

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

Pelo presente instrumento, a Empresa **PA ALIMENTOS LTDA (PÃO E ARTE ALIMENTOS)**, estabelecida na Rua P, Nº 295, Distrito Industrial, Cuiabá – MT, CEP 78098-420, inscrita no C.N.P.J sob nº 03.095.111/0001-17, em conformidade com as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD)¹, a Pão e Arte Alimentos tem o compromisso contínuo de salvaguardar a privacidade e a segurança dos dados pessoais de nossos clientes, parceiros de negócios e funcionários. A LGPD, como marco legal em proteção de dados no Brasil, exige que as organizações adotem medidas rigorosas para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais que coletamos, processamos e armazenamos. Como parte desse compromisso, desenvolvemos o Relatório de Impacto à Proteção de Dados Pessoais, ou RIPD, um instrumento que visa identificar, avaliar e mitigar potenciais riscos à privacidade dos dados e demonstrar nossa dedicação à transparência e conformidade com a LGPD.

Cabe ressaltar o presente Relatório de Impacto à Proteção de Dados Pessoais (RIPD) está estritamente relacionado às atividades e processos de trabalho das áreas administrativas e de contratação, juntamente com o departamento de informática da empresa Pão e Arte Alimentos. Este enfoque no RIPD é fundamental para que possamos analisar de forma aprofundada os processos envolvidos nessas áreas específicas, identificar riscos potenciais à privacidade de dados e implementar medidas eficazes de proteção.

1. OBJETIVO

O objetivo do Relatório de Impacto à Proteção de Dados Pessoais é fornecer uma descrição abrangente dos procedimentos de tratamento de informações pessoais que possam potencialmente comprometer as liberdades civis e os direitos fundamentais. Além disso, o relatório detalha as ações tomadas para mitigar esses riscos, incluindo medidas, salvaguardas e mecanismos de segurança².

2. DEFINIÇÕES

RIPD: Relatório de Impacto à Proteção de Dados Pessoais.

Anonimização: A técnica que envolve o processamento de dados pessoais de modo a remover elementos suficientes para que não seja mais possível identificar o titular dos dados, de forma irreversível. Em outras palavras, os dados devem ser tratados de tal maneira que não possam mais ser utilizados para identificar uma pessoa específica, utilizando todos os meios razoavelmente disponíveis, tanto pelo responsável pelo tratamento quanto por terceiros.

¹ https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

² Art. 5º, XVII da Lei 13.709/2018 (LGPD)

Autoridade Nacional de Proteção de Dados: Órgão da administração pública responsável por supervisionar, implementar e fiscalizar o cumprimento da legislação de proteção de dados.

Consentimento do Titular dos Dados: A expressão voluntária, específica, informada e inequívoca da vontade do titular dos dados, mediante declaração ou ação positiva, pela qual ele concorda que os dados pessoais relacionados a si sejam submetidos a tratamento.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relacionadas ao tratamento de dados pessoais. Para os fins desta política, a entidade responsável é a Pão e Arte Alimentos.

Dados Pessoais: Qualquer informação de natureza diversa, relacionada a uma pessoa natural identificada ou identificável (titular dos dados), independentemente do suporte utilizado. Uma pessoa é considerada identificável quando pode ser direta ou indiretamente identificada, por exemplo, por meio de um número de identificação ou outros elementos específicos que se referem à sua identidade física, fisiológica, psicológica, econômica, cultural ou social.

Dados Pessoais Sensíveis: Informações que se referem à origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, dados genéticos, identificadores biométricos, informações sobre vida sexual, orientação sexual ou estado de saúde de uma pessoa.

Definição de Perfis: Qualquer forma de processamento automatizado de dados pessoais que envolve o uso desses dados para categorizar uma pessoa em relação ao seu desempenho profissional, situação econômica, saúde, preferências pessoais, interesses, comportamento, localização ou movimentos.

Encarregado da proteção de dados (*Data Protection Officer* - DPO): Indivíduo designado pela Pão e Arte Alimentos para assumir a responsabilidade pela integridade dos dados pessoais e servir como o ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

LGPD: Abreviação da Lei Geral de Proteção de Dados, referente à Lei nº 13.709, de 14 de agosto de 2018, que regula o tratamento de dados pessoais por pessoas naturais ou jurídicas.

Operador: Indivíduo ou entidade, de direito público ou privado, encarregado de realizar o processamento de dados pessoais em nome do controlador.

Pseudonimização: O ato de tratar dados pessoais de forma que eles não possam ser atribuídos a um titular de dados específico sem o uso de informações adicionais. Essas informações adicionais devem ser mantidas separadamente e sujeitas a medidas técnicas e organizacionais para garantir que os dados pessoais não possam ser relacionados a uma pessoa singular identificada ou identificável.

Terceiro: Indivíduo ou entidade, serviço ou organização que não seja o titular dos dados, o controlador, o operador e as pessoas que, sob a autoridade direta do controlador ou do operador, estejam autorizadas a processar os dados pessoais.

Titular dos Dados: Pessoa singular identificada ou identificável a quem os dados pessoais dizem respeito.

Tratamento: Operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como coleta, registro, organização, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, comparação ou interconexão, a limitação, o apagamento ou a destruição.

Responsável pelo tratamento: Pessoa física ou jurídica, autoridade pública, agência ou qualquer outro organismo que, de forma individual ou em conjunto com outros, determine as finalidades e os meios de tratamento de dados pessoais.

Violação de dados pessoais: Violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

3. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador	
Pão e Arte Alimentos (quando atua junto aos seus colaboradores)	
Operador	
Pão e Arte Alimentos (quando atua processando dados de clientes, fornecedores e terceiros)	
Encarregado	
Paulo Roberto dos Santos Junior	
E-mail do encarregado	Telefone
dpo@paoearte.com.br	(62)3224-2550

4. NECESSIDADE DE ELABORAR O RELATÓRIO

A PÃO E ARTE ALIMENTOS realiza o tratamento de dados pessoais que se relacionam a pessoa natural identificada ou identificável (art. 5º, I, da LGPD), Também se encontram os dados pessoais sensíveis, que englobam informações sobre a origem racial ou étnica, crenças religiosas, opiniões políticas, filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, bem como dados relativos à saúde, vida sexual, informações genéticas ou biométricas, desde que estejam associados a um indivíduo natural, (art. 5º, inciso II, da LGPD) como parte de suas atividades de contratação de colaboradores/funcionários. Nesse

contexto, é necessário elaborar um relatório que detalhe todos os aspectos relacionados à coleta e recebimento de dados, finalidade do tratamento, compartilhamento e armazenamento. O objetivo é apresentar todas as medidas e mecanismos adotados pelo controlador para mitigar os riscos inerentes ao tratamento de dados, conforme estabelecido no artigo 5º, inciso XVII da Lei Geral de Proteção de Dados (LGPD).

