PANDAPÉ

Segurança da informação e Proteção de dados pessoais

PANDAPÉ

Somos líderes mundiais em soluções digitais de RRHH

Temos o compromisso de ajudar nossos clientes a selecionar e gerenciar os melhores talentos. Por isso, criamos o Pandapé, o conjunto de soluções de RH mais popular da América Latina. Oferecemos a você Pandapé que

- ✓ simplifica, transforma e aprimora seus processos de recrutamento.
- ✓ digitaliza o gerenciamento de talentos, melhora a comunicação e aumenta o desempenho.

No centro de nosso sucesso está nosso foco em privacidade e proteção de dados. Aqui lhe contamos sobre isso.

Índice

Segurança da informação

Proteção de dados pessoais

PANDAPÉ

Estamos comprometidos com a segurança da informação em nossos serviços

Temos um Sistema de Gerenciamento de Segurança da Informação (ISMS) certificado de acordo com a norma **ISO/IEC 27001:2022** para os serviços que nós oferecemos. Isso inclui o **Infojobs**.

Nossos processos e sistemas estão sujeitos a auditorias regulares, testes de penetração, detecção e prevenção de invasões. Monitoramos e aprimoramos nossa tecnologia, infraestrutura e processos para garantir o máximo de qualidade, eficiência e segurança.

Computação na nuvem

O **AWS** e o **Azure** são nossos **fornecedores de computação na nuvem.**
Contamos com a experiência, os recursos e a reputação da Amazon e da Microsoft para garantir operações em nuvem seguras, robustas e confiáveis.

Equipe de segurança

Temos uma equipe técnica dedicada para monitorar nossa infraestrutura. Nossos sistemas operam 24/7 dias por semana, para garantir a segurança do serviço

Proteção de redes

Usamos firewalls, NACL, NACL e HTTPS para o transporte seguro da rede. Temos sistemas (IDS/IPS) que detectam e bloqueiam tráfego e ataques mal-intencionados

Arquitetura de redes

Dividimos nossa arquitetura de segurança por zonas (DMZ). Usamos DMZ entre a Internet ou sub-redes públicas (load balancers)

Firewall

Filtramos o tráfego de rede de entrada com firewalls. Identificamos e negamos conexão a tráfego não autorizado

Testes de penetração

Terceiros externos realizam um extenso teste de penetração anual em nossas redes públicas e privadas e auditorias trimestrais de produtos

Acesso

O acesso a todos os nossos sistemas de rede e administração é baseado em funções. Cada usuário deve ser identificado e autenticado

Mitigação de DDoS

Monitoramos o tráfego em todos os gateways HTTP e usamos o WAF para bloquear automaticamente as técnicas de DDoS na camada 7 e os ataques nas camadas 3 e 4

Segurança das operações

Gerenciamento de mudanças
Gerenciamos as mudanças no sistema por meio de um procedimento de gerenciamento de mudanças. Monitoramos mudanças, analisamos riscos e aprovamos impactos.

Atualizações
Com o Azure DevOps, automatizamos as atualizações por meio de pipelines. Testamos para implantar novas versões e fazemos reversões automáticas se houver falhas no serviço.

Gerenciamento de recursos
Monitoramos a demanda atual e futura por recursos tecnológicos para otimizar o desempenho, planejar a capacidade e gerenciar a demanda por serviços.

Controle de malware
Implementamos soluções antimalware que são atualizadas continuamente. Monitoramos constantemente nossos ativos para protegê-los contra ameaças cibernéticas.

Resposta a incidentes de segurança
Após os alertas, nossas equipes de operações, redes e segurança 24/7, escalam os incidentes. Informamos o cliente sobre qualquer impacto na segurança no prazo máx de 48hr

Registro e monitoramento
Coletamos extensos registros de eventos. Nosso sistema alerta a equipe de segurança sobre eventos correlacionados para investigação e resposta.

Criptografia em trânsito
Criptografamos todas as nossas comunicações com o protocolo TLS (Transport Layer Security) em redes públicas com suítes de cifras novas e não fracas.

Criptografia em repouso
Criptografamos todos os arquivos e armazenamentos de dados com sistemas de gerenciamento de chaves baseados em algoritmos robustos e programações de rotação padrão do setor.

Desenvolvimento seguro

Como parte de nosso Secure Development Life Cycle (SDLC), temos várias ferramentas que usamos em cada estágio do desenvolvimento de software para garantir a segurança de nossos serviços, desde a concepção até a implementação e a manutenção.

