraestrutura de TI esteja preparada para suportar o gerenciamento eficaz de solicitações de acesso é um objetivo prático, incluindo capacidade de armazenamento e poder de processamento.

A integração de sistemas e ferramentas que suportem o processo de gerenciamento de solicitações de acesso de maneira segura e eficiente é uma prioridade.

Por fim, a User Access Request Management busca integrar a capability no modelo operacional da organização, garantindo que todos os departamentos e equipes envolvidos colaborem de maneira eficaz no processo.

A User Access Request Management gera impactos significativos em várias dimensões tecnológicas.

A infraestrutura de TI deve ser dimensionada adequadamente para lidar com o aumento das solicitações de acesso, considerando a capacidade de armazenamento e poder de processamento necessários.

A arquitetura de segurança da informação deve ser atualizada para incluir controles de acesso rigorosos e autenticação adequada.

A implementação de sistemas de gerenciamento de identidade e acesso (IAM) é essencial, automatizando o processo de solicitação e concessão de acesso e garantindo a execução precisa das políticas de segurança.

A cibersegurança é uma preocupação constante, envolvendo a aplicação rigorosa de políticas de segurança para proteger os sistemas e dados.

A integração de políticas e procedimentos de segurança da informação em todas as operações é fundamental, garantindo a conformidade contínua com regulamentações e normas.

Em resumo, a User Access Request Management é uma capability crítica que desempenha um papel essencial na gestão de acessos de usuários aos sistemas e serviços de TI.

Ela contribui significativamente para a segurança, conformidade e eficiência operacional da organização, promovendo a excelência em serviços de TI.

Conceitos e Características

A User Access Request Management é essencial para garantir a integridade dos sistemas de TI, a segurança dos dados e o cumprimento de regulamentações, além de proporcionar uma experiência de usuário eficiente e segura.

Ela desempenha um papel crucial no ambiente de serviços de TI, facilitando a gestão de acessos de forma transparente e compatível com as melhores práticas do setor.

Conceitos

- Gestão de Pedidos de Acesso: Refere-se ao processo de solicitação, revisão, aprovação e concessão de direitos de acesso aos recursos de TI.
- Políticas de Segurança e Conformidade: Estabelecem as diretrizes e regras que regem a segurança da informação e a conformidade com regulamentações, garantindo que todos os acessos estejam alinhados com esses padrões.
- Revisão de Acessos: Envolve a avaliação regular dos direitos de acesso dos usuários para garantir que permaneçam apropriados e necessários.
- Automação de Processos: A utilização de ferramentas e sistemas para agilizar e automatizar o fluxo de trabalho de gerenciamento de solicitações de acesso.

Características

- Segurança Aprimorada: Garante que todos os acessos estejam em conformidade com as políticas de segurança, reduzindo os riscos de violações de dados e ameaças cibernéticas.
- Conformidade Regulatória: Contribui para o cumprimento de regulamentações relevantes, o que é essencial em setores altamente regulados, como o financeiro e o de saúde.
- Eficiência Operacional: Automatiza processos, reduzindo a carga de

trabalho manual e melhorando a eficiência no gerenciamento de acessos.
- Auditoria e Rastreabilidade: Facilita a auditoria interna e externa ao manter registros detalhados de todas as solicitações e aprovações de acesso.
- Resposta Rápida às Mudanças: Permite ajustar rapidamente os direitos de acesso conforme as mudanças nas necessidades dos usuários e na estrutura organizacional.

Propósito e Objetivos

A capability de User Access Request Management desempenha um papel fundamental na organização, concentrando-se na gestão dos pedidos de acesso dos usuários aos sistemas e serviços de TI.

Seu propósito é garantir que todos os acessos sejam concedidos de acordo com as políticas de segurança e conformidade estabelecidas, ao mesmo tempo em que permite que os direitos de acesso sejam revisados e ajustados conforme necessário.

Esta capability é de suma importância para a organização, pois afeta diretamente a segurança da informação, a eficiência operacional e a conformidade regulatória.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da User Access Request Management são os seguintes:

- Eficiência Operacional: Simplificar e agilizar o processo de solicitação e concessão de acesso, reduzindo o tempo gasto pelos usuários e pela equipe de TI.
- Inovação: Garantir que os direitos de acesso sejam concedidos de forma precisa e eficaz, permitindo que os colaboradores tenham acesso às ferramentas e recursos necessários para impulsionar a inovação e a produtividade.
- Vantagem Competitiva: Contribuir para a vantagem competitiva ao garantir que a organização cumpra os requisitos de conformidade, proteja seus ativos de informação e mantenha a confiança dos clientes.

- Infraestrutura: Assegurar que a infraestrutura de TI esteja preparada para suportar o gerenciamento eficaz de solicitações de acesso, incluindo capacidade de armazenamento e poder de processamento.
- Arquitetura: Integrar sistemas e ferramentas que suportem o processo de gerenciamento de solicitações de acesso de maneira segura e eficiente.
- Sistemas: Implementar sistemas de gerenciamento de identidade e acesso (IAM) que automatizem o fluxo de trabalho de solicitações e garantam a execução precisa das políticas de segurança.
- Modelo Operacional: Integrar a capability no modelo operacional da organização, garantindo que todos os departamentos e equipes envolvidos colaborem de maneira eficaz no processo.

