# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**SUMÁRIO**

## 1. OBJETIVO

O objetivo desta Política de Segurança da Informação (“PSI”) consiste em estabelecer regras de boas práticas de tratamento de dados, determinar as medidas de segurança, técnicas e administrativas para proteger os Dados Pessoais, e, ainda, garantir a confidencialidade, integridade, disponibilidade e proteção das informações da Hi Platform. Além disso, visa proteger os Dados e informações da Hi Platform contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

## 2. APLICAÇÃO

Esta Política aplica-se aos Colaboradores e Prestadores de serviços ou pessoas autorizadas a ter acesso às informações, Dados Pessoais e/ou recursos de tecnologia da Hi Platform e/ou de seus clientes, de acordo com as permissões a ele atribuídas.

### 2.1 Definições

**Ameaça:** causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema;

**Ativo:** qualquer coisa que tenha valor para a organização, a exemplo de: instalações, informação, software, hardware, serviços impressos (papéis), mas também em pessoas, habilidades, experiência e coisas intangíveis, como reputação e também imagem.

**Colaborador:** Empregado, estagiário, terceirizado, temporário e/ou menor aprendiz ou qualquer outro indivíduo que tenha relação de trabalho com a Hi Platform.

**Dados pessoais**: informação relacionada a pessoa natural identificada ou identificável.

**Encarregado pelo Tratamento dos Dados Pessoais:** pessoa física ou jurídica indicada pelo controlador e operador, para atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

**Evento:** é qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.

**Evento adverso (ou ofensivo):** é um evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de malware que destrói dados, entre outros.

**Hi Platform ou Empresa**: Trata-se das pessoas jurídicas de direito privado de Razão Social HI PLATFORM COMÉRCIO E TECNOLOGIA S.A e AKNA TECNOLOGIA DA INFORMAÇÃO LTDA, inscritas, respectivamente, nos CNPJs de nº 14.366.418/0001-21 (matriz Hi), 14.366.418/0002-02 (filial Hi) e 04.997.563/0001-57.

**Informação:** conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato. Não necessariamente precisa envolver dados pessoais. Exemplo: incidente envolvendo informações financeiros da Hi Platform.

**Prestador de serviço**: pessoa jurídica que é contratada para realizar uma atividade específica ou fornecer um serviço determinado, que se compromete com o cumprimento desta Política.

**Risco:** combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

**Risco residual**: risco que permanece após o tratamento do risco. O risco residual pode conter riscos não identificados e também pode ser conhecido como “risco retido”.

**Usuários:** são todos os Colaboradores e Prestadores de serviços ou pessoas autorizadas a ter acesso às informações, Dados Pessoais e/ou recursos de tecnologia da Hi Platform, de acordo com as permissões a ele atribuídas.

**Vulnerabilidade**: fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

## 3. RESPONSABILIDADES

A Hi Platform entende que um sistema de segurança da informação somente será eficaz com o comprometimento de todos.

Por isso, é imprescindível que todos tenham ciência e ajam de acordo com suas responsabilidades, conforme abaixo. As principais responsabilidades são direcionadas ao Usuário, Gestores e área de TI.

### 3.1. Responsabilidades dos Usuários:

Os Usuários contemplam os Colaboradores, Prestadores de Serviços, ou pessoas autorizadas a ter acesso às informações, Dados Pessoais e/ou recursos de tecnologia da Hi Platform e/ou de seus clientes:

- Respeitar esta Política e responder pelo descumprimento dos procedimentos aqui previstos;
- Responder pela guarda e proteção dos recursos computacionais e informações colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
- Relatar prontamente ao Comitê de Privacidade e Segurança da Informação qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, através do canal dpo@hiplatform.com e security@hiplatform.com;

- Assegurar que as informações e dados de posse da Hi Platform ou a ela relativos sejam compartilhados somente quando autorizados pela Política de Classificação da Informação.
- Comprometer-se em não auxiliar terceiro e não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro;
- Responder pelo prejuízo ou dano que vier a provocar a Hi Platform ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

### 3.2. Responsabilidades dos Gestores:

- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os Usuários sob a sua gestão;
- Atribuir, na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, neste último caso quando aplicável, após avaliação do DPO, a responsabilidade do cumprimento desta PSI;
- Realizar as atividades concernentes a gestão no controle e gestão de acessos;
- Educar os usuários sobre os princípios e procedimentos de segurança da informação;
- Notificar imediatamente à TI quaisquer vulnerabilidades e ameaças à quebra de segurança;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

### 3.3. Responsabilidades da área de Tecnologia da Informação (TI)

- Configurar equipamentos e sistemas para cumprir com os requerimentos desta PSI;
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;

- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes em sistemas desenvolvidos pela Hi Platform ou ativos (endpoints, softwares, servidores, etc) dentro do ambiente e/ou infraestrutura cibernética interna;
- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da Hi Platform, conforme Política de Backup e Restauração;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio da Hi Platform;
- Proteger todos os ativos de informação da Empresa contra códigos maliciosos e ou vírus;
- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção;
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da Empresa;
- Realizar inspeções periódicas de configurações técnicas e análise de riscos;
- Garantir, assim que solicitado, a concessão do acesso ao novo usuário ou o bloqueio de acesso de usuários por motivo de desligamento da Hi Platform;
- Descartar apropriadamente as mídias contendo informações referentes à Hi Platform e sanitizar as informações lá contidas, ou, apenas sanitizar as informações referentes à Hi Platform e dados pessoais contidos em mídias que serão reutilizadas;
- Promover a conscientização dos Usuários em relação à relevância da segurança da informação;
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;
- Buscar alinhamento com as diretrizes corporativas da Hi Platform;
- Realizar, a qualquer tempo, inspeção física nas máquinas de propriedade da Hi Platform.

