POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Mater Imperium

SUMÁRIO

1. OBJETIVO

A Mater Imperium estabelece esta Política de Segurança da Informação e Privacidade (PSIP) como parte integrante de seu sistema de gestão corporativo, alinhada às boas práticas de mercado, às normas internacionalmente aceitas e à legislação brasileira aplicável, incluindo a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD).

O objetivo desta política é assegurar níveis adequados de proteção às informações e aos dados pessoais tratados pela organização, seus clientes, parceiros e colaboradores, preservando sua confidencialidade, integridade, disponibilidade e privacidade, e promovendo o uso responsável e seguro dos recursos informacionais sob sua responsabilidade.

2. PROPÓSITO

Esta política tem como propósito estabelecer diretrizes e normas de Segurança da Informação e Privacidade, orientando os colaboradores da Mater Imperium quanto à adoção de comportamentos, controles e processos que assegurem:

- O atendimento aos requisitos legais, regulatórios e contratuais relacionados à Segurança da Informação e à Privacidade de Dados Pessoais;
- A proteção das informações da Mater Imperium e de seus clientes, garantindo os princípios de confidencialidade, integridade e disponibilidade;
- A prevenção de incidentes de segurança, reduzindo riscos operacionais, financeiros, legais e de imagem;
- A preservação da confiança de clientes, fornecedores, parceiros e colaboradores, fortalecendo a cultura de segurança na organização;
- A minimização de perdas decorrentes de falhas de segurança, vazamentos de dados ou interrupções operacionais.

3. CONTEXTO DA ORGANIZAÇÃO

A Mater Imperium é uma empresa brasileira do setor de tecnologia, sujeita à legislação nacional — incluindo a LGPD (Lei nº 13.709/2018) e a requisitos contratuais de seus clientes e parceiros. As partes interessadas relevantes para a segurança da informação incluem: colaboradores, prestadores de serviço, fornecedores, clientes, órgãos reguladores e autoridades competentes.

O escopo do Sistema de Gestão de Segurança da Informação (SGSI) abrange todos os processos, sistemas, pessoas e instalações que tratam informações da Mater Imperium e de seus clientes, incluindo ambientes locais (on-premises) e em nuvem. Esta política é revisada anualmente ou sempre que ocorrerem mudanças significativas no contexto interno ou externo da organização (ex.: mudanças regulatórias, mudanças relevantes nos sistemas, alterações no perfil de risco ou na estrutura organizacional).

4. PAPÉIS E RESPONSABILIDADES

4.1 Responsável de Segurança da Informação e Privacidade (RSIP)

O Responsável pela Segurança da Informação e Privacidade (RSIP) é o papel responsável por gerenciar e supervisionar o Sistema de Gestão de Segurança da Informação (SGSI) da Mater Imperium, sendo designado pela Alta Direção. O RSIP deve possuir conhecimento técnico em segurança da informação e atuar como ponto de referência para todas as questões relacionadas à proteção das informações e privacidade de dados da organização.

4.1.1 É responsabilidade do RSIP:

- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
- Garantir que as atividades de segurança da informação e privacidade de dados sejam executadas em conformidade com a PSIP;
- Promover a divulgação da PSIP e tomar as ações necessárias para disseminar uma cultura de segurança da informação e privacidade de dados pessoais no ambiente da Mater Imperium;
- Coordenar o processo de avaliação de riscos e reportar os resultados à Alta Direção;
- Analisar e deliberar sobre a aplicação de sanções em caso de violações à PSIP;
- Monitorar o compliance de fornecedores e terceiros com os requisitos de segurança contratados.

4.2 Alta Direção

A Alta Direção da Mater Imperium é responsável por aprovar formalmente esta política, garantir os recursos necessários para sua implementação, e demonstrar liderança e comprometimento com o Sistema de Gestão de Segurança da Informação (SGSI).

4.3 Comitês

A Mater Imperium pode constituir comitês de apoio à governança da segurança da informação. A composição, atribuições e regras de funcionamento de cada comitê são documentadas em regimentos internos ou outros documentos específicos, complementares a esta política.

4.4 Colaboradores e Prestadores de Serviço

Todos os colaboradores e prestadores de serviço são responsáveis por conhecer e cumprir as diretrizes desta política e das normas complementares, bem como por reportar prontamente ao RSIP quaisquer suspeitas de incidentes de segurança.

5. POLÍTICA

Esta política se aplica a todos os colaboradores, fornecedores e parceiros da Mater Imperium que possuem acesso às informações e dados pessoais da Mater Imperium e/ou fazem uso de recursos computacionais compreendidos na infraestrutura interna.

