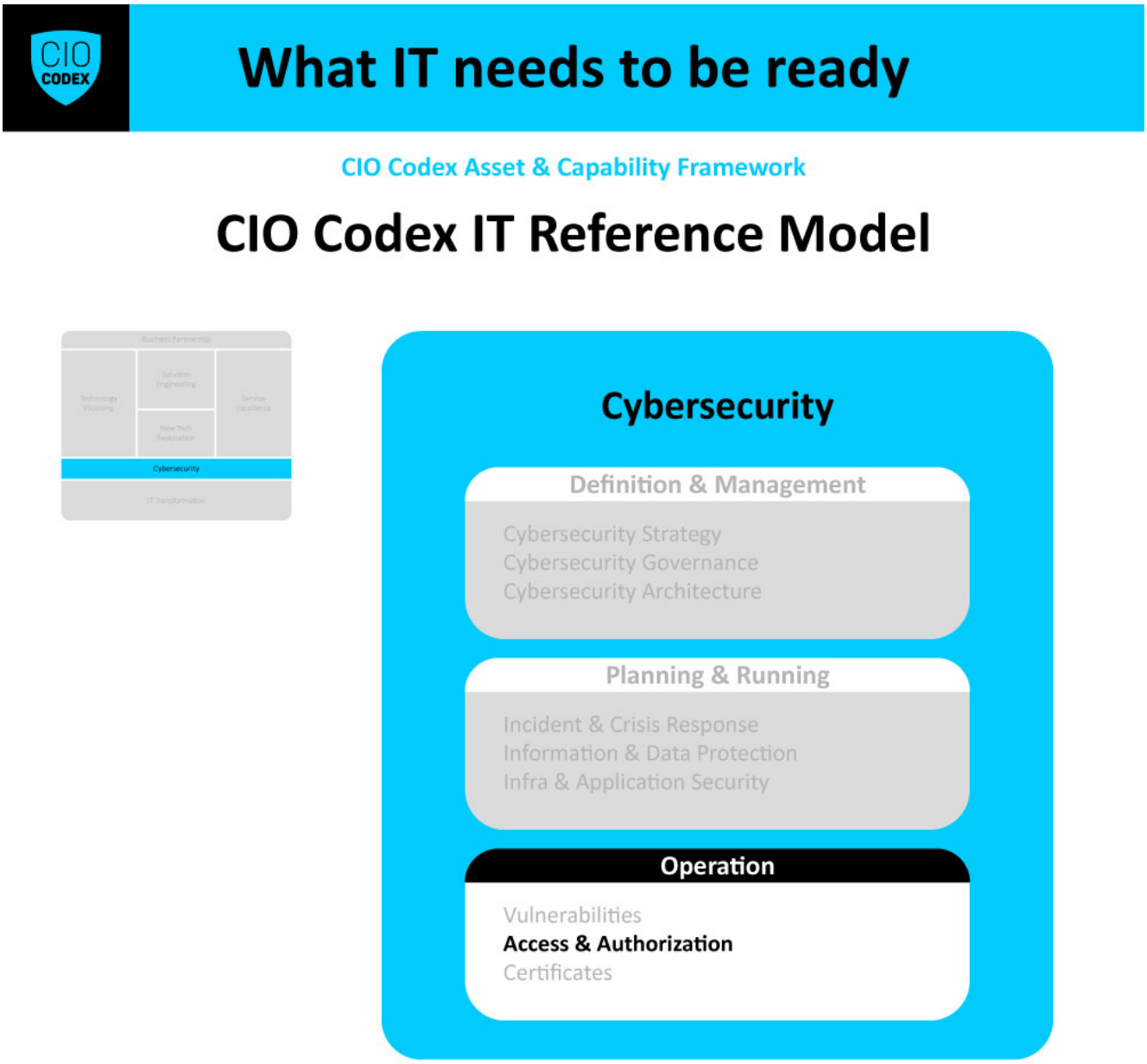

A capability de Access & Authorization Management, inserida na macro capability Operation e na camada Cybersecurity do CIO Codex Capability Framework, desempenha um papel crucial na proteção de informações críticas e na prevenção do acesso não autorizado.

Esta função é essencial na estratégia de defesa cibernética de uma organização, assegurando a proteção de seus ativos mais valiosos.

Dentro dos conceitos-chave, Gestão de Identidades trata do gerenciamento completo do ciclo de vida das identidades dos usuários, Autenticação é o processo de verificação da identidade do usuário, e Autorizações determinam os recursos ou ações que um usuário tem permissão para acessar ou executar após a autenticação.

As características desta capability incluem Controle Granular para políticas de acesso específicas, Auditoria e Monitoramento para registro de atividades de acesso, Proteção contra Ameaças Internas para mitigar riscos de segurança interna, Segurança em Nuvem para extensão da gestão de identidades e autorizações ao ambiente de nuvem, e Autenticação Multifatorial (MFA) para reforçar a segurança.

O propósito da Access & Authorization Management é garantir um controle rigoroso sobre o acesso a sistemas e dados, assegurando que apenas indivíduos autorizados possam acessar recursos específicos.

Esta capability é vital para manter a confidencialidade, integridade e disponibilidade dos ativos de TI da organização.

Os objetivos dentro do CIO Codex Capability Framework incluem a melhoria da Eficiência Operacional, promovendo a Inovação e contribuindo para a Vantagem Competitiva da organização.

Estes objetivos são alcançados através de um controle de acesso robusto que inspira confiança em clientes e parceiros.

No impacto tecnológico, a Access & Authorization Management influencia várias dimensões: na Infraestrutura, implementa sistemas de gestão de identidades e acessos, na Arquitetura, define políticas de autenticação e autorização, nos Sistemas, gerencia permissões de acesso, em Cybersecurity, assegura o acesso autorizado aos ativos tecnológicos, e no Modelo Operacional, estabelece processos para revisão, aprovação e monitoramento contínuo de contas de usuários.

Em síntese, a Access & Authorization Management é uma capability essencial que fornece às organizações os meios para controlar rigorosamente o acesso aos seus sistemas e dados.

Esta função é crucial para garantir a segurança dos sistemas e dados da organização, contribuindo significativamente para a eficiência operacional, inovação e vantagem competitiva em um ambiente de negócios onde a segurança cibernética é um fator crítico para o sucesso e a confiança.

Conceitos e Características

A capability de Access & Authorization Management é vital para salvaguardar informações críticas, prevenir o acesso não autorizado e garantir a conformidade com regulamentações de segurança cibernética.

Ela desempenha um papel central na estratégia de defesa cibernética de uma organização, protegendo seus ativos mais valiosos.

Conceitos

- Gestão de Identidades: Envolve o gerenciamento completo do ciclo de vida das identidades dos usuários, desde a criação até a desativação, garantindo que as informações de acesso sejam precisas e atualizadas.
- Autenticação: Refere-se ao processo de verificação da identidade do usuário, normalmente por meio de senhas, autenticação multifatorial (MFA) ou biometria.
- Autorizações: Determinam quais recursos específicos ou ações um usuário ou sistema tem permissão para acessar ou executar após a autenticação.

Características

- Controle Granular: Permite a definição de políticas de acesso altamente específicas, concedendo permissões com base em funções, departamentos e níveis de privilégio.
- Auditoria e Monitoramento: Registra e rastreia todas as atividades de acesso, permitindo a detecção de comportamentos suspeitos ou violações de segurança.
- Proteção contra Ameaças Internas: Ajuda a mitigar os riscos de insider threats, onde colaboradores internos podem representar uma ameaça à segurança da organização.
- Segurança em Nuvem: Estende a gestão de identidades, autenticação e autorizações para ambientes de nuvem, garantindo a segurança dos recursos hospedados na nuvem.
- Autenticação Multifatorial (MFA): Reforça a autenticação exigindo múltiplos métodos de verificação de identidade, tornando mais difícil para invasores acessarem sistemas ou dados.

Propósito e Objetivos

A Access & Authorization Management é uma capability de extrema importância no cenário da segurança cibernética.

Seu propósito principal reside em garantir um controle rigoroso sobre o acesso a sistemas e dados, assegurando que apenas indivíduos autorizados tenham permissão para acessar recursos específicos.

Essa capability desempenha um papel crítico na proteção contra acessos não autorizados, seja de ameaças internas ou externas.

Ela é essencial para preservar a confidencialidade, integridade e disponibilidade dos ativos de TI da organização.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, a Access & Authorization Management tem os seguintes objetivos:

- Eficiência Operacional: Esta capability busca otimizar a gestão de identidades, autenticação e autorizações, tornando os processos mais eficientes e ágeis. Isso reduz a sobrecarga administrativa e facilita o acesso seguro aos recursos de TI.
- Inovação: Ao garantir um controle granular sobre o acesso a sistemas e dados, a organização pode inovar com confiança, implementando novas tecnologias e abordagens com segurança incorporada desde o início.
- Vantagem Competitiva: A Access & Authorization Management contribui para a vantagem competitiva, uma vez que a segurança robusta inspira confiança nos clientes e parceiros. Isso pode resultar em uma posição mais forte no mercado.

Impacto na Tecnologia

A Access & Authorization Management influencia diversos aspectos da tecnologia em uma organização:

- Infraestrutura: Implementa sistemas de gestão de identidades e acessos que controlam o acesso físico e lógico aos ativos de TI.

- Arquitetura: Define políticas de autenticação e autorização que orientam a arquitetura de sistemas e aplicativos, garantindo que a segurança seja uma consideração central.
- Sistemas: Gerencia permissões de acesso a nível de usuário, garantindo que apenas pessoas autorizadas tenham acesso aos recursos apropriados.
- Cybersecurity: O gerenciamento de acesso e autorização garante que apenas usuários autorizados tenham acesso aos ativos tecnológicos.
- Modelo Operacional: Estabelece processos para revisar, aprovar e monitorar continuamente as contas de usuário e as permissões, garantindo a conformidade e a segurança.

Roadmap de Implementação

A capability de Access & Authorization Management desempenha um papel crítico na proteção de informações sensíveis, na prevenção de acessos não autorizados e na garantia de conformidade com regulamentações de segurança cibernética.

Para implementá-la eficazmente, é fundamental seguir um roadmap estratégico que considere os princípios do CIO Codex Capability Framework.

