POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS

INORPEL cybersecurity

INORPEL cybersecurity	**POLÍTICA INORPEL CYBERSECURITY**				**Data de Criação: 13/11/2024**
	Número: 0017	**Localizador: POL-SI**	**Revisão:** v 2.0	**Folhas: 10**	**Data para Revisão: 28/04/2026**
Título: Política de Privacidade e Proteção de Dados Pessoais				**Área Emitente: White Team**	
Elaborador: Maria Luiza dos Santos Macêdo			**Aprovadores: Comitê Gestor de Compliance, Privacidade e Segurança**		
Data da Publicação: 06/05/2025			**Auditor: Auditoria**		
Classificação da Informação: PUBLICA					

Sumário

1. OBJETIVO E PRINCÍPIOS:

A presente Política de Privacidade e Proteção de Dados Pessoais visa garantir que os dados pessoais dos titulares de direito tramitem dentro da INORPEL CYBERSECURITY com segurança e privacidade, respeitando os processos de tratamento e assegurando que os procedimentos realizados estejam em conformidade com a legislação e regulamentações vigentes.

A Política possui princípios que visam assegurar a proteção de:

a) Autenticidade: garante que os dados sejam provenientes de fontes confiáveis e que quem está acessando ou manipulando as informações seja realmente quem diz ser, ou seja, assegura que não ocorram alterações de forma não autorizada das informações;
b) Confidencialidade: o acesso à informação será permitido conforme prévia autorização e de acordo com a necessidade;
c) Disponibilidade: os dados estarão acessíveis quando necessários, ou seja, para que as pessoas autorizadas possam acessar as informações assim que precisarem;
d) Minimização de Dados: Evitar a coleta de dados desnecessários ou excessivos;
e) Integridade: assegura que os dados permaneçam precisos, completos e inalterados durante o seu ciclo de vida. Isso significa que, ao serem armazenados ou transmitidos, os dados não devem ser corrompidos, alterados ou destruídos de forma indevida, mantendo assim a sua devida veracidade.

2. ESCOPO

Esta Política de Privacidade e Proteção de Dados Pessoais se aplica à todos nossos clientes e titulares de dados bem como ao administradores, colaboradores, estagiários, jovens aprendizes, fornecedores de serviços, sistemas e serviços, incluindo trabalhos realizados externamente ou por terceiros que usem os ambientes físicos ou virtuais da INORPEL CYBERSECURITY, com base no que a LGPD (Lei Geral de Proteção de Dados) dispõe e define como normas essenciais para proporcionar um ambiente de Segurança e Privacidade dentro dos padrões exigidos.

3. DEFINIÇÕES

Para os fins da política em questão, aplicam-se as definições a seguir:

a) Dados Pessoais: Qualquer informação que identifique ou torne identificável a pessoa física, como: nome, CPF, telefone etc;
b) Dados Pessoais Sensíveis: Informações que requerem uma proteção mais assídua em virtude do seu teor, visto que se trata de assuntos como origem racial, convicção religiosa, dados referentes a saúde e entre outros;
c) Titular de Dados: Pessoa física a quem se referem os dados pessoais;
d) Tratamento de Dados: Todo processo operacional realizado com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

e) Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
f) Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
g) Encarregado (DPO): Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
h) Autoridade Nacional de Proteção de Dados (ANPD): Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) em todo o território nacional.
i) Violação de Dados: Qualquer evento/incidente que resulte em acesso, divulgação, alteração, vazamento, perda ou destruição não autorizado de dados pessoais tratados.
j) Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
k) Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
l) Banco de dados: é um conjunto estruturado de dados pessoais, ou seja, um repositório organizado onde os dados pessoais são armazenados, organizados e gerenciados de forma que possam ser acessados, consultados, alterados ou processados de forma rápida e eficiente.
m) ID de Sessão: Identificação única gerada quando o usuário acessa nosso site.
n) IP (Internet Protocol): Endereço numérico que identifica dispositivos na Internet.

