Ketra
soluções inteligentes

POLITICA DE SEGURANÇA DA INFORMAÇÃO

Objetivo:

A Política de Segurança da Informação da Ketra tem como propósito:

- Proteger os ativos de informação da empresa
- Minimizar os riscos ao negócio
- Preservar as informações e o patrimônio da organização
- Garantir o atendimento aos requisitos legais
- Fortalecer a imagem da empresa perante a sociedade
- Esta política se aplica a todos os funcionários, prestadores de serviços, estagiários e qualquer pessoa que utilize os Recursos Tecnológicos da empresa

Ketra
soluções inteligentes

Conceitos e definições:

IAtivos de Informação

- Tudo que tem valor para a empresa: bases de dados, contratos, códigos-fonte, manuais, planos, relatórios, etc.

Ativos Físicos

- Equipamentos como computadores, notebooks, celulares, mídias removíveis e demais dispositivos.

Backup

- Cópias de segurança dos arquivos da empresa (ex: nuvem, HD, storage, etc).

BYOD (Bring Your Own Device)

- Uso de equipamentos pessoais (notebooks, celulares, tablets) para acessar dados da empresa.

Colaboradores

- Todos que atuam na Ketra — presencial, remoto, híbrido, terceirizado ou estagiário.

Ketra
soluções inteligentes

Conceitos e definições:

Continuidade de Negócios

- Capacidade da empresa de manter as operações mesmo em incidentes ou interrupções.

Classificação da Informação

- Define o nível de proteção de cada informação (confidencial, restrita, interna ou pública).

Informações

- Conjunto de dados que tenham valor para a empresa, seus clientes e parceiros.
- Confidencial: pode causar prejuízos se divulgada.
- Restrita: só acessos autorizados.
- Interna: não deve ser conhecida por terceiros.
- Pública: pode ser divulgada livremente.

Ketra
soluções inteligentes

Conceitos e definições:

Incidente de Segurança da Informação
- Interrupção ou falha que ameaça a segurança e o funcionamento dos sistemas.

Gestão de Riscos
- Atividades para identificar e controlar riscos à segurança da informação.

Gestor
- Colaborador com cargo de liderança (Diretor, Gerente, Coordenador, etc).

Recursos Tecnológicos
- Equipamentos, sistemas, metodologias ou qualquer suporte tecnológico da empresa.

Segurança da Informação
- Proteção contra ameaças que possam comprometer a continuidade dos negócios.

Software
- Programas, aplicativos e sistemas usados pela empresa.

TIC (Tecnologia da Informação e Comunicação)
- Conjunto de recursos tecnológicos integrados que permitem a automação e comunicação de processos.

Usuários
- Todas as pessoas que utilizam os recursos da empresa, independentemente do cargo

Ketra
soluções inteligentes

Papeis e responsabilidades:

Esta política é de responsabilidade da Diretoria e da área de Governança e Compliance.

Diretoria e Governança e Compliance

- Aprovar a Política de Segurança da Informação e todas as suas revisões.
- Definir e aprovar os proprietários das informações.
- Tomar decisões e medidas quando houver descumprimento das políticas de Segurança da Informação.
- Garantir o acesso de todos os colaboradores a esta Política, para que conheçam e sigam suas diretrizes

Ketra
soluções inteligentes

Papeis e responsabilidades:

Comitê de Segurança da Informação

- Promover melhorias contínuas nas políticas e procedimentos de Segurança da Informação.
- Aprovar processos, políticas e procedimentos derivados da Política de Segurança da Informação (com aval de pelo menos um de seus representantes).
- Analisar casos de irregularidades ou violações e, quando necessário, encaminhar à Governança e compliance e à Diretoria.
- Propor projetos e iniciativas para melhorar a Segurança da Informação da Ketra.
- Participar da elaboração de relatórios, levantamentos e análises que auxiliem a Gestão de Segurança da Informação e a tomada de decisão.
- Realizar reuniões bimestrais (ou extraordinárias, quando necessário).
- Ser composto por membros da Diretoria e demais gestores indicados.

Ketra
soluções inteligentes

Papeis e responsabilidades:

Gestor de Segurança da Informação – Ketra
Responsável: Governança e compliance ou Diretoria

- Elaborar e revisar políticas e procedimentos de Segurança da Informação;
- Convocar e coordenar reuniões do Comitê Gestor de Segurança da Informação;
- Fornecer informações solicitadas pelo CGSI;
- Avaliar projetos e analisar incidentes de Segurança da Informação, acompanhando suas soluções;
- Realizar análises de vulnerabilidades e gerenciar riscos;
- Divulgar as políticas e procedimentos e promover treinamentos e orientações sobre o tema;
- Registrar e controlar não conformidades relacionadas à Segurança da Informação.

Ketra
soluções inteligentes

Papeis e responsabilidades:

Gestores das Áreas – Ketra

- Ser referência em Segurança da Informação para suas equipes;
- Garantir o cumprimento das diretrizes e aspectos definidos nesta Política;
- Assegurar que suas equipes conheçam as políticas e procedimentos de Segurança da Informação.

Colaboradores e Prestadores de Serviços – Ketra

- Seguir as diretrizes desta Política;
- Conhecer e cumprir as políticas e procedimentos de Segurança da Informação;
- Utilizar os ativos e informações de forma adequada e segura;
- Buscar orientação sempre que tiver dúvidas sobre o manuseio das informações;
- Comunicar ao CGSI casos de violação ou falhas de segurança;
- Manter a confidencialidade e complexidade das senhas, sem compartilhá-las;
- Devolver os ativos de informação ao encerrar suas atividades na empresa;
- Fora do ambiente da empresa: garantir segurança física e evitar uso de redes pública

Ketra
soluções inteligentes

Papeis e responsabilidades:

Proprietário da Informação – Ketra

- Autorizar o acesso às informações sob sua responsabilidade;
- Fiscalizar os registros e controles dos acessos concedidos;
- Participar das reuniões do Comitê Gestor de Segurança da Informação quando convocado.

Ketra
soluções inteligentes

Politicas para dispositivos - BYOD

Uso de Recursos Tecnológicos:

- Por padrão, devem ser utilizados apenas equipamentos fornecidos pela Ketra.
- Caso seja necessário utilizar dispositivos pessoais (BYOD), o colaborador deve comunicar seu gestor imediato e o Comitê Gestor de Segurança da Informação.
- Dispositivos pessoais poderão ser monitorados pela Ketra para prevenir violações de segurança.
- Um profissional designado poderá auditar o dispositivo e instalar ferramentas de monitoramento e remoção remota, com concordância do colaborador.

Requisitos de Segurança para BYOD:

- Participar de treinamentos de segurança promovidos pelo Comitê Gestor de Segurança da Informação;
- Aceitar a gestão de soluções móveis da Ketra, incluindo:
  - Bloqueio remoto,
  - Remoção de arquivos,
  - Restauração de fábrica,
  - Monitoramento constante das atividades;

Ketra
soluções inteligentes

Politicas para dispositivos - BYOD

Requisitos de Segurança para BYOD:

- Utilizar disco rígido criptografado (laptops);
- Ter antivírus/malware com atualizações diárias e automáticas;
- Manter o sistema operacional sempre atualizado;
- Usar autenticação de múltiplos fatores (2FA);
- Não utilizar logins pessoais para tarefas da empresa;
- Não emprestar o dispositivo a terceiros;
- Não instalar aplicativos não homologados pela Ketra;
- Evitar redes Wi-Fi públicas e e-mails suspeitos;
- Em caso de desligamento, devolver o dispositivo para sanitização pelo Comitê de Segurança da Informação.

Ketra
soluções inteligentes

Princípios e aspectos:

Nosso compromisso com a proteção das informações da Ketra e de nossos clientes se baseia nos seguintes princípios:

Confidencialidade

- Proteger as informações conforme seu grau de sigilo, garantindo que apenas pessoas autorizadas tenham acesso, preservando a privacidade e os dados proprietários.

Integridade

- Manter as informações como foram disponibilizadas, prevenindo alterações indevidas, intencionais ou acidentais.

Disponibilidade

- Garantir que as informações estejam acessíveis aos usuários de forma oportuna e confiável.

Autenticidade

- Assegurar que toda troca de informação com usuários ou sistemas seja feita com identidades verificadas e confiáveis.

Conformidade

- Cumprir obrigações legais, regulatórias e éticas, seguindo as diretrizes estabelecidas pela alta direção da empresa.

Ketra
soluções inteligentes

Disposições gerais:

Os procedimentos de Segurança da Informação devem ser estruturados de forma a orientar a aplicação dos princípios, aspectos, diretrizes e responsabilidades definidos nesta política.
As informações da Ketra podem estar presentes em diversos formatos, como:

- Sistemas de informação
- Diretórios de rede
- Serviços em nuvem
- Bancos de dados
- Mídias impressas, magnéticas ou ópticas
- Dispositivos eletrônicos e equipamentos portáteis
- Microfilmes
- Comunicação oral

Todas as informações de propriedade da Ketra poderão ser monitoradas por meio dos recursos de processamento da informação disponibilizados pela empresa.

O acesso às informações da Ketra será concedido apenas a colaboradores e prestadores de serviço devidamente autorizados, de acordo com seus perfis de acesso e mediante concordância com esta política

Ketra
soluções inteligentes

Diretrizes principais:

As informações da Ketra e de seus clientes devem ser tratadas de forma ética, sigilosa e em conformidade com as leis, regulamentações vigentes e normas internas, evitando-se o mau uso e a exposição indevida.

- Todas as informações obtidas no exercício das atividades trabalhistas, sejam relacionadas à função ou não, serão consideradas Informações Restritas.
- Toda informação relacionada às operações da Ketra constitui ativo essencial da empresa, indispensável à condução, continuidade e existência do negócio.
- Independentemente da forma ou meio de armazenamento/compartilhamento, a informação deve ser utilizada exclusivamente para a finalidade autorizada.
- Devem ser adotadas medidas técnicas para prevenir acessos ilegais, alterações não autorizadas, falsificações, destruições ou interferências que comprometam a confidencialidade, integridade e/ou disponibilidade das informações.
- A identificação, armazenamento, proteção, recuperação, tempo de retenção e descarte das informações devem ser feitos conforme as necessidades da organização, com processos documentados e autorizados.
- Os recursos tecnológicos da Ketra devem ser usados apenas para fins profissionais, no exercício das atividades funcionais e alinhados às estratégias de negócio.

Ketra
soluções inteligentes

Diretrizes principais:

- A Ketra reserva-se o direito de, sempre que necessário e conforme a legislação, monitorar, inspecionar ou auditar as informações armazenadas ou trafegadas em seus recursos e redes corporativas.
- Os colaboradores devem estar vinculados a instrumentos contratuais que assegurem sigilo e confidencialidade, sendo vedada a divulgação de qualquer informação da empresa sem autorização formal, especialmente aspectos operacionais, comerciais, jurídicos, regulatórios, financeiros, contábeis e tecnológicos.
- As informações devem ser armazenadas pelo tempo definido pela organização e recuperadas somente quando necessário, seguindo os procedimentos e legislações aplicáveis.
- A concessão de acesso aos sistemas deve respeitar o perfil funcional de cada colaborador, sendo proibida a atribuição de privilégios sem autorização formal da liderança.
- A liderança deve revisar periodicamente os perfis de acesso dos colaboradores sob sua responsabilidade para garantir níveis adequados de privilégio.
- Dispositivos móveis, mídias removíveis e sistemas de comunicação eletrônica (como e-mail e mensagens instantâneas) devem ser utilizados apenas para fins corporativos, seguindo os padrões éticos, normativos e legais da Ketra.

Ketra
soluções inteligentes

Diretrizes principais:

- É proibido o encaminhamento, armazenamento ou envio de informações da Ketra para locais externos ou particulares (ex.: e-mail pessoal) sem autorização prévia.
- As credenciais de acesso (login e senha) são pessoais e intransferíveis, devendo ser mantidas em sigilo. O compartilhamento é proibido e o usuário é responsável pelas ações realizadas com suas credenciais.
- Toda informação, interna ou transmitida externamente, deve ser protegida por operações seguras e pelo uso correto dos ativos de informação.
- Os requisitos de segurança devem estar presentes na aquisição, desenvolvimento e manutenção de softwares utilizados na Ketra.
- Riscos aos ativos de informação que comprometam a confidencialidade, integridade ou disponibilidade devem ser reportados ao Comitê Gestor de Segurança da Informação.
- Toda informação deve ser classificada conforme o nível de confidencialidade exigido.
- Devem ser definidos e implementados requisitos de continuidade de negócios, visando reduzir impactos em processos críticos causados por desastres ou falhas de segurança da informação.

Ketra
soluções inteligentes

Diretrizes principais:

- Deve existir um processo de Gerenciamento de Incidentes para restabelecer serviços interrompidos e minimizar impactos negativos ao negócio.
- A Política de Segurança da Informação deve ser definida, aprovada e divulgada pela Diretoria e pela Gerência de Operações de TI, garantindo que suas diretrizes sejam compreendidas e aplicadas por todos os colaboradores e prestadores de serviço.
- A Ketra deve garantir, por meio de um plano de treinamentos de Segurança da Informação, que todos os colaboradores sejam periodicamente orientados sobre a política e boas práticas de segurança.
- A utilização de softwares nos recursos corporativos deve ser homologada e autorizada pela Gerência de Operações de TI, sendo o uso de softwares não autorizados considerado incidente de segurança, sujeito às penalidades cabíveis.
- A Ketra deve manter uma Política de Backup alinhada às necessidades do negócio, assegurando a criação de cópias de segurança das informações, softwares e sistemas.
- A Ketra deve registrar e monitorar eventos críticos (logs) para garantir a rastreabilidade e atender auditorias e exigências regulatórias.
- A Ketra deve implementar controles de detecção, prevenção e recuperação contra malwares e outras ameaças digitais.
- A Ketra deve realizar auditorias periódicas para monitorar o uso de todos os recursos tecnológicos da empresa.
- A Ketra deve implementar controles de Segurança da Informação que assegurem conformidade com leis, regulamentações e contratos vigentes.

Ketra
soluções inteligentes

Das normas de uso da internet:

- A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Conforme definido por essa legislação, a internet é um sistema estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.
- No ambiente corporativo, as normas de uso da internet visam garantir a proteção e a integridade dos sistemas de informação. Por se tratar de uma conexão de alto risco, é fundamental que os usuários estejam cientes das responsabilidades e requisitos básicos de utilização antes de acessá-la ou utilizar seus recursos.
- São estabelecidas as seguintes diretrizes para o uso da internet no ambiente de trabalho:
- É proibido acessar sites que não estejam em conformidade com esta Política de Segurança da Informação, mesmo que não estejam bloqueados pelos sistemas de segurança.
- É proibido utilizar a internet para atos ilícitos, proibidos por lei ou por esta norma, que possam ser lesivos aos direitos e interesses da empresa ou de terceiros.
- É proibido o uso de aplicações que priorizem o tráfego de banda da internet (como serviços de streaming e torrents), bem como o uso de gerenciadores de download.
- É proibido realizar downloads ou utilizar programas de entretenimento, assim como baixar qualquer material que não seja pertinente às atividades profissionais.
- Em caso de dúvidas sobre o uso de algum recurso que possa estar em desacordo com esta Política de Segurança da Informação, o usuário deve consultar previamente o Comitê de Segurança da Informação e obter autorização formal antes de realizar qualquer operação relacionada aos ativos de tecnologia da informação

Ketra
soluções inteligentes

Das normas de uso da rede:

Rede de computadores é um conjunto de computadores e dispositivos interconectados que utilizam protocolos para compartilhar recursos.

O uso dos Recursos Tecnológicos pertencentes à Ketra é autorizado exclusivamente para fins relacionados ao exercício das funções do colaborador, à prestação de serviços, ao acesso e à disseminação de informações de interesse da empresa e outras atividades compatíveis com suas atribuições.

São estabelecidas as seguintes diretrizes para o uso da rede corporativa:

- É terminantemente proibido tentar obter acesso não autorizado a qualquer servidor, rede ou conta, incluindo tentativas de fraudar mecanismos de segurança.
- É proibido interferir nos serviços de outros usuários, servidores ou redes, incluindo ataques, tentativas de congestionamento, sobrecarga ou invasão de servidores.
- Ao ausentar-se da estação de trabalho ou notebook, independentemente do período, o usuário deve efetuar logout/logoff da rede ou bloquear o equipamento com senha.
- É responsabilidade do usuário monitorar o funcionamento e atualização do antivírus instalado em seu equipamento. Caso não esteja funcionando, deve comunicar imediatamente seu gestor imediato e o Comitê Gestor de Segurança da Informação.

Ketra
soluções inteligentes

Das normas de uso da rede:

- É proibido desativar, remover ou impedir a execução de qualquer software ou ferramenta de segurança adotada pela empresa, mesmo que temporariamente.
- Devem ser implementados controles para impedir que usuários com direitos de administrador desativem ou desinstalem ferramentas de segurança, incluindo controles organizacionais e técnicos.
- É proibido acessar diretórios ou pastas de outros usuários sem autorização expressa, mesmo que estejam visíveis na rede.
- É proibido acessar, armazenar ou compartilhar conteúdos de natureza pornográfica, racista ou relacionados à pedofilia.
- Arquivos pessoais não relacionados às atividades profissionais não devem ser armazenados nos drives de rede. Caso sejam identificados, serão excluídos imediatamente.
- Todos os arquivos de trabalho devem ser salvos na rede corporativa, e não diretamente no computador local, visto que arquivos salvos localmente não possuem garantia de backup. A responsabilidade por perdas decorrentes desse descumprimento será do usuário.
- Os usuários devem realizar a cada três meses uma revisão em seus diretórios na rede, excluindo arquivos obsoletos ou desnecessários.
- O uso de dispositivos USB (pendrives) é permitido somente para fins profissionais, sendo obrigatória a verificação com antivírus antes de acessar seu conteúdo.
- A empresa poderá realizar auditorias a qualquer momento nos Recursos Tecnológicos em posse de seus colaboradores, a fim de verificar a conformidade com esta política.

Ketra
soluções inteligentes

Das normas de contas e senhas de usuário:

- As normas de contas e senhas têm como objetivo definir os procedimentos adequados para a criação, uso e gestão dos acessos aos recursos tecnológicos da rede corporativa da Ketra.
- A senha é o meio de autenticação que identifica o usuário em um sistema de informação ou serviço, conforme suas funções e responsabilidades.
- A Ketra adota três níveis de usuários, definidos de acordo com o tipo de permissão concedida:
- Administrador Geral: responsável pela administração da rede, e-mails, contas de usuários, backups e conteúdos armazenados no servidor.
- Administrador Local: possui acesso administrativo ao sistema operacional do próprio computador ou notebook.
- Usuário Comum: utiliza os recursos de TI para desempenhar suas atividades e é responsável pelo uso adequado das ferramentas disponibilizadas pela empresa.
- A criação das contas de acesso é de responsabilidade do setor de Recursos Humanos, mediante solicitação do gestor imediato, que deverá informar o nível de acesso do colaborador.
- Cada usuário deve alterar a senha temporária fornecida pela Ketra logo após o primeiro acesso. As senhas são pessoais, sigilosas e intransferíveis, sendo proibido o seu compartilhamento ou divulgação a terceiros. É vedado anotá-las em papel ou armazená-las de forma digital.

Ketra
soluções inteligentes

Das normas de contas e senhas de usuário:

- Durante a digitação, o usuário deve garantir a confidencialidade, evitando que terceiros observem o processo. Recomenda-se o uso de senhas de fácil digitação e difícil decodificação, que não exijam olhar constante para o teclado.
- Cada colaborador é responsável por todas as ações realizadas com sua senha, incluindo usos indevidos ou negligência. Caso haja suspeita de comprometimento ou uso indevido, o fato deve ser comunicado imediatamente ao Comitê Gestor de Segurança da Informação, e a senha deve ser alterada de imediato.
- O compartilhamento de senhas de rede ou sistemas internos é estritamente proibido. Todas as atividades são registradas e vinculadas ao login do usuário, responsabilizando-o por eventuais irregularidades.
- As credenciais de acesso são fornecidas exclusivamente para fins corporativos. Ao ativar uma credencial, o colaborador declara estar ciente e de acordo com as normas de segurança da informação da Ketra. A empresa reserva-se o direito de revogar acessos a qualquer momento, caso seja identificada a origem de um incidente de segurança.

Ketra
soluções inteligentes

Das normas de contas e senhas de usuário:

Para a criação de senhas seguras, devem ser observados os seguintes critérios:

- Mínimo de 8 caracteres;
- Uso de pelo menos um caractere especial (ex: @, #, $, %);
- Uso de letra maiúscula e minúscula;
- Alteração obrigatória a cada três meses;
- Proibição de reutilizar as últimas 12 senhas;
- Senhas podem ser alteradas a qualquer momento pelo próprio usuário.
- Evite utilizar informações pessoais, como datas de nascimento, nomes de familiares ou sobrenomes. Recomenda-se também a troca periódica das senhas para maior segurança.
- Em casos de acesso temporário por pessoas sem conta de usuário, o acesso poderá ser concedido por meio da conta de um colaborador cadastrado, desde que a senha não seja compartilhada e o uso seja acompanhado pelo responsável da conta.

Ketra
soluções inteligentes

Das normas de utilização de email:

- As mensagens enviadas e recebidas por e-mail corporativo são propriedade da Ketra, independentemente de sua localização física. Todo conteúdo de e-mail é considerado registro oficial das atividades da empresa.
- O endereço de e-mail corporativo é uma ferramenta de trabalho concedida pela Ketra aos colaboradores, representando tanto o usuário quanto a imagem da organização. Portanto, a comunicação deve seguir linguagem, comportamento e conduta profissional adequados.
- O uso do e-mail é pessoal e intransferível, sendo o usuário responsável por todas as mensagens enviadas por sua conta.

Regras de Utilização:

- Utilizar o e-mail corporativo exclusivamente para fins profissionais relacionados às atividades da Ketra.
- As mensagens devem ser redigidas em linguagem clara, profissional e respeitosa, evitando gírias, abreviações, enfeites e brincadeiras.
- Conferir o conteúdo e os destinatários antes do envio, garantindo que a mensagem chegue apenas a quem for necessário.
- Utilizar a assinatura padrão da Ketra, sem alterações não autorizadas.
- Manter a organização da caixa de e-mails, excluindo mensagens desnecessárias.

Ketra
soluções inteligentes

Das normas de utilização de email:

Segurança e Responsabilidade

- Não abrir anexos ou links de remetentes desconhecidos ou suspeitos.
- É proibido abrir arquivos com extensões perigosas como: .bat, .exe, .src, .lnk, .com ou similares.
- Qualquer uso irregular do e-mail deve ser denunciado ao Comitê Gestor de Segurança da Informação.
- A Ketra poderá monitorar e auditar o uso do e-mail corporativo, bem como gerar relatórios gerenciais sobre os conteúdos enviados e recebidos.

Proibições

- Cadastrar o e-mail corporativo em sites, aplicativos ou listas de uso pessoal.
- Utilizar o e-mail para fins ilícitos, envio de spam, assédio, fake news ou qualquer prática contrária à legislação brasileira.
- Enviar mensagens de corrente, propagandas, reflexões ou outros conteúdos que não tenham relação com as atividades da Ketra.

Ketra
soluções inteligentes

Das normas para gestão de ativos:

- Todos os sistemas, informações, equipamentos e serviços disponibilizados aos colaboradores são propriedade exclusiva da Ketra, sendo vedado o uso para fins pessoais.

Propriedade Intelectual

- Nos projetos de desenvolvimento ou aprimoramento de softwares e sistemas, a titularidade da propriedade intelectual pertence integralmente à Ketra. O colaborador não possui direito sobre o programa desenvolvido, cabendo à empresa fornecer os recursos técnicos e financeiros necessários para a execução das atividades.

Regras de Utilização

- É proibida a abertura de equipamentos sob qualquer pretexto, exceto por técnicos autorizados pela Ketra.
- É vedado o uso de softwares, hardwares ou dispositivos sem autorização prévia da empresa.
- Documentos impressos e arquivos confidenciais devem ser armazenados e protegidos adequadamente.
- O armazenamento de músicas ou arquivos não relacionados ao trabalho é proibido, conforme a Lei 9.610/98 (Direitos Autorais).
- O uso de serviços de tecnologia externos (como aplicativos ou ferramentas não fornecidas pela TI) requer aprovação prévia, pois podem representar riscos à segurança da informação e proteção de dados pessoais.

Ketra
soluções inteligentes

Das normas para gestão de ativos:

Segurança da Informação e LGPD

A Lei Geral de Proteção de Dados (LGPD) estabelece obrigações quanto ao tratamento de dados pessoais, físicos ou digitais. Dessa forma:

- É proibida a divulgação de informações internas, dados pessoais de clientes, colaboradores ou fornecedores, bem como detalhes sobre projetos e operações internas.
- A troca de dados pessoais e sensíveis deve ocorrer somente por e-mail corporativo ou sistemas autorizados pela Ketra.
- Qualquer suspeita de violação ou vazamento de dados pessoais deve ser comunicada imediatamente ao Comitê Gestor de Segurança da Informação.
- É vedado anotar senhas ou informações sigilosas em papel ou documentos visíveis.
- As credenciais de acesso que precisem ser compartilhadas devem estar registradas no TeamPass, ferramenta oficial da Ketra.

Proteção de Informações e Direitos Autorais

- Não é permitido reaproveitar folhas impressas contendo informações sigilosas — devem ser descartadas de forma segura.
- É proibida a cópia, instalação ou distribuição não autorizada de materiais protegidos por direitos autorais (livros, fotos, softwares, etc.).
- É vedado o uso de softwares sem licença válida ou produtos “pirateados”.
- A Ketra não admite violação de direitos autorais, patentes ou segredos comerciais de terceiros.

Ketra
soluções inteligentes

Das normas para gestão de ativos:

Parceiros e Fornecedores

As regras de segurança da informação também se aplicam aos parceiros de negócios e fornecedores.

- Antes da autorização de uso de ativos da Ketra, os parceiros devem passar por diligência de segurança, comprovando práticas compatíveis com as da empresa.
- Devem ser firmados contratos com cláusulas de segurança da informação e proteção de dados pessoais.
- Todos os parceiros que utilizarem recursos de TI da Ketra devem estar inventariados, com responsáveis de segurança e encarregado de dados devidamente registrados.
- O dever de cuidado com dados pessoais se estende a todos os fornecedores, que devem agir com responsabilidade, ética e conformidade.

Comunicação de Incidentes

Os usuários devem comunicar imediatamente ao Comitê Gestor de Segurança da Informação qualquer:

- Ameaça ou incidente tecnológico (vírus, invasão, spam, e-mails suspeitos, falhas de sistema etc.);
- Ocorrência relacionada à conduta ética, como roubo de informações, acesso indevido, uso de credenciais de terceiros ou divulgação não autorizada de dados.

Ketra
soluções inteligentes

Das infrações e penalidades:

Os casos de violação desta Política de Segurança da Informação serão analisados pelo Comitê Gestor de Segurança da Informação, que avaliará a gravidade da infração e aplicará as penalidades cabíveis.
O descumprimento das normas aqui estabelecidas, seja de forma isolada ou cumulativa, poderá resultar nas seguintes sanções:

- Aviso de Descumprimento;
- Advertência ou Suspensão Disciplinar;
- Demissão por Justa Causa;
- Abertura de processo civil ou criminal, conforme a gravidade do caso.

O Aviso de Descumprimento será encaminhado por e-mail ao colaborador e ao gestor imediato na primeira violação, indicando claramente a norma infringida.
A Advertência ou Suspensão Disciplinar será aplicada por escrito em casos de infrações leves ou reincidência, sendo devidamente registrada na ficha pessoal do colaborador.
A Demissão por Justa Causa será aplicada nas situações de maior gravidade, conforme previsto no artigo 482 da Consolidação das Leis do Trabalho (CLT), bem como em demais hipóteses legais.

Ketra
soluções inteligentes

OBRIGADA

Ketra
soluções inteligentes