A seguir, as principais etapas desse roadmap:

- Avaliação Inicial: Realize uma avaliação abrangente dos sistemas e recursos de TI existentes para entender as necessidades de controle de acesso. Isso inclui a identificação de ativos críticos, sistemas sensíveis e grupos de usuários.
- Identificação de Requisitos de Segurança: Defina os requisitos de segurança específicos para diferentes categorias de ativos e usuários. Isso envolve a classificação de ativos e a atribuição de níveis de acesso.
- Seleção de Ferramentas: Escolha as ferramentas de gestão de identidades e acessos mais adequadas às necessidades da organização. Certifique-se de que essas ferramentas ofereçam recursos de autenticação forte e autorização granular.
- Políticas de Acesso: Desenvolva políticas claras de controle de acesso que estabeleçam quem tem permissão para acessar quais recursos e sob quais condições. Certifique-se de que essas políticas estejam alinhadas com os

requisitos regulatórios.

- Implementação de Autenticação Forte: Reforce a autenticação dos usuários, considerando a implementação de autenticação multifatorial (MFA) sempre que possível. Isso aumenta significativamente a segurança do acesso.
- Integração de Sistemas: Integre as soluções de gestão de identidades e acessos com os sistemas existentes, garantindo que as políticas de controle de acesso sejam aplicadas de forma consistente em toda a organização.
- Monitoramento Contínuo: Implemente sistemas de monitoramento contínuo para detectar e responder a atividades de acesso suspeitas ou não autorizadas. Isso inclui o registro e a análise de eventos de autenticação e autorização.
- Treinamento e Conscientização: Forneça treinamento regular aos funcionários sobre as políticas de controle de acesso e boas práticas de segurança. A conscientização é fundamental para o sucesso dessa capability.
- Revisões Periódicas: Realize revisões regulares das políticas e permissões de acesso para garantir que elas permaneçam atualizadas e alinhadas com as necessidades da organização.
- Auditorias e Conformidade: Realize auditorias de controle de acesso para garantir a conformidade com regulamentações de segurança cibernética e normas internas. Mantenha registros detalhados para fins de auditoria.
- Resposta a Incidentes: Desenvolva um plano de resposta a incidentes relacionados a acessos não autorizados. Esteja preparado para agir rapidamente em caso de violações de segurança.
- Melhoria Contínua: Estabeleça um ciclo de melhoria contínua, revisando e aprimorando constantemente as políticas, procedimentos e tecnologias de controle de acesso com base nas lições aprendidas e nas mudanças no cenário de ameaças.

A implementação eficaz da Access & Authorization Management é essencial para proteger os ativos de TI, garantir a confidencialidade dos dados e cumprir as regulamentações de segurança.

Essa capability contribui para a eficiência operacional, a inovação e a vantagem competitiva, ao mesmo tempo em que minimiza os riscos de acessos não autorizados e violações de segurança.

Melhores Práticas de Mercado

No âmbito do CIO Codex Capability Framework, a capability de Access & Authorization Management desempenha um papel crítico na proteção de informações cruciais, prevenção de acesso não autorizado e garantia de conformidade com regulamentações de segurança cibernética.

Para alcançar uma gestão eficaz de acesso e autorização, é essencial adotar as melhores práticas de mercado, amplamente reconhecidas e implementadas por organizações líderes.

Abaixo estão as principais melhores práticas dentro dessa capability:

- Gestão de Identidades Completa: Implemente um sistema completo de gestão de identidades que abranja o ciclo de vida completo do usuário, desde a criação até a desativação. Isso assegura que as informações de acesso sejam precisas e atualizadas.
- Autenticação Multifatorial (MFA): Reforce a autenticação exigindo múltiplos métodos de verificação de identidade, como senhas, tokens, biometria ou autenticação de dispositivo. Isso aumenta a segurança das autenticações.
- Controle Granular de Autorizações: Estabeleça políticas de autorização detalhadas que determinem quais recursos específicos ou ações um usuário ou sistema tem permissão para acessar ou executar após a autenticação.
- Auditoria e Monitoramento Rigorosos: Implemente um sistema robusto de auditoria e monitoramento que registre e rastreie todas as atividades de acesso. Isso permite a detecção precoce de comportamentos suspeitos ou violações de segurança.
- Proteção contra Ameaças Internas: Utilize o Access & Authorization Management para mitigar os riscos de insider threats, monitorando e restringindo o acesso de colaboradores internos a recursos sensíveis.
- Segurança em Nuvem: Estenda a gestão de identidades, autenticação e autorizações para ambientes de nuvem, garantindo que os recursos hospedados na nuvem sejam igualmente seguros.
- Políticas Baseadas em Funções: Implemente políticas de acesso baseadas

em funções, onde os usuários recebem permissões de acordo com suas funções e responsabilidades na organização.
- Revisões Periódicas de Autorizações: Realize revisões periódicas das permissões de acesso para garantir que apenas as pessoas autorizadas tenham acesso contínuo aos recursos.
- Treinamento de Conscientização: Forneça treinamento e conscientização em segurança cibernética para todos os funcionários, enfatizando a importância do uso responsável de credenciais de acesso.
- Implementação de Política de Senhas Fortes: Exija senhas fortes e complexas para autenticação, e promova a troca regular de senhas para evitar comprometimentos de segurança.
- Gerenciamento de Privacidade: Assegure a conformidade com regulamentos de privacidade, como o GDPR, ao controlar e proteger o acesso a dados pessoais.