Impacto na Tecnologia

A capability de User Access Request Management tem impactos significativos em várias dimensões tecnológicas:

- Infraestrutura: A infraestrutura de TI deve ser dimensionada adequadamente para lidar com o aumento das solicitações de acesso, incluindo capacidade de armazenamento e poder de processamento.
- Arquitetura: A arquitetura de segurança da informação deve ser atualizada para incluir controles de acesso rigorosos e autenticação adequada.
- Sistemas: Implementação de sistemas de gerenciamento de identidade e acesso (IAM) que automatizem o processo de solicitação e concessão de acesso.
- Cybersecurity: Gerenciar o acesso dos usuários envolve a aplicação rigorosa de políticas de segurança.
- Modelo Operacional: Integração de políticas e procedimentos de segurança da informação em todas as operações, garantindo a conformidade contínua com regulamentações e normas.

Roadmap de Implementação

A capability de User Access Request Management, inserida na macro capability Service Offering e situada na camada Service Excellence, desempenha um papel fundamental na gestão eficiente e segura dos pedidos de acesso aos sistemas de TI.

Para garantir o sucesso na adoção dessa capability, é essencial seguir um roadmap bem definido, considerando os princípios do CIO Codex Capability Framework:

- Definição de Objetivos Estratégicos: O primeiro passo é estabelecer objetivos estratégicos claros para a User Access Request Management, alinhados com a visão e missão da organização. Esses objetivos devem considerar a melhoria da segurança, eficiência operacional e conformidade.
- Avaliação de Políticas e Regulamentações: Realize uma revisão detalhada das políticas de segurança da informação e regulamentações relevantes para garantir que os processos de acesso estejam alinhados com esses padrões. Identifique requisitos específicos para setores regulados.
- Identificação de Recursos e Tecnologias: Determine os recursos necessários, incluindo pessoal qualificado, ferramentas de gerenciamento de identidade e acesso (IAM) e sistemas de automação. Avalie as tecnologias disponíveis no mercado que melhor atendam às necessidades da organização.
- Desenvolvimento de Processos: Projete processos de User Access Request Management que incluam solicitação, revisão, aprovação e concessão de acesso. Integre esses processos às políticas de segurança e conformidade.
- Automação de Fluxos de Trabalho: Implemente soluções de IAM que automatizem os fluxos de trabalho de gerenciamento de solicitações de acesso. Isso inclui a criação de scripts de aprovação, verificação de conformidade e provisionamento de acessos.
- Treinamento da Equipe: Garanta que a equipe esteja devidamente treinada para operar as ferramentas de IAM e seguir os processos estabelecidos. A capacitação é essencial para a eficiência do processo.
- Testes e Validação: Realize testes rigorosos para garantir que os processos de User Access Request Management funcionem conforme o esperado. Isso inclui simulações de solicitações, aprovações e auditorias.
- Integração com a Cultura Organizacional: Integre a capability no modelo

operacional da organização, promovendo a cultura de segurança da informação e conformidade. Estimule a colaboração entre departamentos e equipes envolvidas.

- Monitoramento e Auditoria Contínua: Estabeleça um processo de monitoramento contínuo para garantir a conformidade com as políticas de segurança e regulamentações. Realize auditorias internas e externas regularmente.
- Melhoria Contínua: Mantenha uma abordagem de melhoria contínua, ajustando os processos, políticas e tecnologias conforme necessário para acompanhar as mudanças nas necessidades da organização e no cenário regulatório.
- Comunicação e Conscientização: Comunique de forma eficaz os benefícios da User Access Request Management a toda a organização e promova a conscientização sobre a importância da conformidade e segurança da informação.

A implementação bem-sucedida da User Access Request Management é essencial para garantir a integridade dos sistemas de TI, a segurança dos dados e a conformidade com regulamentações.

Ao seguir o roadmap delineado acima, a organização estará mais bem preparada para gerenciar eficazmente os pedidos de acesso, proporcionar uma experiência de usuário eficiente e segura e alcançar seus objetivos estratégicos de segurança, eficiência operacional e conformidade regulatória.

Melhores Práticas de Mercado

A User Access Request Management desempenha um papel crítico na organização, garantindo a integridade dos sistemas de TI, a segurança dos dados e a conformidade com regulamentações.

Melhores Práticas de Mercado para User Access Request Management:

- Automação de Processos de Solicitação: Implementar um sistema automatizado para solicitações de acesso, permitindo que os usuários solicitem permissões de forma eficiente e rastreável.