Nesse contexto, conforme estabelecido no art. 38, caput, da Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), a Autoridade de Proteção de Dados Pessoais (ANPD) tem a autoridade para, a qualquer momento, solicitar à PÃO E ARTE ALIMENTOS a elaboração de um relatório de impacto à proteção de dados pessoais, incluindo dados sensíveis. Portanto, surgiu a necessidade de criar este documento.

5. DESCRIÇÃO DO TRATAMENTO

A natureza do tratamento de dados pessoais realizado pela Pão e Arte Alimentos envolve a gestão e administração de informações relacionadas aos seus colaboradores e funcionários. Isso inclui, mas não se limita a, coleta, armazenamento, atualização e utilização desses dados para fins de gestão de recursos humanos, processamento de salários, benefícios, avaliações de desempenho, registro de presença, e todas as atividades inerentes à relação empregatícia.

Destacando que as Políticas de Segurança da Informação da Pão e Arte Alimentos, divulgadas internamente e através de sistema próprio de gestão de informações, têm como objetivo direcionar as medidas essenciais para garantir a segurança da informação, o que contribui para reduzir os riscos enfrentados pelos ativos de informação, evitando assim potenciais impactos nas operações da Pão e Arte Alimentos e no cumprimento de sua missão institucional.

A Pão e Arte Alimentos possui manuais de sistema de gestão, os quais são atualizados periodicamente afim de manter suas certificações de qualidade, sendo que os seus manuais incorpora princípios de segurança e privacidade. Em suas revisões posteriores, foram integradas as Políticas de Privacidade de Dados e o Manual de Gestão de Riscos, Controles Internos e Políticas e Procedimentos de Segurança para os Sistemas de Informação, sendo que a estrutura de sistemas, *backup*, *firewall* e antivírus conta com tecnologias de ponta sempre visando a proteção dos dados pessoais, sendo que nesta seção, apresentam-se os procedimentos de tratamento de dados pessoais, sejam eles em formato digital ou físico, que têm o potencial de acarretar riscos para as liberdades civis e os direitos fundamentais. Isso engloba a descrição detalhada da natureza, âmbito, contexto e finalidade do tratamento desses dados.

5.1. Natureza do Tratamento

Em diversos departamentos, a Pão e Arte Alimentos utiliza software para facilitar o preenchimento de informações pessoais do promitente candidato à vaga de emprego, funcionários, colaboradores e clientes, a fim de otimizar a eficiência operacional da empresa. Para atender às necessidades de negócios, a Pão e Arte Alimentos recebe, coleta e processa dados específicos em seus departamentos, as modalidades de coleta e tratamento de dados pessoais adotadas pela Pão e Arte Alimentos seguem os seguintes parâmetros:

5.1.1. Informações para relação comerciais e de negócios

Coleta o que?	Dados da Pessoa Jurídica (todos que contemplam o carão CNPJ); Nome completo do representante legal; telefones e endereços de e-mail; números do RG, CPF e CNH.
Coleta dado sensível?	Não
Coleta como?	Os dados são coletados via contato por e-mail organizacional ou contato telefônico por nossos colaboradores internos.
Coleta ciente?	Em todas as solicitações e demandas de informações: clientes (distribuidores e representantes), fornecedores e parceiros são informados e manifestam consentimento livre com relação aos dados informados, conforme consta nas Políticas de Privacidade da PA Alimentos.
Processamento como?	Os dados são empregados exclusivamente com a finalidade de cumprir rigorosamente as operações comerciais estabelecidas entre a Pão e Arte Alimentos e seus distribuidores, representantes, equipe de vendas e demais parceiros comerciais. Isso inclui a elaboração de contratos comerciais, o acompanhamento do histórico de atendimentos e o atendimento das obrigações legais, incluindo aquelas de natureza fiscal.
Processamento onde?	Os dados coletados são registrados diretamente nos sistemas organizacionais: que fazem o gerenciamento e processamento interno das informações.

Armazenamento	Os dados são armazenados nos sistemas operacionais da indústria, que adotam um método rigoroso de controle de acesso. Além disso, a empresa utiliza servidores em nuvem gerenciados por uma empresa certificada e qualificada para garantir a segurança e a proteção dos dados. Isso é feito como uma medida de garantia da integridade dos dados.
Compartilhamento	Os dados são compartilhados internamente visando o eficiente fluxo de processos e para promover a colaboração entre as partes, contribuindo para o crescimento dos negócios. Além disso, são compartilhados com o departamento jurídico e/ou bancário para atender às obrigações legais pertinentes.
Eliminação	Os dados coletados de parceiros e clientes que não foram utilizados para contratos ou para futuros negócios, permanecem registrados nos sistemas, mas trata dos como inativos e somente utilizado para controle de eventuais contatos futuros.

5.1.2. Informações pessoais para processo de seleção e recrutamento, registros e contratos de funcionários

Coleta o que?	Nome completo; telefones; endereços de residência; endereços de e-mail; imagem e dados de CTPS, CNH, RG, CPF; estado civil, nome de filhos, de dependentes legais e nome de cônjuge e escolaridade.
Coleta dado sensível?	Origem étnica ou raça; filiação sindical; dados biométricos para utilização no ponto eletrônico e acesso as dependências da empresa; dados relacionados com saúde como exames admissionais, demissionais, periódicos e de saúde, podendo ser coletado vídeo e voz.

Coleta como?	<p>Por meio de formulários digitais, os quais são acessados na aba de recrutamento e seleção constante no site da P A Alimentos, e/ou através de formulários enviados por e-mail, whatsapp ou preenchidos por acesso telefônico ou os currículos físicos depositados na sede da Industria, sendo que a ação de preenchimento ocorre mediante o consentimento expresso do indivíduo interessado.</p> <p>No que se refere aos dados biométricos, eles são cadastrados diretamente em máquinas de ponto eletrônico ou em máquinas de controle de acesso localizadas internamente, as quais são utilizadas para registrar as entradas e saídas dos colaboradores no ambiente de trabalho. Sendo que vídeo e voz pode ser coletado através de campanhas da empresa, através de consentimento dado pelo participante.</p>
Coleta ciente?	<p>Antes de preencher qualquer formulário e/ou enviar seus dados nos canais da PA Alimentos, o candidato à vaga, funcionário e/ou colaborador está plenamente ciente das informações fornecidas e, como parte desse processo, declara ter tido acesso às Políticas de Privacidade da PA Alimentos, as quais esclarecem detalhadamente como os dados serão tratados, fornecendo ao candidato, funcionário e/ou qualquer colaborador uma compreensão completa dos procedimentos envolvidos.</p>
Processamento como?	<p>Os dados são coletados com o consentimento dos candidatos, funcionários e/ou qualquer colaborador, e são utilizados para confeccionar contratos de trabalho, efetuar registros nos sistemas de folha de pagamento e benefícios, plano de saúde, segurança do trabalho, bem como para cumprir obrigações legais, incluindo o e-Social, assegurando a conformidade com os regulamentos trabalhistas e fiscais.</p>
Processamento onde?	<p>Os dados coletados são registrados diretamente nos sistemas organizacionais: que fazem o gerenciamento e processamento interno das informações do Departamento de Recrutamento, Departamento Pessoal e Recursos Humanos</p>

