adaQuest

CNJ Resolução 396

Versão 1.0 – 1º de março de 2022

Autores:

Hiram Machado (Master in Cybersecurity and Leadership)

Fabricio Assumpção, MCP, MBA (Arquiteto de Solução de Segurança)

Tom Vitti (Design Gráfico, Ilustração e Revisão)

Adriana Tanikawa (Edição e Revisão de Texto)

Disclaimer

As informações veiculadas neste eBook são recomendações fornecidas apenas para fins informativos. Estas informações não constituem assessoria jurídica, certificações ou garantias relativas ao cumprimento regulatório; cabe a cada organização avaliar a eficácia dessas recomendações em seu respectivo ambiente regulatório antes da implementação. As organizações devem consultar seus próprios profissionais legais para determinar como as normas ou regulamentos se aplicam à sua organização e como garantir melhor a conformidade.

A ADAQUEST NÃO DISPONIBILIZA GARANTIAS, EXPRESSAS, IMPLÍCITAS OU ESTATUTÁRIAS, QUANTO ÀS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO. Este eBook é fornecido "como está". As informações e recomendações expressas neste eBook podem ser trocadas ou atualizadas sem aviso prévio.

Índice

Prefácio

"O mundo mudou na última década, isso está mais que evidente e todos nós vivenciamos uma mudança hercúlea nos nossos hábitos diários e o consumo de recursos tecnológicos explodiram de forma vertiginosa, cujo o qual, nossos devices são literalmente extensões de nossos corpos, até mesmo os vestimos. Com esse aumento de consumo de tecnologia, precisamos nos atualizar como indivíduos e como corporações públicas ou privadas sobre Segurança Cibernética, e nessa década de 20 é o grande tema para todas as organizações em todo o mundo.

As agências governamentais são particularmente vulneráveis a ataques cibernéticos de maneiras diferentes das organizações comerciais. Elas geralmente mantêm dados confidenciais de cidadãos e de segurança nacional em sua infraestrutura de TI, o que muda o comportamento do atacante, pois, diferentemente de uma empresa comercial, normalmente o atacante não busca um retorno financeiro direto com um ataque em uma instituição governamental, mas sim Informação, o que em pesquisas recentes colocam o Brasil como o 2 maior alvo de ataques cibernéticos.*

À medida que o mundo da TI se move para a nuvem e cada vez mais dispositivos pessoais se conectam à rede, torna-se imperativo estabelecer soluções de segurança mais sofisticadas para combater os ataques cibernéticos sofisticados em constante crescimento. Muitas novas regulamentações e leis estão sendo emitidas por órgãos legisladores para ajudar a forçar um nível mínimo de melhores práticas de segurança cibernética e governar as expectativas. Órgãos governamentais estão emitindo resoluções específicas para abordar o cumprimento dessas normas e leis e garantir que haja a consistência da aplicação das melhores práticas de segurança cibernética entre todos os órgãos\filiais de uma determinada entidade governamental, como é o caso da Resolução 396 emitida pelo CNJ.

Tive o prazer de ter a oportunidade de ler este eBook e ver como os diferentes aspectos da Resolução 396 do CNJ foram organizados de uma forma mais simples de entender, e quais soluções técnicas específicas podem ser consideradas e aplicadas. Este eBook fornece uma visão geral estratégica que deve ajudar as diferentes Tribunais afetados por esta resolução a começar com seu próprio planejamento estratégico de cibersegurança, aumentando a adoção de tecnologias, garantindo sua transformação digital com segurança e o cumprimento das exigencias estabelecidas nesta resolução. Tenho certeza de que os leitores também vão gostar."

*Brasil é 2º maior alvo mundial de ciberataques, revela estudo - Notícias - R7 Tecnologia e Ciência

Luciano Lourenço

Security Executive for Public Sector

Microsoft

Introdução

Este ebook tem o objetivo de esclarecer os requisitos estabelecidos na Resolução do CNJ Nº 396 de 7 de julho de 2021 e fazer o alinhamento destes requerimentos com tecnologias Microsoft que podem ser adotadas para assegurar conformidade com esta resolução.

Esperamos que este documento possa ser usado como guia para construir um planejamento estratégico de como utilizar tecnologias Microsoft com recursos que muitas vezes já estão disponíveis na contratação de licenças do Microsoft 365 ou Serviços do Azure, mas a equipe de gestão pode não ter o conhecimento desses recursos.

Nesta Resolução existem referências a outras resoluções, normas, leis, portarias e atos normativos. O escopo deste documento se destina apenas ao estudo e alinhamento das soluções com a Resolução CNJ Nº 396.

Dividimos as necessidades de ações baseadas nos requisitos da resolução entre as seguintes áreas de atuação:

Todas as ações a serem aplicadas devem usar como base a Lei Geral de Proteção de Dados (LGPD) e a Norma NBR ISO/IEC 27001:2013 como referência de melhores práticas de implementação dos recursos técnicos.

As principais áreas de atuação incluem a Gestão de Identidade & Acesso, que endereça os controles e a segurança das identidades e acesso de usuários do sistema tanto internos como externos. A Gestão de Dispositivos exige um tratamento adequado ao controle de dispositivos móveis ou fixos para que evitem que dispositivos antigos ou fora de conformidade com as regras de segurança acessem a rede. A Gestão da Segurança e Tratamento de Incidentes de ameaças cibernéticas tem como objetivo criar uma postura proativa e atuante na detecção, investigação e remediação dessas ameaças, tornando todo o ambiente digital mais seguro e resiliente. Por fim, em Avaliações da Postura de Segurança, será preciso criar um ritmo de avaliação semestral para garantir que todas as ações e implementações estejam de fato gerando resultados positivos e melhorando a maturidade e postura da segurança.

Cada um destes assuntos será tratado nos capítulos seguintes.

Expectativas da Resolução

Todos os órgãos governamentais associados ao CNJ deverão entrar em conformidade com esta resolução. Para assegurar uma Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), passa a ser obrigatória a criação de um Comitê de Governança de Segurança da Informação em cada TJ, e um mesmo comitê a nível de CNJ. Este comitê deverá dar apoio a criação de um Centro de Prevenção, Tratamento e Reposta a Incidentes Cibernéticos (CPTRIC-PJ).

Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)

A Resolução CNJ Nº 396 tem como objetivo assegurar uma Estratégia Nacional de Segurança Cibernética (ENSEC-PJ), no âmbito dos órgãos do Poder Judiciário, inclusive do Supremo Tribunal Federal (STF).

Esta estratégia aborda temas relacionados à segurança da informação que sejam essenciais para a segurança cibernética, incluindo segurança física e proteção dos dados pessoais e institucionais. A Resolução visa assegurar a: Disponibilidade, Integridade, Confidencialidade e Autenticidade dos dados e informações. Estes que são considerados os pilares que fazem parte dos princípios básicos de segurança da informação.

Conformidade com esses pilares objetivam assegurar o funcionamento dos processos de trabalho e a continuidade operacional das atividades administrativas de cada órgão afetado. É preciso também levar em consideração ações relacionadas a comunicação, conscientização, educação, formação de cultura e direcionamento institucional.

A criação desta Estratégia Nacional tem também o intuito de aprimorar o nível de maturidade em segurança cibernética do Poder Judiciário, com o objetivo de tornar o espaço cibernético dos órgãos do poder judiciário mais desenvolvido, confiável, resistente, inclusivo e seguro no ambiente digital, permitindo assim a manutenção e a continuidade dos serviços; ou o seu restabelecimento em menor tempo possível no caso de eventual incidente cibernético.

Para se obter sucesso é essencial o engajamento da alta administração de cada tribunal, incluindo a liderança de alto escalão e tomadores de decisão; em caso de algum ataque comprometer a rede e decisões rápidas precisarem ser tomadas a respeito de uma eventual pausa nos serviços disponíveis ao público para evitar maiores danos e alastramento de um eventual ataque.

D	**Disponibilidade** Garantir que usuários legítimos tenham sempre acesso aos dados e recursos tecnológicos quando necessário.
I	**Integridade** Garantir a consistência dos dados, prevenindo a criação, alteração ou destruição dos dados por pessoas não autorizadas.
C	**Confidencialidade** Garantir que as informações não serão reveladas a pessoas não autorizadas.
A	**Autenticidade** Garantir que a pessoa usando uma identificação é de fato quem ela diz ser.

Comitê de Governança da Segurança da Informação (CGSI)

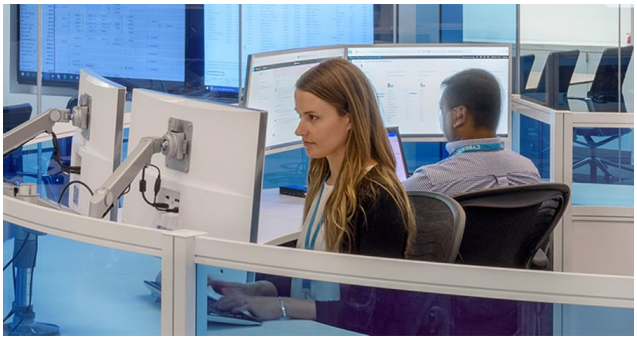
Todos os Órgãos do Poder Judiciário deverão constituir um "Comitê de Governança de Segurança da Informação (CGSI). O CGSI tem como obrigação garantir que haja profissionais com formação acadêmica e formação técnica bem como garantir a reciclagem de profissionais de tecnologia da informação e comunicação que atuem na área de cibersegurança.

Além do CGSI de cada órgão, está constituído também o CGSI-PJ a nível de CNJ. É um comitê que deverá ser composto com os seguintes integrantes de cada um dos seguintes órgãos:

- ❑ **Conselho Nacional de Justiça (2)**
- ❑ **Supremo Tribunal Federal (2)**
- ❑ **Superior Tribunal de Justiça (1)**
- ❑ **Tribunal Superior Eleitoral (1)**
- ❑ **Tribunal Superior do Trabalho (1)**
- ❑ **Conselho Superior da Justiça do Trabalho (1)**
- ❑ **Conselho da Justiça Federal (1)**
- ❑ **Superior Tribunal Militar (1)**
- ❑ **Tribunais de Justiça Estaduais (2)**

Todos esses representantes serão designados pela Presidência do Conselho Nacional de Justiça. Este grupo será coordenado por um representante do CNJ. O Conselho poderá então convidar outros representantes de órgão públicos e privados que estejam dispostos a subsidiar os respectivos trabalhos, mas é uma exigência que estes representantes tenham conhecimento técnico na área de segurança da informação. Esse comitê se reunirá semestralmente, mas poderá ser convocado por seu coordenador para reuniões extraordinárias.

Caberá a esse comitê assessorar o CNJ para estabelecer normas sobre a definição de requisitos metodológicos para a implementação da gestão de risco dos ativos da informação do Poder Judiciário assim como aprovar políticas, diretrizes, estratégias, normas e recomendações relacionas a segurança da informação, elaborar e implementar programas de conscientização e capacitação dos servidores do Poder Judiciário.



Centro de Prevenção, Tratamento e Resposta a Incidentes Ciberbéticos (CPTRIC-PJ)

Será função do CGSI também estabelecer critérios que permitam monitorar e avaliar o nível de maturidade em segurança da informação de cada órgão do Poder Judiciário assim como estabelecer norma de criação e funcionamento do Centro de Prevenção, Tratamento e Reposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ). O CPTRIC-PJ funcionará como um canal oficial de ações preventivas e corretiva em caso de ameaças ou ataques cibernéticos. E será o canal para promover a troca de informações e experiências com os comitês de gestores da informação de outros Poderes e Sociedade.

Cada órgão do Poder Judiciário deverá instituir e manter Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR). O ETIR funcionará como uma rede de equipes onde cada órgão do Poder Judiciário estará vinculado ao CPTRIC-PJ.

Gestão de Identidade e Acesso

Está estabelecido também a necessidade da implementação de um segundo fator de verificação para acesso externo. No que diz respeito ao acesso externo, podemos de um modo geral, considerar três grupos distintos de usuários do seu ambiente corporativo que possam precisar de acesso a recursos e aplicativos de sua rede:

1. Colaboradores internos que tenham a necessidade de acessar recursos da sua rede quando estão conectados dentro ou fora do seu domínio;
2. Prestadores de serviço que possam precisar de acesso a recursos do seu ambiente para uma melhor colaboração, mas não fazem parte do quadro de funcionários. De um modo geral, são funcionários ou colaboradores associados com uma organização privada ou governamental externa aos órgãos do Poder Judiciário;
3. Cidadãos ou usuários externos que possam depender de acesso a informações contidas no ambiente dos órgãos.

A Resolução também expressa a necessidade do respeito a promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de privacidade e o acesso à informação. Se busca também a garantia do sigilo das informações imprescindíveis à segurança da sociedade e do Estado e inviolabilidade da vida privada, da honra e da imagem das pessoas.

É obrigação de cada órgão, garantir os direitos de acesso citados acima, mas também é exigido o tratamento das informações com restrições de acesso, principalmente no que diz respeito à proteção dos dados pessoais e dos dados pessoais sensíveis, em conformidade com a legislação específica. Neste caso, a resolução se refere a Lei 13.709/2018 – Lei Geral de Proteção de Dados, que vamos tratar mais à frente.

O Capítulo VIII trata da gestão dos usuários. É exigido que sejam estabelecidos recursos tecnológicos para o gerenciamento de identidades, gerenciamento de acesso e gerenciamento de privilégios. É importante ter o entendimento da diferença entre esses requerimentos:

Gestão de Identidades	Gestão de Acesso	Gestão de Privilégios
Diz respeito ao tratamento do ciclo de vida de um usuário/credencial que tem direito de acesso ao ambiente digital da organização. Trata-se do ciclo de vida de uma identidade como cadastro, alteração de atributos e desligamento ou desativação da credencial.	Trata-se do entendimento e manutenção do direito de acesso de cada usuário/credencial. Ou seja, quais aplicativos, dados, sites ou informação que cada usuário tem o direito de acessar, editar, apagar ou apenas visualizar.	Toda organização tem diferentes níveis de acesso privilegiado, como Administradores Globais da rede, ou Administradores do Exchange. A gestão de privilégio permite por exemplo que esses administradores tenham apenas acesso administrativo quando precisam, e não sejam Administradores Globais permanentes. Podendo por exemplo, usar o MFA quando elevar a credencial para Administrador Global, e voltar a ser um usuário comum da rede quando não precisa de acesso privilegiado.

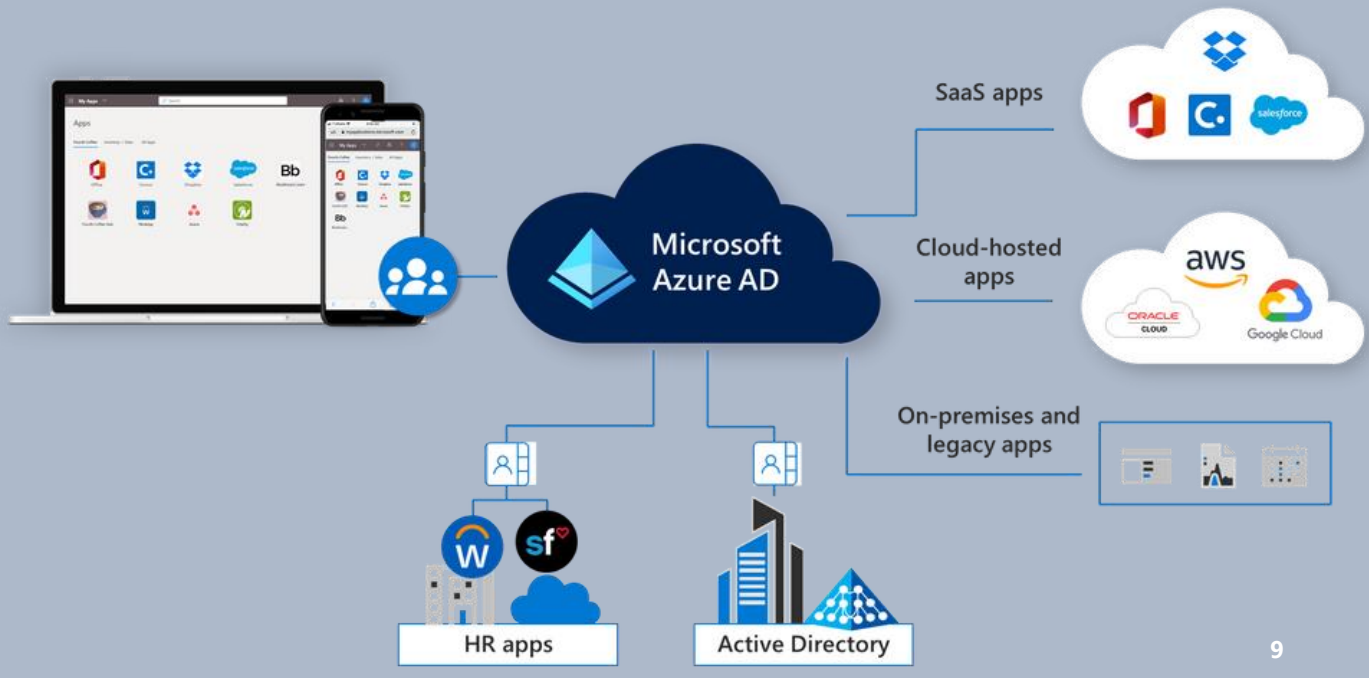
É possível abordar todos esses aspectos com o Azure Active Directory Premium 2 (AADP2), no que diz respeito a gestão de identidades. O AADP2 traz por exemplo recursos de governança tais como Vulnerabilidades e Contas de Risco. Para endereçar o Gerenciamento de Acesso, pode-se implementar "Políticas de Acesso Condicional Baseadas em Risco" e "Avaliações de Acesso". E para o Gerenciamento de Privilégios, pode-se implementar o PIM (Privileged Identity Management) e a "Gestão de Direitos".