A adoção dessas melhores práticas de mercado dentro da Access & Authorization Management é essencial para garantir um controle estrito sobre o acesso a sistemas e dados, protegendo a confidencialidade, integridade e disponibilidade dos ativos de TI da organização.

Além disso, contribui para uma postura de segurança cibernética robusta, minimizando os riscos de acesso não autorizado e mantendo a confiança de clientes e parceiros.

Desafios Atuais

A Capability de Access & Authorization Management desempenha um papel vital na segurança cibernética das organizações, garantindo que o acesso a sistemas e dados seja estritamente controlado e autorizado.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam diversos desafios atuais de mercado.

Abaixo, os principais desafios com base nas melhores práticas do mercado:

- Identidade Digital Complexa: Com o aumento do número de dispositivos e aplicativos usados no ambiente corporativo, a gestão de identidades se

torna mais complexa, exigindo soluções que garantam identidades digitais precisas e atualizadas.

- Autenticação Forte: A necessidade de implementar autenticação forte, como a autenticação multifatorial (MFA), para proteger contra ameaças cibernéticas torna-se um desafio, especialmente para garantir a usabilidade e a segurança simultaneamente.
- Controle Granular de Acesso: Definir políticas de acesso altamente específicas e controlar o acesso com base em funções, departamentos e níveis de privilégio é um desafio, garantindo que apenas usuários autorizados tenham acesso apropriado.
- Auditoria Abrangente: Registrar e monitorar todas as atividades de acesso para detecção de comportamentos suspeitos ou violações de segurança exige recursos significativos.
- Segurança na Nuvem: Estender o gerenciamento de identidades, autenticação e autorizações para ambientes de nuvem apresenta desafios específicos relacionados à integração e segurança em um cenário em constante evolução.
- Gestão de Identidades Privilegiadas: Gerenciar identidades com privilégios elevados, como administradores de sistema, é crítico para evitar abusos e ameaças internas, mas requer uma abordagem específica.
- Conformidade Regulatória: Garantir que os sistemas de Access & Authorization estejam em conformidade com regulamentações de segurança cibernética é um desafio constante, especialmente em ambientes altamente regulamentados.
- Complexidade do Ambiente Tecnológico: A integração da Access & Authorization Management em um ambiente tecnológico diversificado e em constante mudança requer planejamento e estratégias adaptáveis.
- Treinamento e Conscientização: Educar os funcionários sobre as melhores práticas de segurança cibernética e conscientizá-los sobre os riscos é fundamental, mas pode ser um desafio em uma organização em constante evolução.
- Adoção de Novas Tecnologias: Incorporar novas tecnologias, como biometria e autenticação baseada em comportamento, pode ser desafiador devido aos investimentos necessários e à necessidade de integração com sistemas legados.

Esses desafios atestam a importância crítica da Capability de Access & Authorization

Management no contexto da segurança cibernética.

Superá-los exige abordagens inovadoras, investimentos em tecnologia e treinamento, além de uma cultura de segurança sólida em toda a organização.

A capability de gerenciar o acesso de forma eficaz é essencial para garantir que apenas usuários autorizados tenham acesso a recursos específicos, protegendo assim a confidencialidade, integridade e disponibilidade dos ativos de TI da organização.

Tendências para o Futuro

A Capability de Access & Authorization Management, inserida na macro capability de Operation e na camada de Cybersecurity, desempenha um papel crucial na proteção de informações críticas, prevenindo o acesso não autorizado e garantindo a conformidade com regulamentações de segurança cibernética.

Para compreender as tendências futuras que moldarão essa capability, é fundamental considerar as expectativas do mercado e as inovações emergentes.

A seguir, as principais tendências para o futuro no contexto do CIO Codex Capability Framework:

- Zero Trust como Padrão: A abordagem Zero Trust, que não confia automaticamente em nenhum usuário ou dispositivo, se tornará a norma na Access & Authorization Management, reforçando a segurança em todos os pontos de acesso.
- Autenticação Contínua: A autenticação contínua, que monitora e verifica constantemente a identidade dos usuários durante suas sessões, será amplamente adotada para combater ameaças persistentes.
- Inteligência Artificial na Detecção de Anomalias: A IA será implementada para a detecção de comportamentos anômalos, permitindo uma resposta rápida a atividades suspeitas que possam indicar acesso não autorizado.
- Blockchain para Gestão de Identidades: A tecnologia blockchain será utilizada na gestão de identidades, proporcionando um registro inalterável de identidades e permissões, aumentando a confiabilidade.
- Biometria Avançada: A biometria evoluirá com métodos avançados, como análise de padrões de digitação e reconhecimento de veias, fortalecendo a autenticação biométrica.

- Proteção de Dados na Origem: A Access & Authorization Management se concentrará na proteção de dados desde a sua criação, incorporando criptografia e controle de acesso em nível granular.
- Integração de IoT e Acesso: Com a expansão da Internet das Coisas (IoT), a capability se adaptará para gerenciar o acesso de dispositivos IoT de forma segura.
- Foco em Privacidade: A privacidade dos dados do usuário ganhará destaque, com o consentimento explícito e o controle dos próprios dados sendo prioridades na gestão de acessos.
- Gestão de Acessos em Nuvem Híbrida: Com ambientes de nuvem híbrida, a Access & Authorization Management será estendida para garantir que os acessos sejam consistentes em todas as plataformas.
- Zero Passwords: A eliminação gradual de senhas tradicionais em favor de métodos mais seguros, como MFA e biometria, será uma tendência importante na autenticação.