- Políticas de Segurança Claras: Estabelecer políticas de segurança de acesso bem definidas e comunicá-las claramente aos usuários, garantindo que todos compreendam os requisitos e responsabilidades.
- Revisão Periódica de Acessos: Realizar revisões regulares dos direitos de acesso dos usuários para garantir que permaneçam apropriados e estejam alinhados com suas funções e responsabilidades.
- Autenticação Multifatorial (MFA): Exigir autenticação multifatorial para acessos sensíveis ou críticos, aumentando a segurança das contas de usuário.
- Aprovações Hierárquicas: Implementar um processo de aprovação em várias etapas para garantir que as solicitações de acesso sejam revisadas e aprovadas por partes autorizadas.
- Auditoria Abrangente: Manter registros detalhados de todas as solicitações e aprovações de acesso para fins de auditoria e rastreabilidade.
- Treinamento de Usuários: Oferecer treinamento aos usuários sobre práticas seguras de acesso e conscientização em segurança da informação.
- Monitoramento de Comportamento de Acesso: Utilizar ferramentas de monitoramento de comportamento de acesso para identificar atividades suspeitas ou não autorizadas.
- Integração com IAM: Integrar a User Access Request Management com sistemas de gerenciamento de identidade e acesso (IAM) para garantir uma execução precisa das políticas de segurança.
- Resposta a Incidentes de Segurança: Ter um plano de resposta a incidentes de segurança em vigor para lidar com violações de segurança de acesso de forma rápida e eficaz.
- Feedback dos Usuários: Coletar feedback dos usuários sobre o processo de solicitação de acesso e fazer melhorias com base nas sugestões.

Essas melhores práticas de mercado refletem os padrões estabelecidos pela indústria para o gerenciamento eficaz das solicitações de acesso, protegendo os recursos de TI e proporcionando uma experiência de usuário segura e eficiente.

Desafios Atuais

A Capability de User Access Request Management, inserida na macro capability Service Offering e pertencente à camada Service Excellence, desempenha um papel crucial na gestão dos pedidos de acesso dos usuários aos sistemas e serviços de TI.

No entanto, a adoção e integração dessa capability nos processos de negócios e operações de TI das organizações enfrentam desafios atuais que refletem a complexidade do ambiente de segurança da informação e a necessidade de garantir acesso eficiente e seguro aos recursos de TI.

Seguindo as melhores práticas de mercado, identificam-se os seguintes desafios atuais no contexto do CIO Codex Capability Framework:

- Aumento das Ameaças Cibernéticas: O cenário de ameaças cibernéticas em constante evolução exige que as organizações adotem medidas rigorosas para proteger os acessos, incluindo autenticação multifatorial e controles de acesso mais robustos.
- Conformidade Regulatória: Setores altamente regulados, como o financeiro e o de saúde, enfrentam desafios adicionais para garantir que o acesso esteja em conformidade com regulamentações, como GDPR e HIPAA.
- Complexidade de Acesso: À medida que as organizações adotam ambientes de TI híbridos e serviços em nuvem, gerenciar acessos torna-se mais complexo, exigindo soluções de gerenciamento de identidade e acesso (IAM) eficazes.
- Integração com Outras Capabilities: A User Access Request Management deve ser integrada de forma eficiente com outras capabilities, como Service Desk e Security Incident Response, para garantir uma abordagem holística à segurança.
- Eficiência Operacional: Assegurar que o processo de solicitação e concessão de acesso seja eficiente, reduzindo o tempo de resposta e a carga de trabalho manual, é um desafio constante.
- Privacidade dos Dados: Garantir a privacidade dos dados dos usuários é essencial, especialmente em um contexto em que a proteção de informações pessoais é um tema crítico.
- Identificação de Acessos Não Autorizados: Detectar e responder rapidamente a acessos não autorizados é crucial para evitar violações de

segurança.

- Avaliação de Riscos Contínua: A User Access Request Management deve incluir processos contínuos de avaliação de riscos para garantir que os direitos de acesso permaneçam apropriados e necessários.
- Treinamento e Conscientização dos Usuários: Educar os usuários sobre boas práticas de segurança e a importância do acesso responsável é um desafio constante.
- Resposta a Mudanças nas Necessidades dos Usuários: À medida que as necessidades dos usuários e a estrutura organizacional evoluem, ajustar rapidamente os direitos de acesso é um desafio que exige agilidade.

Esses desafios atuais destacam a importância estratégica da User Access Request Management na garantia da integridade dos sistemas de TI, na segurança dos dados e no cumprimento de regulamentações.

Para superá-los, as organizações devem adotar soluções de IAM robustas, implementar políticas de segurança rigorosas, manter uma cultura de conscientização de segurança e integrar efetivamente essa capability com outras dentro do contexto do CIO Codex Capability Framework.

A gestão eficaz dos pedidos de acesso não apenas aprimora a segurança, mas também impulsiona a eficiência operacional e o cumprimento regulatório, contribuindo para a excelência em serviços de TI.

Em um ambiente tecnológico dinâmico e repleto de ameaças, a capacidade de gerenciar pedidos de acesso de forma precisa e segura se torna um elemento crítico para o sucesso das operações de TI e para a proteção dos ativos de informação da organização.

Tendências para o Futuro

A User Access Request Management desempenha um papel crítico na gestão de acessos aos sistemas de TI, garantindo a integridade dos dados, a segurança da informação e a conformidade regulatória.

Para compreender como essa capability pode evoluir e se adaptar às mudanças antecipadas no mercado, bem como às inovações que moldarão seu desenvolvimento futuro, é essencial analisar as tendências e expectativas para o futuro.

