F&MD

POLÍTICA DE SEGURANÇA CIBERNÉTICA

A segurança das suas informações está no nosso DNA e sabemos que parte importante da excelência de nossos serviços é a proteção de dados e informações relativas aos nossos clientes, às nossas operações e aos nossos sistemas internos. Por isso, disponibilizamos aqui nossa Política de Segurança Cibernética para que você possa conhecer um pouco mais das nossas diretrizes para proteção dos seus dados.

Estão sujeitos a esta política a Agência F&MD e todos os seus funcionários, consultores, terceiros, fornecedores e parceiros, caso acessem, armazenem, processem ou transmitam informações pertencentes, ou sob a nossa guarda.

Nosso objetivo é manter a confidencialidade, integridade e disponibilidade das informações de propriedade ou sob nossa guarda, estabelecer medidas para a proteção da infraestrutura que suporta os serviços e atividades de negócio e prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Visamos garantir que as informações são disponibilizadas apenas a indivíduos e entidades autorizadas, além de serem precisas, completas e protegidas de alterações indevidas e intencionais.

O acesso a sistemas, recursos e outros ativos de informação são concedidos baseados na necessidade de negócio e com segregação de funções.
Os acessos são gerenciados através de um ciclo de vida desde a criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação.
Ressaltamos a necessidade das senhas serem compostas seguindo os requisitos de complexidade, não podendo ser reutilizadas, compartilhadas, armazenadas em arquivos ou escritas em qualquer lugar.

Os logs e trilhas de rastreabilidade são habilitados em ambientes de produção, protegidos de acessos e alterações não autorizados e registram quais, por quem e quando as atividades foram executadas.

Utilizamos um sistema de programação que armazena as informações implementadas em cada um de nossos projetos, bem como quem foi o programador responsável, qual foi a linha de código implementada e quando determinada ação foi realizada.

Além disso, utilizamos ferramentas e processos para monitorar e impedir que informações sensíveis deixem o ambiente interno de uma organização sem autorização, tais como software anti-malware de detecção, prevenção e recuperação ou controles equivalentes, além de realizarmos backups periódicos acerca dos bancos de dados.

Por fim, nossos profissionais são treinados e conscientizados para reconhecer situações de risco e agir corretamente quando impactados por elas.

Atualizada em Março de 2022.