Essas tendências refletem a crescente complexidade do cenário de segurança cibernética e a necessidade de inovação contínua na Access & Authorization Management.

À medida que ameaças cibernéticas evoluem, essa capability continuará a desempenhar um papel crítico na proteção dos ativos de TI e na garantia da confidencialidade e integridade das informações.

KPIs Usuais

A capability de Access & Authorization Management, inserida na macro capability Operation e na camada Cybersecurity, desempenha um papel crucial na proteção de informações críticas, na prevenção de acessos não autorizados e na garantia da conformidade com regulamentações de segurança cibernética.

Para avaliar eficazmente o desempenho dessa capability, é essencial acompanhar uma série de KPIs usuais que fornecem insights sobre a gestão de identidades, autenticação e autorização.

Abaixo, uma lista dos principais KPIs usualmente utilizados no mercado dentro do contexto do CIO Codex Capability Framework:

- Taxa de Autenticação Bem-Sucedida (Successful Authentication Rate): Mede a porcentagem de tentativas de autenticação que são bem-sucedidas, demonstrando a eficácia dos métodos de verificação de identidade.
- Tempo Médio de Processamento de Solicitações de Acesso (Mean Access Request Processing Time): Calcula o tempo médio necessário para processar solicitações de acesso, avaliando a eficiência do processo de autorização.
- Taxa de Conformidade com Políticas de Acesso (Access Policy Compliance Rate): Avalia a aderência às políticas de acesso estabelecidas pela organização, garantindo que apenas usuários autorizados tenham permissão para acessar recursos específicos.
- Taxa de Contas de Usuário Desativadas (Disabled User Accounts Rate): Indica a frequência com que contas de usuário são desativadas quando não mais necessárias, reduzindo o risco de acessos não autorizados.
- Taxa de Acessos Não Autorizados Detectados (Detected Unauthorized Access Rate): Mede a porcentagem de acessos não autorizados que são identificados e bloqueados de forma proativa.
- Tempo Médio de Resposta a Incidentes de Acesso Não Autorizado (Mean Unauthorized Access Incident Response Time): Calcula o tempo médio necessário para responder a incidentes de acesso não autorizado, minimizando o tempo de exposição a riscos.
- Taxa de Auditorias de Acesso Realizadas (Access Audits Conducted Rate): Avalia a frequência com que auditorias de acesso são conduzidas para verificar e validar as permissões de usuário.
- Taxa de Acessos Privilegiados Monitorados (Monitored Privileged Access Rate): Indica a porcentagem de acessos privilegiados que são continuamente monitorados para detectar atividades suspeitas.
- Taxa de Acessos Baseados em Função (Role-Based Access Rate): Avalia a proporção de acessos concedidos com base nas funções e responsabilidades dos usuários, seguindo uma abordagem de menor privilégio.
- Taxa de Autenticação Multifatorial Implementada (Implemented Multifactor Authentication Rate): Mede a adoção de autenticação multifatorial (MFA) para reforçar a segurança de autenticação.
- Taxa de Auditorias de Contas de Usuário (User Account Audits Rate): Avalia a frequência com que as contas de usuário são auditadas para

identificar contas inativas ou suspeitas.

- Taxa de Treinamento em Segurança de Acesso (Access Security Training Rate): Indica a porcentagem de membros da equipe que receberam treinamento em práticas de segurança de acesso.
- Taxa de Revisão de Políticas de Acesso (Access Policy Review Rate): Mede a frequência com que as políticas de acesso são revisadas e atualizadas para acompanhar as mudanças nas necessidades de segurança.
- Taxa de Identidades de Usuário Gerenciadas (Managed User Identities Rate): Avalia a proporção de identidades de usuário gerenciadas de forma centralizada, garantindo a precisão das informações de acesso.
- Taxa de Acessos em Nuvem Gerenciados (Managed Cloud Access Rate): Indica a porcentagem de acessos a recursos em nuvem que são gerenciados e controlados de acordo com as políticas de segurança.

Esses KPIs desempenham um papel fundamental na avaliação da eficácia da Access & Authorization Management.

Eles fornecem uma visão abrangente da segurança de identidades, autenticação e autorização, permitindo que as organizações identifiquem áreas de melhoria, fortaleçam suas defesas cibernéticas e garantam que apenas usuários autorizados tenham acesso a recursos críticos.

A medição constante desses indicadores é essencial para manter a integridade e a confidencialidade dos ativos de TI da organização.

Exemplos de OKRs

A capability de Access & Authorization Management na macro capability Operation da camada Cybersecurity desempenha um papel vital no controle rigoroso do acesso a sistemas e dados.

Essa capability inclui a gestão de identidades, autenticação e autorizações, assegurando que apenas usuários autorizados tenham acesso aos recursos adequados.

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

Gestão de Identidades Eficiente

Objetivo: Garantir que todas as identidades de usuário sejam gerenciadas de forma eficaz e segura.