Armazenamento	Os dados são armazenados nos sistemas operacionais da indústria, que adotam um método rigoroso de controle de acesso. Além disso, a empresa utiliza servidores em nuvem gerenciados por uma empresa certificada e qualificada para garantir a segurança e a proteção dos dados. Isso é feito como uma medida de garantia da integridade dos dados. Sendo que os documentos e imagens necessários são arquivados em pasta funcional, armazenada em local de acesso restrito dentro de armários.
Compartilhamento	Os dados são compartilhados com várias partes, incluindo bancos para o processamento de pagamentos de salários, operadoras de planos de saúde, fornecedores de vale alimentação e vale refeição, sindicatos para possíveis acordos e contratos, o e-Social para cumprimento de obrigações legais, o departamento jurídico para elaboração de contratos individuais e coletivos, bem como o departamento médico para a realização de exames periódicos. Esse compartilhamento é realizado em conformidade com as necessidades operacionais e legais da empresa, garantindo a proteção dos dados pessoais dos funcionários.
Eliminação	Os dados físicos registrados em pastas funcionais são eliminados após um período de 10 anos, seguindo os requisitos legais aplicáveis. Durante esse período, esses registros são armazenados em um depósito nas dependências da empresa, com controle rigoroso de acesso, garantindo a segurança e a conformidade com as políticas de retenção de dados. Já os dados digitais, permanecem registrados nos sistemas, mas trata dos como inativos e somente utilizado para controle de eventuais contatos futuros.

Todos os sistemas mencionados para o processamento e armazenamento de dados no item 5, são respaldados por contratos comerciais que incluem cláusulas de Proteção de Dados, conforme exigido pela LGPD, e possuem acessos restritos por *login* e senhas com hierarquia de acesso.

O armazenamento em Data Center de terceiros é protegido por medidas de segurança, incluindo criptografia, e é gerenciado por empresa reconhecida por sua expertise em segurança de dados, a qual detém padrão e certificação internacional de qualidade e segurança.

O armazenamento local é acessado apenas por indivíduos autorizados e conta com registros de controle de acesso, garantindo a segurança e a conformidade com as regulamentações de proteção de dados.

A PÃO E ARTE ALIMENTOS, em seu departamento de Gestão de Pessoas, efetua o tratamento dos atestados médicos fornecidos por seus funcionários e colaboradores, para a análise do absenteísmo, bem como documentos relativos à medicina do trabalho e segurança alimentar. Nesse processo, o colaborador encarregado da recepção e tratamento desses dados deve obter o consentimento do titular das informações, seguindo o formulário Termo de Consentimento de Dados Pessoais e cumprir integralmente os requisitos estabelecidos pela LGPD, dado que tais dados são considerados sensíveis.

O tratamento dos dados pessoais é realizado durante o horário comercial em dias úteis, salvo em situações excepcionais que demandem horas adicionais, com o propósito de atender a demanda da PÃO E ARTE ALIMENTOS.

5.2.Contexto do Tratamento

A finalidade do tratamento dos dados pessoais pela PÃO E ARTE ALIMENTOS é fundamentada na execução de contratos ou procedimentos preliminares relacionados a contratos dos quais os titulares fazem parte, no consentimento dos titulares, no legítimo interesse do controlador e na execução de suas atividades comerciais. Os resultados desejados pelos titulares de dados pessoais incluem todas as fases de industrialização dos produtos fabricados pela PÃO E ARTE ALIMENTOS, como a comercialização dos produtos através de representantes e distribuidores, compra de matéria prima (fornecedores) e demais relações comerciais.

Além disso, espera-se que os dados sejam relevantes para as operações internas da empresa, como processamento de pagamentos e concessão de benefícios. A PÃO E ARTE ALIMENTOS equilibra seus interesses com os interesses dos indivíduos com os quais mantém relacionamento. A natureza desse relacionamento, no contexto de indústria de alimentos, gira em torno de contratos diversos (fornecedores, distribuidores, prestação de serviço e outros), que é responsável por fornecer dados relacionados à relação contratual.

A natureza do relacionamento dos titulares dos dados, que incluem funcionários e colaboradores, com a PÃO E ARTE ALIMENTOS diz respeito à relação de trabalho voltada para a gestão dos negócios da empresa. Nesse contexto, os funcionários e colaboradores são responsáveis por fornecer informações profissionais e pessoais.

A PÃO E ARTE ALIMENTOS não compartilha informações relativas aos dados pessoais dos indivíduos com terceiros, a menos que haja uma solicitação específica. Além disso, os titulares dos dados não têm acesso às informações armazenadas na PÃO E ARTE ALIMENTOS, a menos que façam uma solicitação específica. É importante ressaltar que

dados pessoais de crianças e adolescentes, como filhos de funcionários e colaboradores, bem como jovens em programas de aprendizado e outros que tenham acesso às instalações onde a PÃO E ARTE ALIMENTOS presta serviços, podem ser tratados, sempre em conformidade com a legislação aplicável.

O tratamento de dados é conduzido de acordo com as expectativas dos titulares, em conformidade com as leis, regulamentos, políticas de privacidade e a LGPD da PÃO E ARTE ALIMENTOS. Os titulares dos dados são informados sobre o tratamento de seus dados e têm a oportunidade de consentir para que a PÃO E ARTE ALIMENTOS possa utilizá-los

Embora a PÃO E ARTE ALIMENTOS não possua uma vasta experiência em tratamento de dados pessoais, tem tomado medidas para garantir a conformidade com a LGPD, incluindo a contratação de consultoria especializada. A empresa também implementa medidas de segurança para proteger os dados pessoais e conduziu treinamentos para garantir a aplicação adequada das práticas de privacidade e proteção de dados. Programas de treinamento contínuos serão mantidos para aprimorar constantemente as metodologias e a cultura de proteção de dados.

