MAF
Consultoria e Treinamento

Política de Segurança da Informação

1. Objetivo

A presente Política de Segurança da Informação (SI) da MAF Consultoria, Treinamento e Auditoria Interna ("MAF" ou "Empresa") tem como objetivo estabelecer as diretrizes e responsabilidades para proteger os ativos de informação da Empresa e de seus clientes contra ameaças, garantindo a continuidade dos negócios, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. Esta política visa assegurar a **confidencialidade**, a **integridade** e a **disponibilidade** de todas as informações sob a custódia da MAF. [1]

2. Escopo

Esta política aplica-se a todos os colaboradores, diretores, conselheiros, prestadores de serviço, estagiários e terceiros que tenham acesso a informações ou utilizem os recursos de tecnologia da informação da MAF, independentemente de sua localização física ou vínculo contratual. Abrange todos os sistemas, redes, aplicações, bancos de dados e qualquer outro ativo de informação, seja em formato digital ou físico.

3. Princípios de Segurança da Informação

A segurança da informação na MAF é fundamentada em três princípios essenciais:

- **Confidencialidade:** Garantir que a informação seja acessível apenas por pessoas autorizadas. A proteção da informação contra divulgação não autorizada é vital para a confiança de nossos clientes e para a proteção de nossa propriedade intelectual.
- **Integridade:** Assegurar a exatidão e a completude da informação e dos métodos de seu processamento. A informação deve ser protegida contra alterações não autorizadas, garantindo sua confiabilidade.
- **Disponibilidade:** Garantir que os usuários autorizados tenham acesso à informação e aos ativos associados sempre que necessário. Os sistemas e processos devem ser resilientes para suportar as operações de negócio da Empresa.

4. Diretrizes Gerais de Segurança

Para implementar os princípios de segurança, a MAF adota as seguintes diretrizes, baseadas nas melhores práticas de mercado, como as normas ISO/IEC 27001 e 27002 e o NIST Cybersecurity Framework. [1] [2]

4.1. Classificação da Informação

Toda informação produzida ou mantida pela MAF deve ser classificada de acordo com seu nível de sensibilidade e criticidade para o negócio. As categorias são: **Pública**, **Interna**, **Confidencial** e **Restrita**. Cada classificação possui requisitos específicos de manuseio, armazenamento, transporte e descarte.

4.2. Controle de Acesso

O acesso aos sistemas e informações da MAF deve ser controlado com base no princípio do "menor privilégio" e da "necessidade de saber". As senhas devem ser fortes, trocadas periodicamente e não devem ser compartilhadas. O uso de autenticação de múltiplos fatores (MFA) é obrigatório para acesso a sistemas críticos.

4.3. Segurança de Recursos Humanos

A segurança da informação é uma responsabilidade de todos. Todos os colaboradores devem receber treinamento sobre esta política e suas responsabilidades. A verificação de antecedentes pode ser realizada durante o processo de contratação, e as responsabilidades de segurança devem ser incluídas nos contratos de trabalho. No desligamento, os acessos devem ser revogados imediatamente.

4.4. Segurança Física e do Ambiente

As instalações da MAF e os locais onde as informações são processadas ou armazenadas devem ser protegidos por controles de acesso físico. Medidas devem ser tomadas para proteger os equipamentos contra roubo, danos e acesso não autorizado. Adota-se uma política de "mesa limpa e tela limpa" para reduzir o risco de acesso não autorizado.

4.5. Gestão de Ativos

Todos os ativos de informação (hardware, software, etc.) devem ser inventariados e ter um proprietário designado. O uso de ativos da empresa para fins pessoais deve ser limitado e seguir as diretrizes específicas. O descarte de equipamentos deve ser feito de forma segura para garantir que nenhuma informação sensível possa ser recuperada.

4.6. Criptografia

A criptografia deve ser utilizada para proteger informações confidenciais e restritas, tanto em repouso (armazenadas) quanto em trânsito (transmitidas por redes). As chaves criptográficas devem ser gerenciadas de forma segura.

4.7. Segurança nas Operações e Comunicações

Os sistemas devem ser protegidos contra malware e outras ameaças. As alterações nos sistemas devem seguir um processo formal de gestão de mudanças. Backups regulares das informações críticas devem ser realizados e testados periodicamente. A segurança das redes deve ser garantida por meio de firewalls, segregação de redes e monitoramento contínuo.

4.8. Gestão de Incidentes de Segurança da Informação

Todos os incidentes de segurança da informação devem ser reportados imediatamente ao responsável pela área. A MAF manterá um plano de resposta a incidentes para garantir uma

reação rápida e eficaz, minimizando os impactos. Os incidentes serão investigados, e as lições aprendidas serão utilizadas para aprimorar os controles.

4.9. Gestão da Continuidade dos Negócios

A MAF deve desenvolver e manter um Plano de Continuidade de Negócios (PCN) para garantir que as operações essenciais possam ser recuperadas em tempo hábil após uma interrupção significativa. O plano deve ser testado e atualizado regularmente.

5. Responsabilidades

- **Alta Direção:** Prover os recursos necessários e demonstrar apoio contínuo à segurança da informação.
- **Gestor de Segurança da Informação (ou Comitê):** Coordenar a implementação e a manutenção desta política e dos controles de segurança.
- **Gestores de Áreas:** Garantir que a política seja cumprida em suas respectivas áreas de responsabilidade.
- **Colaboradores e Terceiros:** Cumprir as diretrizes desta política e reportar quaisquer violações ou incidentes de segurança.

6. Conformidade e Revisão

O cumprimento desta política é mandatório. Violações podem resultar em medidas disciplinares, incluindo a rescisão do contrato de trabalho ou de prestação de serviços, além das sanções civis e criminais cabíveis. A MAF realizará auditorias periódicas para verificar a conformidade com esta PSI. Esta política será revisada anualmente ou sempre que ocorrerem mudanças significativas no ambiente de negócio ou tecnológico.

Referências

[1] International Organization for Standardization. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection.

[2] National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. Disponível em: https://www.nist.gov/cyberframework

[3] Presidência da República. Decreto nº 9.637, de 26 de dezembro de 2018 - Política Nacional de Segurança da Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm

Página de assinaturas

Antonio Filho
097.000.288-28
Signatário

HISTÓRICO

12 fev 2026 08:29:35 — **Antonio Martiningo Filho** criou este documento. (Email: martiningo29@gmail.com, CPF: 097.000.288-28)

12 fev 2026 08:29:36 — **Antonio Martiningo Filho** *(Email: martiningo29@gmail.com, CPF: 097.000.288-28)* visualizou este documento por meio do IP 177.96.223.203 localizado em Brasília - Federal District - Brazil

12 fev 2026 08:29:41 — **Antonio Martiningo Filho** *(Email: martiningo29@gmail.com, CPF: 097.000.288-28)* assinou este documento por meio do IP 177.96.223.203 localizado em Brasília - Federal District - Brazil