3.1 É POLÍTICA DA MATER IMPERIUM:

- Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade das informações e dados pessoais operados na Mater Imperium sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: Colaboradores, terceiros contratados, fornecedores e, onde pertinente, clientes;
- Garantir a educação e a conscientização sobre as práticas de segurança da informação e privacidade de dados adotadas pela Mater Imperium para colaboradores, terceiros contratados, fornecedores e, onde pertinente, clientes;
- Atender integralmente requisitos de segurança da informação e privacidade dos dados pessoais aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Tratar integralmente incidentes de segurança da informação e a privacidade de dados pessoais, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicados às autoridades apropriadas;
- Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- Melhorar continuamente a Gestão de Segurança da Informação e Privacidade através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

6. RETENÇÃO, COMUNICAÇÃO E APROVAÇÃO DA POLÍTICA

Esta política deve ser aprovada formalmente pela Alta Direção da Mater Imperium antes de entrar em vigor. Cada versão desta política, em formato físico ou eletrônico, deve ser retida pelo período em que estiver vigente acrescido de no mínimo 5 (cinco) anos após sua substituição.

A política deve ser comunicada a todos os colaboradores, prestadores de serviço e partes interessadas relevantes por meio de treinamento no ingresso e atualizações anuais, e deve estar disponível no portal interno da organização. Mudanças materiais na política devem ser comunicadas a todos os destinatários imediatamente após a aprovação.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações tratadas pela Mater Imperium devem ser classificadas de acordo com as seguintes categorias, para garantir que os controles aplicados sejam proporcionais ao risco:

Restrita: Informações altamente sensíveis cujo acesso não autorizado pode causar dano grave à organização ou a indivíduos. Exemplos: dados pessoais sensíveis (saúde, biometria), senhas, chaves criptográficas, dados de cartão de pagamento, segredos comerciais. Acesso limitado a indivíduos expressamente autorizados.

Confidencial: Informações internas de negócio não destinadas ao público. Exemplos: registros financeiros, contratos, dados de clientes, relatórios internos, dados pessoais de colaboradores. Acesso restrito às áreas responsáveis e mediante necessidade de conhecimento.

Uso Interno: Informações de uso geral dentro da organização, sem necessidade de proteção especial, mas não destinadas ao público externo. Exemplo: comunicações internas, políticas gerais, manuais de procedimento.

Pública: Informações aprovadas para divulgação pública. Exemplo: conteúdo do site institucional, materiais de marketing. Não requer controles especiais além de garantir sua integridade.

Todo colaborador e prestador de serviço é responsável por identificar e tratar adequadamente as informações conforme sua classificação. O RSIP definirá procedimentos complementares de rotulagem e manuseio para cada categoria.

8. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A Mater Imperium deve manter um processo contínuo de identificação, análise, avaliação e tratamento de riscos de segurança da informação, em conformidade com a ISO/IEC 27001:2022 (seção 6). O processo de gestão de riscos deve:

- Ser realizado pelo menos anualmente ou sempre que ocorrerem mudanças significativas nos sistemas, processos ou ambiente de negócio;
- Identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade das informações;
- Avaliar a probabilidade e o impacto de cada risco identificado;
- Definir e implementar planos de tratamento para os riscos, podendo incluir: aceitação, mitigação, transferência ou eliminação;
- Documentar os resultados e manter um Registro de Riscos atualizado;
- Ser submetido à apreciação da Alta Direção pelo menos uma vez ao ano.

O RSIP é responsável por coordenar o processo de gestão de riscos e reportar os resultados à Alta Direção, que deve aprovar formalmente o apetite ao risco da organização e os planos de tratamento propostos.

9. CONTROLE DE ACESSO

O acesso a sistemas, aplicações e dados da Mater Imperium deve ser controlado com base no princípio do menor privilégio, garantindo que cada usuário acesse apenas o necessário para o desempenho de suas funções. As seguintes diretrizes se aplicam:

Provisionamento de Acesso: Todo acesso deve ser formalmente solicitado, aprovado pelo gestor responsável e concedido pelo time de TI com base na função do usuário. Contas compartilhadas são proibidas, exceto em casos expressamente autorizados pela área de Infraestrutura e Segurança.

Política de Senhas: As senhas devem ter no mínimo 12 caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais. Senhas não devem ser reutilizadas nas últimas 5 trocas e devem ser alteradas a cada 180 dias. É vedado o compartilhamento de senhas.

Autenticação Multifator (MFA): O uso de MFA é obrigatório para acesso a sistemas que tratam informações Restritas ou Confidenciais, incluindo acesso remoto e administrativo. O fator adicional deve ser baseado em aplicativo autenticador ou hardware (chave física); SMS não é um fator aceito.

Revisão e Revogação de Acessos: Os acessos devem ser revisados conforme periodicidade definida no procedimento de Gestão de Acessos em conjunto com os gestores. Em caso de desligamento ou mudança de função, o acesso deve ser revogado imediatamente pelo time de TI, após notificação do RH. Contas inativas por mais de 90 dias devem ser desabilitadas.