Linguagem

Nosso stack de software é baseada em várias linguagens de programação para nossos sites e APIs. O Azure DevOps oferece suporte a linguagens de programação com alta escalabilidade, confiabilidade e segurança.

Treinamento em segurança

Treinamos nossos desenvolvedores internamente em segurança de código, design, seguindo as práticas recomendadas para combater ataques comuns e usando controles de segurança.

Quality Assurance

Nossa equipe de controle de qualidade analisa e testa nosso código, integrando vários testes manuais e automatizados para que apenas o código que foi avaliado e aprovado seja implementado.

Audit Logs

Mantemos registros de todos os acessos e alterações feitos por cada usuário (logs de auditoria). O registro é armazenado com acesso restrito e só pode ser consultado no caso de um incidente.

Verificações de segurança OWASP

Alinhamos nosso desenvolvimento de software com as práticas do setor da OWASP. Isso inclui controles que reduzem nossa exposição a XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery) e SQL Injection (SQLi), entre outros.

Ambientes isolados

Separamos física e logicamente os ambientes de teste, preparação e desenvolvimento. Fazemos essa separação por meio de isolamento de rede, firewalls e NACL. Não usamos dados reais de produção no ambiente de desenvolvimento ou de teste.

Disponibilidade e Continuidade

Redundância

Nossa infraestrutura de serviços de produção tem redundância para evitar pontos únicos de falha. Se um sistema primário falhar, o hardware redundante o substituirá. Usamos o agrupamento de serviços e a redundância de rede para reduzir os pontos únicos de falha.

Cópia de segurança

A AWS/Azure fornece nossa infraestrutura de backup que reside em armazenamentos de dados de longo prazo por trás de redes privadas logicamente protegidas e criptografadas em repouso. Fazemos backup de dados de ambientes de produção diariamente e semanalmente, por meio de uma verificação aleatória, verificamos a integridade do backup.

Recuperação de desastres

Nosso plano garante a disponibilidade e recuperação de desastres dos serviços, por meio de um ambiente técnico robusto e planos de recuperação com redundância de fornecedores, de acordo com os RTOs e RPOs que definimos.

Gerenciamento de vulnerabilidades

Temos uma série de ferramentas que nos permitem detectar vulnerabilidades técnicas

Varredura de vulnerabilidade dinâmica interna

Empregamos ferramentas de segurança de terceiros qualificadas para escanear continuamente e dinamicamente nossos aplicativos em relação às regras OWASP, entre outras. Todos os controladores HTTP têm um WAF ativo que bloqueia todas as regras OWASP conhecidas e as principais regras conhecidas em tempo real.

Varredura de vulnerabilidade dinâmica externa

Usamos tecnologias de escaneamento personalizadas e padrão da indústria para testar infraestrutura e software de forma eficiente, minimizando os riscos potenciais associados ao escaneamento ativo. Realizamos testes e escaneamentos sob demanda conforme necessário. Os escaneamentos são realizados durante janelas de menor movimento.

Análise de código estático

Nossos repositórios de código-fonte são continuamente escaneados em estágios de teste e revisão em pipelines e fluxos de CI/CD (integração contínua) e são integrados a todos os fluxos de controle de qualidade.

Teste de Penetração de Segurança

Contamos com especialistas externos em segurança para realizar testes de penetração detalhados e análises dinâmicas de código.

Recursos de segurança em nossos serviços

Esses recursos nos permitem preservar a segurança das informações que circulam ou são armazenadas por meio do uso de nossos serviços.

Recurso	Descrição
Opções de autenticação	Para aplicativos Web GUI, oferecemos login de conta com 2FA. Para APIs de produtos e/ou integrações de clientes, oferecemos um fluxo de autenticação com chaves de API e/ou segredos/tokens para autenticar e autorizar todas as chamadas e ações de API com o backend. Os usuários que acessam a ferramenta são identificados de forma única e exclusiva por meio do sistema de autenticação obrigatório, que consiste em um usuário único e uma senha. O sistema gera automaticamente uma chave ou senha inicial que deve ser alterada mediante o uso de duplo fator de autenticação (2FA), necessário para agentes e administradores. A autenticação 2FA fornece outra camada de segurança para sua conta, dificultando que outra pessoa faça login como você. Por motivos de segurança, a chave ou senha deverá conter um formato específico para evitar chaves fracas.
Autenticação de dois fatores (2FA)	O duplo fator de autenticação (2FA) é necessário para agentes e administradores. A autenticação 2FA fornece outra camada de segurança para sua conta, dificultando que outra pessoa faça login como você.
Política de senha	As senhas só podem ser redefinidas pelo usuário final com um endereço de e-mail. O usuário final pode gerar uma URL temporária de redefinição de senha na página de login. As políticas de senha seguem as principais recomendações para garantir sua segurança.
Armazenamento seguro de credenciais	Seguimos as melhores práticas para armazenamento seguro de credenciais. Todas as senhas são armazenadas criptografadas, ou seja, elas nunca são armazenadas em formato legível por humanos. Um hash unidirecional seguro é usado, com criptografia em repouso e de todas as operações em trânsito para o backend.