- KR1: Manter um registro centralizado de todas as identidades de usuário.
- KR2: Implementar políticas de senha fortes e práticas de autenticação multifator.
- KR3: Automatizar o processo de provisionamento e desprovisionamento de contas de usuário.

Controle de Acesso Baseado em Funções

Objetivo: Implementar um modelo de controle de acesso baseado em funções.

- KR1: Definir funções de usuário com base nas responsabilidades e necessidades de acesso.
- KR2: Atribuir permissões de acordo com as funções de usuário.
- KR3: Realizar revisões regulares das funções e permissões para garantir a conformidade.

Monitoramento de Acesso e Atividades

Objetivo: Monitorar e registrar todas as atividades de acesso.

- KR1: Implementar ferramentas de monitoramento de acesso em tempo real.
- KR2: Registrar todas as tentativas de acesso, incluindo as não autorizadas.
- KR3: Analisar regularmente os logs de acesso para detectar atividades suspeitas.

Auditorias de Conformidade

Objetivo: Garantir que todas as políticas de acesso estejam em conformidade.

- KR1: Realizar auditorias regulares de conformidade.
- KR2: Identificar e corrigir desvios de conformidade.
- KR3: Manter documentação completa das políticas de acesso e

procedimentos.

Resposta a Incidentes de Segurança

Objetivo: Responder rapidamente a incidentes de acesso não autorizado.

- KR1: Ter um plano de resposta a incidentes de segurança bem definido.
- KR2: Implementar procedimentos para bloquear contas comprometidas.
- KR3: Realizar análises pós-incidente para identificar falhas e melhorar a segurança.

Educação e Conscientização dos Usuários

Objetivo: Educar os usuários sobre práticas seguras de acesso.

- KR1: Oferecer treinamento de segurança cibernética para todos os usuários.
- KR2: Promover a conscientização sobre phishing e engenharia social.
- KR3: Estabelecer um programa contínuo de conscientização em segurança.

Através desses OKRs, a capability de Access & Authorization Management busca garantir que apenas usuários autorizados tenham acesso aos recursos adequados, prevenindo assim o acesso não autorizado e protegendo contra ameaças internas e externas.

O controle rigoroso do acesso é fundamental para manter a segurança dos sistemas e dados da organização.

Critérios para Avaliação de Maturidade

A capability Access & Authorization Management, inserida na macro capability Operation e na camada Cybersecurity, desempenha um papel crítico no controle rigoroso do acesso a sistemas e dados.

Para avaliar sua maturidade, seguem critérios inspirados no modelo CMMI,

considerando cinco níveis de maturidade: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

Nível de Maturidade Inexistente

- Não há processos para gerenciar acessos e autorizações.
- Ausência de políticas de controle de acesso.
- Falta de mecanismos de autenticação.
- Inexistência de registros de atividades de acesso.
- Nenhuma revisão de permissões de acesso.

Nível de Maturidade Inicial

- Alguns esforços iniciais para gerenciar acessos, mas sem processos definidos.
- Políticas de controle de acesso rudimentares.
- Autenticação básica implementada.
- Registros limitados de atividades de acesso.
- Revisões esporádicas de permissões.

Nível de Maturidade Definido

- Processos formalizados para gerenciar acessos e autorizações.
- Políticas de controle de acesso estabelecidas e documentadas.
- Implementação de autenticação robusta.
- Registros detalhados e armazenamento seguro de atividades de acesso.
- Revisões regulares e controle de permissões.

Nível de Maturidade Gerenciado

- Processos de gerenciamento de acessos eficazes e eficientes.
- Políticas de controle de acesso adaptativas às necessidades.
- Autenticação avançada e monitoramento contínuo de identidades.
- Análise de atividades de acesso para detecção de anomalias.

- Revisões automáticas e auditorias de permissões.

Nível de Maturidade Otimizado

- Processos de gerenciamento de acessos altamente otimizados e integrados.
- Políticas de controle de acesso dinâmicas baseadas em inteligência de ameaças.
- Autenticação avançada, incluindo autenticação multifator.
- Análise de comportamento de usuários e detecção proativa de ameaças.
- Revisões automatizadas e adaptação dinâmica de permissões.

A avaliação de maturidade da capability Access & Authorization Management é essencial para garantir que apenas usuários autorizados tenham acesso aos recursos adequados, prevenindo o acesso não autorizado e protegendo contra ameaças internas e externas.

À medida que a maturidade aumenta, o controle de acessos se torna mais eficaz e adaptável às ameaças em constante evolução.

Convergência com Frameworks de Mercado

A capability Access & Authorization Management, parte da macro capability Operation na camada Cybersecurity, é essencial para o controle rigoroso do acesso a sistemas e dados.

Esta capability inclui a gestão de identidades, autenticação e autorizações, garantindo que apenas usuários autorizados tenham acesso aos recursos adequados.

Esta função é vital para prevenir o acesso não autorizado e proteger contra ameaças internas e externas.

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, com sua ênfase na governança de TI e gestão de riscos, alinha-se estreitamente com Access & Authorization Management. Esta capability apoia o COBIT na implementação de controles eficazes para a governança de acesso e identidades, contribuindo para a mitigação de riscos de segurança da informação.

