POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

JP Gestora de Fundos Ltda.

Versão: 1.0

Data da Última Revisão: 20 de agosto de 2025

1. Objetivo

Esta Política de Segurança da Informação ("PSI") tem como objetivo estabelecer as diretrizes, responsabilidades e normas para proteger os ativos de informação da JP Gestora de Fundos Ltda. (“JP Gestora” ou “Empresa”) contra ameaças, sejam elas intencionais ou acidentais.

Buscamos assegurar a Confidencialidade, a Integridade e a Disponibilidade das informações utilizadas em nossos processos de negócio, protegendo os dados de nossos clientes, a propriedade intelectual da empresa e a nossa reputação no mercado, em conformidade com as leis e regulamentações aplicáveis.

2. Abrangência

Esta política aplica-se a:

* Pessoas: Todos os diretores, colaboradores, estagiários, prestadores de serviço e terceiros que tenham acesso a informações ou utilizem os recursos de tecnologia da JP Gestora.

* Informações: Todos os dados e informações, em qualquer formato (digital, impresso, falado), que sejam criados, recebidos, processados, armazenados ou descartados pela Empresa.

* Ativos: Todos os recursos tecnológicos, incluindo computadores, notebooks, servidores, dispositivos móveis, sistemas, softwares, redes de comunicação e instalações físicas.

3. Definições Principais

* Ativo de Informação: Qualquer informação ou recurso de tecnologia que tenha valor para a JP Gestora.

* Confidencialidade: Garantia de que a informação é acessível somente por pessoas autorizadas.

* Integridade: Garantia da exatidão e completude da informação e dos métodos de seu processamento.

* Disponibilidade: Garantia de que os usuários autorizados tenham acesso à informação e aos ativos associados sempre que necessário.

* Incidente de Segurança da Informação: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores que ameace a confidencialidade, integridade ou disponibilidade da informação.

4. Papéis e Responsabilidades

* Alta Gestão: Aprovar esta política e garantir os recursos necessários para sua implementação e manutenção.

* Comitê de Segurança da Informação (liderado pela área de Compliance): Supervisionar a implementação da PSI, revisar e aprovar normas e procedimentos, analisar relatórios de segurança e gerenciar a resposta a incidentes críticos. O ponto de contato central é o e-mail compliance@jetprive.com.br.

* Equipe de Tecnologia da Informação (TI): Implementar, manter e monitorar os controles técnicos de segurança (firewalls, antivírus, backups, controle de acesso, etc.).

* Gestores de Áreas: Garantir que suas equipes compreendam e cumpram esta política e seus procedimentos. Conceder acessos com base na necessidade do negócio.

* Todos os Colaboradores e Terceiros: Conhecer, compreender e cumprir esta política no seu dia a dia. É responsabilidade de todos zelar pela segurança da informação.

5. Diretrizes de Segurança da Informação

5.1. Classificação da Informação

Toda informação produzida ou manipulada pela JP Gestora deve ser classificada para receber o nível de proteção adequado. As classificações são:

* Confidencial: Informação altamente sensível, cujo vazamento pode causar danos graves à empresa, seus clientes ou parceiros (ex: dados de clientes, estratégias de investimento, informações financeiras não públicas). Requer o mais alto nível de controle de acesso e segurança.

* Restrito: Informação de uso interno que, se divulgada, pode causar algum prejuízo ou embaraço à empresa (ex: relatórios internos, planos de projetos, comunicações entre equipes). O acesso é limitado a grupos específicos de colaboradores.

* Uso Interno: Informação que se destina à circulação entre todos os colaboradores da JP Gestora, mas não deve ser divulgada externamente (ex: comunicados gerais, procedimentos internos).

* Público: Informação que pode ser divulgada livremente, sem risco para a empresa (ex: materiais de marketing aprovados, informações do site institucional).

5.2. Controle de Acesso Lógico

* O acesso a sistemas e informações será concedido com base no princípio do "menor privilégio" (need-to-know), ou seja, cada usuário terá acesso apenas aos recursos estritamente necessários para o desempenho de suas funções.

* As senhas de acesso são de uso pessoal, intransferível e confidencial. É obrigatório seguir a Política de Senhas Seguras (Anexo I).

* O acesso a sistemas críticos deve utilizar, sempre que possível, autenticação de múltiplos fatores (MFA).

* As contas de usuário devem ser bloqueadas ou removidas imediatamente após o desligamento do colaborador ou término do contrato.

5.3. Uso Aceitável dos Ativos de Tecnologia

* E-mail Corporativo: Deve ser utilizado para fins profissionais. É expressamente proibido o envio de informações classificadas como Confidenciais ou Restritas para e-mails pessoais ou serviços de e-mail públicos não autorizados. Fique atento a e-mails de phishing.

* Internet: A navegação deve ser para fins profissionais. O acesso a sites com conteúdo ilegal, impróprio ou que represente risco de segurança é proibido.

* Software: Apenas softwares licenciados e homologados pela área de TI podem ser instalados nos equipamentos da empresa. A instalação de software pirata ou não autorizado é terminantemente proibida.

* Equipamentos: Os computadores e notebooks são de propriedade da JP Gestora e devem ser utilizados de forma responsável.

5.4. Segurança Física e do Ambiente

* O acesso às instalações da JP Gestora é controlado. Visitantes devem ser identificados e acompanhados.

* Adota-se a Política de Mesa Limpa e Tela Bloqueada: documentos sensíveis não devem ser deixados sobre as mesas ao final do expediente, e os computadores devem ser bloqueados (Ctrl+Alt+Del ou Win+L) sempre que o usuário se ausentar de sua estação de trabalho.

* O acesso a áreas restritas, como a sala de servidores, é limitado a pessoal autorizado.

5.5. Dispositivos Móveis e Acesso Remoto

* O uso de dispositivos móveis (corporativos ou pessoais - BYOD, se aplicável) para acessar informações da empresa deve seguir as normas de segurança, incluindo o uso de senha/biometria para bloqueio de tela e, quando aplicável, a instalação de softwares de segurança.

* O acesso remoto à rede da empresa deve ser feito exclusivamente através da Rede Privada Virtual (VPN) homologada pela TI.

* A perda ou roubo de um dispositivo com acesso a dados corporativos deve ser comunicada imediatamente à TI e ao Compliance.

5.6. Gestão de Backups

A área de TI é responsável por realizar cópias de segurança (backups) das informações críticas em intervalos regulares. Esses backups devem ser testados periodicamente para garantir sua integridade e capacidade de restauração.

6. Gestão de Incidentes de Segurança da Informação

Todo e qualquer incidente de segurança, ou suspeita de um, deve ser reportado imediatamente para compliance@jetprive.com.br e para a área de TI.

O processo de resposta a incidentes seguirá as etapas de:

* Notificação: Comunicação do evento.

* Análise: Avaliação do impacto e da gravidade do incidente.

* Contenção: Adoção de medidas para limitar o dano.

* Erradicação: Remoção da causa do incidente.

* Recuperação: Restauração dos sistemas e serviços afetados.

* Pós-Incidente (Lições Aprendidas): Análise do ocorrido para aprimorar os controles de segurança.

7. Conscientização e Treinamento

A JP Gestora promoverá programas de treinamento contínuo para todos os colaboradores sobre segurança da informação, incluindo temas como phishing, engenharia social, uso seguro de senhas e proteção de dados. A participação é obrigatória.

8. Sanções por Descumprimento

A violação desta política ou de suas normas complementares é considerada uma falta grave e sujeitará o infrator a medidas disciplinares, que podem variar de advertência verbal até a rescisão do contrato de trabalho por justa causa, além de possíveis sanções civis e criminais, conforme a legislação vigente.

9. Revisão da Política

Esta política será revisada anualmente, ou sempre que ocorrerem mudanças tecnológicas, legais ou de negócio significativas, pelo Comitê de Segurança da Informação.

Anexo I - Política de Senhas Seguras

* Comprimento: Mínimo de 12 caracteres.

* Complexidade: Deve conter uma combinação de letras maiúsculas, letras minúsculas, números e símbolos especiais (ex: @, #, $, %).

* Não Reutilização: Não utilizar senhas de outros serviços (e-mail pessoal, redes sociais). Senhas antigas não devem ser reutilizadas.

* Troca Periódica: As senhas de acesso a sistemas críticos deverão ser alteradas a cada 90 dias.

* Confidencialidade: Jamais anote senhas em locais de fácil acesso (post-its, bloco de notas no computador) e nunca as compartilhe com ninguém, incluindo a equipe de TI.