O Microsoft Azure Active Directory possui modalidades de licenciamento diferentes que endereçam as necessidades de organização, gestão, controle de acesso e proteção de cada um destes três grupos de usuários mencionados acima provendo recursos e capacidades que permitam conformidade com as legislações que tratam de proteção e tratamento de dados sensíveis. São eles:

- Azure Active Directory Premium 1 and Premium 2
- Azure Active Directory B2B (Business to Business)
- Azure Active Directory B2C (Business to Consumer)

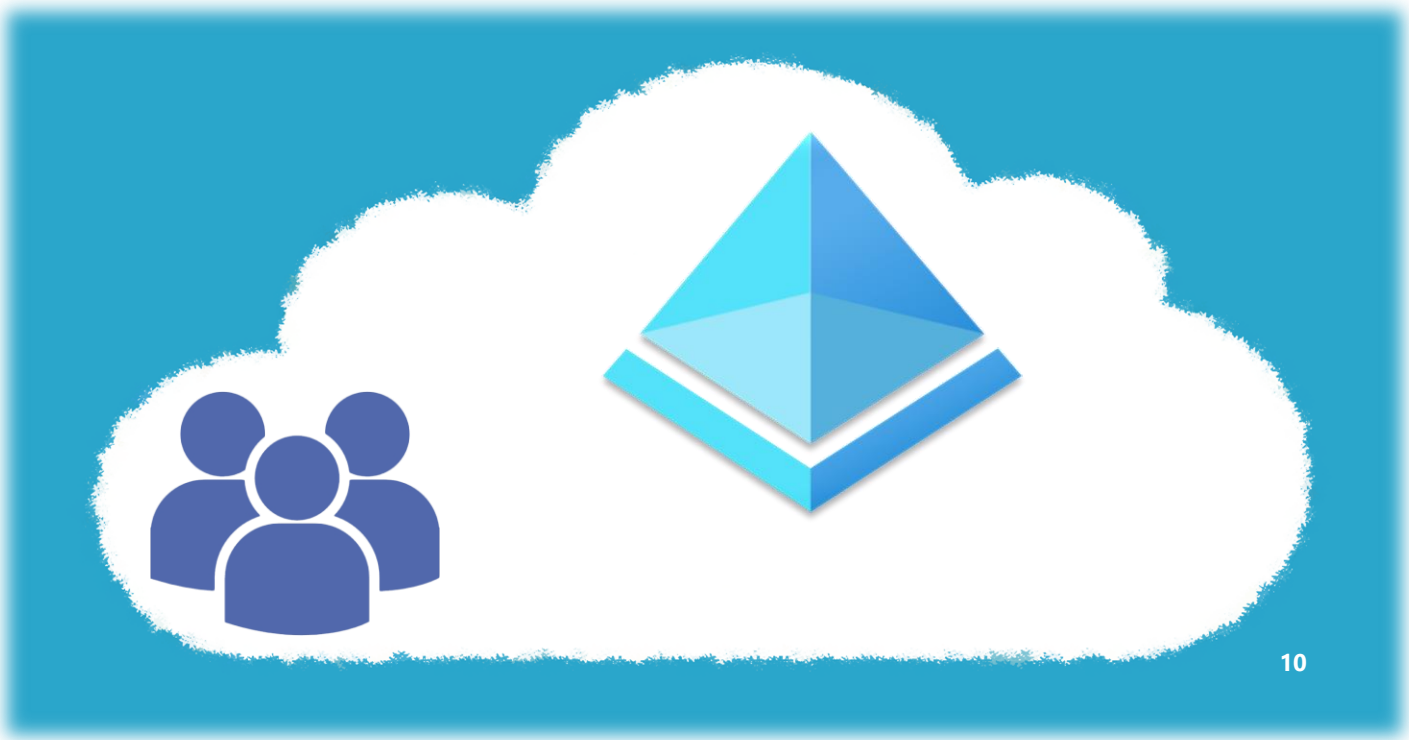
Azure Active Directory Premium 1 and Premium 2

O primeiro seria o Azure Active Directory Premium 1 ou Premium 2. Também conhecido como AADP1 e AADP2. Esta solução se aplicaria primeiramente ao primeiro grupo de usuários (Colaboradores Internos). AADP está incluso nas licenças de Microsoft 365 E3 (AADP1) e Microsoft 365 E5 (AADP2). Estas bases de dados de controle de identidade estão na nuvem, mas para uma organização que possui um ambiente local com Active Directory (AD) em um servidor local, é possível fazer a sincronização em tempo real do seu AD com o AADP usando o Azure AD Connect. Uma vez conectados, todos os recursos de segurança e administração de usuários se aplicarão aos dois ambientes.



AADP1 otimiza a gestão de controle de identidades e acesso provendo as seguintes funcionalidades:

Autenticação	Permite o controle de acesso e implementação de serviços tais como SSPR (Self-Service Password Reset), Multi-Factor Authentication, banir a habilidade do usuário de usar senhas fracas ou já conhecidas, bloquear o usuário em caso de atividades suspeitas e muito mais.
Gerenciamento de Acesso a Aplicações	Permite fazer a gestão de controle de acesso às aplicações na nuvem e em seu ambiente local usando um Application Proxy, utilização de SSO (Single Sign-On), e a utilização do My Apps Portal que é um portal que permite que usuários da sua rede facilmente descubram quais aplicativos estão aprovados para uso. Ele também se integra com Microsoft Defender for Cloud Apps.
Para desenvolveres de aplicativos	Através do uso de Microsoft Graph e APIs, é possível criar aplicativos que usem métodos de autenticação modernos e seguros.
Relatórios	Possui relatórios de segurança e de uso avançados para melhorar o monitoramento e as investigações.
Gestão de Acesso de Grupos	Ele permite também uma gestão integrada de acesso de grupos que incluem a criação de grupos dinâmicos, delegar permissão de criação de grupos, criar políticas de nome de grupo, expiração de grupos, dentre outros.



O AADP2 possui todos os recursos do P1, além de recursos mais avançados de governança como os descritos abaixo:

Vulnerabilidades e Contas de Risco	Recomendações personalizadas para melhorar a postura geral de segurança, destacando vulnerabilidades, calculando os níveis de risco de login, e calculando os níveis de risco do usuário.
Investigação de Eventos de Risco	Envio de notificações para detecção de risco, investigar detecções de risco usando informações relevantes e contextuais, fluxos de trabalho básicos para acompanhar investigações, e fácil acesso a ações de remediação, como redefinição de senha.
Políticas de acesso condicional baseadas em riscos	Política para mitigar logins arriscados bloqueando logins ou exigindo desafios de autenticação de vários fatores, política para bloquear ou proteger contas de usuários de risco, e política para exigir que os usuários se registrem para autenticação multifatorial.
Gestão de Identidade Privilegiada (PIM)	Acesso privilegiado just-in-time aos recursos da rede. Atribuição de acesso vinculado ao tempo, aos recursos usando datas de início e término, exigir aprovação para ativar funções privilegiadas, impor a autenticação multifatorial, recebimento de notificações quando funções privilegiadas são ativadas, realizar revisões de acesso para garantir que os usuários ainda precisam de funções, e baixar o histórico de auditoria para auditoria interna ou externa.
Avaliações de Acesso	Permite uma melhor avaliação de acesso, mais automatizada. Permite a coleta de status de acesso, e aplicar regras para mudança de acesso e manter um histórico destas mudanças.
Gestão de Direitos	Permite criar pacotes de acesso a recursos tais como aplicativos, SharePoint Sites e associar políticas de segurança. Uma vez criado, é possível permitir que gestores da organização fora do grupo de TI possam aplicar esses direitos a novos usuários que se envolvam com seus respectivos departamentos ou projetos.

**** Veja Anexo A – Visão Geral do Azure Active Directory***

Azure Acive Directory B2B

Os recursos de controle de acesso do AAD B2B permitem que o time de TI controle de maneira mais eficiente o acesso de parceiros, fornecedores e prestadores de serviço ao seu ambiente através das contas de e-mails da organização externa aos órgãos do Tribunal de Justiça, mas com o mesmo nível de segurança e controle que possuem as contas de usuários criados no seu próprio ambiente. Este serviço pode ser adquirido como carga de trabalho do Azure ao invés de aquisições de licenças por usuário.

Neste caso, como o acesso a terceiros será concedido através de sua própria conta de e-mail, não será necessário criar uma conta de usuário no AADP do órgão, diminuindo assim o número de licenças que seria preciso adquirir, e para este usuário cujo acesso foi concedido, quando desligado de sua organização de origem, será revogado automaticamente o acesso dele no seu AADP também.

Recentemente, a Microsoft está adicionando a habilidade de "Cross-Tenant Access". Neste caso a colaboração B2B é ativada por padrão, mas definições de administração abrangentes permitem controlar a sua colaboração B2B com parceiros e organizações externas.

As definições de acesso de saída controlam se os seus usuários podem acessar recursos numa organização externa. Estas definições podem ser aplicadas a todos, ou podem especificar usuários, grupos e aplicações individuais.

As definições de acesso à entrada controlam se os usuários de organizações externas da Azure AD podem acessar recursos na sua organização. Estas definições podem ser aplicadas a todos, ou podem especificar usuários, grupos e aplicações individuais.

As configurações de confiança (entrada) determinam se as suas políticas de Acesso Condicional confiarão na autenticação de vários fatores (MFA), dispositivo compatível e a AD híbrida aderente a pedidos de uma organização externa se os seus usuários já cumpriram estes requisitos nos seus inquilinos domésticos. Por exemplo, quando configurar as suas definições de confiança para confiar no MFA, as suas políticas de MFA ainda são aplicadas a usuários externos, mas os usuários que já tenham concluído MFA em seus inquilinos domésticos não terão que completar MFA novamente no seu inquilino.

Veja Anexo B – Visão Geral da Colaboração com Azure AD B2B

Azure Active Directory B2C

Já os recursos de controle de acesso do Azure AD B2C permitem uma melhor administração e controle de acesso para usuários finais, por exemplo, no caso de usuários que deveriam ter acesso a aplicações com a habilidade de alterar seus dados cadastrais, estes usuários poderiam acessar usando uma identificação de terceiros como @hotmail, @yahoo, @gmail, entre outros. Uma vez que o usuário esteja cadastrado com uma de suas contas pessoais, é possível aplicar controles de segurança e acesso sem a necessidade de criar um usuário no seu AADP. É uma solução robusta e ideal para conceder e controlar acesso de milhões de usuários por um custo baixo.

Este também é um recurso que pode ser adquirido como serviço do Azure ao invés de uma licença por usuário. Isso permite um controle centralizado de acesso, mas com todas as políticas de segurança aplicadas. Uma vez implementada a solução, ele permite até 50.000 usuários ativos mensais sem nenhum custo.

A implementação de uma Solução B2C inclui os seguintes recursos:

Solução de Identidade com Marca Registrada. O Azure AD B2C é uma solução de autenticação de rótulo branco. Você pode personalizar toda a experiência do usuário com sua marca para que ela se integre diretamente com seus aplicativos Web e móveis.

Acesso de logon único com uma identidade fornecida pelo usuário. O Azure AD B2C usa protocolos de autenticação baseados em padrões, incluindo OpenID Connect, OAuth 2.0 e SAML (Security Assertion Markup Language). Ele se integra aos aplicativos mais modernos e softwares comerciais "off-the-shelf".

Integrar a repositórios de usuários externos. O Azure AD B2C fornece um diretório que pode conter 100 atributos personalizados por usuário. No entanto, você também pode integrar a sistemas externos. Por exemplo, use o Azure AD B2C para autenticação, mas delegue a um CRM (gerenciamento de relacionamento com o cliente) externo ou a um banco de dados de fidelidade do cliente como a fonte verdadeira dos dados do cliente.

Criação de perfil progressiva. Outra opção de percurso do usuário inclui a criação de perfil progressiva. A criação de perfil progressiva permite que seus clientes concluam rapidamente sua primeira transação coletando uma quantidade mínima de informações. Em seguida, colete gradualmente mais dados de perfil do cliente em logins futuros.

Verificação de identidade de terceiros e revisão. Use o Azure AD B2C para facilitar a verificação de identidade e a revisão coletando dados do usuário, passando-os para um sistema de terceiros para executar validação, pontuação de confiança e aprovação para a criação da conta de usuário.

Veja Anexo C – Visão Geral da Arquitetura Azure AD B2C

Gestão de Dispositivos

Além de exigir uma gestão de incidentes de segurança mais sofisticado, a resolução também exige a elaboração de requisitos específicos de segurança para todos os ativos de TI incluindo ambientes de servidores, dispositivos móveis ou qualquer dispositivo conectado à rede ou algum sistema de comunicação inclusive telefones celulares. Também é necessário criar requisitos de segurança específicos relacionados com o contexto de trabalho remoto.

Para uma melhor gestão e garantir conformidade com esse requisito, a melhor ferramenta será a utilização de um MDM (Mobile Device Management). Uma boa implementação de MDM permitirá uma melhor gestão de dispositivos móveis incluindo assegurar que determinados padrões de segurança estejam configurados em todo e qualquer dispositivo conectado à rede. É possível, por exemplo, exigir que os dispositivos tenham antivírus atualizado, firewall no dispositivo ativo, ou exigir que o dispositivo esteja configurado com uma senha de proteção entre outras configurações de segurança para que estes dispositivos possam se conectar à rede ou acessar uma aplicação. Estes requisitos de configurações podem se aplicar para diferentes sistemas operacionais tais como Windows, iPhone e Android.

Uma vez que estes dispositivos estejam sendo ativamente gerenciados, será possível usar análises de risco em tempo real para determinar o nível de acesso que será concedido ao usuário como por exemplo, permitir, bloquear ou limitar o acesso do usuário à rede se o dispositivo não está em conformidade com os recursos de segurança exigidos pela organização, ou está sendo usado a partir de uma localidade não comum para aquele usuário. É possível também, bloquear ou limitar acesso de dispositivos que se encontram fora do país.

