PSICOMANAGER

Política de Segurança da Informação (PSI)	EMISSÃO 02/05/2018	Referências ISO27001 / HIPAA / GDPR
	VERSÃO 1.0	RESPONSÁVEL Segurança da Informação

1. OBJETIVO

Este documento tem por objetivo orientar e definir diretrizes de condutas e responsabilidades, no manuseio das informações e ativos tecnológicos, visando garantir a confidencialidade, integridade e disponibilidade das informações necessárias para a continuidade do negócio, conforme previsto nas leis brasileiras.

A presente PSI está baseada nas recomendações da norma ISO/IEC 27001, que possui as principais práticas de Segurança da Informação (SI) aplicadas mundialmente, assim como nas determinações do HIPAA e GDPR.

2. ABRANGÊNCIA

As diretrizes definidas neste documento aplicam-se a todos os colaboradores e informações em qualquer meio ou suporte relacionados ao PsicoManager

3. SUMÁRIO

4. DIRETRIZES

O PsicoManager tem seus processos de segurança da informação disciplinados pelas seguintes diretrizes:

4.1 Organização da Segurança da Informação

Definir e manter uma estrutura para gerenciar a Segurança da Informação do PsicoManager.

4.2 Segurança dos Recursos Humanos

Assegurar que os colaboradores, fornecedores, e terceiros entendam seus papéis e responsabilidades, antes, durante e no encerramento ou mudança da contratação, visando reduzir o risco de roubo, fraude e mau uso de recursos.

4.3 Segurança Física

Fornecer mecanismos físicos de proteção, que abrangem desde perímetro externo até o espaço interno de trabalho, prevenindo o acesso físico não autorizado, danos, furtos e interferências com as instalações e informações críticas do PsicoManager.

4.4 Controle de Acessos

Controlar os acessos à informação, recursos de informação e processos, com base nos requisitos de negócio e segurança da informação.

4.5 Gestão das Operações e Comunicações

Garantir a operação segura e correta dos recursos de informação do PsicoManager, incluindo as atividades de rede, bem como o controle e detecção de atividades não autorizadas.

4.6 Gestão de Continuidade de Negócios

Assegurar a continuidade das linhas críticas de negócio por intermédio de planos de contingência.

5. DETALHAMENTO DAS DIRETRIZES

As diretrizes de Segurança da Informação que disciplinam as atividades do PsicoManager são detalhadas da seguinte forma:

5.1 Organização da Segurança da Informação

a) A alta direção deve apoiar ativamente a segurança da informação no PsicoManager;
b) A coordenação das atividades de segurança da informação deve ser realizada pela diretoria, em conjunto com representantes de diferentes áreas estratégicas do PsicoManager, nas reuniões do Comitê de Segurança da Informação;
c) As responsabilidades pela segurança da informação devem estar claramente definidas e divulgadas, inclusive nos casos de terceiros;
d) O PsicoManager deve dispor de políticas de segurança que descrevem as políticas corporativas e procedimentos, estabelecendo critérios de segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações existentes;
e) O PsicoManager deve manter uma Política de Privacidade disponível para acesso público, assim como esta PSI;
f) As políticas e procedimentos de segurança devem ser revisados e atualizados anualmente, considerando todos os fatos e eventos relevantes que exijam, inclusive, revisão imediata;
g) A diretoria deve definir o DPO – Data Protection Officer, responsável pela proteção dos dados pessoais dos clientes/usuários.

5.2 Segurança dos Recursos Humanos

a) Assegurar que todos os candidatos a emprego sejam adequadamente analisados, especialmente em cargos ou serviços com acesso a informações confidenciais. São obrigatórias as verificações de referências pessoais, financeiras (de crédito) e de registros criminais;
b) Garantir que todos os novos colaboradores recebam instruções sobre sua responsabilidade pela segurança da informação e que todos assinem o Contrato de Segurança desta política, assim como no caso de terceiros, quando não estiver explícito em contrato;
c) Estabelecer planos de conscientização periódicos, garantindo a ciência e aderência dos colaboradores e terceiros aos princípios e diretrizes da segurança da informação;
d) Garantir a devolução dos ativos do PsicoManager e a retirada de direitos de acesso de todos os colaboradores e terceiros no encerramento de suas atividades, contratos ou acordos;
e) Aplicar as medidas disciplinares formais vigentes para os colaboradores que tenham cometido violação de Segurança da Informação garantindo, inclusive, dissuasão para que novas violações não ocorram.