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL, focado na gestão de serviços de TI, integra a Access & Authorization Management em seus processos, especialmente na gestão de serviços e operações. Esta integração ajuda a garantir que os serviços de TI sejam acessados de forma segura e controlada.

SAFe

- Nível de Convergência: Médio
- Racional: O SAFe, como um framework ágil, beneficia-se da Access & Authorization Management para assegurar que as práticas ágeis sejam realizadas em um ambiente seguro, especialmente em organizações que aplicam DevSecOps.

PMI

- Nível de Convergência: Baixo
- Racional: Embora o PMI, com foco na gestão de projetos, não trate diretamente de aspectos de segurança, a Access & Authorization Management pode ser aplicada nos projetos de TI para garantir a segurança do acesso às informações do projeto.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI, ao focar na maturidade dos processos de TI, se beneficia da Access & Authorization Management para integrar práticas de segurança nos processos, contribuindo para a melhoria contínua.

TOGAF

- Nível de Convergência: Médio
- Racional: O TOGAF, que aborda a arquitetura empresarial, pode incorporar a Access & Authorization Management para assegurar que a segurança seja uma consideração central na arquitetura de TI.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em DevOps SRE, onde a segurança é integrada ao ciclo de vida de desenvolvimento e operação, a Access & Authorization Management é crucial para garantir a segurança no processo de entrega contínua.

NIST

- Nível de Convergência: Alto
- Racional: O NIST, com suas diretrizes de segurança cibernética, alinha-se fortemente com a Access & Authorization Management. Esta capability apoia as recomendações do NIST na implementação de controles de acesso eficazes e na gestão de identidades.

Six Sigma

- Nível de Convergência: Baixo
- Racional: O Six Sigma, focado na melhoria da qualidade dos processos, tem uma convergência limitada com a Access & Authorization

Management. No entanto, práticas eficazes de gestão de acesso podem contribuir para a redução de defeitos e melhorias na qualidade.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT, com seu foco em eficiência e eliminação de desperdícios, pode se beneficiar indiretamente da Access & Authorization Management ao garantir a segurança e eficiência nos processos de TI.

A capability Access & Authorization Management é fundamental no atual panorama de segurança cibernética, fornecendo a base para uma postura de segurança robusta e adaptável.

KPIs relevantes podem incluir o número de violações de acesso detectadas, o tempo médio para concessão de acesso e a eficácia dos controles de autorização.

Esta capability assegura a integridade e a confidencialidade dos dados e sistemas, sendo crucial para a resiliência cibernética da organização.

Processos e Atividades

Develop Access Management Plans

O desenvolvimento de planos detalhados para a gestão de acessos e autorizações é um processo essencial para assegurar que todos os usuários tenham o acesso correto e necessário aos recursos de TI.

Este processo envolve a criação de um framework abrangente que define políticas, procedimentos e responsabilidades relacionados ao acesso.

Inicialmente, é feita uma análise das necessidades de acesso, considerando as funções e responsabilidades de cada usuário.

Em seguida, são estabelecidas as políticas de acesso, incluindo a definição de permissões e restrições baseadas em funções.

O plano também deve incorporar métodos de autenticação, como autenticação

multifatorial (MFA), para fortalecer a segurança.

Além disso, o plano precisa incluir procedimentos de revisão periódica de acessos e auditorias para garantir a conformidade e a eficácia das políticas implementadas.

A documentação detalhada do plano é crucial para que todos os stakeholders compreendam suas responsabilidades e as medidas a serem adotadas para proteger os recursos de TI contra acessos não autorizados.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Access Needs Analysis	Realizar análise das necessidades de acesso dos usuários e sistemas.	Dados de funções e responsabilidades	Relatório de necessidades de acesso	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Define Access Policies	Definir políticas de acesso com base nas necessidades identificadas.	Relatório de necessidades de acesso	Políticas de acesso definidas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity

3	Establish Authentication Methods	Estabelecer métodos de autenticação, incluindo MFA.	Políticas de acesso definidas	Métodos de autenticação definidos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Develop Review Procedures	Desenvolver procedimentos para revisão periódica dos acessos e auditorias.	Métodos de autenticação definidos	Procedimentos de revisão definidos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
5	Document Access Management Plan	Documentar detalhadamente o plano de gestão de acessos e autorizações.	Procedimentos de revisão definidos	Plano de gestão de acessos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Identify Access Requirements

A identificação dos requisitos de acesso é um processo fundamental para garantir que os usuários e sistemas tenham as permissões adequadas e necessárias para desempenhar suas funções.

Este processo envolve a coleta de informações sobre as funções e responsabilidades dos usuários, bem como a análise dos sistemas e dados aos quais precisam ter acesso.

A colaboração com as diversas áreas de TI e negócios é crucial para compreender as necessidades específicas de cada departamento.

Uma vez coletadas as informações, os requisitos de acesso são documentados e classificados, garantindo que todas as permissões sejam atribuídas com base na

necessidade de saber e no princípio do menor privilégio.

Este processo também inclui a revisão de quaisquer requisitos de conformidade e regulamentações que possam impactar a gestão de acessos.