## 4. IDENTIFICAÇÃO - LOGIN E SENHA

- Os sistemas de login e senha protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra;
- Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %);
- É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados;
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseadas em informações pessoais, como o próprio nome, familiares, nascimento, endereço, placa de veículo, nome da empresa, e ou não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “123456”, entre outras;
- Os usuários devem proceder a troca de senha caso suspeitem de quebra por terceiros ou obrigatoriamente a cada 6 meses;
- O login e senha devem ser imediatamente bloqueados quando se tornarem desnecessários;
- Tentativa de violação e burla de senhas de acesso, criptografia ou identificação biométrica, se identificada, será alvo de ação disciplinar.

## 5. REVISÃO DE ACESSO

A cada 6 (seis) meses, a TI e gestores responsáveis pela concessão e revogação de acessos aos sistemas devem revisar os usuários cadastrados para deliberar sobre a manutenção, revisão ou revogação dos perfis de acesso existentes.

Na eventualidade de transferências ou alterações de cargo, função ou área, os perfis de acesso são revisados.

O acesso às informações e Dados Pessoais será restrito a certos perfis de acesso definidos pela TI e pelos Gestores da Hi Platform.

O acesso aos Dados Pessoais cadastrados pelos Clientes da Hi Platform será restrito e limitado ao estritamente necessário para o cumprimento da finalidade do Tratamento, de forma que somente os profissionais essenciais às funções poderão ter acesso permitido.

## 6. REVOGAÇÃO DE ACESSO

O acesso de usuários desligados da Hi Platform deve ser revogado imediatamente, pela TI ou gestor responsável pela administração de acessos aos sistemas sob sua responsabilidade, no momento da comunicação do desligamento realizado pelo setor de Recursos Humanos.

As credenciais de acesso dos usuários que encerraram suas atividades na Hi Platform não devem ser removidas das bases cadastrais, mas devem ser bloqueadas de forma que o usuário desligado não consiga utilizá-las.

Devem ser mantidos registros que permitam identificar os usuários responsáveis pelas ações realizadas por meio das credenciais de acesso, mesmo depois de bloqueadas.

## 7. RECURSOS COMPUTACIONAIS

Os recursos de TI alocados pela Hi Platform aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho.

É proibida a intervenção do usuário para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação do equipamento corporativo. O uso de equipamento pessoal deverá seguir as diretrizes previstas na Política de BYOD da Hi Platform.

É proibida a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros.

Todo computador em desuso, deverá ser encaminhado à TI para a remoção das informações, descarte ou reuso.

## 8. TELA E MESA LIMPA

O usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostos ao acesso não autorizado.
Os computadores deverão ser bloqueados por senha quando não estiverem sendo utilizados. Ao se ausentar ou se distanciar de seu equipamento (monitor, notebooks, etc.) o usuário deverá sempre bloquear sua tela a fim de impedir acesso não autorizado a informações da Hi Platform ou Dados Pessoais.

## 9. DESCARTE DE MÍDIAS E DADOS

Mídias deverão ser encaminhadas à TI para a sanitização da informação antes do descarte, destruição ou reutilização da mídia.

## 10. CLASSIFICAÇÃO DA INFORMAÇÃO

O gestor de cada área, se necessário com auxílio do DPO, deve estabelecer os critérios relativos ao nível de confidencialidade da informação gerada por sua área e classificá-las em Pública, Confidencial, Restrita ou Interna.

As informações devem ser definidas conforme procedimento específico.

## 11. POLÍTICA DE BACKUP

A Política de Backup e Restauração da Hi Platform deverá seguir as orientações em procedimento específico.

## 12. SALVAGUARDA DE ARQUIVOS

Não é permitido o armazenamento de Dados Pessoais de Clientes nas estações locais de trabalho dos usuários, devendo ficar armazenados em locais dotados de proteção à confidencialidade, com acesso limitado ao estritamente necessário e às pessoas autorizadas.

## 13. UTILIZAÇÃO DE E-MAILS

O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas devem ser de caráter exclusivamente profissional, não podendo existir expectativa de privacidade sobre o conteúdo e utilização de e-mail profissional.

Mensagens recebidas de origem desconhecida deverão ser previamente visualizadas, avaliadas e, se for o caso, eliminadas imediatamente, em caso de suspeita de atividade maliciosa, sendo vedado clicar em links ou baixar anexos e documentos para evitar contaminação por vírus e outros riscos.

As mensagens trafegadas sob o domínio da Hi Platform poderão ser auditadas.

## 14. CONFORMIDADE

O usuário deve estar ciente e seguir as recomendações desta PSI, interpretando a classificação atribuída às informações e Dados, e assegurando que recebam tratamento adequado.

As violações às disposições estabelecidas na presente Política, devidamente apuradas, poderão implicar:

- Na aplicação das sanções previstas na legislação trabalhista, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado a Hi Platform, seus clientes e/ou fornecedores, entre outros;
- Na aplicação das sanções previstas na LGPD;
- Na aplicação das sanções previstas em contrato aos Prestadores de Serviço e estagiários;
- Na aplicação dos procedimentos legais cabíveis.

## 15. DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Hi Platform.

Esta política deve estar disponível e ser divulgada para todos os Colaboradores e Prestadores de Serviços da Hi Platform.