5.3 Segurança Física

a) Definir, controlar e monitorar os perímetros de segurança física das instalações do PsicoManager, garantindo não haver brechas nem pontos de fácil invasão;
b) Nenhum indivíduo, não colaborador, deve ter acesso às dependências do PsicoManager sem que este seja anunciado e sua entrada autorizada por um colaborador;

c) Deve ser criado um mecanismo de acesso de colaboradores em horários especiais, fora do expediente normal, indicando quem teve acesso, data, hora e quem autorizou;
d) O cabeamento de energia e de telecomunicação que transporta dados ou dá suporte aos serviços de informação deve ser protegido contra interceptação ou danos.

5.3.1 Política de Mesa Limpa

a) Esta política refere-se à Mesa, Tela, Impressora e Lixo Limpos;
b) Ao se ausentar, o colaborador não deve deixar sobre a mesa de trabalho impressos, anotações, agendas e cadernos. Estes devem ser guardados em gavetas ou armários com trancas;
c) A utilização de proteção de tela com senha em computadores é responsabilidade obrigatória do colaborador. Apesar da proteção de tela ser acionada automaticamente, em períodos de inatividade do mouse ou teclado, o colaborador deve acioná-la imediatamente antes de sua ausência da mesa de trabalho;
d) É imperativo manter documentos impressos e dispositivos de armazenamento devidamente protegidos, não deixando estes materiais na impressora ou na lixeira. Devem ser guardados em armários com chaves, descartados em lixos protegidos ou triturados.

5.4 Controle de Acessos

a) Os acessos críticos ao ambiente computacional do PsicoManager devem ser rastreáveis (logs de eventos);
b) Novas solicitações de acesso devem ser aprovadas pela diretoria e devem ser rastreáveis;
c) As tentativas de acessos não autorizados devem ser monitoradas;
d) Os colaboradores devem ter identificação única, pessoal e intransferível, qualificando-os como responsáveis pelas ações realizadas por intermédio desta identificação. Deve-se impedir os acessos simultâneos (“multi-login”);
e) A concessão de acessos aos colaboradores deve obedecer ao critério de menor privilégio, no qual os colaboradores têm acesso somente aos recursos de informação necessários para o pleno desempenho de suas atividades;
f) Os processos de trabalho do PsicoManager devem ser resguardados através da segregação de funções, de forma que atividades não sejam executadas e controladas pelo mesmo colaborador;
g) As senhas nunca deverão ser compartilhadas, reveladas a outras pessoas ou escritas, inclusive em programas, e devem ser armazenadas criptografadas nos sistemas;
h) Deve-se utilizar o processo de Senha Forte, com senhas formadas por um número mínimo de caracteres alfabéticos e numéricos, com letras maiúsculas e minúsculas, isentas de caracteres idênticos consecutivos;
i) As senhas iniciais de acesso fornecidas aos colaboradores devem estar auto-expiradas, exigindo a sua troca na primeira utilização;
j) As senhas padrões (“default”) de produtos e aplicativos adquiridos devem ser alteradas imediatamente após sua ativação;
k) Identificações de colaboradores devem ser desabilitadas após um número máximo de tentativas inválidas de acesso;
l) Colaboradores em férias ou com ausência prolongada, por qualquer outro motivo planejado, devem ter seus acessos bloqueados imediatamente;
m) Os direitos de acesso de colaboradores e terceiros desligados devem ser removidos imediatamente do cadastro;
n) Os direitos de acesso de colaboradores e terceiros que mudaram de função na empresa devem ser desabilitados na antiga função e validados, novamente, na nova função. Em nenhuma hipótese poderá haver “junção” dos direitos de acesso nesse caso, a não ser que seja uma nova função na empresa;