As tendências que se destacam neste contexto são as seguintes:

- Inteligência Artificial na Avaliação de Solicitações: A inteligência artificial será cada vez mais utilizada para avaliar e classificar as solicitações de acesso, acelerando o processo de aprovação com base em critérios de risco e histórico de acesso.
- Autenticação Multifatorial Avançada: A autenticação multifatorial evoluirá com a incorporação de tecnologias biométricas avançadas, como reconhecimento facial e de íris, para garantir a segurança do acesso.
- Automatização de Fluxo de Trabalho: A automação de fluxo de trabalho se tornará uma prática comum, agilizando o processo de solicitação, revisão e aprovação de acesso.
- Gestão de Acessos Privilegiados (PAM): A necessidade de proteger acessos privilegiados crescerá, levando à ampla implementação de soluções de PAM para garantir o controle e a visibilidade adequados.
- Zero Trust Security: A abordagem Zero Trust se consolidará, exigindo que todos os acessos sejam verificados continuamente, independentemente da localização ou do dispositivo.
- Monitoramento Comportamental: A análise de comportamento do usuário se tornará uma parte fundamental da gestão de acessos, permitindo a detecção precoce de atividades suspeitas.
- Migração para a Nuvem: A gestão de solicitações de acesso se adaptará à migração contínua de sistemas para a nuvem, garantindo uma abordagem consistente e segura.
- Privacidade e Conformidade de Dados: As regulamentações de privacidade de dados desempenharão um papel importante nas políticas de acesso, garantindo que os dados dos usuários sejam protegidos adequadamente.
- Colaboração com Fornecedores de Identidade: A integração estreita com provedores de identidade externos permitirá a autenticação e o acesso a serviços de terceiros de forma segura.
- Auditoria em Tempo Real: A capacidade de auditar solicitações e concessões de acesso em tempo real se tornará um requisito essencial para fins de conformidade e segurança.

Essas tendências refletem a crescente complexidade do ambiente de segurança cibernética e a importância da User Access Request Management na garantia de que

apenas usuários autorizados tenham acesso aos recursos de TI, protegendo assim a organização contra ameaças internas e externas.

Adaptar-se a essas tendências será crucial para manter a segurança e a eficiência operacional no cenário de serviços de TI em constante evolução.

KPIs Usuais

A capability de User Access Request Management, inserida na camada Service Excellence e pertencente à macro capability Service Offering, desempenha um papel crucial na gestão dos pedidos de acesso dos usuários aos sistemas e serviços de TI.

Para avaliar seu desempenho e garantir a integridade dos sistemas, a segurança dos dados e a conformidade com as regulamentações, é essencial monitorar os KPIs apropriados.

Aqui estão os principais KPIs usuais dentro do contexto do CIO Codex Capability Framework:

- Tempo Médio de Resposta a Pedidos de Acesso (Average Response Time to Access Requests): Mede o tempo necessário para responder e processar solicitações de acesso dos usuários.
- Taxa de Concessão de Acessos (Access Grant Rate): Calcula a proporção de solicitações de acesso que são aprovadas e concedidas.
- Taxa de Aprovação Automatizada (Automated Approval Rate): Avalia a porcentagem de solicitações de acesso que são automaticamente aprovadas pelo sistema, sem intervenção humana.
- Taxa de Cumprimento de Políticas de Segurança (Security Policy Compliance Rate): Mede o quão bem as solicitações de acesso estão em conformidade com as políticas de segurança estabelecidas.
- Tempo Médio para Revogação de Acessos (Average Time to Access Revocation): Avalia o tempo necessário para revogar os direitos de acesso de um usuário quando não são mais necessários.
- Taxa de Acesso Negado (Access Denied Rate): Calcula a proporção de solicitações de acesso que são negadas devido a não conformidade com políticas ou outros motivos.
- Taxa de Acesso por Categoria de Usuário (Access Rate by User Category):

Segmenta a taxa de concessão de acessos por categorias de usuários, como funcionários, contratados, parceiros, etc.

- Taxa de Auditoria de Acessos (Access Audit Rate): Mede a frequência com que são realizadas auditorias nos acessos concedidos para garantir conformidade contínua.
- Tempo Médio para Atualização de Políticas de Acesso (Average Time to Access Policy Update): Avalia o tempo necessário para atualizar as políticas de acesso quando necessário.
- Taxa de Incidentes de Segurança Relacionados a Acessos (Access-Related Security Incidents Rate): Calcula a frequência de incidentes de segurança relacionados a acessos não autorizados.
- Taxa de Acessos Revistos (Access Review Rate): Mede com que frequência os direitos de acesso dos usuários são revisados para garantir que permaneçam apropriados.
- Taxa de Treinamento em Segurança da Informação (Information Security Training Rate): Avalia a proporção de usuários que recebem treinamento em segurança da informação.
- Tempo Médio para Detecção de Acessos Não Autorizados (Average Time to Detect Unauthorized Access): Avalia o tempo necessário para detectar acessos não autorizados e tomar medidas corretivas.
- Taxa de Satisfação dos Usuários com o Processo de Solicitação de Acesso (User Satisfaction Rate with Access Request Process): Mede a satisfação dos usuários em relação à facilidade e eficácia do processo de solicitação de acesso.
- Taxa de Recusa de Acesso por Violação de Conformidade (Access Denial Rate due to Compliance Violation): Calcula a proporção de acessos negados devido a violações de conformidade.

Esses KPIs desempenham um papel fundamental na avaliação do desempenho da User Access Request Management, garantindo que todos os acessos sejam concedidos de acordo com as políticas de segurança e conformidade estabelecidas.

A monitorização constante desses indicadores permite manter a segurança da informação, melhorar a eficiência operacional e garantir a conformidade regulatória.

Exemplos de OKRs

A capability de User Access Request Management na macro capability Service Offering da camada Service Excellence desempenha um papel fundamental na gestão dos pedidos de acesso dos usuários aos sistemas e serviços de TI.

Ela assegura que todos os acessos sejam concedidos de acordo com as políticas de segurança e conformidade, além de garantir que os direitos de acesso sejam revistos e ajustados conforme necessário.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Eficiência no Gerenciamento de Acessos

Objetivo: Aumentar a eficiência no processamento de pedidos de acesso dos usuários, reduzindo o tempo médio de resposta.

- KR1: Reduzir o tempo médio de processamento de pedidos de acesso em 30%.
- KR2: Implementar um sistema de automação para processar pedidos de acesso de forma mais eficiente.
- KR3: Criar um portal de autoatendimento para que os usuários possam fazer solicitações de acesso de forma mais rápida.

Conformidade e Segurança

Objetivo: Garantir que todos os pedidos de acesso estejam em conformidade com as políticas de segurança e conformidade da organização.

- KR1: Realizar verificações de conformidade em 100% dos pedidos de acesso recebidos.
- KR2: Implementar um processo de revisão de pedidos para identificar possíveis violações de segurança.
- KR3: Manter um registro de todas as concessões e revogações de acesso para fins de auditoria.

Revisão Periódica de Direitos de Acesso

Objetivo: Realizar revisões regulares dos direitos de acesso dos usuários para garantir que estejam alinhados com suas funções e responsabilidades.

- KR1: Estabelecer um ciclo de revisão trimestral de direitos de acesso.
- KR2: Implementar um sistema de notificação automática para alertar sobre direitos de acesso não utilizados.
- KR3: Garantir que 95% dos usuários tenham direitos de acesso revisados regularmente.

Portal de Autoatendimento Aprimorado

Objetivo: Aprimorar o portal de autoatendimento para facilitar a solicitação e o acompanhamento de pedidos de acesso pelos usuários.

- KR1: Implementar um portal mais intuitivo e de fácil utilização.
- KR2: Reduzir em 20% o número de chamados de suporte relacionados a pedidos de acesso.
- KR3: Aumentar a satisfação dos usuários com o portal de autoatendimento em 15%.

Relatórios e Auditoria

Objetivo: Manter registros detalhados de todas as atividades relacionadas a pedidos de acesso para fins de relatórios e auditoria.

- KR1: Gerar relatórios mensais que detalhem o volume de pedidos de acesso, as conformidades e as revisões realizadas.
- KR2: Realizar auditorias internas trimestrais para avaliar a eficácia do processo de gerenciamento de pedidos de acesso.
- KR3: Implementar um sistema de registro de atividades que rastreie todas as ações relacionadas a pedidos de acesso.

Esses OKRs refletem a importância crítica da capability de User Access Request Management na macro capability Service Offering, dentro da camada Service Excellence.

Ao focar na eficiência no gerenciamento de acessos, garantir conformidade e

segurança, realizar revisões periódicas de direitos de acesso, aprimorar o portal de autoatendimento e manter registros detalhados, esta capability contribui significativamente para a gestão eficaz dos pedidos de acesso dos usuários e para o cumprimento das políticas de segurança e conformidade da organização.

Critérios para Avaliação de Maturidade

A capability User Access Request Management, inserida na macro capability Service Offering e na camada Service Excellence, desempenha um papel crucial na gestão dos pedidos de acesso dos usuários aos sistemas e serviços de TI.

Para avaliar a maturidade dessa capability dentro do contexto do CIO Codex Capability Framework, foram desenvolvidos critérios de avaliação de maturidade inspirados no modelo CMMI, abrangendo cinco níveis de maturidade:

Nível de Maturidade Inexistente

- Não há reconhecimento da necessidade de gerir pedidos de acesso de usuários.
- Ausência de políticas ou procedimentos para a gestão de pedidos de acesso.
- Falta de documentação relacionada aos processos de gestão de pedidos de acesso.
- Não existem controles de segurança ou conformidade implementados.
- Não há métricas ou indicadores de desempenho definidos.

Nível de Maturidade Inicial

- Reconhecimento inicial da importância da User Access Request Management.
- Processos básicos de gerenciamento de pedidos de acesso estão sendo desenvolvidos.
- Início da documentação de procedimentos e políticas.
- Implementação de controles de segurança iniciais.
- Primeiros indicadores de desempenho estão sendo definidos.

Nível de Maturidade Definido

- Políticas e procedimentos para User Access Request Management estão documentados e comunicados.
- Processos estão bem definidos e consistentemente seguidos.
- Documentação abrangente de procedimentos e políticas está disponível.
- Controles de segurança e conformidade são parte integrante do processo.
- Métricas são usadas para monitorar o desempenho e a eficácia do gerenciamento de pedidos de acesso.

Nível de Maturidade Gerenciado

- User Access Request Management é monitorado e medido regularmente.
- Processos são altamente eficazes e adaptáveis às mudanças nas necessidades do negócio.
- Documentação é atualizada continuamente e acessível a toda a organização.
- Controles de segurança e conformidade são constantemente aprimorados.
- Análise de tendências e melhorias contínuas são parte integrante da gestão de pedidos de acesso.

Nível de Maturidade Otimizado

- User Access Request Management é altamente automatizado e eficaz.
- Processos são altamente otimizados e adaptáveis às mudanças nas demandas dos usuários e negócios.
- Documentação é atualizada em tempo real e facilmente acessível.
- Utilização de tecnologias avançadas, como automação e análise de dados, para otimizar a gestão de pedidos de acesso.
- Previsão proativa de necessidades de acesso e otimização contínua são parte da estratégia de gestão de pedidos de acesso.

Esses critérios de maturidade são essenciais para avaliar e aprimorar a capability User Access Request Management, garantindo que todos os acessos sejam concedidos de

acordo com as políticas de segurança e conformidade, e que os direitos de acesso sejam revistos e ajustados conforme necessário.

À medida que a organização avança nos níveis de maturidade, sua capacidade de gerenciar eficazmente os pedidos de acesso dos usuários aumenta, contribuindo para a segurança e conformidade de TI.

Convergência com Frameworks de Mercado

No contexto do CIO Codex Capability Framework, a capability de User Access Request Management, vinculada à macro capability Service Offering e integrada à camada Service Excellence, desempenha um papel essencial na gestão operacional de acessos aos usuários por parte da TI.

A implementação efetiva de User Access Request Management requer uma abordagem estratégica, incluindo a definição de processos claros e a utilização de tecnologias adequadas para gerenciamento de solicitações e revisões de acesso.

A seguir, é analisada a convergência desta capability em relação a um conjunto dez frameworks de mercado reconhecidos e bem estabelecidos em suas respectivas áreas de expertise:

COBIT

- Nível de Convergência: Alto
- Racional: O COBIT valoriza o gerenciamento de acesso como um elemento crítico para a governança de TI, alinhando-se com a capability de User Access Request Management pela ênfase em controles de acesso e conformidade.

ITIL

- Nível de Convergência: Alto
- Racional: O ITIL estabelece práticas de gerenciamento de serviço que incluem o gerenciamento de acesso como parte do processo de segurança

da informação. A capability em análise integra-se perfeitamente ao ITIL, promovendo a eficiência na gestão de acesso dos usuários.

SAFe

- Nível de Convergência: Médio
- Racional: Embora o SAFe seja mais focado em agilidade e escalabilidade, a eficiência no gerenciamento de acesso dos usuários facilita a colaboração e o acesso a ferramentas, alinhando-se aos princípios de Lean-Agile.

PMI

- Nível de Convergência: Médio
- Racional: O PMI não trata especificamente de gerenciamento de acesso, mas a eficácia no gerenciamento de acesso dos usuários pode suportar a governança de projetos através de acesso adequado a informações e sistemas.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI foca na maturidade dos processos de negócios. A capability de gerenciamento de acesso dos usuários contribui para a maturidade organizacional ao garantir processos de acesso controlados e auditáveis.

TOGAF

- Nível de Convergência: Baixo
- Racional: O TOGAF se concentra na arquitetura empresarial. Enquanto o gerenciamento de acesso é menos enfatizado, a capability ainda apoia o TOGAF ao garantir que os usuários tenham acesso adequado aos recursos arquiteturais.

DevOps SRE

- Nível de Convergência: Médio
- Racional: No DevOps e SRE, o gerenciamento de acesso é importante para a operação e segurança. A capability analisada alinha-se ao garantir que as mudanças de acesso sejam feitas de maneira controlada, suportando a continuidade operacional.

NIST

- Nível de Convergência: Alto
- Racional: A NIST fornece frameworks de segurança cibernética que incluem controle de acesso robusto. A capability de User Access Request Management está altamente alinhada com o NIST ao assegurar a conformidade com políticas de segurança.

Six Sigma

- Nível de Convergência: Médio
- Racional: O Six Sigma visa a melhoria contínua e redução de erros. A gestão eficiente de solicitações de acesso dos usuários apoia esses objetivos, reduzindo erros e otimizando processos.

Lean IT

- Nível de Convergência: Médio
- Racional: O Lean IT enfatiza a eficiência operacional, que pode ser reforçada pela capability de User Access Request Management ao minimizar o desperdício e melhorar o tempo de resposta para solicitações de acesso.

Cada um desses frameworks oferece uma perspectiva única sobre a importância do gerenciamento de acesso, e a integração dessa capability reforça a segurança,

conformidade, eficiência e governança dentro das organizações.

A avaliação de maturidade dessa capability pode ser feita através de indicadores como o tempo de resposta para solicitações de acesso, o número de erros de acesso e a satisfação do usuário, refletindo seu alinhamento com as práticas de mercado e a capacidade de atender às necessidades de negócios.

Processos e Atividades

Develop Access Request Plans

Desenvolver planos de gestão de requisições de acesso é essencial para garantir que os procedimentos e políticas estejam alinhados com os objetivos de segurança e conformidade da organização.

Este processo envolve a criação de um plano abrangente que define como as solicitações de acesso serão gerenciadas, desde a solicitação inicial até a aprovação final.

As atividades incluem a análise das necessidades de acesso dos usuários, a definição de políticas de acesso baseadas em funções, a identificação de ferramentas e tecnologias apropriadas para gerenciar solicitações de acesso e a definição de métricas para monitorar a eficácia do plano.

A colaboração entre diferentes áreas de TI e negócios é crucial para assegurar que todas as necessidades de acesso sejam consideradas.

A documentação clara e precisa do plano de gestão de requisições de acesso garante que todos os stakeholders compreendam suas responsabilidades e os objetivos do processo, proporcionando um roteiro detalhado para a gestão eficaz de acessos.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Identify Access Needs	Identificar as necessidades de acesso dos usuários.	Necessidades de negócios, feedback de usuários	Necessidades de acesso identificadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
2	Define Access Policies	Definir políticas de acesso baseadas em funções.	Necessidades de acesso, melhores práticas	Políticas de acesso definidas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation
3	Select Tools and Technologies	Selecionar ferramentas e tecnologias apropriadas para gerenciar solicitações de acesso.	Políticas de acesso, necessidades de acesso	Ferramentas e tecnologias selecionadas	Responsible: Data, AI & New Technology; Accountable: Data, AI & New Technology; Consulted: IT Infrastructure & Operation; Informed: Solution Engineering & Development	Decider: Data, AI & New Technology; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Data, AI & New Technology

4	Develop Access Procedures	Desenvolver procedimentos detalhados para a gestão de requisições de acesso.	Ferramentas e tecnologias, políticas de acesso	Procedimentos de acesso desenvolvidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
5	Document Access Plan	Documentar o plano de gestão de requisições de acesso e obter aprovação.	Procedimentos de acesso, políticas de acesso	Plano de gestão de acesso documentado	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation

Identify Access Requirements

Identificar os requisitos para a gestão de requisições de acesso é fundamental para garantir que as políticas e procedimentos de segurança sejam robustos e eficazes.

Este processo envolve a coleta de dados para determinar as necessidades específicas de acesso dos usuários, incluindo a análise de funções e responsabilidades dentro da organização.

As atividades incluem a realização de entrevistas com stakeholders, a análise de dados históricos de acesso, a utilização de ferramentas de análise para identificar padrões e a definição de requisitos específicos de acesso.

A colaboração entre diferentes áreas de TI e negócios é essencial para garantir que todos os aspectos das necessidades de acesso sejam capturados e compreendidos.

A documentação dos requisitos de acesso fornece uma base sólida para o desenvolvimento de políticas e procedimentos eficazes de gestão de acesso e garante que todos os stakeholders estejam alinhados quanto às expectativas e objetivos.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Stakeholder Interviews	Realizar entrevistas com stakeholders para entender necessidades de acesso.	Necessidades de stakeholders, dados históricos	Entrevistas realizadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Governance & Transformation
2	Analyze Current Access	Analisar os acessos atuais para identificar necessidades não atendidas.	Dados de acesso, feedback de stakeholders	Necessidades de acesso identificadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Identify Access Gaps	Identificar lacunas de acesso com base na análise dos dados.	Dados de acesso, feedback de stakeholders	Gaps de acesso identificados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

4	Define Access Requirements	Definir os requisitos de acesso necessários para preencher as lacunas identificadas.	Gaps de acesso, melhores práticas	Requisitos de acesso definidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation
5	Document Access Requirements	Documentar todos os requisitos de acesso identificados.	Requisitos de acesso, feedback de stakeholders	Requisitos de acesso documentados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation

Execute Access Request Activities

Executar as atividades de gestão de requisições de acesso conforme planejado é crucial para garantir que os acessos sejam concedidos de forma eficiente e segura.

Este processo envolve a implementação das políticas e procedimentos definidos no plano de gestão de acesso, desde a solicitação inicial até a aprovação e provisionamento do acesso.

As atividades incluem o recebimento e registro de solicitações de acesso, a validação das solicitações de acordo com as políticas de segurança, a aprovação ou rejeição das solicitações e o provisionamento do acesso para os usuários aprovados.

A utilização de ferramentas e tecnologias avançadas, como sistemas de gerenciamento de identidade e acesso (IAM), pode melhorar significativamente a eficiência e a segurança do processo.

A documentação de todas as atividades é essencial para garantir a rastreabilidade e a conformidade com as políticas de segurança e regulamentações.

