



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.



CIO Codex

Com o advento da era digital, a Tecnologia da Informação assumiu um papel de destaque dentro das estratégias corporativas das empresas dos mais diversos portes e setores de atuação. O CIO Codex Framework foi concebido com o propósito de oferecer uma visão integrada dos conceitos de uma área de tecnologia pronta para a era digital.



The IT framework

O conteúdo apresentado neste website, incluindo o framework, é protegido por direitos autorais e é de propriedade exclusiva do CIO Codex. Isso inclui, mas não se limita a, textos, gráficos, marcas, logotipos, imagens, vídeos e demais materiais disponíveis no site. Qualquer reprodução, distribuição, ou utilização não autorizada desse conteúdo é estritamente proibida e sujeita às penalidades previstas na legislação aplicável