5.3.Finalidade do Tratamento

A finalidade da coleta de dados pessoais pela PÃO E ARTE ALIMENTOS atende exclusivamente a:

- O cumprimento de obrigações legais fiscais, comerciais ou regulatórias;
- A execução de contratos de compra e venda de mercadorias, bem como procedimentos preliminares relacionados a contratos dos quais os titulares dos dados fazem parte, a pedido dos próprios titulares;
- A satisfação de interesses legítimos necessários para o pleno funcionamento da indústria.

6. PARTES INTERESSADAS CONSULTADAS

Diversas partes interessadas foram consultadas durante este processo, incluindo o Encarregado pelo tratamento de dados pessoais, gerentes de departamentos, diretores, operadores, o controlador, um especialista em segurança da informação e consultor jurídico.

O Encarregado desempenhou um papel central na coleta e avaliação das informações técnicas, administrativas, legais e de riscos fornecidas pelas demais partes consultadas, incluindo os departamentos internos da empresa e colaboradores.

Os gerentes de departamentos identificaram os dados coletados e apontaram áreas de vulnerabilidade na gestão de dados, como o envio de informações pessoais por e-mail e o uso de mídias removíveis, mesmo que autorizado. Essas áreas de vulnerabilidade

continuam sendo tratadas de acordo com as Políticas de Privacidade de Dados e Manual de Privacidade de Dados da PÃO E ARTE ALIMENTOS.

Colaboradores do departamento de Gestão de Pessoas forneceram informações sobre a quantidade de dados armazenados no banco de dados após o término da finalidade, como desligamento de funcionários ou encerramento de contratos com clientes.

O consultor jurídico da empresa emitiu um parecer sobre a conformidade do tratamento de dados em relação aos aspectos legais da LGPD.

Os colaboradores do departamento Jurídico destacaram que alguns contratos não estavam em conformidade com a LGPD devido à ausência de cláusulas relacionadas à confidencialidade e proteção de dados pessoais.

Os analistas de segurança da informação composto pelo departamento de Tecnologia e Informação identificaram oportunidades de melhoria para aprimorar a proteção dos dados pessoais tratados pela empresa. Essas contribuições são essenciais para garantir a segurança e a conformidade com a LGPD.

7. NECESSIDADE E PROPORCIONALIDADE

7.1. Fundamentação Legal

A PÃO E ARTE ALIMENTOS conduz suas operações relacionadas aos dados pessoais com a restrição ao mínimo necessário para atingir seus objetivos, garantindo que os dados sejam pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (conforme estabelecido no artigo 6º, III da LGPD).

A LGPD estabelece um rol taxativo no artigo 7º para a validade do processamento de dados pessoais. No contexto da PÃO E ARTE ALIMENTOS, as bases legais para o tratamento de dados pessoais incluem o consentimento do titular, a execução de contratos e o legítimo interesse do controlador.

A PÃO E ARTE ALIMENTOS pode realizar o tratamento de dados com base em seu legítimo interesse, conforme previsto no artigo 10 da LGPD, quando:

- O tratamento dos dados pessoais for absolutamente necessário;
- Não existir outra base legal viável para alcançar o mesmo propósito;
- O processamento efetivamente contribuir para a finalidade pretendida.

7.2. Qualidade e minimização dos dados

A PÃO E ARTE ALIMENTOS identificou que ainda mantém informações excessivas em seu banco de dados, que não são necessárias para alcançar os objetivos organizacionais da empresa. Como parte de uma mudança cultural em curso, a empresa está trabalhando na

revisão do término da finalidade do tratamento dos dados coletados, com o objetivo de eliminar dados desnecessários em futuras atualizações do relatório de impacto.

Desde a entrada em vigor da LGPD, a PÃO E ARTE ALIMENTOS implementou práticas destinadas a evitar a coleta de dados que não sejam essenciais para seus processos. Os dados coletados devem ser transparentes e relevantes para a finalidade original, além de serem mantidos atualizados. A empresa também reconhece a necessidade de estabelecer uma nova metodologia de armazenamento para informações que já cumpriram sua finalidade de tratamento e estão atualmente mantidas no banco de dados, sem critérios ou funcionalidades específicas, os quais serão adequados em caráter de urgência.

7.3. Medidas para assegurar conformidade do operador

São conduzidas inspeções nos processos de tratamento de dados realizados pela empresa, com o propósito de avaliar a conformidade desses processos com as diretrizes estabelecidas pelo controlador. Essas inspeções têm o objetivo de garantir que o operador, conforme definido no artigo 5º, VII da LGPD, realize o tratamento de dados pessoais de acordo com as disposições da LGPD e esteja em conformidade com os critérios estabelecidos pela instituição que exerce a função de controlador, neste caso, a PÃO E ARTE ALIMENTOS, sendo que nesse primeiro momento está sendo disponibilizado o Manual de Gestão de Riscos, Controles Internos, Segurança Políticas e Procedimentos, visando uma adequação mais célere.

7.4. Medidas para assegurar direitos do titular dos dados

A PÃO E ARTE ALIMENTOS disponibiliza um canal de comunicação para que os titulares dos dados pessoais possam fazer solicitações conforme estipulado pelo artigo 18º da LGPD. As Políticas de Privacidade e os documentos relacionados à LGPD da PÃO E ARTE ALIMENTOS informam os direitos dos titulares dos dados pessoais, incluindo a capacidade de fazer qualquer uma das solicitações mencionadas. Esses documentos podem ser acessados por meio do link www.paoearte.com/lgpd. Caso um usuário identifique alguma falha ou vulnerabilidade de segurança no sistema, pode comunicá-la ao Encarregado por meio do e-mail dpo@paoearte.com.br. Quando solicitado pelo titular dos dados pessoais, a PÃO E ARTE ALIMENTOS fornecerá informações relacionadas à privacidade, como confirmação da existência de dados pessoais ou acesso a esses dados, de acordo com a preferência do titular.

8. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Os contratos serão avaliados em termos de risco e categorizados como "baixa", "média" ou "alta" sensibilidade, dependendo do grau de coleta, tratamento e armazenamento de dados envolvidos.

Antes de definir as medidas, salvaguardas e mecanismos junto a clientes, candidatos a vagas de emprego, colaboradores e fornecedores em geral, é fundamental identificar os riscos que podem afetar potencialmente os titulares dos dados pessoais.

Para cada categoria de sensibilidade, será criada uma minuta contratual ou documento específico, acompanhada de um procedimento correspondente, com o objetivo de mitigar os riscos envolvidos.