10. SEGURANÇA EM RECURSOS HUMANOS

Pré-contratação: Verificações de antecedentes devem ser realizadas para todos os candidatos à contratação, proporcionais à sensibilidade da função e às informações que serão acessadas, observando a legislação aplicável. Os contratos de trabalho e de prestação de serviços devem conter cláusulas de confidencialidade e de responsabilidade sobre segurança da informação.

Treinamento e Conscientização: Todo colaborador e prestador de serviço deve receber treinamento de segurança da informação no momento do ingresso e anualmente. O conteúdo mínimo inclui: política de segurança, classificação da informação, uso aceitável dos recursos, engenharia social e phishing, tratamento de dados pessoais (LGPD) e procedimento de notificação de incidentes. Os registros de conclusão do treinamento devem ser mantidos pelo RSIP.

Desligamento: O RH deve notificar o time de TI imediatamente após o desligamento de qualquer colaborador ou encerramento de contrato de prestador de serviço. Todos os acessos devem ser revogados no mesmo dia. Os equipamentos e ativos da organização devem ser devolvidos. As obrigações de confidencialidade permanecem vigentes após o desligamento.

11. SEGURANÇA DE FORNECEDORES E TERCEIROS

Antes de contratar fornecedores ou terceiros que terão acesso a informações ou sistemas da Mater Imperium, deve ser realizada uma avaliação de segurança proporcional ao risco. Os contratos devem incluir cláusulas de segurança da informação e privacidade, Acordo de Nível de Serviço (SLA) e, quando aplicável, o Acordo de Processamento de Dados (Data Processing Agreement — DPA) exigido pela LGPD.

Os fornecedores devem reportar prontamente quaisquer incidentes de segurança que envolvam dados ou sistemas da Mater Imperium. O RSIP deve monitorar periodicamente o compliance dos fornecedores com os requisitos de segurança contratados, podendo determinar a suspensão ou encerramento da relação em caso de descumprimento. Critérios de encerramento de relação com fornecedores incluem: falha em fornecer informações precisas, recusa em aderir a cláusulas de segurança, descumprimento de obrigações contratuais de segurança, e divulgação de violações de dados.

12. SEGURANÇA NAS OPERAÇÕES E SISTEMAS

Gestão de Ativos: A Mater Imperium deve manter um inventário atualizado de todos os ativos de informação (hardware, software, dados, serviços em nuvem), com proprietários definidos para cada ativo. O inventário deve ser revisado anualmente ou sempre que houver mudanças significativas.

Proteção contra Código Malicioso: Todos os dispositivos e servidores devem possuir solução de antimalware/EDR (Endpoint Detection and Response) instalada, atualizada e habilitada continuamente. Qualquer evento detectado deve ser registrado e analisado.

Gestão de Vulnerabilidades e Patches: Varreduras de vulnerabilidades devem ser realizadas periodicamente nos sistemas. As atualizações e correções de segurança (patches) devem ser aplicadas o mais rapidamente possível, priorizando vulnerabilidades críticas. Vulnerabilidades que não puderem ser corrigidas imediatamente devem ter controles compensatórios documentados.

Backup e Recuperação: Cópias de segurança (backups) das informações críticas devem ser realizadas regularmente, armazenadas em local seguro e separado do ambiente de produção, e testadas periodicamente para garantir a recuperabilidade dos dados.

Registros de Auditoria (Logs): Os logs de acesso, alteração e eventos de segurança devem ser habilitados em todos os sistemas que tratam informações Restritas ou Confidenciais. Os registros devem ser protegidos contra alteração ou exclusão não autorizada, retidos por no mínimo 12 meses, e monitorados para detecção de atividades anômalas ou suspeitas.

Criptografia: Informações classificadas como Restritas ou Confidenciais devem ser criptografadas em trânsito (utilizando TLS 1.2 ou superior) e em repouso. O uso de AES-256 é recomendado para criptografia simétrica. Chaves criptográficas devem ser gerenciadas de forma segura, com controles de acesso e rotação periódica, e não devem ser armazenadas em código-fonte.

Segurança Física: Instalações que abrigam sistemas ou mídias com informações Restritas ou Confidenciais devem possuir controles de acesso físico adequados. O descarte de mídias e

equipamentos deve ser realizado de forma segura, garantindo a destruição irreversível dos dados neles contidos.

Uso de Contas Corporativas e Proibição de Shadow IT: Todos os colaboradores e prestadores de serviço devem utilizar exclusivamente credenciais corporativas provisionadas pela Mater Imperium para acessar sistemas, aplicações e serviços de terceiros utilizados para fins profissionais. É vedado o uso de contas pessoais (ex.: e-mail pessoal, serviços de armazenamento pessoal como Google Drive pessoal ou Dropbox pessoal) para armazenar, transmitir ou processar informações classificadas como Uso Interno, Confidencial ou Restrita.

