

CARTILHA DE PROTEÇÃO DE DADOS

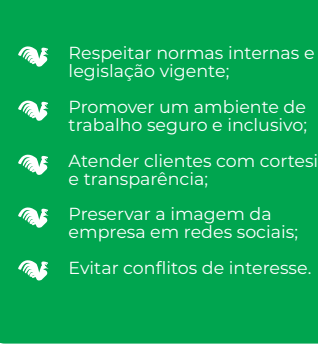


POLÍTICA DE BACKUP

A Política de Backup visa regulamentar o procedimento de backup das informações do sistema pelo setor de Tecnologia da Informação para que seja feito de maneira regular, garantindo, também, que os dados sejam armazenados de maneira segura e de acordo com as leis aplicáveis.

REGRAS DA POLITICA

- 🖱️ Armazenamento em mídias seguras;
- 🖱️ Teste regular da integridade das mídias;
- 🖱️ Não são permitidos backups pessoais;
- 🖱️ Uso restrito de mídias digitais;
- 🖱️ A não observação das medidas é passível de punição via sanção disciplinar.



POLÍTICA DE SENHAS

Esta Política define regras claras para a criação, uso e gerenciamento de senhas para acesso aos sistemas, redes e aplicativos da empresa. Toda senha deve ser forte e para isso deve conter uma combinação de letras maiúsculas, minúsculas, números e símbolos. Recomendamos ainda o uso de frases difíceis de adivinhar.

Exemplo: "Ouvi7Vozes#NaMinha#Cabeça"

Não utilize senhas antigas, a reciclagem de senhas não deve ser efetuada, pois essas senhas podem ter sido comprometidas ou violadas.



RECOMENDADO

- 🖱️ Respeitar normas internas e legislação vigente;
- 🖱️ Promover um ambiente de trabalho seguro e inclusivo;
- 🖱️ Atender clientes com cortesia e transparência;
- 🖱️ Preservar a imagem da empresa em redes sociais;
- 🖱️ Evitar conflitos de interesse.

PROIBIÇÕES

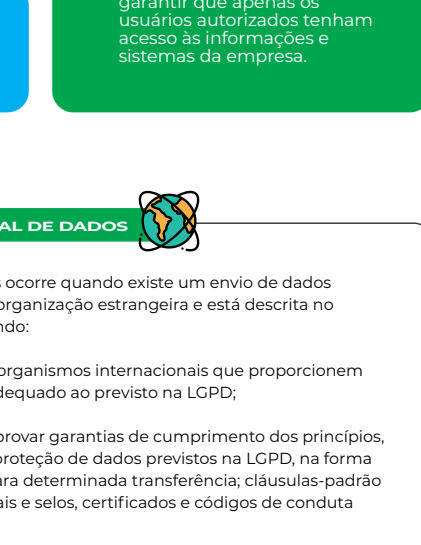
- 🖱️ Compartilhar suas senhas, nem mesmo com seus colegas de trabalho;
- 🖱️ Armazenar senhas em locais visíveis ou de fácil acesso;
- 🖱️ Salvar senhas em navegadores ou aplicativos.

POLÍTICA DE SOFTWARES

A Política de Softwares visa garantir o uso adequado e legal de softwares na empresa, proteger a integridade das máquinas utilizadas pelos colaboradores da companhia e minimizar a possibilidade de violação de direitos autorais.

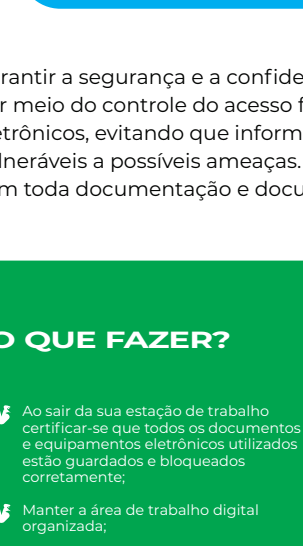
QUAIS REGRAS DEVEM SER SEGUIDAS?

- 🖱️ Softwares adquiridos de fontes legítimas e corretamente licenciados;
- 🖱️ Instalação exclusiva de Softwares autorizados pela gerência;
- 🖱️ Não disponibilização de softwares de uso da empresa para terceiros;
- 🖱️ Proibição do uso de softwares pessoais nas máquinas da empresa;
- 🖱️ O monitoramento e gerenciamento do uso de softwares na empresa e de responsabilidade da Supervisão Geral, Administração e Direção.



HIERARQUIA DE ACESSO

A Supervisão Geral, Administração ou Direção, deve restringir o acesso dos colaboradores somente as informações que necessitam para realização de suas tarefas, devendo haver uma revisão periódica para garantir que apenas os usuários autorizados tenham acesso às informações e sistemas da empresa.



TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados ocorre quando existe um envio de dados pessoais para outro país ou para uma organização estrangeira e está descrita no artigo 33 da LGPD e pode ocorrer quando:

Seja realizada somente parapoais ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD;

Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de cláusulas contratuais específicas para determinada transferência; cláusulas-padrão contratuais; normas corporativas globais e selos, certificados e códigos de conduta regularmente emitidos;

Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter.

POLÍTICA DE MESA LIMPA

Garantir a segurança e a confidencialidade das informações da empresa, por meio do controle do acesso físico aos documentos e equipamentos eletrônicos, evitando que informações sigilosas sejam expostas ou fiquem vulneráveis a possíveis ameaças. Manter o ambiente de trabalho limpo, com toda documentação e documentos sigilosos em seus devidos lugares.

O QUE FAZER?

- 🖱️ Ao sair da sua estação de trabalho certificar-se que todos os documentos e equipamentos eletrônicos utilizados estão guardados e bloqueados corretamente;
- 🖱️ Manter a área de trabalho digital organizada;
- 🖱️ Coletar documentos impressos imediatamente após a impressão;
- 🖱️ O descarte de documento deve ser feito após a fragmentação.



O QUE FAZER SE OCORRER EXTRAVIO?

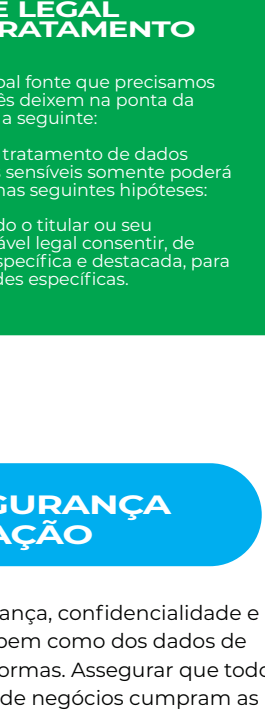
Caso ocorra um extravio de documento, informar imediatamente a Supervisão Geral, Administração ou Direção.

POLÍTICA DE CONTROLE DE ACESSO

Garantir em meios físicos e digitais que apenas os usuários autorizados tenham acesso aos recursos da empresa, e que esse acesso seja concedido de forma apropriada, garantindo a confidencialidade, integridade e disponibilidade das informações.

O QUE FAZER?

- 🖱️ Todos os colaboradores só podem acessar o sistema da empresa por meio de usuário e senhas próprios;
- 🖱️ As credenciais são pessoais e intransferíveis;
- 🖱️ Cada colaborador deve acessar apenas os documentos que necessitarem para exercer suas funções;
- 🖱️ Definições de hierarquia de acesso, alguns locais só podem ser acessados por determinados funcionários;
- 🖱️ Realizar o registro digital das atividades dos colaboradores;
- 🖱️ Revogação de acesso a colaboradores desligados.



POLÍTICA DE GERENCIAMENTO DE DISPOSITIVOS MÓVEIS

Prática essencial para garantir a segurança das informações e a privacidade dos dados em dispositivos móveis.

O QUE FAZER?

- 🖱️ Todos os colaboradores só podem acessar o sistema da empresa por meio de usuário e senhas próprios;
- 🖱️ As credenciais são pessoais e intransferíveis;
- 🖱️ Cada colaborador deve acessar apenas os documentos que necessitarem para exercer suas funções;
- 🖱️ Definições de hierarquia de acesso, alguns locais só podem ser acessados por determinados funcionários;
- 🖱️ Realizar o registro digital das atividades dos colaboradores;
- 🖱️ Revogação de acesso a colaboradores desligados.



O QUE É PROIBIDO?

O uso de dispositivos móveis pessoais, não sendo caso de urgência e sem autorização de Superior hierárquico, é desencorajado para preservar a qualidade e produtividade do trabalho, em virtude do uso do excessivo ou inadequado.

POLÍTICA DE PRIVACIDADE

Informamos nossos clientes que somos uma companhia que se preocupa com a proteção de seus dados, essa política fica disponível no site companhia para todos os clientes.

NOMENCLATURA

Dado Pessoal: É uma informação relacionada a uma pessoa física e que seja capaz de identificar a pessoa ou tornar possível a sua identificação. São exemplos de dados pessoais que podem permitir a sua identificação: Nome, CPF, telefone, e-mail, placa do seu veículo etc.

Tratamento: É toda forma de uso que podemos fazer dos seus Dados Pessoais, incluindo, mas não se limitando às seguintes atividades: coleta, armazenamento, consulta, uso, compartilhamento, transmissão, classificação, reprodução, exclusão e avaliação.

Titular Política: É você, a pessoa física a quem os Dados Pessoais se referem.

Lei Geral de Proteção de Dados: A lei regula todo tratamento de dados pessoais dos cidadãos brasileiros feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais, seja dentro ou fora do Brasil, assegurando a titularidade dos dados pessoais, exigindo consentimento para seu uso e aplicando sanções ao descumprimento. Na prática, pessoas jurídicas, bem como o governo, deverão garantir maior segurança aos dados pessoais coletados (sejam físicos ou digitais), observando os objetivos, fundamentos e princípios da lei.

VIGÊNCIA

Esta política está em vigor desde abril de 2024 e deve ser rigorosamente seguida por todos na empresa.

BASE LEGAL DE TRATAMENTO

A principal fonte que precisamos que vocês deixem na ponta da língua é a seguinte:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O objetivo dessa política é garantir a segurança, confidencialidade e integridade das informações da empresa, bem como dos dados de clientes e fornecedores, em todas as suas formas. Assegurar que todos os colaboradores, terceirizados e parceiros de negócios cumpram as práticas de segurança definidas nesta política e nos demais procedimentos e políticas relacionados. Proteger a empresa e seus ativos contra ameaças externas ou internas, incluindo ataques cibernéticos, vazamentos de informações, perda de dados, entre outros. Cumprir as normas e regulamentações aplicáveis à segurança da informação

Este documento estará disponível a todos os colaboradores na sede da empresa e também estará disponível no site da Petniva.

As políticas mencionadas nesta cartilha também podem ser consultadas integralmente na sede da empresa ou por meio do site institucional.