Boas Práticas de Gestão de Identidade e Acesso (IAM) para Fornecedores

Introdução
A segurança da informação é um pilar essencial para a proteção dos dados e ativos corporativos. Este documento estabelece diretrizes abrangentes sobre as melhores práticas de **Gestão de Identidade e Acesso (IAM)** que todos os fornecedores devem adotar. A adesão a essas práticas é indispensável para garantir a **integridade, confidencialidade e disponibilidade** das informações da Dock.

---

1. Autenticação Segura

- **Criação de Senhas Fortes:**
  As senhas devem conter no mínimo 12 caracteres, incluindo uma combinação de letras maiúsculas, minúsculas, números e símbolos especiais. A reutilização de senhas antigas ou o uso de informações pessoais deve ser evitado.
- **Múltiplos Fatores de Autenticação (MFA):**
  A utilização do **MFA** adiciona uma camada extra de segurança às credenciais de acesso, verificando a identidade do usuário. Na Dock, utilizamos o aplicativo homologado **Okta Verify**, integrado aos nossos sistemas, para garantir um acesso seguro e eficiente.
- **Single Sign-On (SSO):**
  Sempre que possível, utilize o **Login Unificado (SSO)** para acessar os ambientes corporativos da Dock, assegurando autenticação centralizada e protegida.

---

2. Acesso Controlado

- **Privilégios Baseados em Função (RBAC):**
  Os acessos devem ser concedidos exclusivamente aos sistemas e informações necessárias para a execução dos serviços contratados.
- **Princípio do Menor Privilégio:**
  As permissões devem ser limitadas ao mínimo essencial para o desempenho das atividades, reduzindo o risco de vulnerabilidades associadas a acessos desnecessários.
- **Revisão Periódica de Acessos:**
  Todos os acessos serão revisados periodicamente com base na criticidade, assegurando alinhamento com as políticas de segurança da Dock.

---

3. Segurança da Informação

- **Proteção de Dados Sensíveis:**
  Informações confidenciais relacionadas aos serviços contratados devem ser tratadas

com sigilo. Elas devem ser armazenadas de forma segura, classificadas adequadamente e, sempre que aplicável, protegidas por criptografia.

- **Atenção ao Phishing:**
  Esteja atento a e-mails ou mensagens com características suspeitas. Evite clicar em links ou baixar anexos de fontes desconhecidas.
- **Treinamentos Recorrentes:**
  Incentivamos os fornecedores a participarem de treinamentos periódicos sobre segurança da informação, reforçando conceitos e boas práticas que garantam um ambiente de trabalho seguro.

---

4. Uso Responsável de Recursos

- **Utilização de Dispositivos Autorizados:**
  Apenas dispositivos seguros e previamente autorizados devem ser utilizados para acessar os sistemas corporativos da Dock.
- **Logout Após o Uso:**
  Realize o logout de todas as contas e sistemas ao concluir suas atividades, especialmente em dispositivos compartilhados ou públicos.

---

5. Monitoramento e Relato de Incidentes

- **Monitoramento de Atividades Incomuns:**
  Fornecedores devem estar atentos a atividades ou comportamentos anômalos em seus acessos aos sistemas da Dock. Qualquer irregularidade deve ser reportada imediatamente.
- **Relato Ágil de Incidentes:**
  Em caso de comprometimento de credenciais ou qualquer incidente de segurança relacionado aos serviços fornecidos, informe imediatamente a equipe de segurança da informação da Dock.

---

6. Encerramento de Acesso

- **Revogação de Acesso:**
  O acesso aos sistemas da Dock deve ser desativado imediatamente após o término do contrato ou serviço, garantindo a segurança das informações.
- **Desligamento Imediato:**
  Em casos de encerramento de contrato com fornecedores que possuem acessos privilegiados, a revogação deve ser feita de forma imediata. Gestores podem utilizar o **bot disponível no canal #dock-managers no Slack** para solicitar a desativação.

Conclusão
A aplicação das práticas descritas neste documento é essencial para proteger os dados, sistemas e ativos da Dock. Contamos com a colaboração de todos os fornecedores para manter um ambiente corporativo seguro e resiliente.

Contato
Para quaisquer dúvidas ou solicitações de informações adicionais, entre em contato com a equipe de IAM da Dock.