- PDCA focus: Do

- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Receive Access Requests	Receber e registrar solicitações de acesso dos usuários.	Solicitações de acesso, políticas de acesso	Solicitações de acesso registradas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
2	Validate Access Requests	Validar solicitações de acesso de acordo com as políticas de segurança.	Solicitações de acesso, políticas de acesso	Solicitações de acesso validadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: IT Governance & Transformation	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: IT Governance & Transformation; Executer: Cybersecurity
3	Approve or Reject Requests	Aprovar ou rejeitar solicitações de acesso com base na validação.	Solicitações de acesso validadas, políticas de acesso	Solicitações de acesso aprovadas/rejeitadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

4	Provision Access	Provisionar acesso para os usuários aprovados.	Solicitações de acesso aprovadas, políticas de acesso	Acesso provisionado	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
5	Document Access Activities	Documentar todas as atividades de acesso para fins de auditoria e conformidade.	Acesso provisionado, políticas de acesso	Atividades de acesso documentadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation

Monitor Access Performance

Monitorar continuamente o desempenho da gestão de requisições de acesso é essencial para garantir que as atividades estejam alinhadas com os objetivos de segurança e conformidade da organização.

Este processo envolve a coleta e análise de dados sobre a performance das atividades de gestão de requisições de acesso, utilizando ferramentas de monitoramento para identificar áreas de melhoria.

As atividades incluem a definição de métricas de desempenho, o monitoramento em tempo real das atividades de acesso, a geração de relatórios de desempenho e a realização de revisões periódicas.

A análise dos dados coletados ajuda a identificar tendências e padrões que podem ser usados para melhorar os processos e aumentar a eficácia da gestão de acessos.

A documentação e a comunicação dos resultados do monitoramento são essenciais para garantir que as partes interessadas estejam cientes do desempenho atual e das melhorias necessárias.

- PDCA focus: Check
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Define Performance Metrics	Definir métricas de desempenho para a gestão de requisições de acesso.	Plano de gestão de acesso, melhores práticas	Métricas de desempenho definidas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation
2	Monitor Access Activities	Monitorar as atividades de gestão de acesso em tempo real.	Informações de acesso, ferramentas de monitoramento	Dados de monitoramento coletados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Analyze Performance Data	Analisar os dados de desempenho das atividades de gestão de acesso.	Dados de monitoramento, métricas de desempenho	Relatório de análise de desempenho	Responsible: Data, AI & New Technology; Accountable: Data, AI & New Technology; Consulted: IT Infrastructure & Operation; Informed: IT Governance & Transformation	Decider: Data, AI & New Technology; Advisor: IT Infrastructure & Operation; Recommender: IT Governance & Transformation; Executer: Data, AI & New Technology

4	Generate Performance Reports	Gerar relatórios de desempenho periódicos para as partes interessadas.	Relatório de análise de desempenho, feedback dos stakeholders	Relatórios de desempenho gerados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
5	Conduct Performance Reviews	Conduzir revisões periódicas de desempenho com as partes interessadas.	Relatórios de desempenho, feedback dos stakeholders	Revisões de desempenho realizadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

Review and Optimize Access Processes

Revisar e otimizar os processos de gestão de requisições de acesso com base nos resultados obtidos é essencial para garantir a melhoria contínua e a eficácia das atividades de gestão de acesso.

Este processo envolve a análise detalhada dos dados de desempenho e feedbacks coletados, a identificação de áreas de melhoria e a implementação de mudanças nos processos de gestão de acesso.

As atividades incluem a realização de análises pós-implementação, a revisão das políticas e procedimentos existentes, a identificação de melhores práticas e a integração das lições aprendidas nos processos atualizados.

A documentação das mudanças e a comunicação eficaz com todas as partes interessadas são essenciais para garantir que as melhorias sejam compreendidas e implementadas de maneira eficiente.

Este processo assegura que as atividades de gestão de acesso continuem a

proporcionar valor significativo à organização, permitindo uma resposta proativa e eficaz a eventos futuros.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Evaluate Access Performance	Avaliar o desempenho das atividades de gestão de acesso.	Dados de desempenho, feedback dos stakeholders	Relatório de avaliação	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: IT Infrastructure & Operation; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: IT Infrastructure & Operation; Recommender: Cybersecurity; Executer: IT Governance & Transformation
2	Identify Improvement Areas	Identificar áreas de melhoria com base na avaliação dos resultados.	Relatório de avaliação, feedback dos stakeholders	Lista de áreas de melhoria	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Data, AI & New Technology	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation

3	Update Access Processes	Atualizar os processos de gestão de acesso para incorporar as melhorias identificadas.	Lista de áreas de melhoria, melhores práticas	Processos de gestão de acesso atualizados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
4	Document Changes	Documentar as mudanças nos processos de gestão de acesso.	Processos de gestão de acesso atualizados, feedback dos stakeholders	Documentação de mudanças	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: IT Infrastructure & Operation	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: IT Infrastructure & Operation; Executer: IT Governance & Transformation
5	Communicate Updates	Comunicar as atualizações dos processos aos stakeholders relevantes.	Documentação de mudanças, plano de comunicação	Comunicação de atualizações	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Governance & Transformation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Governance & Transformation