GUIA PRÁTICO

Política Segurança da Informação - PSI

AccessBrasil

INOVAÇÃO NO MUNDO INFORMATIZADO

Este **Guia Prático de Segurança da Informação** tem como objetivo traduzir as diretrizes estratégicas da **AccessBrasil** em ações operacionais claras, padronizando a conduta técnica tanto no desenvolvimento de sistemas quanto na gestão de infraestrutura e manutenção. Em um cenário de ameaças digitais crescentes, este documento serve como uma ferramenta de consulta rápida para garantir que a segurança seja integrada de forma nativa (security by design) em cada entrega, mitigando riscos de interrupções e vazamentos, e assegurando a resiliência dos serviços prestados aos nossos clientes.

GUIA PRÁTICO

Política Segurança da Informação - PSI

1. Desenvolvimento de Sistemas
2. Infraestrutura e Redes
3. Manutenção e Suporte Técnico
4. Estações de Trabalho
5. Checklist de Incidentes

AccessBrasil
INOVAÇÃO NO MUNDO INFORMATIZADO

Desenvolvimento de Sistemas

Para nossa equipe de Desenvolvedores, a segurança começa no código:

- Gestão de Secrets: Nunca suba chaves de API, senhas de banco de dados ou tokens no código-fonte (Git). Utilize variáveis de ambiente ou cofres de senhas (ex: Vault, AWS Secrets Manager).
- Sanitização de Dados: Todo input de usuário deve ser validado para prevenir ataques de SQL Injection e XSS.
- Code Review: Antes do merge para produção, o código deve passar por revisão de pares com foco em brechas de segurança.
- Bibliotecas de Terceiros: Verifique vulnerabilidades em dependências (npm, pip, nuget) antes de integrá-las aos projetos da AccessBrasil.

AccessBrasil
INOVAÇÃO NO MUNDO INFORMATIZADO

Código seguro é o alicerce da nossa infraestrutura: protegemos o dado do cliente como se fosse o segredo do nosso sucesso.

capítulo 2

AccessBrasil
INOVAÇÃO NO MUNDO INFORMATIZADO

Infraestrutura e Redes

A disponibilidade é nossa entrega, mas a segurança é nossa garantia: uma rede só é forte quando é impenetrável.

Para nossa equipe de campo e suporte:

- Princípio do Privilégio Mínimo: Ninguém deve ter acesso "Root" ou "Admin" por padrão. Libere apenas o acesso necessário para a tarefa específica e revogue-o após a conclusão.
- Hardening de Servidores: Todo novo servidor deve passar pelo processo de desativação de serviços desnecessários e fechamento de portas de comunicação não utilizadas.
- Backup 3-2-1: Mantenha 3 cópias dos dados, em 2 tipos de mídia diferentes, com 1 cópia fora do site (off-site/cloud). Teste a restauração mensalmente.
- Criptografia em Trânsito: Todo tráfego de dados entre sistemas e clientes deve utilizar protocolos seguros (HTTPS/TLS, SSH, VPN).

Manutenção e Suporte Técnico

No atendimento ao cliente:

- Identificação de Usuário: Nunca altere senhas ou forneça acessos baseando-se apenas em solicitações por chat ou telefone sem a devida validação de identidade (MFA ou pergunta de segurança).

- Acesso Remoto Seguro: Utilize apenas ferramentas de acesso remoto autorizadas pela AccessBrasil que gerem logs de auditoria (ex: AnyDesk Enterprise, TeamViewer com logs).

- Descarte de Hardware: Discos rígidos (HDs/SSDs) de servidores substituídos devem sofrer destruição física ou sanitização lógica (Wipe) antes do descarte.

A confiança do usuário é o nosso maior ativo: suporte de excelência começa no sigilo e termina na segurança dos dados.

capítulo 4

AccessBrasil
INOVAÇÃO NO MUNDO INFORMATIZADO

Estações de Trabalho

A segurança da AccessBrasil começa no seu login: sua estação de trabalho protegida é o primeiro escudo contra qualquer invasão.

Regras para o ambiente interno:

- Criptografia de Disco: Todos os notebooks da empresa devem estar com o disco criptografado (BitLocker/FileVault).
- Antivírus e EDR: É proibido desativar o software de proteção de endpoint para "ganhar performance".
- Updates: Atualizações de Segurança de SO e Browsers devem ser instaladas em no máximo 48h após o lançamento.

Checklist de Incidentes

O QUE FAZER AGORA?

Se detectar algo estranho (lentidão atípica na rede, arquivos com extensão estranha, acesso não autorizado):

1. **Isole**: Desconecte a máquina da rede (tire o cabo ou desligue o Wi-Fi). Não desligue o computador (para preservar evidências na memória RAM).

2. **Reporte**: Avise o CGS via canal oficial imediatamente.

3. **Documente**: Anote o que você estava fazendo e o horário exato da anomalia.

Um incidente ignorado é uma brecha aberta: sua agilidade em reportar é o que separa um susto de uma crise.

A segurança da informação na **AccessBrasil** não é um estado estático, mas um processo contínuo que depende do compromisso individual de cada colaborador. Ao integrar estas práticas ao seu fluxo de trabalho, você não apenas protege a nossa infraestrutura e os dados dos nossos clientes, mas consolida a nossa reputação como uma empresa de tecnologia confiável e resiliente.

Lembre-se: a tecnologia nos dá as ferramentas, mas a sua vigilância é o que garante a nossa proteção.

AccessBrasil

INOVAÇÃO NO MUNDO INFORMATIZADO

Comunicação

rhecomunicacao@accessbrasil.net.br
Tel. (11) 5641.5243 ramal 200
www.accessbrasil.net.br