A contratação, instalação ou uso de sistemas, aplicações, serviços em nuvem ou ferramentas de software sem aprovação prévia da área de TI e do RSIP é expressamente proibida, prática conhecida como Shadow IT. Todo novo serviço ou ferramenta que venha a tratar informações da Mater Imperium deve ser previamente avaliado e aprovado, seguindo o processo de avaliação de fornecedores descrito na seção 11 desta política. Exceções devem ser formalmente documentadas e aprovadas pelo RSIP.

13. GESTÃO DE INCIDENTES DE SEGURANÇA

Todo colaborador, prestador ou parceiro que identificar ou suspeitar de um incidente de segurança da informação deve reportá-lo imediatamente ao RSIP ou ao canal de notificação designado. O processo de gestão de incidentes deve contemplar as seguintes etapas:

- Identificação e registro do incidente;
- Classificação e priorização com base no impacto e urgência;
- Contenção imediata para limitar o dano;
- Investigação e análise das causas-raiz;
- Erradicação da causa e recuperação dos sistemas afetados;
- Comunicação às partes afetadas, autoridades reguladoras (incluindo a ANPD, quando exigido pela LGPD) e titulares de dados, nos prazos legais;
- Lições aprendidas e atualização dos controles preventivos.

Todos os incidentes devem ser documentados em um registro de incidentes, mantido pelo RSIP. Incidentes críticos devem ser reportados à Alta Direção. O RSIP deve elaborar e manter um Plano de Resposta a Incidentes (PRI) detalhado como documento complementar a esta política.

14. CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

A Mater Imperium mantém um Plano de Continuidade de Negócios e Recuperação de Desastres (BCP/DRP) como documento complementar a esta política. O BCP/DRP define os procedimentos a serem adotados em resposta a eventos que possam interromper ou degradar as operações críticas da organização, incluindo falhas de infraestrutura, desastres naturais, ataques cibernéticos, indisponibilidade de fornecedores essenciais ou outros incidentes de grande impacto.

O BCP/DRP deve:

- Identificar os processos e sistemas críticos para o negócio e seus respectivos Objetivos de Tempo de Recuperação (RTO) e Objetivos de Ponto de Recuperação (RPO);
- Definir papéis, responsabilidades e canais de comunicação durante uma crise;
- Estabelecer procedimentos de ativação, resposta e retomada das operações;
- Ser revisado após cada teste ou após qualquer incidente que tenha exigido sua ativação, incorporando as lições aprendidas.

O RSIP é responsável por coordenar a elaboração, manutenção e testes do BCP/DRP. Todos os colaboradores com responsabilidades específicas dentro do plano devem ser formalmente comunicados e treinados sobre suas atribuições.

15. SANÇÕES E PUNIÇÕES

As violações a esta Política de Segurança da Informação e Privacidade, incluindo omissões, tentativas de violação ou descumprimento de normas e procedimentos de segurança, estão sujeitas à aplicação de sanções disciplinares proporcionais à gravidade da infração. As penalidades podem incluir:

- Advertência verbal ou escrita;
- Suspensão temporária não remunerada;
- Demissão por justa causa, no caso de colaboradores contratados sob regime CLT;
- Rescisão contratual imediata, no caso de prestadores de serviço, cooperados ou pessoas jurídicas.

A análise e deliberação sobre a aplicação das sanções serão conduzidas pelo RSIP, que levará em consideração fatores como gravidade da infração, recorrência, impacto e dolo. O RSIP poderá encaminhar o caso ao Gestor imediato ou Alta Gestão, para aplicação da penalidade correspondente, conforme as normas internas.

Quando as violações configurarem atividade ilícita ou dano à organização, o infrator será responsabilizado civil, administrativa e criminalmente, sendo adotadas as medidas legais pertinentes.

16. CASOS OMISSOS

Os casos omissos nesta política serão analisados pelo Comitê Gestor de Segurança da Informação, que deliberará sobre as medidas cabíveis, considerando as melhores práticas de segurança, conformidade regulatória e os princípios da ISO/IEC 27001:2022. As diretrizes estabelecidas nesta política, bem como nas demais normas e procedimentos internos de segurança e privacidade, não se esgotam neste documento, em virtude da constante evolução tecnológica e do surgimento de novas ameaças. Dessa forma, esta política não constitui um rol taxativo, devendo os usuários e

colaboradores da Mater Imperium adotar, sempre que possível, medidas adicionais de segurança e boas práticas.

17. HISTÓRICO DAS ALTERAÇÕES

Data	Revisão	Histórico	Responsável
09/10/2025	1.0	Elaboração Inicial e Aprovação	Vinicius Henrique Manca José F. Gandra de Carvalho