o) As identificações funcionais (genéricas) devem ter controles de uso que assegurem a segurança da informação e a responsabilidade dos usuários;
p) O acesso remoto aos sistemas e aplicativos do PsicoManager, incluindo o trabalho remoto, deve ser regulamentado e protegido contra o uso não autorizado, conforme anexo Uso dos Softwares e Equipamentos desta política;
q) Deve-se garantir o controle do uso de dispositivos móveis conforme anexo Uso dos Softwares e Equipamentos desta política;
r) O ambiente de Produção deve ser segregado dos ambientes de Teste e Desenvolvimento. Deve-se obedecer ao critério de menor privilégio nos acessos a estes ambientes e seus recursos e, em nenhuma hipótese, deve haver conflito de interesses nos direitos de acesso;
s) As permissões de acesso concedidas devem ser revisadas periodicamente pelo responsável;
t) Sessões inativas devem ser automaticamente bloqueadas, por meio de protetores de tela e sua liberação deve exigir senha.

5.5 Gestão das Operações e Comunicações

a) Os procedimentos e descrição dos sistemas do PsicoManager estão no anexo Ambiente e Sistemas PsicoManager (anexo restrito por motivos de segurança) desta política;
b) Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os colaboradores que deles necessitem;
c) As modificações nos recursos de informação e sistemas devem ser controladas por meio de um processo de Mudanças, conforme anexo Ambiente e Sistemas PsicoManager desta política;
d) Deve-se garantir a aderência aos controles de uso da Internet e de Correio Eletrônico (e-mails), conforme definido no anexo Ambiente e Sistemas PsicoManager desta política;
e) A utilização dos recursos deve ser monitorada, garantindo o desempenho requerido do sistema;
f) Devem ser implantados controles de detecção e prevenção para proteção contra códigos maliciosos;
g) As cópias de segurança das informações e softwares (backups) devem ser realizadas e testadas regularmente e seu armazenamento deve ser em local diferente e distante da localidade dos dados originais, conforme Política de Continuidade de Negócios desta política (anexo restrito por motivos de segurança);
h) As mídias e equipamentos devem ser descartados de forma segura e protegida quando não forem mais necessários, observando-se a criticidade das informações armazenadas, conforme anexo Uso dos Softwares e Equipamentos desta política;
i) As unidades de mídias removíveis (Pendrive, CD e USB) devem ser utilizadas com a devida justificativa e aprovação, conforme anexo Uso dos Softwares e Equipamentos – ANEXO 05 desta política;
j) O transporte externo de mídias e documentos deve ser realizado de forma a não permitir acesso não autorizado, uso impróprio ou alteração indevida;
k) O gerenciamento da segurança nas redes do PsicoManager é descrito no anexo Ambiente e Sistemas PsicoManager desta política, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes.

5.6 Gestão de Continuidade de Negócios

a) Deve-se garantir a aderência à Política de Continuidade de Negócios desta política para Gestão de Continuidade de Negócio, abrangendo Pessoas, Processos, Ambientes Físicos e Tecnológicos;
b) Os incidentes de segurança devem ser comunicados para a diretoria, por meio do email contato@psicomanager.com.br;
c) O PsicoManager deve informar às autoridades competentes, em até 72hs, qualquer incidente de segurança que envolva dados pessoais.

6. RESPONSABILIDADES

6.1 Comitê de Segurança da Informação:

a) Tem por objetivo garantir um direcionamento claro e um suporte de gestão evidente para as iniciativas de segurança do PsicoManager;
b) É composto pelos diretores da empresa. Representantes de outras áreas poderão ser convocados para participarem de reuniões específicas;
c) É coordenado pelo CEO do PsicoManager;
d) Esse Comitê reúne-se regularmente e sua frequência é de acordo com as necessidades identificadas.

6.1.1 Atribuições do Comitê de Segurança da Informação:

a) Análise crítica e permanente da Política de Segurança da Informação e das responsabilidades envolvidas, deliberando sobre eventuais alterações, sempre que necessário;
b) Análise crítica e monitoração dos principais riscos e incidentes de segurança da informação;
c) Aprovação das principais iniciativas para aumentar o nível de segurança da informação.

6.2 DPO – Data Protection Officer:

a) Tem por objetivo garantir o cumprimento aos padrões estabelecidos pelo GDPR – General data Protection Regulation
b) Deve ser o ponto de contato com as autoridades, inclusive para reporte de incidentes;
c) Assegura o cumprimento do requisito de Data Protection by Design and by Default, assim como o DPIA – Data Protection Impact Assessment;
d) Mantém as informações e conscientização da empresa em relação aos requisitos de segurança e GDPR.

6.3 Gestores:

a) Garantir o cumprimento desta Política e procedimentos de segurança que forem emitidos, por todos os colaboradores sob sua responsabilidade;
b) Manter as normas e os procedimentos internos da área alinhados com esta Política;
c) Divulgar a importância de sigilo de senhas, bem como o cuidado com seu uso, evitando a utilização de uma mesma senha por um grupo de diversos colaboradores;
d) Adotar cautelas quando da admissão, transferência ou desligamento de funcionários, a fim de evitar que documentos ou informações do PsicoManager e de seus clientes sejam usados ou divulgados indevidamente;
e) Providenciar a desativação imediata de todos os direitos de acessos de um colaborador no caso de desligamento ou de transferência para outra área;
f) Analisar periodicamente a necessidade de acessos às bases de dados e acesso a aplicativos por parte dos colaboradores sob sua responsabilidade;
g) Garantir que os contratos celebrados com outras entidades e pessoas externas ao PsicoManager (parceiros, terceiros, prestadores de serviços, fornecedores, temporários e contratados) contenham cláusulas que preservem a segurança das informações do PsicoManager, de seus clientes, parceiros e colaboradores;
h) Garantir que nos contratos de serviços em que os funcionários vinculados à empresa contratada venham a desempenhar atividades que impliquem o acesso ou o manuseio de informações do PsicoManager, cada um desses funcionários tenha firmado o Contrato de Segurança, ou que esta garantia conste do contrato firmado com a empresa;
i) Orientar os colaboradores que, por necessidade e natureza do trabalho, tenham de manusear ou tomar conhecimento de documentos com informações críticas, quanto ao zelo que devem ter com tais informações;

j) Reportar à diretoria as falhas e os riscos que podem levar à exposição indevida de informações críticas.

6.4 Responsabilidades Gerais

a) Todas as informações trocadas ou armazenadas nos recursos de informação do PsicoManager, independentemente de conteúdo, são de propriedade única e exclusiva do PsicoManager. Os colaboradores devem utilizar os recursos disponibilizados pelo PsicoManager para a condução dos negócios do PsicoManager;
b) Compete a todos os colaboradores o cumprimento das diretrizes constantes desta Política e das demais políticas de Segurança da Informação, bem como do Código de Conduta do PsicoManager;
c) Todo colaborador deve aderir formalmente ao Contrato de Segurança e Termo de Responsabilidade e Confidencialidade.

7. RISCOS

A não observância dos princípios e diretrizes constantes nesta Política pode impactar seriamente os clientes do PsicoManager, possibilitar a violação de leis e regulamentos e, negativamente, afetar a reputação e a estabilidade financeira do PsicoManager. Desvios e exceções devem ser tratados pelo Comitê de Segurança da Informação.

8. VIGÊNCIA E REVISÃO

Esta política entra em vigor em 02 de maio de 2018 com revisão anual.

9. APROVAÇÃO

Data da Aprovação: 02/05/2018
Aprovador: Comitê de Segurança da Informação