Recursos de segurança em nossos serviços

Esses recursos nos permitem preservar a segurança das informações que circulam ou são armazenadas por meio do uso de nossos serviços.

Recurso	Descrição
Privilégios e funções de acesso	O acesso aos dados é governado por direitos de acesso e pode ser configurado para definir privilégios de acesso granulares. Os aplicativos têm vários níveis de permissões para usuários (proprietário, administrador, agente, usuário final, etc.) e uma granularidade de funções por grupo.
Alta disponibilidade e acessibilidade do produto	Para garantir baixa latência e alta disponibilidade na entrega de conteúdo, é utilizada uma rede de entrega de conteúdo (CDN), que garante baixa latência e alta disponibilidade.
Dados do cliente	Os dados e a documentação de cada cliente são armazenados de forma criptografada em seu próprio espaço lógico independente.
Arquivos anexos privados	Por padrão, todas as instâncias de nossos aplicativos são protegidas, todos os ativos e anexos são privados e exigem um login e permissão/função. Além disso, todos os ativos e anexos são armazenados em um repositório de dados criptografado.

Nossa prioridade é ajudá-lo a proteger os dados pessoais de seus candidatos e funcionários.

No **Pandapé**, entendemos suas obrigações como controlador dos dados pessoais de seus candidatos e funcionários. É por isso que oferecemos soluções que o ajudam a cumprir suas responsabilidades e respeitam a privacidade.

Desde a nossa criação, o grupo de empresas Redarbor tem se concentrado no desenvolvimento de soluções centradas na proteção de dados pessoais. Isso significa que, na prática, desenvolvemos ferramentas, implementamos medidas e fornecemos informações para que as pessoas tomem decisões informadas e sempre tenham controle sobre seus dados pessoais.

Você nos instrui sobre quais dados tratar e por que tratá-los em um Acordo de Tratamento de Dados

Infojobs Brasil Atividades de Internet LTDA é a operadora de tratamento de dados

PANDAPÉ

Dos dados pessoais de

Seus candidatos
As pessoas que se candidataram às suas vagas de emprego e cuja candidatura você gerencia no **Pandapé**

Seus funcionários
As pessoas que têm uma relação de trabalho com você, que você gerencia na **Pandapé**

O **meio** pelo qual o tratamento é feito

A **finalidade** do tratamento, ou seja, em geral, selecionar e gerenciar talentos

Você é o **controlador** dos Dados, e responsável pelo tratamento porque determinou

Princípios

Como operadores, nos esforçamos para garantir que nosso relacionamento com você seja baseado nos princípios de

Finalidade
Sempre deve ter uma base legal para tratar dados pessoais

Adequação
Trata dados pessoais para atingir finalidades claras, específicas e atuais decididas pelo Controlador

Necessidade
Trata os dados pessoais que são estritamente necessários para cumprir as finalidades

Transparência
Fornece informações acessíveis, compreensíveis, concisas e relevantes

Qualidade
Mantém dados completos, exatos, precisos, precisos e que reflitam a realidade

Responsabilização e prestação de contas
Deve cumprir suas obrigações como controlador e manter evidências disso

Segurança
Pode manter a integridade, a confidencialidade e a disponibilidade

Pandapé é *privacy-friendly*

Projetamos e desenvolvemos o **Pandapé** para que você, como Controlador, possa dar a seus candidatos e colaboradores o controle de seus dados pessoais e saber o que acontece com eles. Não toleramos práticas invasivas, enganosas ou confusas que afetem a privacidade.