Microsoft Intune com SCCM Co-Gerenciamento

A Microsoft possui o Microsoft Intune para gestão de dispositivos em ambiente na nuvem. O Microsoft Intune pode prover capacidade de Mobile Device Management (MDM) e Mobile Application Management (MAM). Intune é parte das licenças Enterprise Mobility and Security E3 e E5 ou Microsoft 365 E3 e E5. O Microsoft Intune se integra com o Azure Active Directory (Azure AD) para controlar quem tem acesso e quais aplicativos e recursos de sua rede. Com o Intune, você pode:

- Definir regras e configurações em dispositivos pessoais e de propriedade da organização para acessar dados e redes;
- Implantar e autenticar aplicativos em dispositivos -- no ambiente local e no celular;
- Proteger as informações da sua organização controlando a forma como os usuários acessam e compartilham informações;
- Certificar-se de que os dispositivos e aplicativos estejam em conformidade com seus requisitos de segurança;
- Atualizar certificados nos dispositivos para que os usuários possam acessar facilmente sua rede Wi-Fi ou usar uma VPN para se conectar à sua rede;
- Adicionar e atribuir aplicativos móveis a grupos de usuários e dispositivos, incluindo usuários em grupos específicos, dispositivos em grupos específicos e muito mais;

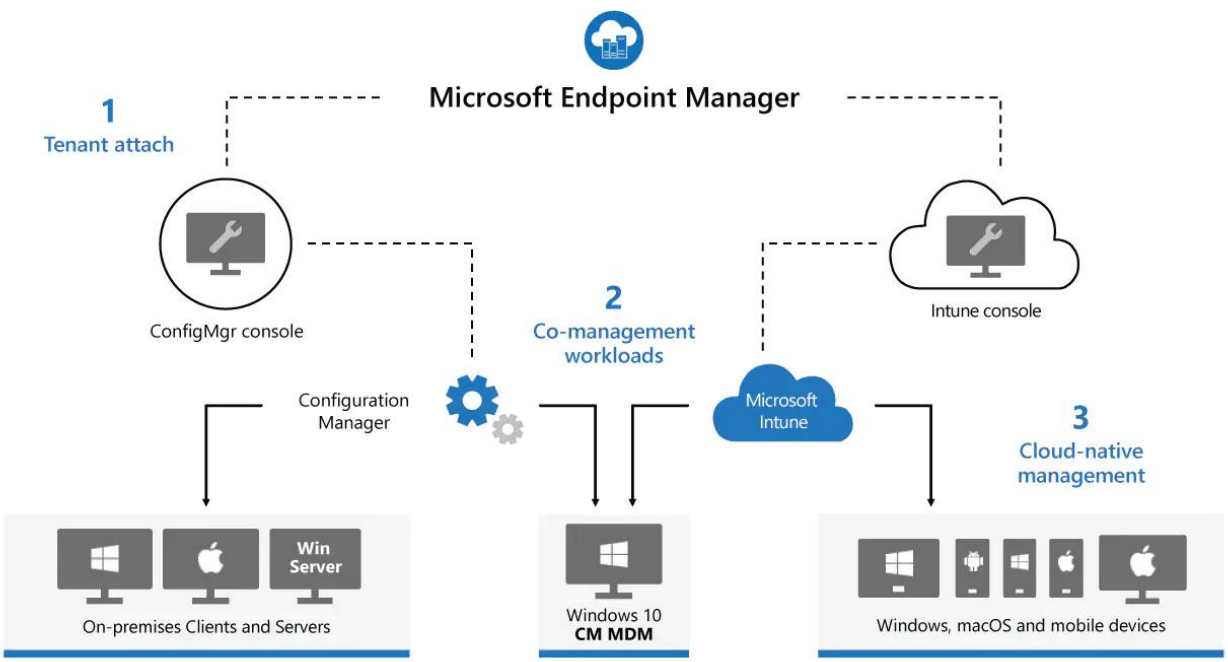
- Configurar aplicativos para iniciar ou executar com configurações específicas ativadas e atualizar aplicativos existentes já no dispositivo;
- Consultar relatórios sobre quais aplicativos são usados e acompanhar seu uso;
- Fazer uma limpeza seletiva removendo apenas dados da organização de aplicativos.

Na maioria dos casos, a organização terá um ambiente híbrido, ou seja, recursos de rede e aplicativos tanto na nuvem quanto no ambiente local.

Neste caso deveríamos usar o Microsoft System Center Configuration Manager (mas nas versões mais recentes do Windows ele é agora chamado de Microsoft Endpoint Manager) para gestão destes dispositivos e aplicativos. É possível usar agora o Intune e SCCM em modo "co-gerenciamento".

O co-gerenciamento permite que você gerencie simultaneamente o Windows 10 usando o SCCM e o Microsoft Intune. Com isso, a organização consegue otimizar o seu investimento no ambiente local sem a necessidade de uma migração para um novo ambiente, mas ao mesmo tempo anexa novas funcionalidades de gerenciamento que só estão disponíveis para nuvem em seu ambiente local.

Veja Anexo D – Visão Geral do Microsoft Intune



A unified platform including both Configuration Manager and Microsoft Intune

Gestão da Segurança e Tratamento de Incidentes

É exigido por esta resolução, estabelecer processo de Gestão da Segurança da Informação baseado em riscos. No capítulo III, Art. 11 I-III, a Resolução exige maior eficiência nas ações de segurança, ou seja, estabelecer a capacidade de responder de forma satisfatória a incidentes de segurança e garantir ao máximo a continuidade dos serviços essenciais de cada órgão do Poder Judiciário.

Em particular, no mesmo Art. parágrafo IV, estabelece-se a necessidade de utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação de ações de usuários, permitindo automatizar ações de controle de segurança e oferecer inteligência à análise de eventos de segurança.

A ferramenta adequada para conformidade com esta exigência será o Microsoft Sentinel. O Microsoft Sentinel permite uma visão ampla de todos os incidentes de segurança em toda organização. Conectando o Microsoft Sentinel ao seu Active Directory, firewall, aplicativos, base de dados de identidade, servidores e outras ferramentas especializadas em segurança tanto no seu ambiente na nuvem como no seu ambiente local.

O Microsoft Sentinel enriquece sua investigação e detecção com IA, e fornece o fluxo de inteligência de ameaças da Microsoft e permite que você traga sua própria inteligência de ameaças.

O Microsoft Sentinel engloba as seguintes características importantes para o tratamento e automação de incidentes cibernéticos:

- **SIEM (Security Information and Event Management** – Segurança de Informação e Gerenciamento de Eventos) – Se refere a capacidade de coletar dados de todo parque computacional incluindo, infraestrutura, aplicativos, dispositivos, comportamento de usuários, firewalls para fazer análises, buscar correlações entre as atividades na rede e gerar alertas e incidentes.
- **SOAR (Security Orquestration Automated Response** – Resposta Automatizada de Orquestração de Segurança) – Se refere a capacidade da ferramenta de oferecer a habilidade de automatizar respostas a incidentes e eventos de diversas fontes reportados pelo SIEM. Isso otimiza o processo de tratamento dos incidentes.
- **XDR (Extended Detection Response – Detecção e Resposta Estendido)** – Um sistema XDR é projetado para fornecer segurança inteligente, automatizada e integrada em todo o domínio de uma organização. Ele ajuda a prevenir, detectar e responder a ameaças em identidades, dispositivos, aplicativos, e-mail, IoT (Internet of Things), infraestrutura e plataforma na nuvem. O XDR permite o acesso a vários serviços de nuvens de fornecedores diferentes para uma visibilidade mais ampla de todo o ambiente, ou seja, ele estende a capacidade de governança sobre todo e qualquer ambiente que a organização possua.

É importante, no entanto, também estabelecer um time que possa fazer o monitoramento e aprimoramento dos filtros e criação de "Playbooks" que vão ajudar a reduzir o número de falso-positivos e melhorar o tempo de resposta e automação como exigido por essa resolução.

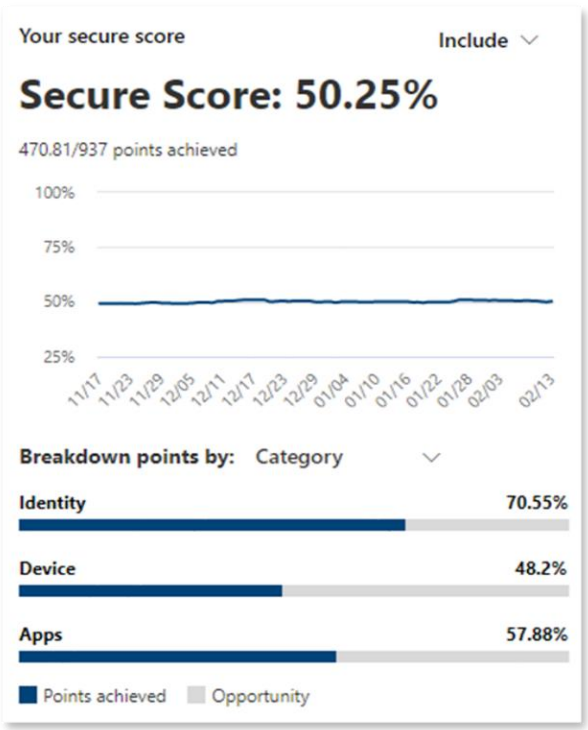
**** Veja Anexo E – Visão Geral do Microsoft Sentinel***

Avaliações da Postura de Segurança Cibernética

A resolução estabelece também a necessidade de realizar pelo menos semestralmente avaliações e testes de conformidade em segurança cibernética para validar a eficácia dos controles estabelecidos. Existem vários recursos dentro do ambiente do Microsoft 365 que podem dar apoio a essas análises e estabelecer "baselines" assim como permitir a avaliação do progresso em uma linha de tempo.

Microsoft Secure Score

O Microsoft Secure Score registra uma pontuação para cada recurso de segurança implementado. Ele também prover sugestões de ações que podem ser tomadas para melhorar a postura de segurança. Essas sugestões contêm detalhes de como cada uma dessas recomendações podem ser implementadas e permite atribuir essas ações a indivíduos dentro da organização que tenham a responsabilidade de endereçar a recomendação e coordenar a implementação.



O Microsoft Secure Score é organizado em três áreas diferentes de avaliação: segurança de Identidade, Dispositivos e Aplicações. O ideal seria estabelecer um ritmo de revisão, ou seja, estabelecer um plano de ações e atividades para endereçar as recomendações. O Microsoft Secure Score já está visível em todo "Tenant" da Microsoft pelo seguinte link: https://security.microsoft.com.

Avaliação de Postura de Segurança Baseado no CIS Benchmark™

Para uma avaliação ainda mais abrangente, recomendamos a adoção de uma "estrutura de referência" como CIS Benchmark, ou qualquer outra referência.

> **Os benchmarks da CIS fornecem um conjunto claro de padrões para a configuração de ativos digitais comuns — desde sistemas operacionais até infraestrutura em nuvem. Isso elimina a necessidade de cada organização 'reinventar a roda' e fornece às organizações um caminho claro para minimizar sua superfície de ataque.**

Sugerimos começar com uma Avaliação de Segurança Cibernética, como exemplo, a ferramenta CSAT da QS Solutions. CSAT permite uma avaliação de toda sua rede em relação aos 18 controles de segurança do CIS 8.0. Esses controles ajudam a estabelecer um caminho de melhoramento da postura de segurança baseado em informações coletadas no ambiente do órgão sendo analisado.

Os controles na versão 8.0 são organizados por atividades com foco nas tarefas que devem ser implementadas. Estes 18 controles contêm 153 "safeguards". Esses controles são organizados em três "Grupos de Implementação" como a seguir:

IG1 – Higiene Cibernética Essencial	Toda organização deveria implementar no mínimo para se defender dos ataques mais comuns.
IG2 – Higiene Cibernética Padrão	Continuação dos controles básicos recomendados para organizações com nível médio de complexidade e acima.
IG3 – Higiene Cibernética Avançada	Recomendado para organizações de médio e grande porte com níveis de complexidade alto.

Uma vez feita a avaliação, deva-se estabelecer um ritmo de melhorias, a cada 6 meses, será possível fazer uma nova Avaliação de Segurança Cibernética com o CSAT e fazer a comparação com o resultado anterior.

Baseado nas exigências da Resolução, todo órgão afetado deveria estar buscando uma conformidade com o IG3. Mas chegar ao nível IG3 é uma jornada, e deve ser caminhada passo-a-passo, começando com a implementação dos controles IG1, depois IG2 e finalmente IG3.

Esta é a base sobre a qual o CSAT fornece recomendações e um plano de ação para melhorar sua segurança. É a maneira perfeita de maximizar a segurança e demonstrar que sua organização leva a segurança a sério.

QS Solutions - Cyber Security Assessment Tool Explainer

***Veja Anexo F – Processo de Avaliação de Segurança Cibernética**

Conformidade com LGPD e Norma ISO/IEC 27001:2013

Esta Resolução faz referência tanto a Lei 13.853/2019 (Lei Geral da Proteção de Dados – LGPD) assim como a Norma NBR ISO/IEC 27001:2013. A grande maioria das organizações tem muitas dificuldades de orquestrar as atividades e implementações de tecnologia da segurança e processos que apoiem ou garantam a conformidade com os requisitos desta Lei ou alinhamento com a melhores práticas de segurança da informação estabelecida pela Norma. Vamos abordar cada um separadamente.

NIST-National Institute of Standards and Technology, ISO 2700 Series

Lei Geral da Proteção de Dados (LGPD)

A LGPD está dividida em 10 capítulos e 65 artigos. A Lei é baseada no GDPR (General Data Protection Regulation) expedida pela União Europeia em 2018. A LGPD estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. O principal objetivo é proteger os direitos fundamentais da liberdade e da privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Lei se aplica tanto às Instituições Privadas como Governamentais.

No Art. 6º, a LGPD determina 10 princípios que devem nortear o tratamento de dados pessoais:

1. **Finalidade.** A Lei exige que os dados pessoais sejam usados apenas para propósitos legítimos, específicos, explícitos e informados ao titular dos dados. A Lei exige que os dados não sejam utilizados para nenhuma outra finalidade além do que foi informado ao usuário ou proprietário da informação.
2. **Adequação.** Refere-se ao tratamento dos dados compatível com o que foi informado ao usuário ou proprietário da informação.
3. **Necessidade.** As organizações têm que garantir que apenas os dados pessoais essenciais para o desenvolvimento do objetivo sejam coletados e tratados.
4. **Livre Acesso.** Diz respeito a garantia que o usuário proprietário da informação tem direito a consulta de seus dados de forma fácil e gratuita e saber sobre a forma e a duração do tratamento dos seus dados bem como sobre sua integridade.
5. **Qualidade do Dados.** É preciso garantir aos usuários a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento.
6. **Transparência.** Exige que as organizações sejam honestas com os usuários a respeito do tratamento dos dados, inclusive informar que agentes terceiros poderiam estar tratando os seus dados.
7. **Segurança.** Envolve a adoção de procedimentos, tecnologias e soluções que garantam maior proteção de dados incluindo incidentes provocados por hackers ou tratamento inapropriado ou ilícito de agentes internos da organização que esteja tratando os dados.
8. **Prevenção.** É importante tomar medidas para prevenir a ocorrência de danos nos dados pessoais antes mesmo que um incidente aconteça.
9. **Não Discriminação.** Os dados pessoais não podem ser usados para discriminar ou promover abusos contra seus proprietários.
10. **Responsabilização e Prestação de Contas.** Exige que o órgão tratando o dado tenha a responsabilidade de comprovar a adoção de medidas eficazes e capazes no que diz respeito ao cumprimento das normas de proteção de dados pessoais.

A LGPD se aplica para organizações privadas, públicas e governamentais.

Norma NBR ISO/IEC 27001:2013

Essa Resolução pontua como referência a norma NBR ISO/IEC 27001:2013. Também conhecida como ISO 27001, é um grupo de padrões e especificações para um sistema de gestão de segurança da informação reconhecidos mundialmente. O objetivo destes padrões é de ajudar as organizações a tornar os ativos digitais pelos quais eles possuem mais seguros. A áreas a serem tratadas são organizadas em 14 domínios que somam 114 controles:

ISO 27001 / 27002 Versão 2013 114 Controles em 14 Domínios	
1	Information Security Policies
2	Organization of Information Security
3	Human Resource Security
4	Asset Management
5	Access Control
6	Cryptography
7	Physical and Environmental Security
8	Operations Security
9	Communications Security
10	System Acquisition, Development, and Maintenance
11	Supplier Relationships
12	Information Security Incident Management
13	Information Security Aspect of Business Continuity Management
14	Compliance

Fazer a uma boa gestão implementação e avaliação de nível de maturidade e conformidade com essas exigências das leis ou melhores práticas das normas é uma tarefa árdua. Para facilitar este trabalho, todo cliente que possui licenças do Microsoft 365 também possui licença para usarem o Microsoft Compliance Manager.

Microsoft Compliance Manager

No que diz respeito a conformidade com a LGPD, existem vários serviços de software gestores de conformidade, mas o ambiente Microsoft 365 tem o Microsoft Compliance Manager. O Microsoft Compliance Manager é uma funcionalidade do Microsoft 365 Compliance Center que ajuda as organizações a realizarem a gestão das atividades que levam a conformidade com diversas leis e "framework de referência" de segurança e conformidade.

Ele também identifica áreas que podem ser melhoradas dentro do seu sistema e permite que essas recomendações de ações sejam "atribuídas" para um membro da equipe que vai atuar e reportar o progresso de suas ações dentro do Microsoft Compliance Manager.

A Microsoft implementa uma média de 220 atualizações de regulamentações diariamente de mais de 1,000 agências reguladoras globalmente.

Com o Compliance Manager, a organização vai ter os seguintes benefícios:

1. **Avaliação Contínua: Detecção automática de configurações do sistema pontuando áreas que devem ser melhoradas.**
2. **Recomendações de Ações: Prover guias para resolução de problemas passo-a-passo.**
3. **Mapa de Controle: Cada ação tomada está associada a várias regulamentações, você ganha visibilidade de exatamente quais artigos de cada regulamentação estão sendo atendidos com aquela ação.**

Veja Anexo G – Microsoft Compliance Manager

Considerações Finais

Vale lembrar que o artigo 25 desta resolução faz menção a outros Manuais de Referência e Protocolos de Gerenciamento que não foram parte deste estudo, no entanto as ações e modelos de implementação sugeridos nesta publicação ajudarão com a conformidade com estes manuais e protocolos. O seguintes Manuais de Referência e Protocolo são mencionados na resolução:

- Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC-PJ)
- Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PIILC-PJ)
- Manual de Referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

Thank you!

Anexo A
Visão Geral do Azure Active Directory

O Azure Active Directory (Azure AD) é um serviço de gerenciamento de identidade e acesso baseado em nuvem. Esse serviço ajuda seus funcionários a acessarem recursos externos, como o Microsoft 365, o portal Azure e milhares de outros aplicativos SaaS. O Azure AD também os ajuda a acessar recursos internos. Estes são recursos como aplicações na rede corporativa e intranet, bem como quaisquer aplicações em nuvem desenvolvidas pela sua organização.

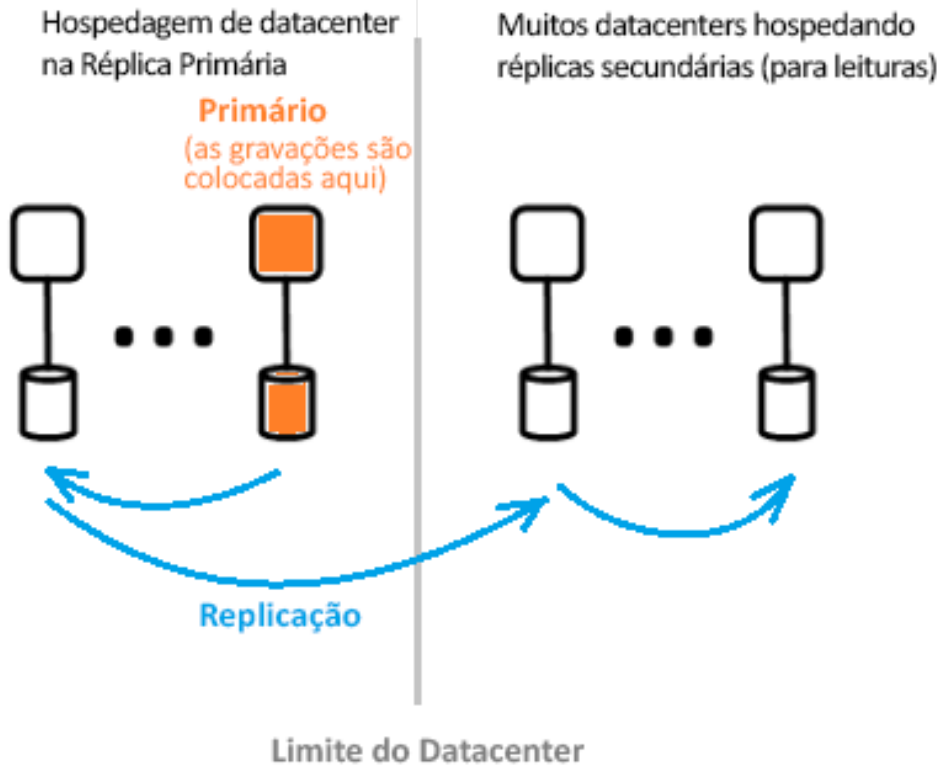
Qual a arquitetura do Active Directory do Azure?

A arquitetura geograficamente dispersa do Azure AD combina monitoramento de ponta a ponta, redirecionamento automático, failover e recursos de recuperação para fornecer aos clientes disponibilidade e desempenho em toda a organização.

Design de arquitetura de serviço

A maneira mais comum de construir sistemas acessíveis, utilizáveis e ricos em dados é usar blocos ou unidades de dimensionamento independentes. Para os níveis de dados do Azure AD, a unidade de dimensionamento é chamada de partição. A camada de dados possui vários serviços de interface que fornecem recursos de leitura e gravação. O diagrama a seguir mostra como os componentes de uma única partição de diretório são distribuídos em data centers geograficamente dispersos.

Os componentes arquitetônicos do Azure AD incluem réplicas primárias e secundárias.



A réplica primária recebe todos os registros da partição a que pertence. Quaisquer gravações são imediatamente replicadas para uma réplica secundária em outro data center antes de retornar o sucesso ao chamador, fornecendo operações de gravação geograficamente redundantes.

Todas as leituras do diretório são manuseadas por réplicas secundárias localizadas em diferentes data centers geograficamente localizados. Como os dados são replicados de maneira simultânea, existem muitas réplicas secundárias. As leituras do diretório, como solicitações de autenticação, são tratadas por um data center localizado perto do cliente. Portanto, as réplicas secundárias são responsáveis pela escalabilidade da leitura.

Escalabilidade

A escalabilidade é a capacidade de um serviço de expansão para atender aos crescentes requisitos de desempenho. A escalabilidade da gravação é alcançada através do particionamento de dados. A escalabilidade da leitura é alcançada replicando dados de uma partição para várias réplicas secundárias distribuídas ao redor do mundo. As solicitações dos aplicativos de diretório são encaminhadas para o data center a que estão fisicamente mais próximos. As gravações são redirecionadas de forma transparente para a réplica primária para garantir a consistência de leitura/gravação.

Réplicas secundárias expandem muito o tamanho da partição, já que o diretório geralmente está fornecendo leituras na maioria das vezes. Os aplicativos de diretório se conectam a data centers próximos. Essa conexão melhora o desempenho de modo que o dimensionamento horizontal é possível. Como as partições de diretórios podem ter muitas réplicas secundárias, réplicas secundárias podem ser localizadas mais perto dos clientes do diretório. Apenas os componentes intensivos de gravação do serviço de diretório interno são direcionados para o principal ativo.

Disponibilidade Contínua

A disponibilidade (ou tempo de atividade) determina a capacidade de um sistema funcionar sem interrupção. A chave para a alta disponibilidade do Azure AD é que os serviços podem mover rapidamente o tráfego através de vários data centers geograficamente dispersos. Cada data center é independente, permitindo modos de falha de correlatados. Com este design de alta disponibilidade, o Azure AD não requer tempo de inatividade para manutenção. A estrutura de partição do Azure AD é simplificada em comparação com a arquitetura AD corporativa com uma única estrutura mestre que inclui um processo de failover de réplica primária cuidadosamente orquestrado e determinista.

Tolerância e Falhas

Um sistema é mais acessível se ele comete erros de hardware, rede e software. Para cada partição de diretório, há uma réplica mestre altamente disponível: a réplica primária. Esta réplica só escreve para a partição. Esta réplica é constantemente monitorada de perto, e se um erro for encontrado, o registro pode ser imediatamente movido para outra réplica (que se torna a nova primária).

Durante o failover, pode haver uma perda de disponibilidade de gravação, normalmente de 1 a 2 minutos. A legibilidade não muda durante este período.

As operações de leitura (das quais há muitas ordens de magnitude, mais do que operações de gravação) são realizadas apenas em réplicas secundárias. Como as réplicas secundárias são idempotentes, ou seja, podem ser replicadas mais do que uma vez sem que o resultado se altere, a perda de uma réplica em uma determinada partição pode ser facilmente compensada redirecionando leituras para outra réplica, geralmente no mesmo data center.

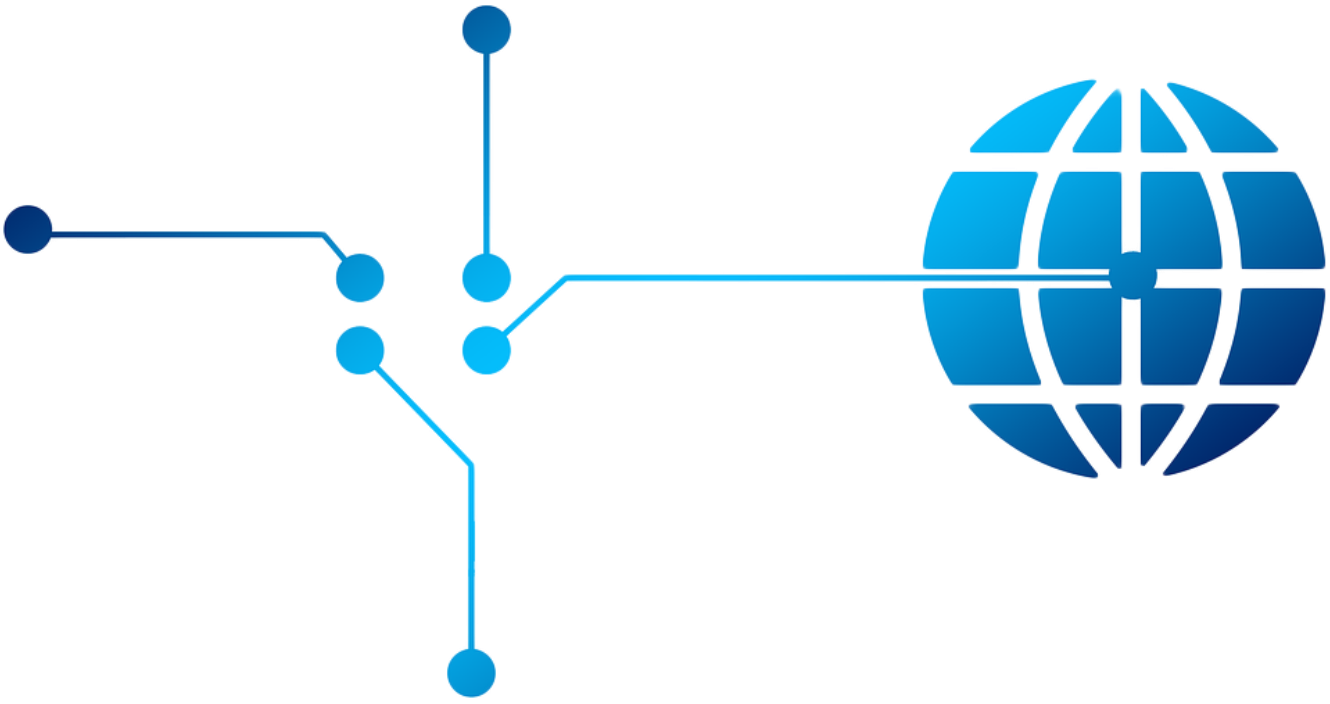
Durabilidade dos Dados

Um registro é capturado permanentemente em pelo menos dois data centers antes de ser reconhecido. Para fazer isso, a gravação é primeiramente comprometida com o banco de dados primário e, em seguida, a gravação é imediatamente replicada para pelo menos um outro data center. Esta ação de gravação garante que uma perda potencialmente fatal do data center hospedando o banco de dados primário não resulte em perda de dados. O Azure AD suporta o Objetivo de Tempo de Recuperação Zero (RTO) para garantir que nenhum dado seja perdido em caso de falha.

Reference:

Visão geral da arquitetura – Azure Active Directory | Microsoft Docs

Lista de verificação da implantação do Azure Active Directory | Microsoft Docs

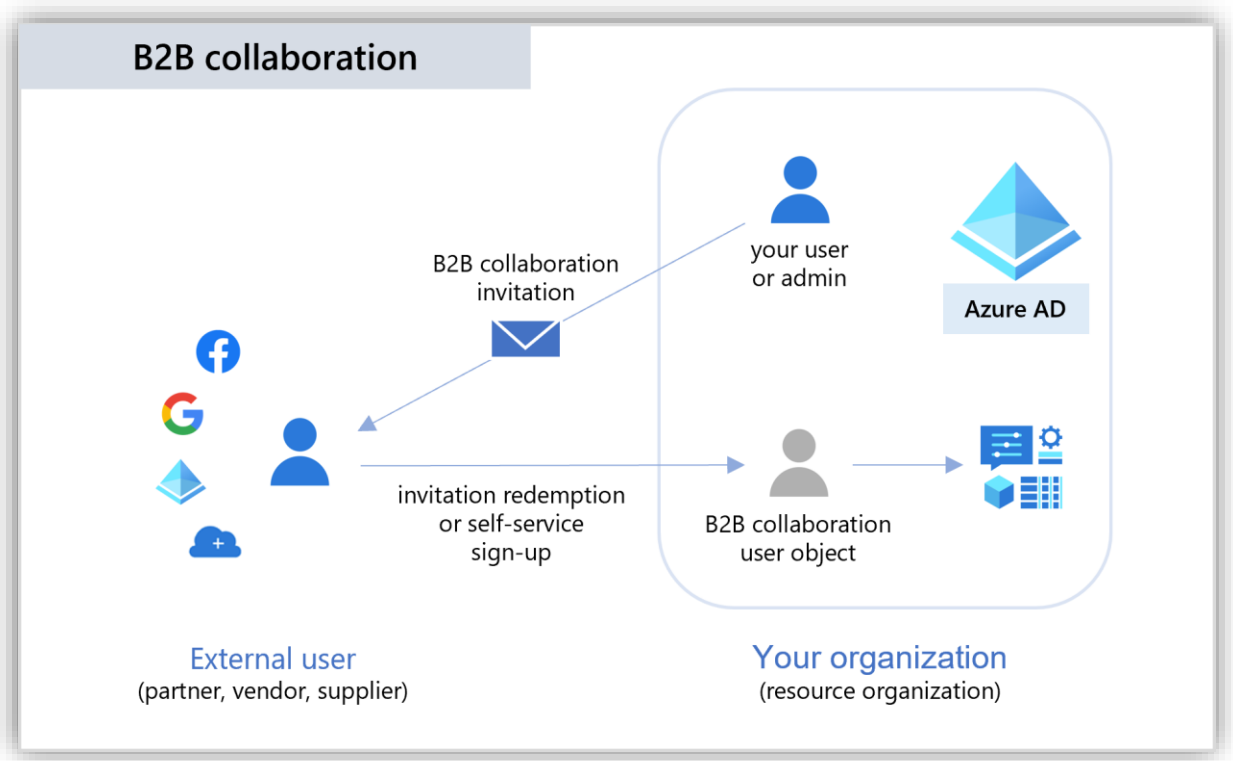


Anexo B
Visão Geral da Colaboração com Azure AD B2B

O Azure Active Directory (Azure AD) B2B é um recurso de identidade externa que permite que você convide usuários de outros tenants a colaborar com sua organização. Com a colaboração B2B, você pode compartilhar com segurança os aplicativos e serviços da sua organização com usuários convidados de qualquer outra organização, mantendo o controle sobre seus dados corporativos. O recurso permite que se trabalhe de forma confiável e segura com parceiros externos, grandes ou pequenos, mesmo que eles não tenham Azure AD ou um departamento de TI.

Um processo simples de convite e resgate permite que os parceiros usem suas credenciais para acessar os recursos da sua organização. Você também pode ativar fluxos personalizados de auto registro para permitir que usuários externos se auto registrem para aplicativos ou recursos. Uma vez que um usuário externo tenha aceitado um convite ou preenchido o registro, ele será apresentado como um objeto de usuário em seu diretório.

Objetos de colaboração B2B personalizados são tipicamente atribuídos ao tipo de usuário "convidado" e podem ser identificados pela extensão #EXT# em seu nome de usuário principal. Os desenvolvedores podem usar a API AD B2B do Azure para personalizar o processo de convite ou criar aplicativos como portais de autoatendimento para inscrição.



Colaborando com usuários externos usando suas próprias credenciais

No Azure AD B2B, os parceiros usam sua própria solução de gerenciamento de identidade, de modo que não há sobrecarga administrativa adicional para a organização. Os usuários convidados fazem login em seus aplicativos e serviços usando sus identidade do trabalho, escola ou sociais. Não há necessidade de gerenciar contas externas ou senhas, bem como não há necessidade de sincronizar contas ou gerenciar ciclos de vida da conta.

Gerenciar o acesso externo com Settings Inbound e Outbound

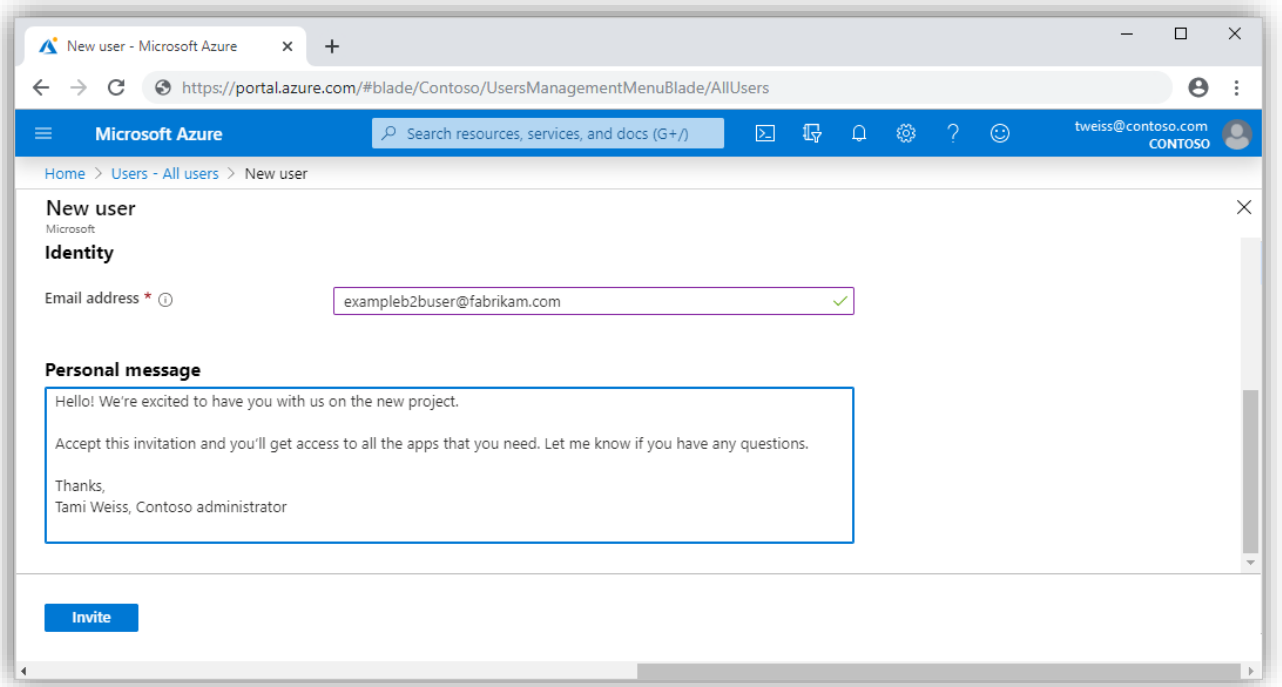
Para a colaboração B2B com outras organizações com Azure AD, você pode usar configurações de acesso entre inquilinos para controlar a colaboração B2B de entrada e saída e o acesso ao escopo para usuários, grupos e aplicativos específicos. Você pode definir uma configuração padrão que se aplica a todas as organizações externas e, em seguida, criar configurações individuais e específicas da organização, conforme necessário.

Usando configurações de acesso entre inquilinos, você também pode confiar em reivindicações multifator (MFA) e por dispositivo (reivindicações híbridas compatíveis e aderidas ao Azure AD) de outras organizações com Azure AD. Você pode usar opções de colaboração externa para restringir quem pode convidar usuários externos, permitir ou bloquear domínios B2B específicos e definir restrições aos usuários convidados que acessam seu diretório.

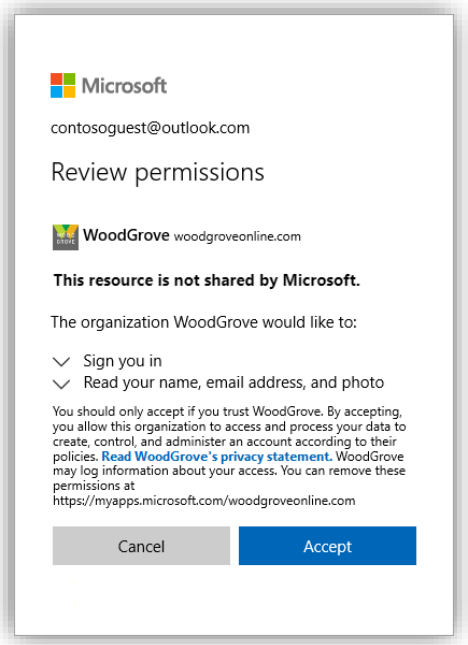
Adicione facilmente usuários convidados do portal Azure AD

Como administrador, você pode facilmente adicionar usuários convidados à sua organização no portal Azure.

- Crie um usuário convidado no Azure AD, semelhante à forma como você adiciona um novo usuário;
- Atribua usuários convidados a aplicativos ou grupos;
- Envie um e-mail de convite contendo um link de ativação ou envie um link direto para o aplicativo que deseja compartilhar.



- Os usuários convidados seguem alguns passos simples de registro para fazer login.

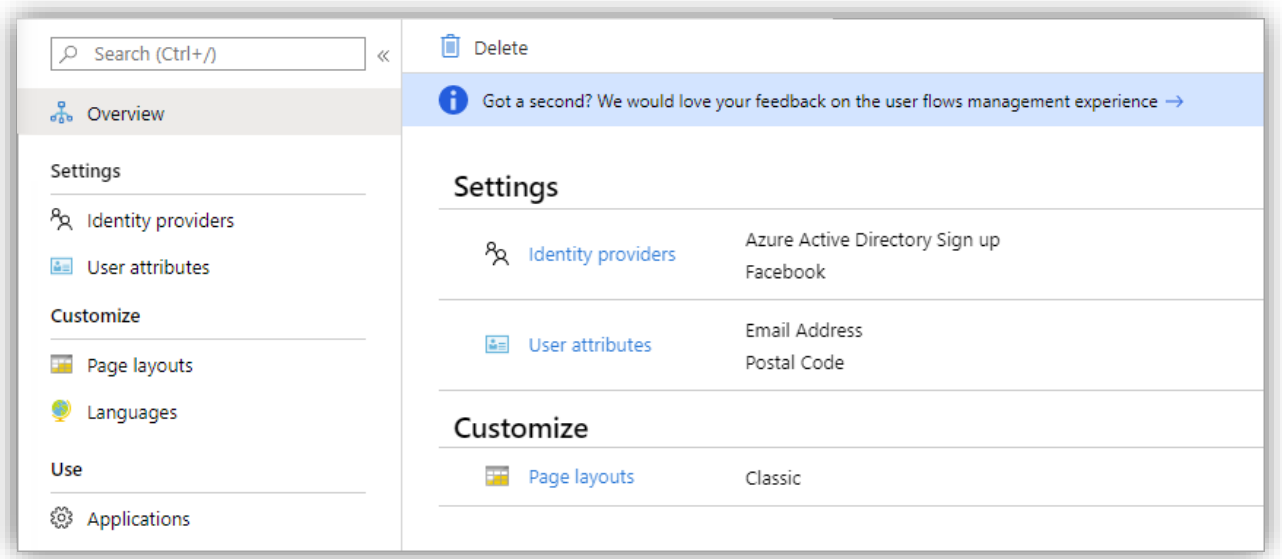


No Azure AD B2B, os parceiros usam sua própria solução de gerenciamento de identidade, de modo que não há sobrecarga administrativa adicional para a organização. Os usuários convidados fazem login em seus aplicativos e serviços usando sua identidade do trabalho, escola ou sociais. Os parceiros usam suas próprias identidades e credenciais, quer tenham uma conta Azure ou não. Não há necessidade de gerenciar contas externas ou senhas, bem como não há necessidade de sincronizar contas ou gerenciar ciclos de vida da conta.

Permitir a inscrição por autoatendimento

Com um fluxo personalizado de auto registro, você pode criar um processo de registro para usuários externos que desejam acessar seus aplicativos. Como parte do processo de registro, você pode fornecer opções para várias redes sociais ou provedores de identidade corporativa e coletar informações do usuário.

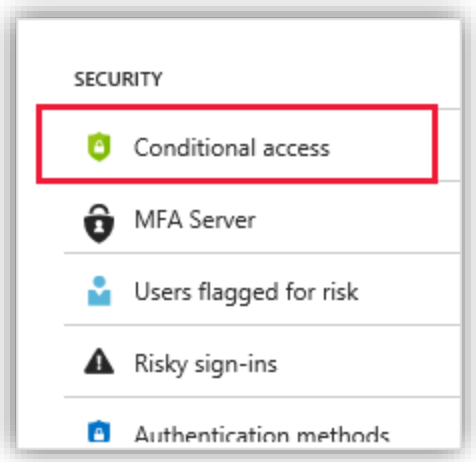
Você também pode usar conectores de API para integrar processos personalizados de auto registro com sistemas de nuvem externos. Você pode se conectar a fluxos de trabalho de aprovação personalizados, executar autenticação, validar informações fornecidas pelo usuário e muito mais.



Usar políticas para compartilhar aplicativos e serviços com segurança

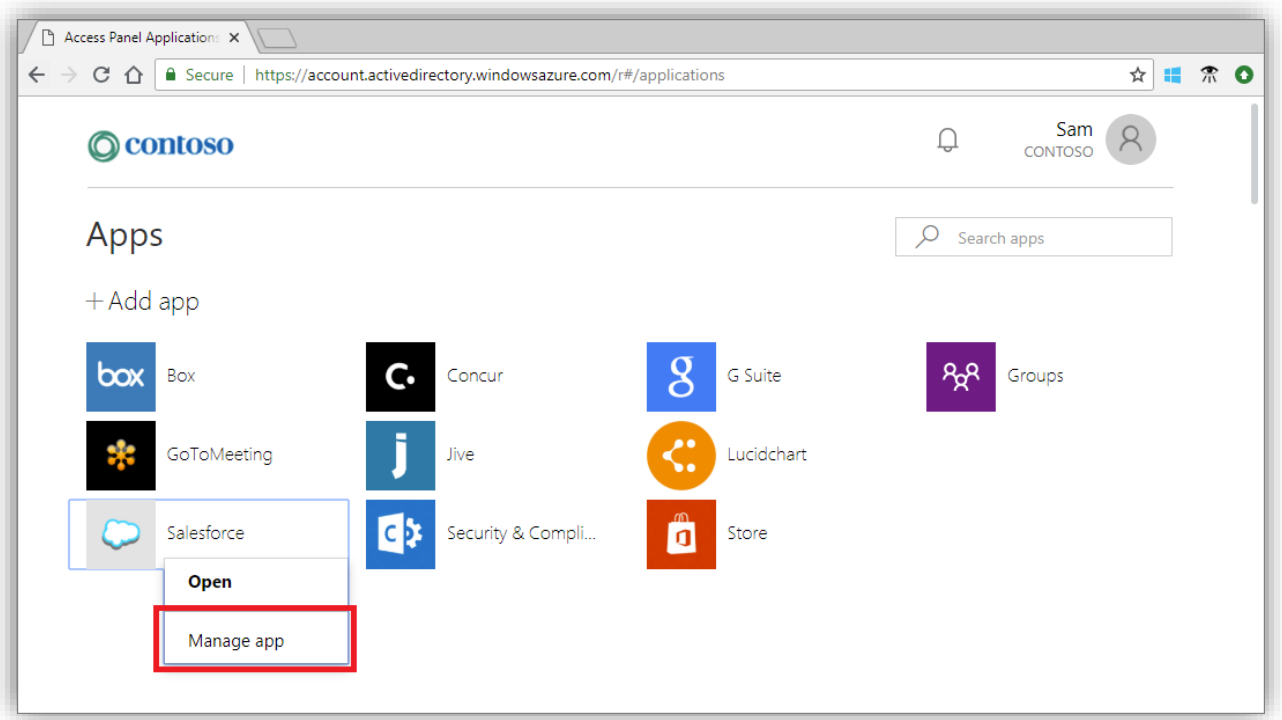
Você pode usar políticas de autenticação e autorização para proteger o conteúdo corporativo.

- No nível do inquilino;
- No nível de aplicação;
- Para usuários convidados específicos para proteger aplicativos e dados corporativos.



Permitir que o aplicativo e os proprietários de grupos gerenciem os próprios usuários convidados

Você pode delegar o gerenciamento de usuários convidados aos proprietários de aplicativos para que eles possam adicionar usuários convidados diretamente a qualquer aplicativo que eles queiram compartilhar, seja um aplicativo da Microsoft ou não. Os administradores configuram o aplicativo de autoatendimento e a gestão de grupos. Usuários não administrativos usam seu painel de login para adicionar usuários convidados a aplicativos ou grupos.

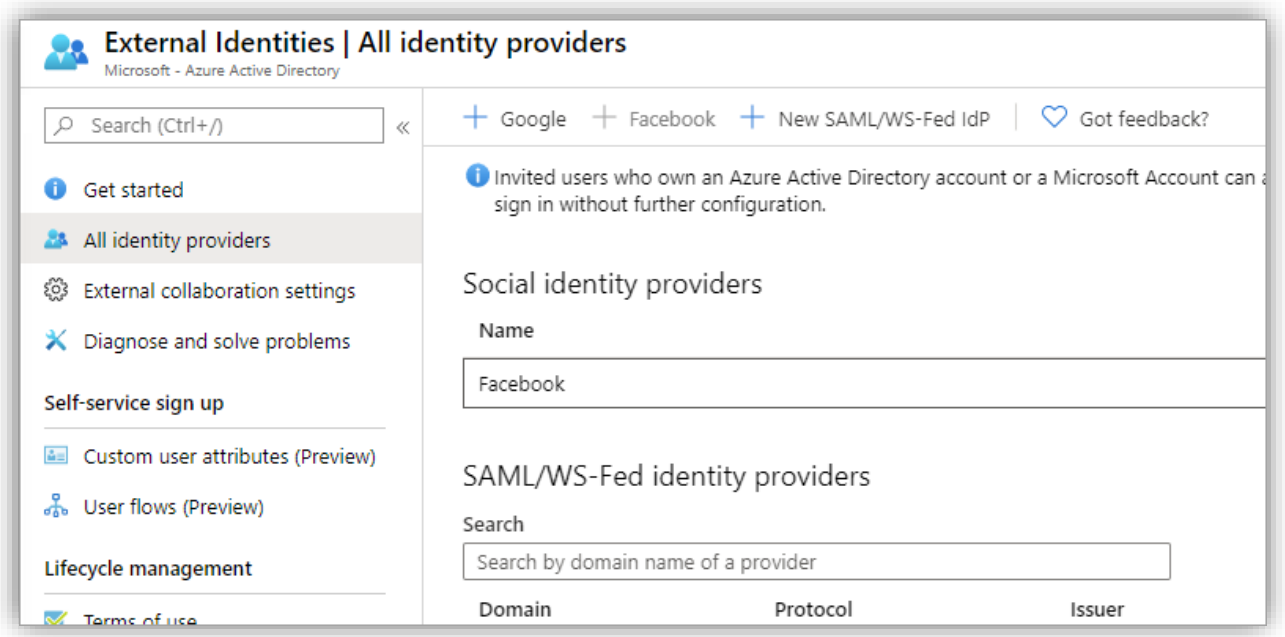


Personalizar a experiência de integração para usuários convidados B2B

Integre parceiros externos individualmente de acordo com as necessidades da sua organização. Use o Azure AD Rights Management para criar políticas que regem o acesso externo ao usuário. Use as APIs do convite de colaboração B2B para personalizar sua experiência de onboarding.

Integrar-se aos Provedores de identidade

O Azure AD suporta provedores de identidade externos, como Facebook, Contas Microsoft, Google ou Provedores de Identidade Corporativa. Em vez de apenas criar contas para o seu aplicativo, você pode configurar uma federação de provedores de identidade para que os usuários externos possam fazer login com suas contas sociais ou corporativas existentes.



Integrar-se com SharePoint e OneDrive

Você pode ativar a integração com o SharePoint e o OneDrive para compartilhar arquivos, pastas, itens de lista, bibliotecas de documentos e sites com pessoas fora de sua organização para autenticação e gerenciamento usando o Azure B2B. Os usuários com os quais você compartilha recursos geralmente são adicionados ao seu diretório como convidados, e permissões e grupos trabalham da mesma maneira para estes hóspedes como para usuários internos. Ao ativar a integração com o SharePoint e o OneDrive, você também pode ativar o recurso de senha de e-mail único no Azure AD B2B como um método de autenticação de recuo.

Reference:

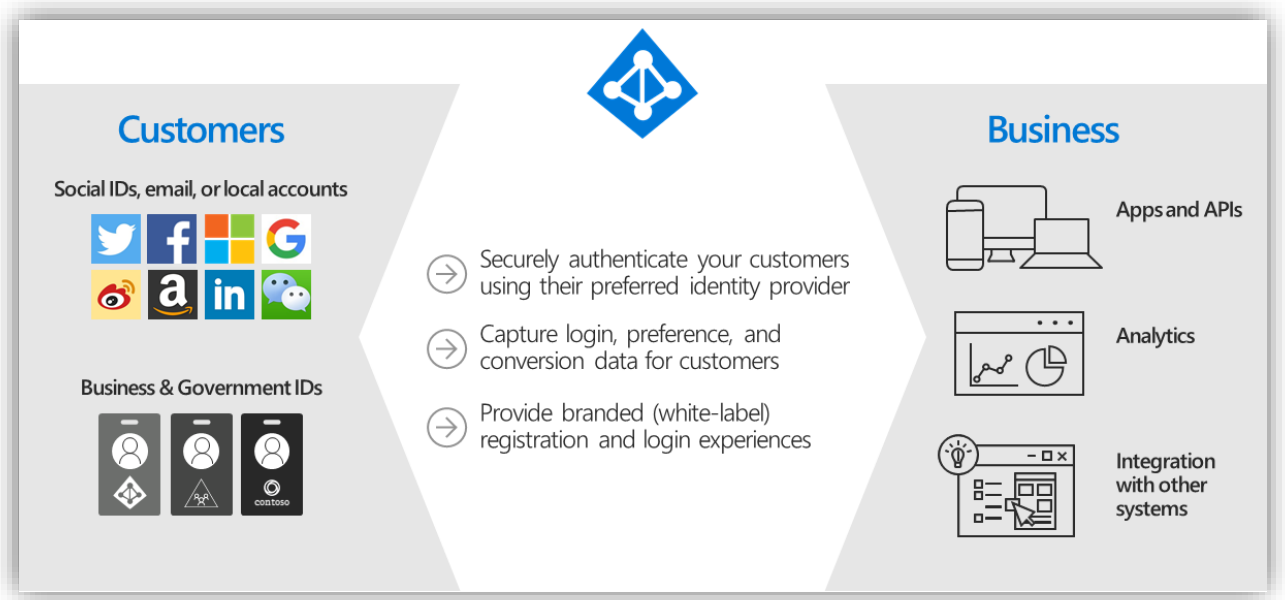
Identidades externas no Azure Active Directory | Microsoft Docs

Visão geral da colaboração B2B – Azure AD | Microsoft Docs

Anexo C
Visão Geral da Arquitetura Azure AD B2C

O Azure Active Directory B2C fornece a identidade de um cliente de negócios como um serviço. Seus clientes usam suas contas sociais, corporativas ou locais preferidas para acessar seus aplicativos e APIs com login único. O Azure AD B2C é uma solução de gerenciamento de acesso à identidade do cliente (CIAM) que pode suportar milhões de usuários e bilhões de autenticações por dia.

Ele fornece a escalabilidade e a segurança de uma plataforma de autenticação, monitorando e gerenciando automaticamente ameaças como negação de serviço, pulverização de senha ou ataques de força bruta. O Azure AD B2C é um serviço separado do Azure Active Directory (Azure AD) que é baseado na mesma tecnologia do Azure AD, mas para um propósito diferente. Isso permite que as organizações criem aplicativos voltados para o cliente e, em seguida, permitir que qualquer pessoa assine esses aplicativos sem restrições de conta de usuário.



Reference:

[What is Azure Active Directory B2C? | Microsoft Docs]

Anexo D
Visão Geral do Microsoft Intune

Seja uma transição para uma política BYOD (trazer seu próprio dispositivo), ou fornecendo laptops, tablets e dispositivos móveis como de costume e enviando-os para trabalhadores remotos, é necessário encontrar uma maneira de garantir a padronização e a conformidade através desses dispositivos. Não somente, é preciso fazer isso de uma maneira que seja eficaz em termos de custo, tempo e segurança, o que é alcançado com um gerenciamento de dispositivos móveis (MDM).

Ao implantar um MDM, você pode atender aos requisitos de proteção de dados organizacionais e ao mesmo tempo fornecer uma experiência simples para o usuário final. Os usuários obtêm a flexibilidade e a segurança que precisam para se manterem produtivos em qualquer lugar, e sua organização pode descansar facilmente sabendo que as informações da organização estão protegidas.

O mais importante é configurar a conformidade do dispositivo. Isto se torna extremamente poderoso quando combinado com o acesso condicional baseado no dispositivo, que é quando se cobre a lista de verificação das melhores práticas de Azure AD. Isso porque o dispositivo se torna literalmente parte de sua identidade e seu status de conformidade pode se tornar um fator na concessão ou negação de acesso a recursos.

Em resumo, o propósito de um MDM é integrar dispositivos e identidades, gerenciar cada dispositivo de qualquer lugar, gerenciamento simplificado de Patch, gerenciar conformidade e segurança, maior produtividade e redução de custos para o negócio.

A implementação com o Microsoft Intune, torna essa gestão de dispositivo simples e completa, atendendo a todos os requisitos de mercado, gestão, segurança e conformidade.

Ao implantar o Microsoft Intune como sua solução de MDM, uma das etapas de configuração é criar perfis baseado em grupos (ex.: Administrativo, Marketing, Assessoria, Contabilidade, etc.) e a partir disso definir quais as políticas deverão ser aplicadas a cada um deles.

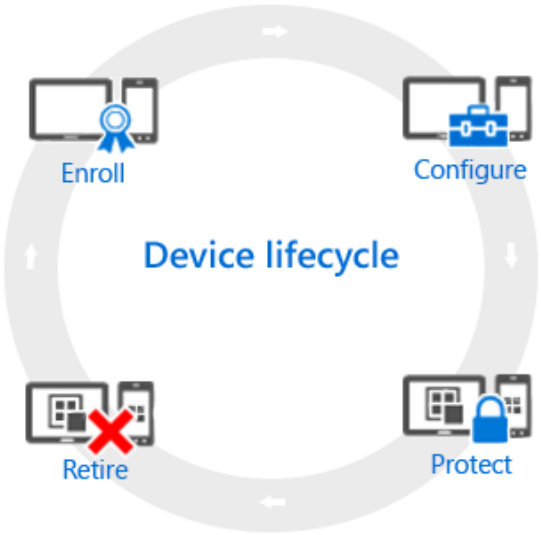
Algumas dessas políticas são, por exemplo, permitir ou negar o acesso a alguma rede WI-FI, permitir ou negar acessos a certos aplicativos, permitir ou negar acesso à VPN entre uma variedade enorme de configurações que abrange as áreas da segurança, conformidade e privacidade, garantindo assim a proteção dos dados.

Não somente visando o controle do usuário final, mas também como uma ferramenta poderosíssima da TI no quesito de atualização do sistema operacional, atualização do antivírus, instalação e controle de aplicativos, e em extensão a opção do Windows Autopilot voltados para sistema operacional Windows 10 e 11, cuja proposta é que o dispositivo chegue até o usuário sem a intervenção da equipe de TI.

Uma vez que o usuário se autentique no dispositivo, automaticamente a máquina é preparada de forma personalizada atendendo aos requisitos da área do colaborador.

A abordagem até agora foi referente aos laptops, mas a solução é para dispositivos móveis, sejam eles iPhone ou Android. Através da configuração do portal da organização, dentro do smartphone pessoal, há o espaço da organização gerenciável, seguro e em conformidade com as políticas internas adequadas.

Todo gerenciamento de dispositivo tem um ciclo de vida desde a compra/registro até a desativação do mesmo, e o Microsoft Intune ajuda em todas as etapas: Registrar, Configurar, Proteger e Desativar.



Fonte: Visão geral do ciclo de vida de MDM do Microsoft Intune | Microsoft Docs

Segue a melhor definição de cada uma das etapas:

1 Registrar:

As estratégias de MDM (gerenciamento de dispositivo móvel) de hoje se aplicam a vários telefones, tablets e PCs (iOS/iPadOS, Android, Windows e MacOS). Se você precisa gerenciar um dispositivo, o que geralmente é o caso para dispositivos corporativos, a primeira etapa é configurar o registro do dispositivo.

2 Configurar:

Registrar seus dispositivos é apenas a primeira etapa. Para tirar proveito de tudo o que o Intune oferece e garantir que seus dispositivos estejam seguros e são compatíveis com os padrões da organização, você pode escolher entre uma ampla variedade de políticas. Elas permitem configurar quase todos os aspectos de funcionamento dos dispositivos gerenciados. Por exemplo, os usuários devem ter uma senha em dispositivos que tem dados da organização? Você pode exigir uma; Você tem Wi-Fi corporativo? Você pode configurá-lo automaticamente.

Estes são os tipos de opções de configuração disponíveis:

- ✓ **Configuração do dispositivo**. Essas políticas permitem configurar os recursos e as funcionalidades dos dispositivos gerenciados. Por exemplo, você pode exigir o uso de uma senha em telefones Android ou desabilitar o uso da câmera em iPhones.
- ✓ **Acesso de recursos da organização**. Quando você permite que os usuários acessem seu trabalho em dispositivos pessoais, isso pode apresentar desafios. Por exemplo, como garantir que todos os dispositivos que precisam acessar o e-mail da organização estejam configurados corretamente? Como garantir que os usuários podem acessar a rede da organização com uma conexão VPN sem precisar saber configurações complexas? O Intune pode ajudar a reduzir essa carga, com a configuração automática dos dispositivos gerenciados para acessar os recursos comuns da organização.

- ✓ **Políticas de gerenciamento de computadores Windows (com o software cliente do Intune)**. Embora o registro de computadores Windows no Intune proporcione a maioria das funcionalidades de gerenciamento de dispositivos, o Intune continua dando suporte ao gerenciamento de computadores Windows com o software cliente do Intune.

3 Proteger:

No moderno mundo de TI, proteger dispositivos contra o acesso não autorizado é uma das tarefas mais importantes que você realiza. Além dos itens descritos na etapa **Configurar**, do ciclo de vida do dispositivo, o Intune fornece essas funcionalidades que ajudam a proteger dispositivos gerenciados contra o acesso não autorizado ou contra-ataques mal-intencionados:

- ✓ **Autenticação multifator**. Adicionar uma camada extra de autenticação aos logins de usuário pode ajudar a tornar os dispositivos ainda mais seguros. Vários dispositivos dão suporte à autenticação multifator que exige um segundo nível de autenticação, como uma chamada telefônica ou mensagem de texto, antes que os usuários possam obter acesso.
- ✓ **Configurações do Windows Hello for Business**. O Windows Hello for Business é um método de entrada alternativo que permite aos usuários usar um *gesto* – como uma impressão digital ou o Windows Hello – para fazer login sem a necessidade de uma senha.
- ✓ **Políticas para proteger computadores Windows (com o software cliente do Intune)**. Quando você gerencia computadores Windows usando o software cliente do Intune, há políticas disponíveis que permitem controlar as configurações do Endpoint Protection, atualizações de software e Firewall do Windows em computadores gerenciados.

4 Desativar:

Quando um dispositivo é perdido, roubado, ele precisa ser substituído ou usuários mudam de cargo, geralmente, esse é o momento de desativar ou apagar o dispositivo. Há várias maneiras de fazer isso – incluindo a redefinição do dispositivo, sua remoção do gerenciamento ou apagamento dos dados corporativos do dispositivo.

Anexo E
Visão Geral do Microsoft Sentinel

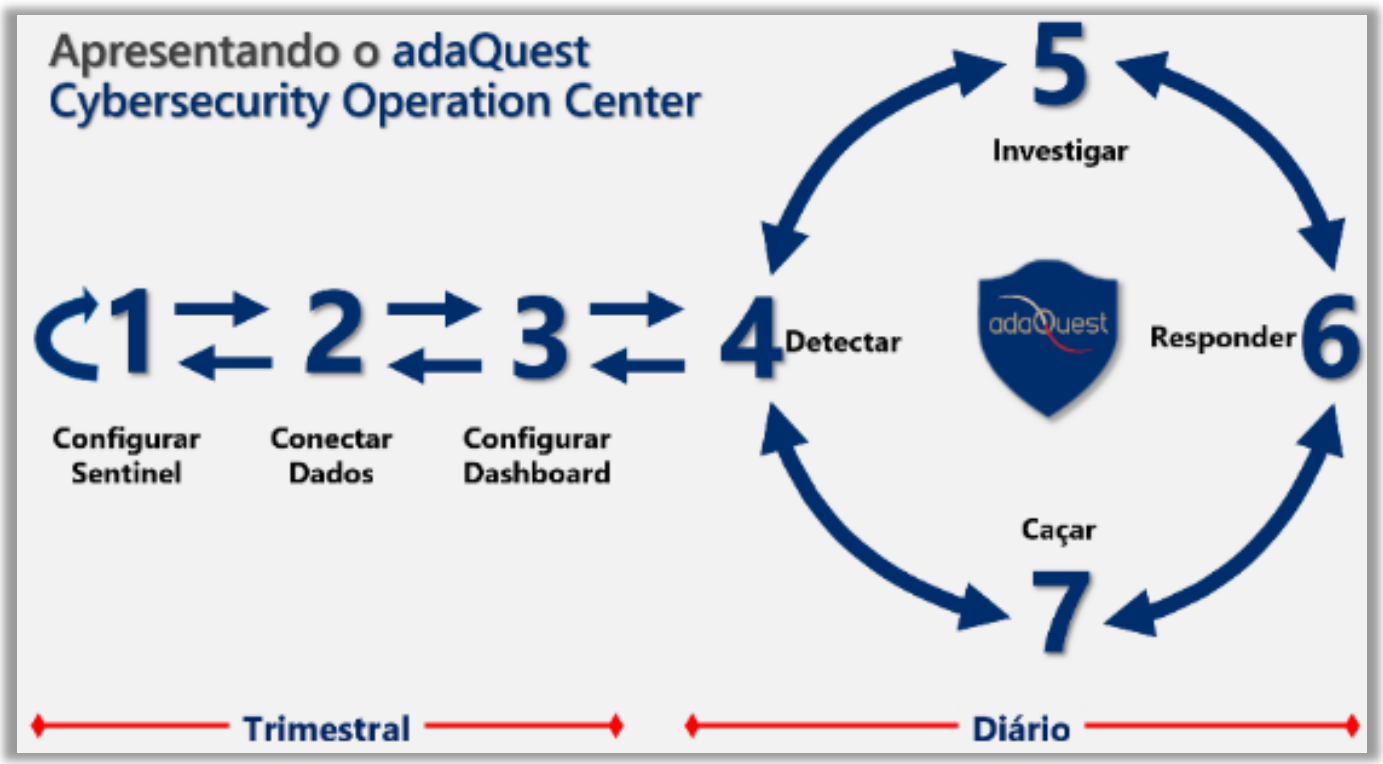
O Microsoft Sentinel facilita a coleta de dados de segurança em toda sua organização híbrida a partir de dispositivos, usuários, aplicativos, servidores e qualquer nuvem. Usando o poder da inteligência artificial e do aprendizado de máquinas, o Microsoft Sentinel garante que as ameaças reais sejam identificadas rapidamente e liberta você da carga das soluções tradicionais de gerenciamento de incidentes e eventos de segurança (SIEMs), automatizando a configuração, manutenção e dimensionamento da infraestrutura.

O Microsoft Sentinel é uma solução de Gerenciamento de Eventos de Segurança da Informação (SIEM) e Orquestração de Segurança Automatizada de Resposta (SOAR). O Microsoft Sentinel fornece análises inteligentes de segurança e inteligência de ameaças em toda a organização, fornecendo uma solução única para detecção de alerta, visibilidade de ameaças, caça proativa e resposta a ameaças.

Então, quais são as melhores práticas que você precisa estar ciente ao projetar e implantar o Microsoft Sentinel?

Nós consideramos 7 passos necessários para uma boa implementação de Microsoft Sentinel:

1. **Configurando o Microsoft Sentinel**
2. **Conectando os Dados**
3. **Configurando Dashboards e Workbooks**
4. **Detectando Ameaças**
5. **Investigando Incidentes**
6. **Respondendo à Ameaças**
7. **Caçando às Ameaças**

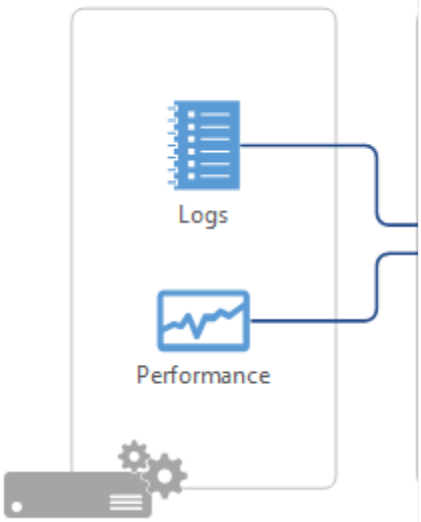


Passo 1: Configurando o Microsoft Sentinel

Citamos aqui 2 boas práticas nas configurações que são: **Desenho do Log Analytics e Reserva de Capacidade**.

O Microsoft Sentinel utiliza um Log Analytics Workspace (espaço de trabalho de análise logística) para armazenar seus dados.

A melhor prática é usar um único Log Analytics Workspace de segurança em seu Tenant, porque você pode ter múltiplos Log Analytics Workspace, alguns para dados de operações como desempenho e métricas de seus recursos do Azure, ou recursos do seu ambiente local. Então ter o Log Analytics Workspace de segurança vai trazer todos os seus dados de segurança de forma centralizada.



Seguindo a boa prática, a localização onde se cria o Log Analytics Workspace deve atender se há a obrigatoriedade de onde os dados devem residir e preferencialmente na mesma região dos seus recursos Azure, se houver, para evitar custos de tráfego de rede entre regiões (cross-tenant bandwidth).

Falaremos agora de um ponto muito importante quando se trata de boas práticas na configuração: **entender a cobrança/custos de utilização do Microsoft Sentinel.**

O Microsoft Sentinel é faturado com base no volume de dados ingeridos para análise e armazenados no espaço de trabalho (Workspace) do Azure Monitor Log Analytics. O Microsoft Sentinel oferece um modelo de preço flexível e previsível e há duas maneiras de pagar pelo serviço: Reservas de capacidade e Pay-As-You-Go. É altamente recomendável estabelecer reservas de capacidade.

Uma vez entendida a quantidade de dados que você está ingerindo no Microsoft Sentinel, você pode definir uma reserva de capacidade que permite à Microsoft dar-lhe um desconto na quantidade de dados que você está ingerindo. Você pode usar a reserva de capacidade para ajudar a reduzir seus custos com o Microsoft Sentinel.

Veja mais em: https://azure.microsoft.com/pt-br/pricing/details/microsoft-sentinel/

Passo 2: Conectando Dados

Hoje existem cerca de 122 conectores e a Microsoft está planejando ter mais, portanto, fique de olho em novos conectores.

Recomendamos a ordem abaixo ao habilitar os conectores de dados para ingestão no Microsoft Sentinel:

1. Habilitar conectores de primeira viagem rapidamente, principalmente porque é muito fácil. Você pode abrir a página de conectores, clique em "ativar", assumindo que você tenha as permissões corretas para aquela fonte de dados, como Microsoft Defender for Endpoint, ou Microsoft Defender for Office 365, Microsoft Defender forCloud Apps, e então você pode clicar em aplicar e já está feito.

2 Muitos desses conectores são gratuitos como Office 365, registro de atividades Azure, Azure AD, e qualquer um dos primeiros alertas de segurança da família Microsoft Defender (Microsoft 365 Defender / Azure Defender) também são gratuitos.

3 Microsoft Sentinel está no Azure e é rápido de habilitar, você pode aproveitar ferramentas para implantar políticas e configurar logs de diagnóstico Azure para qualquer um de seus serviços, recursos como SQL ou Storage. Você pode criar uma política, e colocar essas políticas no Azure, que aplicará e configurará todos os seus recursos para enviar os logs para o Workspace do Sentinel.

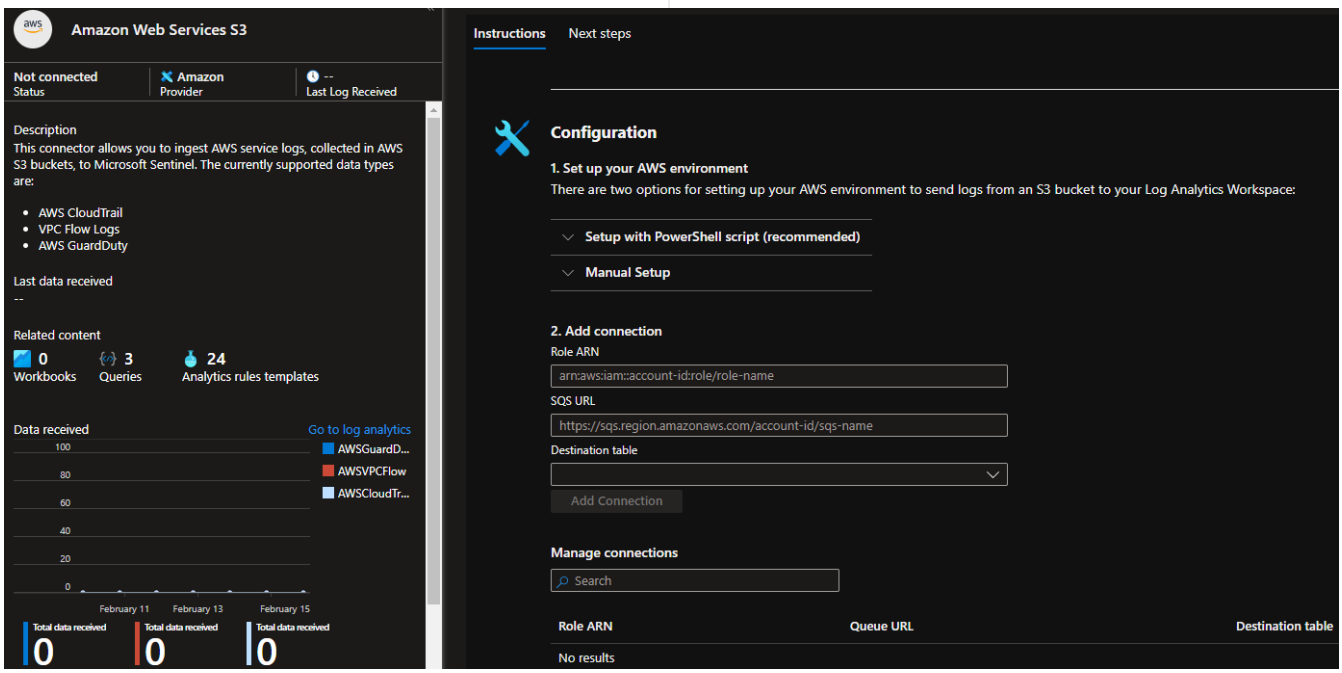
4 Conectar outras fontes de nuvens, tais como aplicações AWS e SaaS. Novamente é fácil de configurar, você pode ir até aquela aplicação de nuvem assumindo que você tenha as permissões corretas e então clicar em "conectar" na página de conectores de dados do Microsoft Sentinel e seguir os passos informados.

5 Implementar agente Windows e Linux no Azure. Isto pode ser feito com a política do Azure. Já existe uma política integrada que facilita o processo, para que você possa simplesmente pegar essa política, aplicá-la ao seu ambiente, editá-la conforme necessário e esse agente será implantado e se reportará ao Microsoft Sentinel rapidamente.

6 Implementar o agente Windows e Linux no data center local e outras nuvens para obter as máquinas das quais você deseja coletar dados. Este agente trabalha em qualquer máquina, não importa se é virtual no Google GCP, no AWS ou no Azure, ou no data center no ambiente local.

7 Implementar sua coleção de formatos de eventos comuns (CEF). Configure uma máquina Linux para fazer a coleta CEF e poderá configurar essas fontes, coisas como firewalls (Fortinet, Palo Alto, entre outros, por exemplo) para enviar seus dados a esse coletor CEF.

8 Integre qualquer alimentação de Threat Intelligence (TI) ao Microsoft Sentinel, isso pode ser feito através do esforço de código aberto como STIX/TAXII (The Trusted Automated Exchange of Indicator Information) ou através da alimentação API de segurança do Microsoft Graph.



Passo 3: Configurando Dashboards e Workbooks

Uma vez que você tenha seus dados no Microsoft Sentinel, através dos Workbooks, você permitirá que analistas e administradores de segurança visualizem os dados em seu ambiente utilizando displays gráficos. Esta é uma ferramenta poderosa porque qualquer dado que possa ser consultado agora também pode ser exibido em um formato gráfico fácil de entender.

Nos Workbooks você será capaz de construir visualizações gráficas para coletar informações táticas tais como:

- **MITRE**[1] são mais comuns no seu ambiente. Estas informações são úteis para determinar quais áreas de segurança da informação e controlar nossa equipe de segurança cibernética precisa se concentrar. Os Workbooks exibem informações que normalmente seriam mais técnicas para serem exibidas à maioria dos outros usuários em um formato muito compreensível.
- **CMMC** (Cybersecurity Maturity Model Certification)[2]. A estrutura da CMMC usa um modelo de maturidade para determinar o nível de segurança em uma organização. O Workbook CMMC tem tanto a descrição de cada nível de maturidade quanto exibições gráficas da segurança atual no ambiente Microsoft para ajudar a determinar se ela atende aos requisitos de segurança para os diferentes níveis de maturidade.
- **Monitoramento da saúde da Coleta de Dados.** Este Workbook coleta "metadados" sobre o tipo de dados que estão sendo coletados em cada Workspace Log Analytic. Isso é útil para determinar as características dos dados recebidos, como o volume de dados, tipo de dados e a frequência com que os dados aparecem.

- **Auditoria.** Este Workbook revisa os dados sobre os Logs Analytics aos quais cada instância do Microsoft Sentinel está conectada. Há abas que revisam quem está consultando o Workspace do Sentinel e com que frequência. Isto pode ser usado tanto para rastrear atividades avançadas de caça quanto para ver que tipo de informação está sendo mais procurada. Há também uma aba "Operações CRUD" que tem informações sobre toda a atividade de criação, leitura, atualização e exclusão que está acontecendo no espaço de trabalho. Isto é útil para ver que tipo de atividade administrativa está acontecendo no espaço de trabalho e quem está realizando estas ações.
- **Insights de investigação.** Este Workbook está focado nas investigações de incidentes do Sentinel e no que aconteceu durante esses incidentes. Um cronograma de incidentes e uma lista de incidentes que aconteceram ao longo do tempo estabelecido estão disponíveis na seção superior. Um incidente pode ser selecionado na lista para visualizar detalhes adicionais sobre o incidente, como os alertas associados a ele. Perto da parte inferior do Workbook há também uma seção chamada "Entity Insights" onde o usuário pode procurar por incidentes que tenham um endereço IP específico, conta, host, URL ou hash de arquivo associado a ele.
- **Análise do Comportamento do Usuário & Entidade.** A característica UEBA (User and Entity Behavior Analytics) é uma adição recente ao Microsoft Sentinel que lhe permite rastrear o comportamento incomum do usuário e levantar alertas com base nesse comportamento incomum. O Workbook baseado na UEBA tira informações da análise do comportamento e as exibe na forma de gráficos interativos. Uma lista de usuários que têm mostrado comportamento suspeito no período de tempo é listada perto do topo do Workbook, e cada um deles pode ser selecionado para visualizar que tipo de comportamento incomum ou suspeito esse usuário tem tido.

- **Relatório de utilização do Sentinel Workspace.** Obtenha informações sobre o uso do seu espaço de trabalho. Neste Workbook, você pode visualizar o consumo de dados de Workspace, o período, as tarefas recomendadas e as estatísticas de Custo e Utilização.

Passo 4: Detectando ameaças, Investigando Acidentes, Respondendo aos Eventos e Agindo proativamente caçando as ameaças (hunting)

Chegamos na etapa das configurações de como se lida com as ameaças. A próxima melhor prática é a Analytics. Isto é simples de implementar usando alguns dos modelos que a Microsoft fornece para o ambiente.

Antes de mais nada, recomenda-se habilitar qualquer regra de incidente da Microsoft. Há uma regra ativada por padrão para a regra do tipo de aprendizagem da máquina Fusion, que é ativada dentro de cada instância Sentinel. O Fusion usa a aprendizagem da máquina para olhar e ver se dois alertas fazem parte do mesmo ataque (Kill Chain).

Então pode-se ativar as regras de incidentes da Microsoft, e estas regras permitem que você crie incidentes automaticamente sempre que receber um alerta de segurança do Microsoft Defender for Endpoint, Defender for Cloud apps, Microsoft Defender for Office 365, Azure Security Center, etc.

Em seguida, pode-se percorrer todos os 'modelos de regras' incorporados e procurar aqueles que são interessantes para seu ambiente em seus conjuntos de dados e habilitá-los rapidamente.

Você também pode verificar a comunidade GitHub. A Microsoft tem uma lista de detecção que pode não estar incluída no Microsoft Sentinel como modelo, portanto, há algumas fontes adicionais que você pode querer ver.

E por último, você pode construir qualquer detecção personalizada que você possa precisar para qualquer caso de falta de uso.

A última melhor prática é a Automação e Resposta de Orquestração de Segurança (SOAR).

O Microsoft Sentinel usa o Azure Logic Apps para ajudar a responder a incidentes dentro do Microsoft Sentinel. A equipe da Microsoft construiu uma boa integração onde você pode automaticamente executar playbooks como parte de uma regra analítica. É possível também executá-los manualmente se quiser selecionar mais dados para uma investigação que está fazendo, e há muitos modelos no Microsoft Sentinel GitHub que você pode usar como um ótimo ponto de partida.

Até agora, apresentamos importantes capacidades do Microsoft Sentinel que podem ser usadas durante o ciclo de vida da resposta ao incidente, como análise e gerenciamento de casos. Entretanto, organizações que têm um Centro de Operações de Segurança (SOC) mais maduro estão começando a investir mais na investigação proativa para identificar indicações de ataque (IOA). Este processo é normalmente chamado de "caça proativa" ou "caça proativa de ameaças".

O Microsoft Sentinel fornece uma plataforma para a caça proativa de ameaças que pode ajudar a identificar comportamentos sofisticados de ameaças usados por agentes, mesmo quando eles ainda estão nos estágios iniciais do ataque. O objetivo é ser capaz de interromper a cadeia de ataque cibernético durante as fases iniciais para evitar explorações.

[1] https://attack.mitre.org/
[2] https://www.acq.osd.mil/cmmc/

Anexo F
Processo de Avaliação de Segurança Cibernética

Mapeie sua maturidade de segurança cibernética por meio de avaliações periódicas e descubra onde estão as vulnerabilidades e riscos. É o primeiro passo indispensável para proteger sua organização contra ataques cibernéticos de forma direcionada e eficiente.

Então, onde começa a resiliência cibernética? E como você cria uma estratégia forte de segurança? O fato é que a segurança de dados tradicional não é mais suficiente. A criação de uma rede no local segura e compatível para sua organização e a tentativa de abrigar todos os recursos da organização lá, está simplesmente desatualizada.

Uma primeira pergunta lógica – e necessária – é: como sua organização lida atualmente com ameaças digitais? Quão maduras são suas medidas atuais de segurança cibernética? Can você age proativamente quando necessário? Mas acima de tudo: por onde você deve começar a rever a estratégia de segurança? Quais são as vulnerabilidades e riscos?

Baseline measurement:

Para poder efetivamente iniciar a estratégia de segurança, é importante determinar o ponto de partida, ou seja, fazer uma medição de linha de base. Quão madura é sua segurança cibernética no momento? Qual é o escopo da sua segurança da informação? Os seguintes elementos fornecem uma forte indicação disso:

1. Quão forte é a **autenticação**? Você usa uma autenticação multifatorial forte? Como você minimiza o risco de roubo de identidade?
2. Quão adaptável é a sua **política de acesso**? Você tem políticas claras para acesso aceitável aos recursos? Como você aplica isso?
3. Você está usando **micro-segmentação**? Até que ponto sua organização está se movendo para uma segmentação abrangente e distribuída usando micro perímetros definidos por software?
4. Você já implementou **alertas automáticos e atrações de recuperação** para minimizar o tempo médio entre ataque e resposta?
5. Você faz uso de **inteligência artificial e inteligência em nuvem** para detectar e responder a anomalias em tempo real?
6. Até que ponto você **classifica e protege** seus dados? Como você protege dados confidenciais da exposição a exfiltrações maliciosas ou acidentais, ou seja, a liberação não tertida de dados de sistemas de computador?

CSAT:

Avaliação de Segurança Cibernética (CSAT) é baseada na estrutura da CEI, um conjunto amplamente utilizado de práticas recomendadas projetadas para gerenciamento estruturado de riscos cibernéticos dentro de empresas e organizações. Ele ajuda você a responder perguntas críticas sobre o programa de segurança cibernética da sua organização, como qual inventário proteger e onde estão as lacunas de segurança.

A avaliação de segurança oferece os seguintes recursos:

- On-premisse – a ferramenta de avaliação é instalada em um servidor na rede;
- Dispositivos – os laptops, desktops e servidores da rede são verificados por meio de uma amostra;

- Microsoft 365 – controle de todos os serviços usados (e compartilhados);
- Plataforma Azure – insight sobre o uso seguro da plataforma em nuvem;
- (Azure) Diretório Ativo – assessment do ambiente completo (Azure) Active Directory;
- Pesquisa – um de nossos consultores de segurança faz perguntas específicas sobre processos e procedimentos de segurança.

Como parte da avaliação de segurança, entre outras coisas, verifica se o Windows está configurado com segurança e se os patches corretos foram aplicados. Também verifica permissões administrativas e usuários externos na Microsoft 365, Teams ou documentos compartilhados no SharePoint. Esses insights determinam a atual maturidade de segurança da organização, com base em ações concretas de melhoria podem ser propostas.

Melhoria Direcionada:

O CSAT oferece um plano claro de ação para melhorar a segurança cibernética de sua organização, exatamente onde ela é necessária. Inclui medidas tecnológicas e processuais claras, para que você possa começar imediatamente e usar seus recursos de forma direcionada.

Uma avaliação de segurança cibernética permite que você obtenha uma visão sobre os riscos de segurança da organização, permitindo que você priorize rapidamente e efetivamente as melhorias propostas com base em fatos.

Continue Monitorando:

Após a implementação das ações de melhoria, é importante fazer uma segunda avaliação para medir o que melhorou em relação à medição da linha de base. Não se esqueça de envolver a equipe de gestão na apresentação dos resultados, para que eles também estejam cientes dos riscos reduzidos e do aumento da maturidade cibernética da organização.

O próximo passo é priorizar, desenvolver e planejar os próximos objetivos. A segurança cibernética não tem um ponto de partida ou fim. É impossível acertar tudo de uma vez, por isso é importante fazer disso um foco contínuo.

Fornecer documentação precisa das ações de status, progresso e melhoria continuamente. Isso não é apenas valioso para uso interno, mas também indispensável no que diz respeito ao cumprimento das leis e regulamentos, por exemplo, aqueles relacionados ao GDPR.

O mundo de TI está mudando em um ritmo rápido, assim como os cibercriminosos. As ameaças digitais estão em constante evolução. Embora uma avaliação pontual forneça uma medição detalhada da maturidade cibernética atual e potenciais vulnerabilidades e riscos, é vital manter o monitoramento e permanecer constantemente em alerta.

Anexo G
Microsoft Compliance Manager

O Microsoft Compliance Manager é um recurso do Microsoft 365 Compliance Center que torna mais fácil e conveniente para você gerenciar os requisitos de conformidade da sua organização. O Microsoft Compliance Manager é uma solução que abrange toda a Microsoft e ajuda a cumprir obrigações complexas de conformidade, inclusive: ISO 27001, ISO 27018, NIST 800-53, HIPAA, GDPR/LGPD entre outros.

O Compliance Manager pode ajudá-lo em todas as etapas de sua jornada de conformidade, desde o inventário de riscos de proteção de dados, até o gerenciamento da complexidade da implementação de controles, atualização com regulamentos e certificações e relatórios aos auditores.

O Gerenciador de Conformidade ajuda a simplificar a conformidade e reduzir o risco fornecendo:

- Avaliações pré-criadas para padrões e regulamentos comuns do setor e regionais ou avaliações personalizadas para atender às suas necessidades de conformidade.
- Ele fornece recursos de fluxo de trabalho para ajudá-lo a concluir com eficiência suas avaliações de risco por meio de uma ferramenta comum.
- Orientações detalhadas passo a passo sobre ações de melhoria sugeridas para ajudá-lo a cumprir os padrões e regulamentos mais relevantes para sua organização. Para ações gerenciadas pela Microsoft, você verá detalhes da implementação e resultados de auditoria.
- Uma pontuação de conformidade baseada em risco para ajudá-lo a entender sua postura de conformidade medindo seu progresso na conclusão de ações de melhoria.

O Microsoft Compliance Manager é composto de quatro elementos principais que trabalham em conjunto para detalhar sua jornada de conformidade:

Controles:

Este elemento detalha os requisitos na norma de conformidade que sua organização está tentando cumprir. Ele define como você precisa avaliar e gerenciar configurações, processos e pessoas responsáveis por atender os requisitos especificados. O Microsoft Compliance Manager ajuda a rastrear esses controles e os divide em duas categorias: Controles gerenciados pela Microsoft, ou aqueles pelos quais a Microsoft é responsável pela implementação, e controles compartilhados, ou controle pelo qual sua organização e a Microsoft compartilham responsabilidade. O Microsoft Compliance Manager avalia esses controles por meio da varredura de seu ambiente, e o status de sua atividade é atualizado diariamente. Isso significa que uma vez que você implemente um controle para atender sua exigência de conformidade, o status será atualizado no dia seguinte.

Avaliações:

As avaliações são um agrupamento de controles a partir de sua norma ou regulamento de conformidade especificado. Estes incluem tudo dentro do elemento de controle, além de serviços no escopo e pontuações de avaliação. Os serviços no escopo são um conjunto de serviços da Microsoft que se aplicam à avaliação, e a pontuação mostra o progresso feito no tratamento dos controles e na obtenção da conformidade. Se você completar todos os controles com uma avaliação específica, isso colocará sua configuração Microsoft em conformidade com o padrão de conformidade inicialmente selecionado.

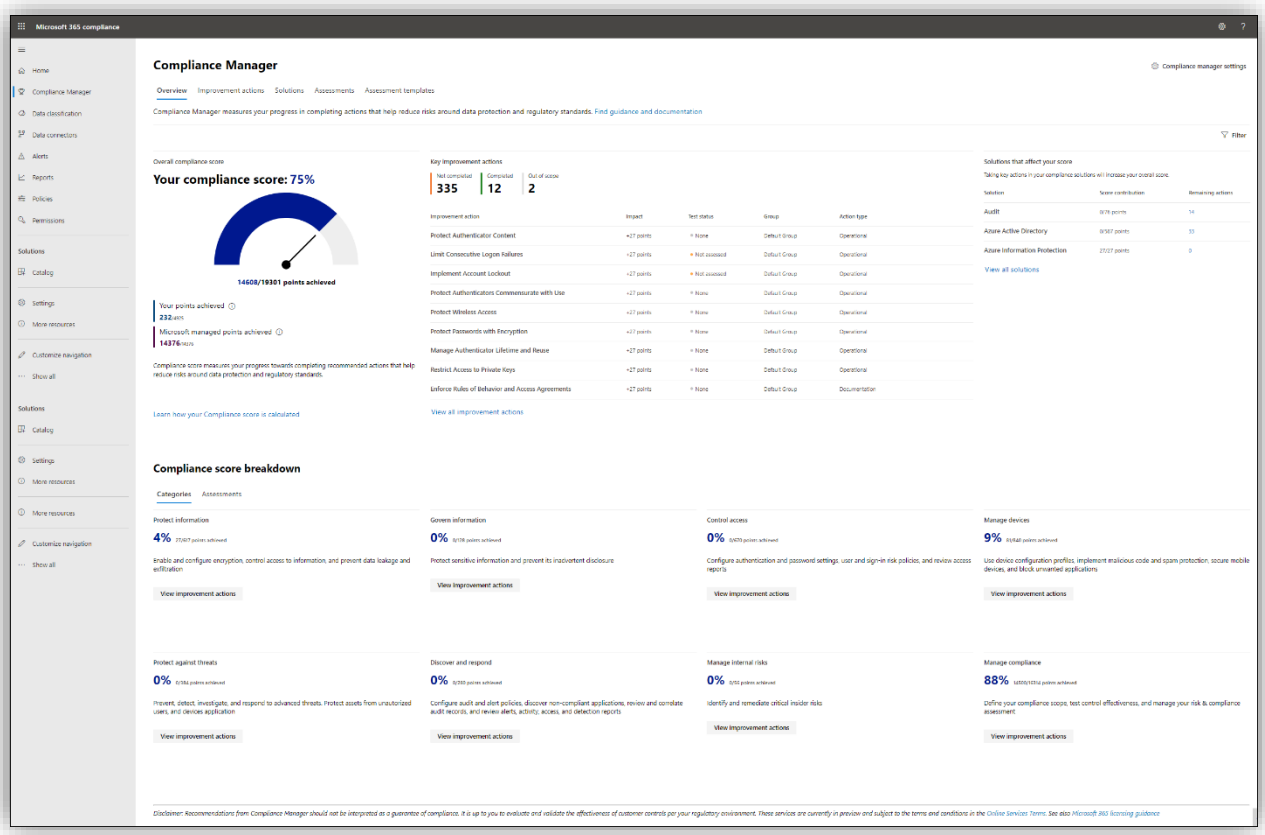
Modelos:

As avaliações são construídas utilizando modelos, que podem ser pré-construídos pela Microsoft ou personalizados de acordo com as necessidades específicas de sua organização. Você pode escolher qual padrão de conformidade sua organização precisa atender. A Microsoft tem mais de 35 modelos pré-construídos, alguns dos quais já estão incluídos e outros que são premium. Alguns dos modelos incluídos são o Microsoft Data Protection Baseline, EU GDPR, ISO/IEC 27001:2013, e NIST 800-53, enquanto alguns dos modelos premium são LGPD, SOC 1 e 2, PCI DSS, Privacy of Consumer Financial and Health Information Regulation, HIPAA/HITECH, FERPA, e Sarbanes-Oxley Act.

Ações de Melhoria:

Ações de melhoria são os elementos finais principais do Microsoft Compliance Manager. Este recurso centraliza suas atividades de conformidade e detalha quais ações específicas sua organização precisa tomar para alinhá-lo com os regulamentos de conformidade especificados. Estas podem ser atribuídas a um usuário específico para serem concluídas e cada ação de melhoria pode armazenar documentos, notas e atualizações de status dentro dela. Quando uma atualização estiver disponível para uma ação de melhoria, como quando houver mudanças regulamentares, você será notificado através de uma ação de melhoria que pode ser aceita ou adiada. As ações de melhoria têm impacto direto e melhoram sua pontuação de conformidade.

No Dashboard do Microsoft Compliance Manager é dada uma pontuação inicial baseada na linha de base de proteção de dados Microsoft 365. Esta linha de base é um conjunto de controles que inclui regulamentos e padrões-chave para proteção de dados e governança geral de dados. Essa pontuação é alterada positivamente mediante ações que venham a ser tomadas para a melhoria da proteção dos dados e negativamente após algum incidente ou brecha que venha a ser encontrada ou que afete as políticas de conformidade.



Fonte: [Gerenciador de Conformidade do Microsoft Purview - Microsoft 365 Compliance | Microsoft Docs]

Precisa de mais ajuda?

"A **adaQuest** é uma empresa Gold parceira da Microsoft para Segurança e Conformidade e um dos poucos parceiros globais para FastTrack. Ajudamos nossos clientes a desenvolver roteiros de transformação digital e a implantar com rapidez e eficácia as ferramentas de segurança e produtividade mais adequadas, incluindo Microsoft Teams, Office 365, Intune, Autopilot, Proteção Avançada contra Ameaças, Microsoft Defender, OneDrive for Business, SharePoint Online e muito mais."

adaQuest

Gold Security
Gold Cloud Platform
Gold Enterprise Mobility Management
Gold Windows and Devices
Gold Cloud Productivity

Microsoft Partner

Microsoft

Gold Application Development
Gold Project and Portfolio Management
Silver Small and Midmarket Cloud Solutions
Silver Collaboration and Content
Silver Data Analytics

Entre em contato conosco!

adaQuest, Rua Funchal, 418 - 350 Andar, São Paulo/SP – CEP: 04551-060
www.adaquest.com
adainfo@adaquest.com
+55 (11) 3500-5993

CNJ Resolução 396

"A segurança cibernética é um grande tema para todas as organizações em todo o mundo. As agências governamentais são particularmente vulneráveis a ataques cibernéticos de maneiras diferentes das organizações comerciais. Eles geralmente mantêm dados confidenciais de cidadãos e de segurança nacional em sua infraestrutura de TI. À medida que o mundo da TI se move para a nuvem e cada vez mais dispositivos pessoais se conectam à rede, torna-se imperativo estabelecer soluções de segurança mais sofisticadas para combater os ataques cibernéticos sofisticados em constante crescimento.

Muitas novas regulamentações e leis estão sendo emitidas por órgãos legisladores para ajudar a forçar um nível mínimo de melhores práticas de segurança cibernética e governar as expectativas. Órgãos governamentais estão emitindo resoluções específicas para abordar o cumprimento dessas normas e leis e garantir que haja a consistência da aplicação das melhores práticas de segurança cibernética entre todos os órgãos\filiais de uma determinada entidade governamental, como é o caso da Resolução 396 emitida pelo CNJ.

Tive o prazer de escrever este eBook e demonstrar como os diferentes aspectos da Resolução 396 do CNJ podem ser organizados de uma forma mais simples de entender, e quais soluções técnicas específicas podem ser consideradas e aplicadas. Este eBook fornece uma visão geral estratégica que deve ajudar as diferentes agências afetadas por esta resolução a começar com seu próprio planejamento estratégico de cibersegurança e avançar aumentando a adoção e o cumprimento das exigencias estabelecidas nesta resolução. Tenho certeza de que os leitores também vão gostar."

O Desenvolvimento deste eBook contou com a ajuda e participação de grandes profissionais, dentre os quais gostaria de deixar meu agradecimento:

Hiram Machado, adaQuest CEO, trabalha na indústria de TI há quase 30 anos. Hiram obteve seu mestrado em segurança cibernética e liderança na Universidade de Washington. Como chefe da adaQuest, Hiram dedica seu tempo para apoiar e ajudar organizações pequenas e empresariais a melhorar sua resiliência a ataques cibernéticos com a aplicação de processos de práticas recomendadas de segurança cibernética, uso de tecnologia avançada e educação do pessoal sobre a importância da conscientização sobre segurança cibernética.