Para cada risco identificado, serão determinados os seguintes aspectos: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco se concretize e a avaliação do nível potencial de risco, considerando as classificações de "baixa", "média" ou "alta" sensibilidade, confrontando os seguintes critérios:

Probabilidade: refere-se à chance de ocorrência de um evento, independentemente de ser quantificada objetiva ou subjetivamente, seja qualitativa ou quantitativamente, ou descrita em termos gerais ou matemáticos (conforme definido em ISO/IEC 31000:2009, item 2.19).

Impacto: se relaciona com as consequências de um evento que afeta os objetivos (conforme definido em ISO/IEC 31000:2009, item 2.18).

O Nível de Risco: é a magnitude de um risco ou combinação de riscos, expressa com base na avaliação das consequências e probabilidades envolvidas (conforme definido em ISSO/IEC 31000:2009, item 2.23 e na IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

Neste contexto, são identificados riscos de privacidade e segurança da informação relacionados à proteção de dados pessoais que estão sujeitos a controles implementados pela Pão e Arte Alimentos. A avaliação do nível de probabilidade, impacto e risco é realizada de acordo com as circunstâncias específicas de cada caso. Os doze primeiros riscos são exemplos de riscos de privacidade extraídos da norma ISSO/IEC 29134:2017, seção 6.4.4.

Riscos referente ao tratamento de dados pessoais	
R01	Acesso não autorizado
R02	Modificação não autorizada
R03	Perda
R04	Roubo
R05	Remoção não autorizada
R06	Coleção excessiva
R07	Informação insuficiente sobre a finalidade do tratamento

R08	Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex. Perda do direito de acesso)
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais
R11	Retenção prolongada de dados pessoais sem necessidade
R12	Circulação/associação indevida, direta ou indireta, dos dados pessoais do titular
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada dentre outros.
R14	Reidentificação de dados pseudonimizados

9. MEDIDAS PARA TRATAR OS RISCOS

A Pão e Arte Alimentos implementa medidas de segurança, tanto técnicas quanto administrativas, que são consideradas adequadas para resguardar os dados pessoais contra acessos não autorizados e situações acidentais ou ilegais, como destruição, perda, alteração, divulgação ou qualquer outra forma de tratamento inadequado ou ilícito, conforme estabelecido pela LGPD (art. 46). Essas medidas são implementadas considerando um nível de risco aceitável para a organização.

A equipe de Segurança da Informação, composta pelo departamento de TI, o comitê de LGPD e o Encarregado de Dados - Data Protection Officer (DPO) da Pão e Arte Alimentos, desempenha um papel fundamental na coordenação e supervisão da conformidade com as políticas e procedimentos de Segurança da Informação em toda a empresa. Isso inclui assegurar a confidencialidade, integridade e segurança dos ativos de informação.

O DPO é encarregado de aplicar as políticas estabelecidas, identificar áreas de preocupação e implementar alterações necessárias de acordo com as demandas da organização.

9.1. Segurança da Informação

Para garantir a eficaz proteção dos sistemas da Pão e Arte Alimentos, é essencial que diversos departamentos e equipes compartilhem uma visão coesa de segurança. A área de Segurança da Informação colabora estreitamente com os gestores, administradores e usuários de sistemas em todos os departamentos para desenvolver políticas, normas e procedimentos de segurança que contribuam para a proteção dos ativos da empresa, especialmente os dados. A Segurança da Informação é representada por um comitê

composto por membros de diferentes áreas, dedicado ao planejamento, educação e sensibilização em relação à segurança. Suas responsabilidades específicas englobam:

- Desenvolver políticas e procedimentos de Segurança da Informação e LGPD, quando necessário.
- Manter e atualizar regularmente as políticas e procedimentos de Segurança da Informação e LGPD existentes.
- Realizar revisões anuais das políticas e auxiliar na aprovação pela administração.
- Atuar como ponto central de coordenação para a implementação das políticas de Segurança da Informação e LGPD.
- Elaborar, manter e distribuir procedimentos para resposta a incidentes e encaminhamento.
- Monitorar e analisar alertas de segurança, compartilhando as informações com o pessoal relevante.
- Conduzir análises regulares dos registros e investigar exceções identificadas.
- Controlar e monitorar o acesso a áreas restritas e informações confidenciais.
- Garantir a disponibilidade de controles adequados em locais que contenham informações confidenciais e sensíveis.
- Tomar decisões relacionadas às Políticas de LGPD e seu conteúdo.
- Aprovar exceções às políticas de forma prévia, com base em análises caso a caso.
- Coordenar verificações de risco formais anuais para identificar novas ameaças e vulnerabilidades, implementando controles apropriados para mitigar esses riscos.
- Rever anualmente as políticas e procedimentos de Segurança da Informação para garantir que permaneçam adequados às necessidades emergentes de negócios e às ameaças à segurança.
- Realizar consultas e auditorias anuais em outras áreas de negócios para verificar a segurança de cada uma delas.
- Implementar as políticas e procedimentos de Segurança da Informação em todos os ativos de informação, conforme aplicável.
- Gerenciar contas de usuários e a autenticação.

As responsabilidades específicas de Segurança da Informação relacionadas ao departamento de TI incluem:

- Monitorar alertas específicos de sistemas e aplicativos em sistemas críticos (por exemplo, falhas no firewall, reinicializações do sistema, antivírus, armazenamento em data center terceiro, etc.).
- Notificar as partes relevantes em caso de falha do sistema de segurança ou eventos de segurança.

- Garantir que as regras de segurança aplicadas aos firewalls e roteadores sejam adequadas para proteger as redes e ativos corporativos da PAO E ARTE ALIMENTOS contra ataques externos e acesso não autorizado.
- Certificar-se de que as regras de segurança aplicadas aos firewalls e roteadores sejam suficientes para evitar que eventos de segurança internos saiam da rede da PAO E ARTE ALIMENTOS.
- Revisar todas as solicitações de alteração das regras de segurança para roteadores e firewalls, garantindo conformidade com a política antes da submissão por meio do processo de gerenciamento de mudanças.
- Documentar adequadamente todos os protocolos/serviços autorizados por meio dos firewalls e roteadores.
- Garantir que protocolos potencialmente arriscados, como FTP, TELNET, POP3, IMAP e SNMP (com autenticação implementada), tenham passado por uma avaliação de risco, tenham documentada uma necessidade de negócios atual e estejam protegidos de acordo com as normas de segurança estabelecidas.
- Monitorar ativamente eventos de segurança nos firewalls e roteadores para identificar incidentes externos de segurança.
- Realizar revisões periódicas de todas as regras definidas nos firewalls e roteadores.

