

Checklist: 7 passos para a segurança corporativa na cloud.

Protocolos e práticas recomendadas da Velora Cloud para proteger seus dados mais sensíveis.

A mudança para a **Nuvem** oferece flexibilidade e escalabilidade sem precedentes, mas também apresenta novos desafios de **segurança cibernética**. Com a crescente complexidade das ameaças digitais, proteger os dados corporativos na *cloud* é mais crítico do que nunca.

Na **Velora Cloud**, entendemos que a segurança é a espinha dorsal de qualquer operação bem-sucedida. Por isso, preparamos um checklist essencial de 7 passos para garantir que sua infraestrutura e seus dados permaneçam seguros no ambiente *cloud*.

1. Implemente uma Governança de Acesso e Identidade (IAM) Robusta

A base da segurança na Nuvem começa com o controle de quem pode acessar o quê.

- **O Que Fazer:**
 - Utilize o princípio do **privilegio mínimo**: conceda aos usuários apenas as permissões necessárias para realizar suas tarefas.
 - Implemente **Autenticação Multifator (MFA)** para todos os usuários, especialmente administradores.
 - Revise regularmente as permissões de acesso, removendo as que não são mais necessárias.
 - Centralize a gestão de identidades para ter uma visão clara de todos os acessos.
- **Velora Cloud Ajuda:** Nossa plataforma permite uma gestão granular de usuários e grupos, facilitando a aplicação de políticas de acesso rigorosas.

2. Criptografe Seus Dados em Repouso e em Trânsito

A criptografia é sua primeira linha de defesa contra acessos não autorizados, tanto para dados armazenados quanto para dados em movimento.

- **O Que Fazer:**
 - Criptografe todos os dados armazenados em discos, *storage* e *backups* (dados em repouso).
 - Use **SSL/TLS** para criptografar a comunicação entre seus servidores e os usuários (dados em trânsito).
 - Gerencie suas chaves de criptografia com segurança, idealmente usando um serviço de gerenciamento de chaves.

- **Velora Cloud Ajuda:** Nossas soluções de *storage* e rede são compatíveis com os mais altos padrões de criptografia, garantindo que seus dados estejam protegidos contra interceptações.

3. Configure Redes e Firewalls de Forma Segura

A segmentação da rede e a configuração correta de *firewalls* são cruciais para isolar recursos e controlar o fluxo de tráfego.

- **O Que Fazer:**
 - Utilize **Redes Virtuais Privadas (VPCs)** para isolar seus recursos na Nuvem.
 - Crie **sub-redes** para diferentes camadas de aplicação (ex: *web, app, database*).
 - Configure **Firewalls Dedicados** com regras de entrada e saída rigorosas, permitindo apenas o tráfego essencial.
 - Mantenha suas interfaces de rede o menos expostas possível à internet pública.
- **Velora Cloud Ajuda:** Oferecemos controle total sobre a configuração de sua rede virtual, permitindo a criação de **redes VPC e VPN seguras**, além de *firewalls* customizáveis para proteger seus ambientes.

4. Gerencie Vulnerabilidades e Aplique Patches Regularmente

Sistemas desatualizados são a porta de entrada para a maioria dos ataques cibernéticos.

- **O Que Fazer:**
 - Mantenha todos os sistemas operacionais, aplicações e bibliotecas atualizados com os últimos *patches* de segurança.
 - Realize **scans de vulnerabilidade** periodicamente para identificar e corrigir falhas antes que sejam exploradas.
 - Implemente um processo de **gestão de mudanças** para garantir que as atualizações não introduzam novas vulnerabilidades.
- **Velora Cloud Ajuda:** Nossa infraestrutura é mantida com os mais altos padrões de segurança, e fornecemos as ferramentas para que você possa gerenciar e aplicar *patches* em seus servidores com facilidade.

5. Monitore Atividades Suspeitas e Logs de Auditoria

A detecção precoce de anomalias é fundamental para responder rapidamente a incidentes de segurança.

- **O Que Fazer:**
 - Centralize e analise os **logs de auditoria** de todos os seus recursos na Nuvem.
 - Monitore o acesso de usuários, mudanças de configuração, tentativas de login falhas e tráfego de rede incomum.

- Configure **alertas** automáticos para atividades que desviam do comportamento normal.
- **Velora Cloud Ajuda:** Nossas ferramentas de monitoramento fornecem *insights* detalhados sobre a performance e o comportamento de sua infraestrutura, permitindo que você configure alertas para eventos críticos.

6. Implemente um Plano Abrangente de Backup e Recuperação de Desastres (DR)

Mesmo com todas as precauções, falhas podem ocorrer. Um plano de DR garante a continuidade dos negócios.

- **O Que Fazer:**
 - Realize **backups regulares** de todos os dados críticos, armazenando-os em locais separados e seguros.
 - Teste seu plano de **Recuperação de Desastres (DR)** para garantir que ele funcione quando necessário.
 - Defina **RTO (Recovery Time Objective)** e **RPO (Recovery Point Objective)** para seus serviços.
 - Criptografe seus backups.
- **Velora Cloud Ajuda:** Oferecemos soluções de **Cloud Backup e DRaaS (Disaster Recovery as a Service)** que replicam seus dados e sistemas em tempo real, garantindo um failover rápido e a proteção contra perda de dados.

7. Conduza Auditorias de Segurança e Testes de Penetração

Avaliadores externos podem identificar vulnerabilidades que sua equipe interna pode ter deixado passar.

- **O Que Fazer:**
 - Contrate especialistas em segurança para realizar **auditorias regulares** em seu ambiente *cloud*.
 - Realize **testes de penetração (pentests)** para simular ataques e identificar pontos fracos em suas defesas.
 - Garanta que sua empresa esteja em conformidade com as regulamentações de segurança relevantes para sua indústria (ex: LGPD, ISO 27001).
- **Velora Cloud Ajuda:** Nossa infraestrutura é construída com os mais altos padrões de segurança e conformidade, e oferecemos a transparência e as ferramentas para que você possa realizar suas próprias auditorias.

A segurança na Nuvem não é um evento, mas um processo contínuo. Seguindo este checklist da **Velora Cloud**, você estará no caminho certo para construir uma postura de segurança corporativa robusta e proteger seus ativos mais valiosos.

Quer saber como a Velora Cloud pode fortalecer a segurança da sua empresa na Nuvem?
Fale com um de nossos especialistas.

www.veloracloud.com.br

contato@veloracloud.com.br