Privacy by default

Em cada estágio de desenvolvimento, tomamos decisões para:

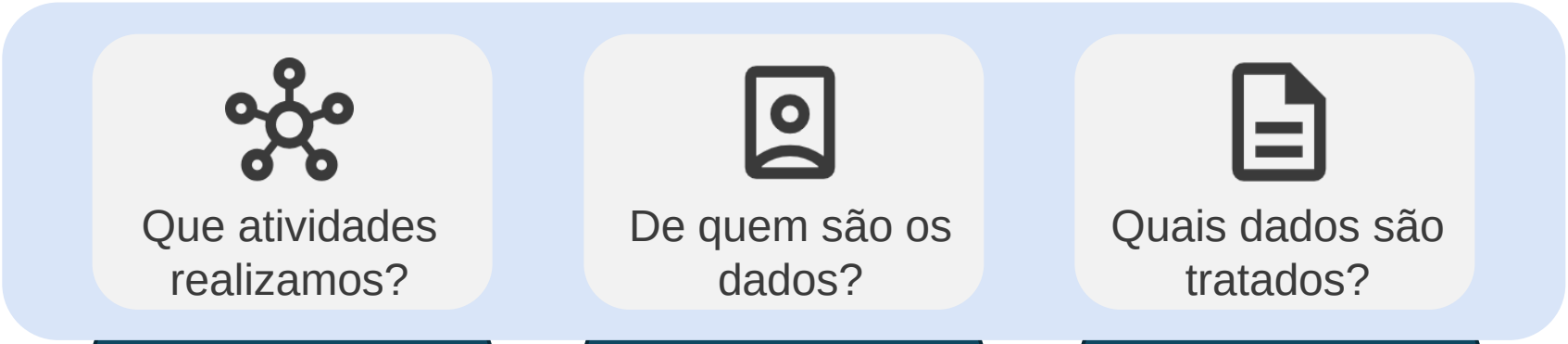
- Garantir a confidencialidade, a integridade, a disponibilidade e a resiliência permanente dos sistemas e serviços
- Restaurar a disponibilidade e o acesso em caso de incidentes de segurança
- Verificar e avaliar continuamente a eficácia das medidas técnicas e organizacionais implementadas

Privacy by design

A configuração original da conta da Pandapé é favorável à privacidade, por exemplo:

- Há cronômetros configuráveis para a exclusão permanente de dados pessoais
- Oferecemos um modelo de política de privacidade para seus candidatos e/ou colaboradores
- Vários alertas e mensagens de notícias permitem que seus destinatários cancelem a assinatura de sua conta

Tratamento de dados que fazemos de acordo com suas instruções



Finalidades

Como **controlador** de dados, **você é quem determina como e para qual finalidade tratará os dados pessoais**. Portanto, é seu dever responder "*por que eu quero o Pandapé?*" e "*o que farei com os dados de meus candidatos e colaboradores?*"

Nós, como **operadores** de dados, não podemos informar qual é a finalidade, e a maneira que os dados serão tratados. Mas, pela natureza de nossas soluções, acreditamos que:

✓ O Pandapé ATS o ajudará a:

- Gerenciar o processo de seleção de seus candidatos
- Comunicar-se com o candidato para discutir os processos de seleção
- Procurar candidatos adequados para preencher as vagas que você tem disponíveis

✓ O Pandapé HCM o ajudará a:

- Gerenciar o relacionamento de trabalho com seus funcionários
- Comunicar-se com seus funcionários sobre questões relacionadas ao trabalho
- Acompanhar o desempenho

No design do Pandapé, incluímos um menu de configurações de privacidade através do qual é possível gerenciar, de forma autônoma, os tempos de retenção, as atualizações da sua política de privacidade, e muito mais.

Com isso, seus candidatos e colaboradores podem ter informações atualizadas e completas sobre o tratamento de dados pessoais que você faz, e informações sobre como exercer os direitos deles.

Direitos

Enquanto operadores, podemos ajudá-lo a responder, como controlador, de forma adequada às solicitações relacionadas aos direitos de

Acesso

O direito do Titular confirmar se seus dados pessoais estão sendo tratados, qual é o tratamento realizado e de receber uma cópia dos dados

Correção

Direito de ter alterar os dados para torná-los completos, exatos e atualizados

Eliminação

O direito de ter exigir que seus dados sejam apagados, observadas as exceções legais

Limitação

Direito de limitar ou restringir, por um período, o tratamento de alguns ou de todos os dados, observadas as exceções legais

Oposição

Direito de limitar ou restringir, por um período, o tratamento de alguns ou de todos os dados, observadas as exceções legais

Portabilidade

Direito de obter dados em um formato estruturado, comumente usado e legível por máquina

Revisão de decisões automatizadas

Que sejam revisadas as decisões automatizadas que possam afetar as liberdades ou os direitos

Como controlador de dados, você decide por quanto tempo manterá os dados pessoais

Por exemplo, isso pode significar

- Para candidatos: o período do processo de seleção
- Para funcionários: a duração do vínculo empregatício
- Que o candidato ou funcionário NÃO solicitou o cancelamento
- Que ainda não ocorreu a prescrição de limitações de obrigações legais ou ações legais

Os usuários administradores que você atribuir no **Pandapé** poderão excluir do sistema os dados para os quais o período de retenção determinado por você expirou.

Compartilhamos dados somente quando é necessário para cumprir as finalidades especificadas

Esses são os terceiros com os quais compartilhamos dados pessoais. Às vezes, esses terceiros estão em países diferentes de seus candidatos ou parceiros.

Dedicamos nossos melhores esforços para contratar fornecedores que estejam em países declarados adequados pelas autoridades de proteção de dados. Na ausência de tal declaração, implementamos cláusulas contratuais ou outros mecanismos para manter o mesmo nível de proteção que os dados têm em seu local de origem.

Suboperadores

Esses são terceiros ou empresas do nosso grupo econômico que, sob nossas instruções, realizam atividades de tratamento. Por exemplo: nuvem, suporte, análise.

Autoridades oficiais

São entidades públicas que, no exercício de suas funções legais e/ou regulatórias, podem nos ordenar o compartilhamento de dados pessoais de seus usuários. Nesses casos, trabalharemos com você para respondê-las.

Sobre os suboperadores

Para fornecer o serviço do **Pandapé**, subcontratamos terceiros que nos apoiam no processamento de dados pessoais em seu nome. Sem eles, não podemos fornecer o serviço. Esses terceiros são sub-operadores pelo tratamento de dados pessoais. Estas são as medidas que adotamos em relação a eles:

Due Diligence

No mínimo, nossos especialistas jurídicos, de segurança e de proteção de dados analisam:

- Políticas, processos e procedimentos de segurança cibernética
- Medidas técnicas e organizacionais de proteção de dados
- Contratos de serviço e suporte

Reputação

Nós nos concentramos em fornecedores que:

- Tenham certificações internacionais de segurança ou de qualidade
- Não tenham multas ou investigações de incidentes de segurança nos últimos 5 anos
- Publicam relatórios de auditoria
- Tenham boa reputação e sejam conhecidos mundialmente
- Estejam localizados em um país adequado à finalidade

Contrato

Elaboramos contratos com os operadores que tenham, no mínimo:

- Obrigação de seguir as instruções do controlador
- Auditorias
- Comunicação de incidentes
- Suporte para resolução de solicitações de exercício de direitos
- Proteção para transferências internacionais de dados

Monitoramento

Após a execução do contrato, monitoramos o relacionamento com eles para:

- Atualizar as mudanças no relacionamento comercial
- Incluir novas obrigações legais no contrato
- Monitorar as políticas de retenção de dados
- Reconhecer alterações nos sub-operadores

Medidas de segurança

Essas são as práticas e ferramentas que implementamos para garantir a confidencialidade, a integridade e a disponibilidade dos dados pessoais dos candidatos e dos usuários profissionais.

Medidas organizacionais

- Temos políticas de desenvolvimento baseadas na proteção de dados.
- Temos um encarregado de dados
- Realizamos avaliações de impacto de proteção de dados para tratamento de alto risco.
- Treinamos nossos funcionários
- Temos uma política de segurança da informação
- Mantemos um registro das atividades de tratamento
- Concentramo-nos em coletar e tratar somente os dados minimamente necessários
- Seguimos as normas aplicáveis de gerenciamento de incidentes

Medidas técnicas

- Criptografamos os dados em trânsito (TLS 1.2) e em repouso (AES 256)
- Controlamos o acesso ao portal por meio da autenticação do usuário
- Temos firewalls, sistemas de detecção/prevenção de intrusão (IDS/IPS)
- Atualizamos nosso antivírus
- Implementamos tecnologias DLP
- Armazenamos dados pessoais na AWS (ISO 27001)
- Implementamos sistemas de monitoramento automático para detectar e responder a atividades suspeitas
- Implementamos técnicas de separação, pseudonimização, mascaramento ou outras, conforme necessário

Gerenciamento de incidentes de dados

Levamos muito a sério a segurança dos dados pessoais de nossos candidatos e usuários profissionais. Nunca economizamos em proteção, mas sabemos que o risco nunca é zero. Algo pode acontecer. Mas quando isso acontece, é isso que fazemos:

Obrigado por confiar no Pandapé. O software de gestão de RH líder na América Latina.

Se tiver alguma dúvida, entre em contato com o executivo designado.

PANDAPÉ