9.2. Acesso às Informações

Toda informação confidencial ou sensível deve ser protegida por controles de acesso rigorosos seja nos sistemas bem como nos arquivos físicos, garantindo que não seja divulgada, alterada, apagada ou utilizada indevidamente.

Registros detalhados (logs) devem ser mantidos para rastrear cada acesso a esses dados, identificando quem acessou e quando o acesso ocorreu. Colaboradores autorizados a visualizar informações em um determinado nível de classificação têm permissão apenas para acessar informações nesse nível ou em níveis inferiores, conforme necessário para o desempenho de suas funções profissionais.

O acesso a sistemas deve ser estritamente configurado para negar acesso a informações não relacionadas às funções de um usuário específico. O acesso a sistemas ou aplicativos contendo informações confidenciais, sensíveis ou privadas requer aprovação da equipe de segurança (TI) da PÃO E ARTE ALIMENTOS. O acesso a dados além do que é autorizado para a função de um colaborador também deve passar pelo processo de solicitação de acesso, incluindo limites documentados, como fonte de acesso e prazo de acesso. O acesso a informações armazenadas em formato físico é feito mediante solicitação ao departamento

responsável pelo dado, com medidas de monitoramento, registro de usuários e restrições de acesso conforme a classificação da informação.

9.3. Política de antivírus

Todos os sistemas geralmente afetados por vírus, como servidores, estações de trabalho e laptops da PÃO E ARTE ALIMENTOS, possuem software antivírus e seguem a política de antivírus descrita no documento Manual de Gestão de Riscos, Controles de Segurança, Políticas e Procedimentos para os Sistemas de Informação da PÃO E ARTE ALIMENTOS.

Todos os sistemas aplicáveis estão configurados com software antivírus aprovados pela equipe de Segurança da Informação e pelo departamento de TI. A solução antivírus é capaz de detectar, remover e proteger contra todos os tipos de software malicioso, como vírus, *trojans*, *worms*, *spyware*, *adware* e *rootkits*. O software está configurado para receber atualizações automáticas, realizar varreduras periódicas, registrar eventos relacionados a vírus em um sistema central de registros, e os usuários finais não têm permissão para configurar ou desativar o software antivírus.

9.4. Plano e procedimento de detecção e notificação de incidentes

A detecção e resposta a incidentes, especialmente relacionados a sistemas críticos, devem estar em conformidade com esta política e com as políticas de segurança da informação estabelecidas pelo departamento de TI.

Todos os colaboradores devem estar cientes de suas responsabilidades na detecção de incidentes de segurança para facilitar a implementação dos planos e procedimentos de resposta a incidentes. É responsabilidade de todos os colaboradores auxiliar nos procedimentos de resposta a incidentes dentro de suas áreas específicas de atuação. Alguns exemplos de incidentes de segurança que os colaboradores podem identificar em suas atividades cotidianas incluem, entre outros:

- Incidentes de segurança física, como roubo, danos ou acesso não autorizado (por exemplo: *logins* não autorizados, objetos desaparecidos de estações de trabalho, violação de cadeados, falta de registros de log, alertas de segurança por parte da equipe de segurança, evidência em vídeo de invasões ou acessos não autorizados não programados).
- Atos fraudulentos que resultem em informações imprecisas em bases de dados, registros em logs, arquivos ou documentos impressos.

- Comportamento anormal do sistema, como reinicializações não programadas, mensagens inesperadas, erros não usuais em registros de log do sistema ou terminais.
- Notificações relacionadas a eventos de segurança, como alertas de integridade de arquivos, detecção de intrusos e alarmes de segurança física.

Todos os colaboradores, não importando suas funções, devem ser conscientizados sobre os sinais de possíveis incidentes e saber a quem relatar nesses casos.

9.4.1. Procedimentos de notificação e reporte de incidentes

O departamento de TI deve ser imediatamente informado de qualquer incidente real ou suspeito envolvendo os ativos de informática da Pão e Arte Alimentos, especialmente sistemas críticos. Exceto pelos passos descritos a seguir, é essencial que qualquer ação investigativa ou corretiva seja realizada apenas pela equipe TI ou sob sua supervisão, a fim de garantir a integridade do processo de investigação e recuperação de incidentes. Quando confrontado com uma situação potencial, siga estas diretrizes:

- Preserve as evidências. Se o incidente envolver um sistema informático comprometido, não altere o estado do sistema. Siga estas instruções:
 - a) Não desligue o computador ou tente reiniciá-lo.
 - b) Desconecte imediatamente o computador da rede, desconectando o cabo de rede ou desligando o Wi-Fi do computador.
 - c) O computador deve permanecer ligado, e todos os programas em execução devem ser mantidos ativos.
 - d) Não faça nenhuma alteração no estado do equipamento.

Essas medidas ajudarão a preservar as evidências e facilitarão a investigação do incidente de segurança.

- Reporte o incidente de segurança e entre em contato com o departamento de TI sobre qualquer incidente real ou suspeito. É importante não comunicar detalhes ou circunstâncias a ninguém além de sua chefia imediata ou o departamento de TI. Toda comunicação com as autoridades legais ou o público será coordenada pela Segurança da Informação.

Essa abordagem ajuda a garantir a confidencialidade e a integridade das investigações de segurança.

- Documente qualquer informação que você tenha conhecimento enquanto aguarda a resposta do departamento de TI ao incidente. Isso deve incluir a data,

hora e a natureza do incidente, sempre que possível. Qualquer informação que você possa fornecer será útil na determinação da resposta apropriada.

- Se você identificar qualquer tipo de incidente, é necessário enviá-lo ao responsável pela equipe de Segurança da Informação (responsável por TI) e ao Encarregado de Dados. Isso é fundamental para que a empresa possa tomar as medidas adequadas para lidar com o incidente e cumprir com suas obrigações legais relacionadas à LGPD.

9.4.2. Gestão de mudanças

Todas as alterações ou modificações relacionadas ao processamento de dados e à segurança da informação, incluindo testes de todas as regras configuradas nos dispositivos de segurança (como firewall, roteador e switch), contratação e aditivos, devem seguir um processo formalizado e documentado. Antes que tais alterações sejam efetivamente implementadas, elas devem ser submetidas à diretoria da Pão e Arte Alimentos e comunicadas ao DPO (Encarregado de Dados) com antecedência. Essa comunicação deve ser registrada, formalizada e devidamente justificada. Esse procedimento visa evitar qualquer impacto negativo no cumprimento dos direitos dos titulares de dados, garantindo sempre a privacidade e confidencialidade das informações.

9.4.2. Classificação da gravidade do incidente

O departamento de TI, em primeiro lugar, buscará avaliar se o incidente de segurança requer uma resposta formal. Caso o incidente de segurança não exija uma resposta formal, a situação será encaminhada para a área de TI apropriada, garantindo assim que todos os serviços de suporte tecnológico necessários sejam disponibilizados. As seguintes descrições serão utilizadas para determinar qual curso de ação o departamento de TI deve seguir:

- **Nível 1:** Uma ocorrência de atividade potencialmente não amigável (por exemplo, Finger, telnet não autorizada, port scan, detecção de vírus corrigida, pico de desempenho inesperado etc.).
- **Nível 2:** Ocorrência de uma tentativa clara de obtenção de informação ou acesso não autorizado (por exemplo, tentativa de download de arquivos de senhas protegidas, acesso a áreas restritas, contaminação por vírus bem-sucedida em um sistema não crítico, varredura de vulnerabilidade não autorizada, etc.) ou uma segunda ocorrência de ataque de Nível 1.
- **Nível 3:** Tentativa séria ou violação real da segurança (por exemplo, ataque *multi-prong*, recusa de tentativa de serviço, infecção por vírus de um sistema ou

rede críticos, *buffer/stack overflow* bem-sucedidos, acesso não autorizado bem-sucedido a informações ou sistemas críticos ou sensíveis, quebra de cadeado, roubo de papéis, etc.) ou um segundo ataque de Nível 2.

Qualquer incidente de Nível 1 verificado em sistemas que armazenem informações confidenciais ou sensíveis ou que se originem em sistemas internos não autorizados será classificado como Nível 2.

9.5. Resposta a incidentes

As ações a serem tomadas pelo departamento de TI após a identificação e classificação do incidente incluem: Identificação, Classificação de Severidade, Contenção, Erradicação, Recuperação, Análise de Causa Raiz e Aprimoramento dos Controles de Segurança.

Nível 1 – Conter e Monitorar:

- Registrar informações sobre o invasor, como usuário, endereço de IP e domínio, sempre que possível.
- Usar controles tecnológicos aprovados para bloquear temporariamente ou permanentemente o acesso do invasor.
- Manter vigilância contínua contra possíveis tentativas futuras de invasão por parte deste usuário ou endereço de IP.

Nível 2 – Conter, Monitorar e Alertar:

- Coletar e proteger as informações relacionadas à intrusão.
- Utilizar controles tecnológicos aprovados para bloquear temporariamente ou permanentemente o acesso do invasor.
- Investigar a origem da conexão.
- Entrar em contato com o Provedor de Serviço de Internet (ISP) para obter mais informações sobre a tentativa de invasão e o invasor.
- Avaliar os riscos potenciais associados ao método de invasão utilizado.
- Reavaliar a classificação do incidente para um nível mais elevado, se necessário, e aplicar medidas de contenção, erradicação e recuperação conforme descrito para incidentes de Nível 3.
- Após a identificação, notificar o usuário malicioso de que suas ações foram identificadas e adverti-lo sobre possíveis consequências futuras em caso de reincidência.
- Se um colaborador for identificado como o usuário malicioso, a administração deve trabalhar em conjunto com o departamento de Gestão de Pessoas (DP, RH e

Recrutamento) e a Segurança da Informação para tratar adequadamente a violação das normas de uso aceitável.

Nível 3 - Conter, Erradicar, Recuperar e Executar Análise de Causa Raiz:

- Implementar medidas para conter a intrusão imediatamente. Isso pode envolver desconectar cabos de rede, aplicar listas de controle de acesso (ACLs) altamente restritivas, desativar ou isolar portas de switch, redefinir senhas de usuário, entre outras ações.
- Coletar e proteger as informações relacionadas à intrusão de maneira *offline* para fins de investigação e evidência.
- Se necessário, envolver especialistas forenses em colaboração com o departamento jurídico e Gestão de Pessoas para conduzir uma investigação forense adequada.
- Notificar a alta direção sobre a situação e manter uma comunicação contínua sobre os desenvolvimentos subsequentes.
- Eliminar quaisquer meios de acesso utilizados pelo invasor e abordar quaisquer vulnerabilidades identificadas.
- Investigar a origem da conexão.
- Entrar em contato com o Encarregado de Dados (DPO) para obter informações adicionais sobre a tentativa e o invasor, lembrando-lhe de sua responsabilidade de assistência nessa questão.
- Avaliar os riscos potenciais associados ou os danos causados pelo método de intrusão utilizado.

9.6. Notificações automáticas de segurança dos sistemas

Qualquer sistema automático de detecção de intrusão dentro do ambiente da Pão e Arte Alimentos, incluindo sensores de detecção de intrusão e sistemas de verificação de integridade, será configurado para notificar automaticamente o departamento de TI sobre qualquer comprometimento potencial ou ataque. Adicionalmente, qualquer detecção automática ou manual de pontos de acesso sem fio não autorizados deve acionar o Plano de Resposta a Incidentes.

10. POLÍTICA DE INTEGRIDADE

PARÁGRAFO PRIMEIRO:

Os colaboradores declaram expressamente que estão plenamente conscientes, possuem conhecimento detalhado, compreendem e estão comprometidos em seguir rigorosamente, no desempenho de suas atividades, toda a legislação anticorrupção que lhes seja aplicável. Isso inclui, mas não se limita, à Lei nº 12.846/2013 e ao Decreto nº 8.420/2015, bem como a qualquer outra regulamentação relacionada à prevenção de suborno ou corrupção.

Adicionalmente, os colaboradores reconhecem a existência das políticas internas da Pão e Arte Alimentos e declaram ter pleno conhecimento das mesmas. Comprometem-se a aderir estritamente a essas políticas, abstendo-se de qualquer atividade que possa constituir uma violação das normas citadas.

Os colaboradores declaram, garantem e concordam de forma inequívoca que, em relação a este Manual, não irão empreender nem tentar qualquer ação que envolva solicitação, exigência, cobrança ou obtenção, seja para si próprios ou para terceiros, de vantagens indevidas ou promessas de vantagens indevidas com o propósito de influenciar decisões tomadas por agentes públicos e/ou privados. Além disso, afirmam categoricamente que não ofereceram, pagaram, doaram ou prometeram direta ou indiretamente qualquer benefício, taxa, dinheiro ou qualquer outro objeto de valor a terceiros.

PARÁGRAFO SEGUNDO:

Os colaboradores também se comprometem a aderir a todas as leis anticorrupção aplicáveis e garantem que não irão, em decorrência deste Manual ou de quaisquer outras transações comerciais, transferir quaisquer ativos de valor, seja de maneira direta ou indireta, a indivíduos do setor privado, funcionários do governo ou de empresas controladas pelo governo, com o propósito de obter ou manter vantagens ou benefícios indevidos. Os colaboradores asseguram que nenhum pagamento realizado será utilizado como forma de compensação ou de qualquer outra maneira para oferecer vantagens ou benefícios em desacordo com a legislação vigente.

PARÁGRAFO TERCEIRO:

Os colaboradores declaram e garantem que não se encontram, de nenhuma forma e sob nenhuma circunstância, direta ou indiretamente: (I) sob investigação em virtude de denúncias de suborno e/ou corrupção; (II) envolvidos em processos judiciais e/ou administrativos em andamento, ou que tenham sido condenados ou acusados sob alegações de corrupção ou suborno; (III) listados em registros de entidades governamentais, tampouco são conhecidos ou suspeitos de envolvimento em práticas de terrorismo e/ou lavagem de dinheiro; (IV) sujeitos a restrições ou sanções econômicas e comerciais impostas por qualquer entidade governamental; e (V) proibidos ou impedidos de acordo com qualquer legislação regulada ou fiscalizada por qualquer entidade governamental.

Os colaboradores comprometem-se a comunicar imediatamente, por escrito, à Pão e Arte Alimentos sobre o recebimento de qualquer notificação de qualquer entidade governamental - seja ela parte dos Poderes Executivo, Legislativo ou Judiciário, bem como de órgãos da administração pública direta ou indireta - relacionada a fatos ou investigações relacionados a atos de corrupção, suspeitas ou violações das leis anticorrupção, bem como envolvimento em práticas de suborno ou corrupção. Além disso, comprometem-se a

informar a Pão e Arte Alimentos sobre qualquer descumprimento das declarações contidas nesta cláusula.

O não cumprimento de qualquer regulamentação anticorrupção aplicável por parte dos colaboradores será considerado uma infração grave e dará à Pão e Arte Alimentos o direito de rescindir imediatamente o contrato. Nesse caso, os colaboradores estarão obrigados a isentar a Pão e Arte Alimentos de qualquer ação legal, perdas e danos resultantes do referido descumprimento.

Adicionalmente, os colaboradores serão responsáveis por indenizar a Pão e Arte Alimentos por quaisquer prejuízos que esta venha a incorrer devido ao não cumprimento das obrigações e declarações estabelecidas nesta cláusula.

11. POLÍTICA DE "BRING YOUR OWN DEVICE" (BYOD)

A Política de BYOD (*Bring Your Own Device*) estabelece as diretrizes e procedimentos relacionados ao uso de dispositivos pessoais dos colaboradores para fins de trabalho na Pão e Arte Alimentos. Esta política visa equilibrar a conveniência e a flexibilidade do BYOD com a necessidade de manter a segurança e a integridade dos dados da empresa. **Os colaboradores que optarem por utilizar seus próprios dispositivos pessoais para fins profissionais devem aderir às seguintes diretrizes:**

- **Responsabilidade pelo Equipamento:** O proprietário do dispositivo é completamente responsável por manter e proteger seu próprio equipamento.
- **Responsabilidade pelo Conteúdo:** Qualquer conteúdo armazenado no dispositivo é de responsabilidade exclusiva do proprietário.
- **Licenças de Software:** O proprietário declara que todos os softwares instalados no dispositivo possuem licenças válidas e em conformidade com as leis de direitos autorais, e se compromete a responder individualmente por qualquer violação de licença.
- **Requisitos Mínimos de Segurança:** O proprietário se compromete a adotar medidas de segurança mínimas, que podem incluir a instalação e atualização regular de antivírus, antispymware, o uso de senhas de bloqueio e a criptografia de dados, conforme exigido pela política de BYOD da empresa.
- **Uso Temporário e Não Oneroso:** O dispositivo é fornecido à empresa em caráter temporário e parcial, sem a cobrança de qualquer taxa ou custo associado ao uso do dispositivo. A empresa não assume qualquer responsabilidade pelo equipamento.
- **Não Responsabilidade por Danos ou Perda:** A empresa não se responsabiliza por perdas, danos, furto, extravio ou quebras do equipamento pessoal do proprietário durante o uso no ambiente de trabalho.

- **Portabilidade Discreta e Zelo:** O proprietário compromete-se a portar o equipamento de forma discreta e com o máximo de cuidado possível, a fim de evitar incidentes e vazamentos de informações da empresa.
- **Acesso e Uso Voluntário:** O mero acesso ou uso do equipamento ou recursos de informação por parte do proprietário não implica em sobreaviso ou sobre jornada. É considerado um ato voluntário, de livre escolha e iniciativa do próprio proprietário.
- **Uso de Dados Empresariais:** O equipamento pessoal não deve ser utilizado para coleta, tratamento ou armazenamento de quaisquer dados pertencentes à Pão e Arte Alimentos para fins profissionais sem prévia autorização. Qualquer utilização do equipamento pessoal para fins profissionais deve ser comunicada à equipe de TI para garantir a conformidade com as políticas de segurança e privacidade da empresa.

12. CLASSIFICAÇÃO DA INFORMAÇÃO E DOS ATIVOS

Avaliamos as informações e ativos de acordo com seu valor, obrigações legais, grau de sensibilidade e importância para evitar qualquer alteração ou divulgação não autorizada. Nesse contexto, classificamos os ativos em três categorias: Públicos, Internos e Confidenciais.

A diretoria, com orientação e suporte da equipe de Segurança da Informação (departamento de TI), liderada pelo Encarregado de Dados - *Data Protection Officer* (DPO) da Pão e Arte Alimentos, juntamente com os coordenadores de cada área, nomeia os responsáveis, custodiantes e usuários das informações de acordo com essa classificação.

Para cada tipo de ativo (público, interno ou confidencial), a Pão e Arte Alimentos possui critérios específicos para seu armazenamento, backup, transmissão e descarte seguro, tanto para informações em formato impresso quanto eletrônico, abrangendo todo o ciclo de vida das informações.

13. APROVAÇÃO

Esta seção tem como objetivo oficializar a aprovação do Relatório de Impacto à Proteção de Dados (RIPD) por meio da obtenção das assinaturas do Responsável pela Elaboração do RIPD, do Encarregado de Dados e dos profissionais que representam a empresa.

O RIPD deve passar por revisão e atualização anualmente ou sempre que houver qualquer alteração que afete o tratamento de dados pessoais realizado pela instituição.

1ª Versão: 01/02/2021

Elaboração: Paulo Roberto dos Santos Jr (Encarregado)

Revisão: Wagner Luiz da Cruz Silva (DP) Elisabete Beatriz Tschope (RH)

Aprovação: Erica Comelli Ferreira Manoel