4. DADOS PESSOAIS QUE COLETAMOS

A INORPEL CYBERSECURITY coleta diversos tipos de dados pessoais, dessa forma, aprimoramos nossos serviços e realizamos uma operação mais eficiente. A coleta é realizada de maneira objetiva e transparente e está em conformidade com as práticas adotadas por outras grandes empresas do setor de cibersegurança:

a) Dados de identificação pessoal fornecidos por meio de contratação: Nome, Email, Telefone, endereço, CPF, dados bancários em virtude de informações do pagamento.
b) Dados de identificação digital: Informações sobre como você interage com nossos serviços, incluindo logs de acesso, dados de navegação e preferências de uso.
c) Dados relacionados a Geolocalização: Por meio do seu consentimento expressado de forma explícita, coletamos informações acerca da localização para que possamos atuar de forma personalizada com os nossos serviços.
d) Dados com finalidade de prestação de serviços: Informações sobre a organização no geral, área de atuação, nível de maturidade de segurança de dados, dados de sistemas e IP de Sessão.

e) Dados Técnicos: Endereço IP, tipo de dispositivo, sistema operacional, dados de localização, entre outros relacionados ao acesso a nossos serviços.

4.1 DADOS DE COLABORADORES

São os dados pessoais dos nossos colaboradores, prestadores de serviços, estagiários e jovens aprendizes da INORPEL CYBERSECURITY. Estes dados são utilizados de acordo com nossa diretriz interna, bem como, em nossos documentos internos. Os dados pessoais são coletados a partir do processo seletivo realizado via empresa de recrutamento, estes são:

a) **Informações de identificação**: São dados essenciais para a formalização do contrato de trabalho, como nome completo, CPF, RG, data de nascimento, e filiação. Esses dados são fundamentais para a identificação do funcionário e para o cumprimento de obrigações fiscais e trabalhistas.
b) **Endereço e contato**: O endereço residencial, telefone e e-mail do funcionário são importantes para a comunicação formal, envio de documentos e para registros administrativos da empresa.
c) **Dados bancários**: Informações como número de conta bancária e agência são necessárias para o pagamento de salários e benefícios.
d) **Documentação profissional**: Dependendo do cargo, a empresa pode coletar dados relacionados à escolaridade, experiência profissional, registros de qualificação e cursos realizados, entre outros, para validar a qualificação do funcionário para a vaga.
e) **Informações sobre dependentes**: Para o fornecimento de benefícios como plano de saúde ou vale-alimentação, a empresa pode coletar dados sobre dependentes do funcionário (como cônjuges e filhos), como nome, CPF, idade e vínculo familiar.

4.2 DADOS DE COLABORADORES DE CLIENTES

São os dados pessoais de colaboradores de clientes da Inorpel. Estes dados são utilizados de acordo com nossa diretriz interna, bem como, em nossos documentos internos para o cadastro de clientes em sistemas da Inorpel para gestão de appliances, solicitação de serviços e apoio técnico (service desk) ou outros sistemas e meios de comunicação necessários à Inorpel para prestação de serviços aos seus clientes.

a) **Informações de identificação**: informações como nome completo e CPF.
b) **Endereço eletrônico e contato**: endereço eletrônico e telefone de contato para cadastros nos sistemas os quais o colaborador do cliente terá acesso.

5. FINALIDADE DA COLETA DE DADOS

Os dados são coletados para serem utilizados das seguintes formas:

1. **Atendimento ao cliente:** Responder a consultas, fornecer suporte técnico e responder a solicitações;
2. **Segurança e prevenção de incidentes:** Proteger os dados pessoais dos nossos clientes contra incidentes ou eventos de segurança, adotar medidas de monitoramento e proteção de dados e sistemas, realização de auditorias de segurança e gestão de incidentes.
3. **Gestão contratual**: Formalizar e administrar contratos com clientes e parceiros comerciais, além de enviar comunicações relacionadas a esses contratos.
4. **Cumprimento das obrigações legais:** Cumprir as exigências legais e regulamentos, relacionados à segurança e a proteção de dados conforme exige a Lei n° 13.709/2018;
5. **Prestação de serviços e melhoria contínua:** Análise de dados para aprimorar a experiência do usuário, desenvolvimento de novos serviços;
6. **Gestão adequada dos benefícios**: Para oferecer benefícios como plano de saúde, vale-alimentação, seguro de vida, auxílio-transporte, entre outros, é necessário coletar dados específicos (como informações bancárias, estado civil, número de dependentes, histórico médico etc.) para garantir que esses benefícios sejam corretamente direcionados e oferecidos ao colaborador e seus dependentes.

6. BASE LEGAL PARA O TRATAMENTO DE DADOS

O tratamento de dados pessoais na INORPEL CYBERSECURITY segue todos os requisitos exigidos e descritos pela Lei Geral de Proteção de Dados Pessoais (LGPD), respeitando os pressupostos da transparência, necessidade e proporcionalidade bem como o consentimento do titular, sendo assim, as bases que utilizamos, são:

a) **Consentimento**: Quando exigido, o consentimento será solicitado de maneira clara e específica para o tratamento de dados;
b) **Execução de Contrato**: O tratamento é necessário para a execução de contratos ou para procedimentos preliminares relacionados a contratos;
c) **Interesses Legítimos**: O tratamento é realizado com base em nossos interesses legítimos, como segurança, prevenção de fraudes e melhoria de serviços;
d) **Cumprimento de Obrigações Legais**: O tratamento é necessário para o cumprimento de obrigações legais ou regulatórias.

7. COMPARTILHAMENTO DE DADOS PESSOAIS

1. **Fornecedores:**

a) Dados de contato e identificação: Nome, endereço de e-mail, telefone e outras informações básicas de contato podem ser compartilhados para facilitar a comunicação e a prestação de serviços.

2. **Órgãos reguladores:**

a) Dados de incidentes de segurança: Caso haja um incidente de segurança significativo, como vazamento de dados ou ataque cibernético, a empresa de cibersegurança pode ser obrigada a relatar os detalhes para órgãos reguladores, incluindo dados pessoais que possam ter sido comprometidos.
b) Relatórios de conformidade e auditoria: Dados sobre como a empresa está implementando controles de segurança e protegendo dados pessoais podem ser compartilhados para auditorias regulares ou em resposta a uma solicitação de fiscalização.
c) Relatórios de risco e impacto: Caso a empresa tenha identificado riscos à segurança da informação ou ao tratamento de dados pessoais, ela pode ser obrigada a compartilhar essa informação com os reguladores, juntamente com dados sobre as medidas tomadas para mitigar esses riscos.

3. Prestadores de Serviços:

a) Dados de clientes e usuários finais: Em alguns casos, os prestadores de serviços podem precisar acessar dados pessoais dos clientes finais, como informações sobre incidentes de segurança ou logs de acesso, para realizar uma análise de ameaças, investigar vulnerabilidades ou aplicar correções.
b) Dados de segurança e monitoramento: Para fornecer serviços de monitoramento contínuo, os prestadores podem ter acesso a logs de segurança, informações sobre ataques detectados, dados sobre tráfego de rede ou alertas de sistemas comprometidos.
c) Dados de conformidade: Os prestadores podem ser encarregados de garantir que a empresa de cibersegurança esteja em conformidade com as regulamentações de segurança e privacidade, necessitando, portanto, de acesso a dados relacionados às políticas de segurança e medidas de proteção implementadas.

4. Parceiros:

a) Fornecimento de benefícios: A organização compartilha dados pessoais com os parceiros, para que esses possam fornecer e administrar os benefícios aos colaboradores. Os dados compartilhados são: Nome completo, data de nascimento e o CPF, é possível que haja o compartilhamento de dados referentes aos dependentes dos funcionários visando garantir que os benefícios sejam adaptados às necessidades dos indivíduos.
b) Cumprimento das obrigações contratuais: A organização pode compartilhar dados pessoais com parceiros como uma forma de cumprir suas obrigações contratuais, relacionadas à concessão de benefícios trabalhistas.

8. ARMAZENAMENTO DE DADOS PESSOAIS

A INORPEL CYBERSECURITY segue de forma rigorosa todas as práticas recomendadas para um armazenamento seguro dos dados de nossos clientes, bem como, encontra-se em conformidade com a legislação aplicável para esta finalidade. Os dados são armazenados e resguardados em servidores protegidos, onde se é aplicado controles de segurança, como restrição de acesso, criptografia e permissões de acesso. Essas medidas incluem, mas não se limitam a:

a) **Controle de Acesso**: Implementação de controles rigorosos de acesso aos dados, garantindo que apenas indivíduos autorizados possam acessar informações sensíveis.
b) **Backup e Recuperação de Dados**: Realização de backups regulares para garantir a integridade dos dados e a continuidade dos serviços em caso de incidentes com o uso de criptografia dos arquivos de Backup.
c) **Monitoramento e Auditoria**: Monitoramento contínuo e auditoria de sistemas para detectar vulnerabilidades e prevenir incidentes de segurança.
d) **Treinamento de Funcionários**: Capacitação contínua dos colaboradores sobre práticas de segurança da informação e proteção de dados pessoais.
e) **Dados Internos Referentes aos Nossos Colaboradores**: Os dados dos nossos colaboradores também são armazenados em ambientes seguros e controlados pelas medidas implantadas.

9. DIREITOS DOS TITULARES DE DADOS

Os titulares de dados assim como os colaboradores podem entrar em contato com a INORPEL CYBERSECURITY para exercer seus direitos previstos na LGPD através do e-mail: dpo@inorpelcybersecurity.com.br, assim, o titular poderá solicitar suas demandas diretamente com nosso encarregado. Dito isto, de acordo com a legislação vigente é direito do titular:

a) **Acesso**: Solicitar uma cópia dos dados pessoais que temos sobre você.
b) **Correção**: Solicitar a correção de dados pessoais incompletos, imprecisos ou desatualizados.
c) **Exclusão**: Solicitar a exclusão de dados pessoais, desde que não haja obrigação legal ou contratual que justifique a retenção.
d) **Portabilidade**: Solicitar a transferência de seus dados pessoais para outro fornecedor de serviços, quando aplicável.
e) **Revogação do Consentimento**: Caso o tratamento de dados seja realizado com base no consentimento, você pode revogar esse consentimento a qualquer momento.
f) **Oposição ao Tratamento**: Caso considere que o tratamento de seus dados pessoais viola a legislação vigente, você pode se opor ao tratamento.

10. DAS RESPONSABILIDADES

São de responsabilidade da INORPEL CYBERSECURITY assegurar que os dados pessoais de clientes, colaboradores e parceiros sejam tratados de maneira responsável, segura e conforme as regulamentações. Garantindo a segurança das informações evitando acessos não autorizados, vazamentos ou perdas de dados. Tais responsabilidades também devem ser seguidas por parceiros ou fornecedores para que adotem as mesmas

práticas de segurança e privacidade, visando a conformidade com as leis de proteção de dados.

11. RETENÇÃO DE DADOS

A INORPEL CYBERSECURITY reterá e armazenará os dados pessoais dos titulares apenas pelo tempo necessário para cumprir as finalidades descritas na presente política, respeitando os prazos mínimos estabelecidos em Lei, conforme exige a legislação vigente. Atingido o período máximo de retenção, os dados serão eliminados de forma ágil e segura, salvo se houver alguma necessidade de mantê-los armazenados.

12. ALTERAÇÕES E APROVAÇÕES

A presente Política de Privacidade pode sofrer alterações devido o entendimento de melhorias e mudanças em nosso modo operante ou para estar em conformidade com a legislação vigente. Portanto, a versão mais recente será publicada e datada com as últimas atualizações.

13. CANAIS DE ATENDIMENTO

Caso tenha dúvidas ou deseje exercer seus direitos relacionados aos dados pessoais, entre em contato com nosso encarregado de proteção de dados por meio dos canais de atendimento a seguir:

a) **Nome do Encarregado**: João Pimentel Neto
b) **E-mail**: dpo@inorpelcybersecurity.com.br
c) **Endereço**: R Jose Soares de Medeiros, 1620, Bloco E Módulos 2, 3 e 4, Térreo, Cabedelo – PB, CEP: 58105-015.
d) **Link para Exercício de direitos**: https://app.podium.com.br/forms/5406b153-7fbb-41da-a4e0-dbc77743d072