- PDCA focus: Plan
- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Gather User Role Information	Coletar informações sobre as funções e responsabilidades dos usuários.	Dados de funções e responsabilidades	Relatório de funções de usuários	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Analyze System Access Needs	Analisar as necessidades de acesso aos sistemas e dados.	Relatório de funções de usuários	Relatório de necessidades de acesso	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Collaborate with Departments	Colaborar com diferentes departamentos para entender as necessidades específicas de acesso.	Relatório de necessidades de acesso	Requisitos de acesso identificados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Document Access Requirements	Documentar os requisitos de acesso identificados de forma detalhada.	Requisitos de acesso identificados	Documentação de requisitos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Review Compliance Needs	Revisar os requisitos de conformidade e regulamentação relacionados ao acesso.	Documentação de requisitos	Requisitos de conformidade revisados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Implement Access Control Solutions

A implementação das soluções de controle de acesso conforme planejado é um passo crucial para assegurar que os sistemas e dados da organização estejam protegidos contra acessos não autorizados.

Este processo envolve a configuração de sistemas de gerenciamento de identidades e acessos (IAM), a aplicação das políticas de acesso definidas e a integração de métodos de autenticação, como MFA.

Além disso, é importante realizar testes para garantir que as soluções de controle de acesso funcionem corretamente e não impactem negativamente a operação dos sistemas.

A colaboração entre as equipes de Cybersecurity, IT Infrastructure & Operation e Solution Engineering & Development é fundamental para garantir que as soluções sejam implementadas de forma eficaz e eficiente.

A documentação completa das implementações realizadas é essencial para auditorias futuras e para a manutenção das soluções de controle de acesso.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Configure IAM Systems	Configurar sistemas de gerenciamento de identidades e acessos (IAM).	Políticas de acesso definidas	Sistemas IAM configurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Apply Access Policies	Aplicar políticas de acesso nos sistemas e dados conforme definido.	Sistemas IAM configurados	Políticas de acesso aplicadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Integrate MFA Methods	Integrar métodos de autenticação multifatorial (MFA) nos sistemas.	Políticas de acesso aplicadas	MFA integrado	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
4	Conduct Access Testing	Realizar testes para garantir a eficácia das soluções de controle de acesso.	MFA integrado	Resultados de testes	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

5	Document Implementations	Documentar as implementações realizadas e as configurações aplicadas.	Resultados de testes	Documentação de implementações	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

Monitor Access Control Performance

O monitoramento contínuo do desempenho dos controles de acesso é vital para assegurar que as políticas e mecanismos de segurança estejam funcionando conforme o esperado e para detectar qualquer anomalia ou tentativa de acesso não autorizado.

Este processo envolve a coleta e análise de logs de acesso, a realização de auditorias regulares e a revisão das métricas de desempenho dos sistemas de controle de acesso.

A implementação de ferramentas de monitoramento em tempo real e a utilização de inteligência de segurança ajudam a identificar e responder rapidamente a incidentes de segurança.

A comunicação regular dos resultados do monitoramento às partes interessadas é essencial para manter a transparência e garantir que os controles de acesso sejam constantemente aprimorados.

- PDCA focus: Check
- Periodicidade: Mensal

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Collect Access Logs	Coletar logs de acesso de sistemas e aplicativos.	Logs de sistemas e aplicativos	Logs de acesso coletados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Analyze Access Metrics	Analisar métricas de acesso para avaliar a eficácia dos controles implementados.	Logs de acesso coletados	Relatórios de análise de métricas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
3	Conduct Access Audits	Realizar auditorias de acesso para identificar possíveis violações ou anomalias.	Relatórios de análise de métricas	Relatórios de auditoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Generate Performance Reports	Gerar relatórios de desempenho com base na análise e nas auditorias realizadas.	Relatórios de auditoria	Relatórios de desempenho	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

5	Communicate Findings	Comunicar as descobertas e recomendações para as partes interessadas.	Relatórios de desempenho	Relatórios comunicados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Review and Optimize Access Control Processes

A revisão e otimização dos processos de controle de acesso são fundamentais para garantir que as medidas de segurança evoluam em resposta a novas ameaças e requisitos organizacionais.

Este processo envolve a análise dos resultados do monitoramento e auditorias para identificar áreas de melhoria.

As práticas de controle de acesso são então ajustadas para reforçar a segurança e melhorar a eficiência operacional.

Este processo também inclui a atualização das políticas de acesso, a realização de treinamentos regulares e a validação das novas práticas de segurança através de testes contínuos.

A otimização contínua garante que a organização esteja sempre preparada para proteger seus ativos contra acessos não autorizados.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Analyze Audit Findings	Analisar as descobertas das auditorias e do monitoramento de desempenho.	Relatórios de auditoria	Análise de descobertas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Identify Improvement Areas	Identificar áreas de melhoria nos processos de controle de acesso com base na análise.	Análise de descobertas	Lista de áreas de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Update Access Policies	Atualizar as políticas de acesso para incorporar as melhorias identificadas.	Lista de áreas de melhoria	Políticas de acesso atualizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Conduct Training Sessions	Realizar sessões de treinamento para assegurar que a equipe esteja familiarizada com as políticas atualizadas.	Políticas de acesso atualizadas	Sessões de treinamento realizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Validate Security Practices	Validar as práticas de segurança através de testes e auditorias contínuas.	Políticas de acesso atualizadas	Práticas validadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity