Política de segurança da informação

2.2 GESTÃO DE ACESSOS

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

cba B+G

Sumário

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

1. Objetivo

Esta política estabelece diretrizes para assegurar que o acesso às informações, sistemas e recursos da empresa seja concedido de forma controlada, rastreável e limitada conforme as responsabilidades de cada usuário. O objetivo é prevenir acessos não autorizados e mitigar riscos de vazamento ou manipulação indevida de dados.

2. Abrangência

Aplica-se a todos os colaboradores, terceiros, parceiros e prestadores de serviço que utilizam sistemas, serviços ou infraestrutura da empresa, incluindo ambientes em nuvem (como Microsoft 365), ferramentas locais ou recursos físicos em colocation.

3. Diretrizes

3.1. Princípios de Acesso

Concedemos os acessos com base no princípio do menor privilégio, limitado ao necessário para o desempenho das funções do usuário. Utilizamos as funcionalidades de gestão de permissão das ferramentas que possuem controle de usuário utilizando a lógica de grupos de segurança, com base em permissionamento vertical, de acordo com o tier de governança e horizontal, de acordo com o departamento.

Para os usuários que possuem permissão de administradores das ferramentas, sempre segmentamos os logins em contas diferentes (contas sys) para evitar acesso à informação ou modificação acidental durante a atuação cotidiana das funções.

Os acessos administrativos irrestritos são compartilhados apenas entre o Head de Informação e o CEO, com possibilidade de auditoria entre eles. Toda concessão de privilégio elevado ou administrativo deve ser justificada e aprovada formalmente, de acordo com as nossas diretrizes de segregação de funções e permissionamento

3.2. Criação, Revisão e Revogação de Acessos

O processo de criação de acessos para os usuários nas ferramentas segue o fluxo de onboarding documentado e controlado pelo time de tecnologia. Já a revogação dos acessos ocorre imediatamente após o desligamento ou mudança de função, com base em processo formal coordenado com o time de people.

Todos os acessos são revistos periodicamente, ao menos a cada 6 meses, para verificar sua pertinência. Fazemos essa validação por usuário e por ferramenta.

A gestão de acessos ao ambiente Microsoft 365 é centralizada via Azure Active Directory (Azure AD) ou Entra ID, com trilhas de auditoria ativadas. A gestão de acessos ao ambiente Google Cloud Platform (GCP) é realizada via IAM (Identity and Access Management) do GCP, com atribuição de papéis e permissões a usuários e grupos vinculados a contas do Google Workspace, além de auditoria ativada via Cloud Audit Logs. A gestão de acessos ao ambiente AWS é centralizada via AWS Identity and Access Management (IAM), com controle por políticas e registro detalhado de atividades por meio do AWS CloudTrail.

3.3. Autenticação e Senhas

O uso de autenticação multifator (MFA) é obrigatório para todos os acessos ao Microsoft 365 e demais sistemas críticos para os usuários dos tiers 1 e 2 de governança. Para os demais colaboradores esses acessos são estimulados. Trocas de senha são recomendadas periodicamente e forçadas em caso de comprometimento.

Realizamos auditoras de login recorrentes do ambiente Microsoft para validar as frequências e localização dos logins para validar potenciais pontos de vulnerabilidade.

3.4. Acessos Físicos

O servidor em colocation possui acesso físico restrito, com controles de entrada realizados pelo parceiro local. Apenas pessoas autorizadas e previamente registradas podem acessar fisicamente o ambiente, mediante autenticação local. Possuímos também uma sala para a manutenção, configuração e envio de equipamentos para os colaboradores. Essa sala segue os mesmos princípios de acesso da sala de servidor.

3.5. Rastreamento e Auditoria

Todos os acessos a sistemas e dados sensíveis são registrados automaticamente. Logs de autenticação, alterações e acessos administrativos são mantidos por no mínimo 3 meses e revisados conforme demanda ou incidentes.

3.6. Segregação de Funções e permissionamento

Os acessos aos sistemas, arquivos e recursos da empresa são organizados em níveis hierárquicos chamados Tiers de Segurança (sec.Tiers). Essa estrutura define o grau de privilégio de cada perfil de usuário, assegurando a aplicação do princípio do menor privilégio, a rastreabilidade e o controle de exposição de informações sensíveis.

Os usuários são adicionados aos grupos no ambiente de acordo com o seu nível de acesso.

Cada Tier representa um agrupamento de permissões conforme o papel e responsabilidade do usuário na organização:

sec.Tier 0 – Head de Informação e Tech Support

Nível mais alto de privilégio. Responsável pela administração de sistemas e gestão dos demais acessos, incluindo a criação e exclusão de contas, controle de convidados externos e acesso irrestrito aos recursos da organização.

sec.Tier 1 – Board

Diretores executivos com acesso total aos arquivos da célula CBA e permissões ampliadas para criação de recursos, visualização e colaboração em múltiplas áreas. Possuem acesso restrito para convidar usuários externos.

sec.Tier 2 – Head

Líderes de áreas com autonomia para criar recursos, gerenciar seus times e acessar integralmente os arquivos e ferramentas sob sua responsabilidade. O convite de usuários externos é controlado.

sec.Tier 3 – Diretores

Usuários com acesso completo aos dados e recursos da sua área de atuação, mas com restrição na criação de estruturas e no convite de terceiros.

sec.Tier 4 – Gerentes

Permissão para criação de conteúdos e colaboração em projetos, com acesso amplo à sua área e recursos compartilhados.

Convidar usuários externos requer aprovação.

sec.Tier 5 – Equipe

Perfil de suporte administrativo com acesso amplo a arquivos operacionais, mas restrição à criação de estruturas e ao convite de usuários externos.

sec.Tier 6 – Fornecedores externos

Nível de acesso mais restrito, voltado a colaboradores temporários. Permissões limitadas à leitura ou edição de arquivos específicos, sem permissão para compartilhamento, download ou convite de terceiros.

3.7. Responsabilidades

Time de tech support: Gerenciar o ciclo de vida dos acessos; manter os controles de autenticação ativos; auditar acessos privilegiados; revisar periodicamente as permissões.

Time de people: Gerencia os processos de contratação, alteração de função e desligamento, dando os gatilhos necessários para o controle de acessos para o time de people.

Gestores de área: Solicitar criação, alteração ou revogação de acessos com base nas funções dos colaboradores.

Todos os usuários: Utilizar os acessos exclusivamente para fins profissionais e manter suas credenciais protegidas.

3.8. Penalidades

O descumprimento desta política poderá resultar em medidas disciplinares, conforme previsto em contrato ou no regulamento interno, incluindo advertência, suspensão ou desligamento.

4. Controle de alterações

Versão	Data	Quem	Anotações
2	04/02/2025	Luis Bartolomei	Aprovação
1	03/12/2024	Thiago Ramiro	Criação

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam