NOME: Procedimento Interno LGPD			
No. DO DOCUMENTO	**PROCPAR-00001**	**No. DA REVISÃO**	**B**
DATA EMISSÃO	25/02/2025	**DATA DA REVISÃO**	03/03/2025
RESPONSABILIDADES: Levi Rodrigues da Silva			
EMISSÃO/REVISÃO	Levi Silva	**APROVAÇÃO**	LEVI

Objetivo

O compartilhamento de dados na empresa tem por objetivo seguir as diretrizes estabelecidas nos protocolos da segurança da informação e comunicações e na Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Este Procedimento tem os seguintes objetivos:

- Apresentar as necessidades de adequação trazidas pela Lei Geral de Proteção de Dados Pessoais na ENGLEVI;
- Orientar seus funcionários quanto às suas responsabilidades na condução ou manipulação dos dados pessoais pela sua equipe;
- Fomentar a importância da mudança cultural em relação à proteção de dados pessoais;
- Incutir nos colaboradores e terceirizados a autorresponsabilidade no quesito da proteção e tratamento de dados pessoais;
- Promover a conscientização contínua acerca da importância da proteção de dados pessoais e segurança da informação.

Escopo

Este Procedimento se aplica a todos que possuem qualquer contato com um dado pessoal, seja seu ou de outra pessoa, não importando se é pessoa física ou jurídica, de direito privado ou público, dentro do ENGLEVI.

Definições

LGPD – Lei Geral de Proteção de Dados
ANPD - Autoridade Nacional de Proteção de Dados
RIPD - Relatório de Impacto à Proteção dos Dados Pessoais
ABNT - Associação Brasileira de Normas Técnicas
ISO - International Organization for Standardization
IEC - International Electrotechnical Commission
NBR - Norma Brasileira (NBR)
CONARQ - Conselho Nacional de Arquivos
SINAR - do Sistema Nacional de Arquivos

Procedimento

A adequação à LGPD passa por compreender como é feito o tratamento de dados e buscar adequá-lo considerando as exigências legais e o contexto da organização.
A Lei Geral de Proteção de Dados, conhecida como LGPD, está em vigor desde setembro de 2020. O intuito dessa norma é garantir que instituições nacionais e entidades estrangeiras com sede no país tenham mais cuidado ao manipular os dados pessoais. A partir do ano de 2023, as empresas que não estiverem em conformidade com esses princípios estarão sujeitas a avisos e sanções, como multa simples (2% faturamento até R$ 50 milhões), multa diária, publicação da infração de não conformidade com a LGPD, Bloqueio, eliminação ou suspensão por até seis meses dos dados pessoais envolvidos e Limitação parcial ou total das atividades relacionadas ao manuseio de dados.

1. Direito dos Titulares

Os direitos dos titulares dos dados são sua liberdade de atuação nas informações, ter intimidade e privacidade deles, acesso total,

confirmação do método de tratamento, correção de dados incompletos, inexatos ou desatualizados, direito a anonimização, bloqueio ou eliminação, direitos a portabilidade ou compartilhamento, eliminação, revogação e decisões de revisão automatizadas, formas de solicitação, prazos para atendimento dos direitos e respostas.
Todos os direitos e os artigos da referência legislativa estão na tabela do documento em anexo "Guia_LGPD".

2. Confirmação da existência de tratamento

Quando pensamos em tratamento de dados, normalmente temos como referência as atividades mais evidentes, como a coleta e o uso do dado, mas tratamento é muito mais amplo, inclui qualquer operação que envolva dados pessoais, em todo o seu ciclo de vida, da coleta ao descarte.
Detalhar a origem dos dados, os critérios usados, a finalidade e como esse tratamento é feito, define o tratamento de dados.

3. Base Legal de Tratamento

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois "agentes de tratamento", o Controlador e o Operador.

3.1. Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, tais como as finalidades e os meios do tratamento (art. 5º, VI).

3.2. Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII), aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada

pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

3.3. Encarregado ou DPO (Data Protection Officer)outra figura essencial para o adequado cumprimento da LGPD é o "Encarregado", definido pelo art. 5º, VIII, como a 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).

O ônus da prova do consentimento cabe ao controlador, sendo proibido o tratamento de dados pessoais mediante vício de consentimento, que de acordo com o Código Civil de 2002, são: erro ou ignorância, dolo, coação, lesão, estado de perigo. O erro consiste em falsa ideia da realidade, do real estado ou situação das coisas. A pessoa supõe que é uma coisa, mas na verdade se trata de outra, podendo tornar o negócio anulável.

4. Topologia de Dados Pessoais

4.1. Dado Pessoal: Uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, então ela é considerada um dado pessoal, como nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde,
cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros.
Antes de solicitar os dados pessoais, checar no contrato ou ferramenta necessária a ser usado, quais dados pessoais serão utilizados e então pedir e explicar ao cliente a importância de informar estes dados e não apenas a confiança em utilizar bem e cuidar destas informações como mostrar as formas de segurança delas no armazenamento.

4.2. Dado pessoal sensível: conceito de dado pessoal trazido pela Lei 12.527/2011 e evoluiu sobre o conceito de informação sensível (Art. 5°, II) dados sensíveis são relativos à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Portanto deve ter mais cautela.

4.3. Dados impessoais: que são informações que não permitem a identificação direta ou indireta de um indivíduo que esteja vivo. Em outras palavras, são informações que não permitem a identificação de uma pessoa específica. Por exemplo, dados como a temperatura média de uma cidade, o número de visitantes de um site, ou a quantidade de vendas de um produto em um determinado período são considerados dados impessoais.

4.4. Dados Qualitativos: são informações que não podem ser medidas numericamente, como por exemplo, a cor dos olhos de uma pessoa, o sabor de um alimento, ou a opinião sobre um determinado assunto. Eles podem ser classificados em duas categorias: nominais e ordinais. Os dados nominais são informações que não possuem uma ordem natural, como por exemplo, o nome de uma pessoa ou a cor de um carro. Já os dados ordinais são informações que possuem uma ordem natural, como por exemplo, a classificação de um filme ou a posição de chegada de um atleta em uma corrida.

4.5. Dados Quantitativos: são informações que podem ser medidas numericamente, como por exemplo, a altura de uma pessoa, o peso de um objeto, ou a quantidade de vendas de um produto. Eles podem ser classificados em duas categorias: discretos e contínuos. Os dados discretos são informações que podem ser contadas e que possuem um valor inteiro, como por exemplo, o número de filhos de uma família ou o número de carros em uma garagem. Já os dados contínuos são informações que podem ser medidas em uma escala contínua, como

por exemplo, a temperatura de um ambiente ou o tempo que uma pessoa leva para completar uma tarefa.

4.6. Dados de processo: é um conjunto sequencial e particular de ações com objetivo comum.

Processos podem ter os mais variados propósitos, como criar, inventar, projetar, transformar, produzir, controlar, manter e usar produtos ou sistemas. No âmbito do direito, um processo pode ser uma ação judicial, a sequência de atos predefinidos de acordo com a lei, com o objetivo de alcançar um resultado com relevância jurídica.

4.7. Dados de empresa jurídica: é o Cadastro Nacional de Pessoas Jurídicas, um número de identificação fiscal atribuído a empresas e outras entidades jurídicas no Brasil. O CNPJ é gerenciado pela Receita Federal do Brasil e é usado para fins fiscais, contábeis e administrativos.

4.8. Dados de Tecnologia: é um conjunto de técnicas, habilidades, métodos e processos usados na produção de bens ou serviços, ou na realização de objetivos, como em investigações científicas. A tecnologia está presente em diversos aspectos da nossa vida, desde a comunicação, a energia, a educação, a saúde, a segurança, até o entretenimento e a cultura.

5. Tratamento de dados

O tratamento de dados envolve qualquer operação relacionada a dados pessoais.

As operações envolvidas são:

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

Armazenamento: ação ou resultado de manter ou conservar em repositório um dado;

ARQUIVAMENTO: ato ou efeito de manter registrado um dado em qualquer

das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

AVALIAÇÃO: analisar o dado com o objetivo de produzir informação;

CLASSIFICAÇÃO: maneira de ordenar os dados conforme algum critério estabelecido;

COLETA: recolhimento de dados com finalidade específica;

COMUNICAÇÃO: transmitir informações pertinentes a políticas de ação sobre os dados;

CONTROLE: ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

DIFUSÃO: ato ou efeito de divulgação, propagação, multiplicação dos dados;

DISTRIBUIÇÃO: ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

ELIMINAÇÃO: ato ou efeito de excluir ou destruir dado do repositório;

EXTRAÇÃO: ato de copiar ou retirar dados do repositório em que se encontrava;

MODIFICAÇÃO: ato ou efeito de alteração do dado;

PROCESSAMENTO: ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

PRODUÇÃO: criação de bens e de serviços a partir do tratamento de dados;

RECEPÇÃO: ato de receber os dados ao final da transmissão;

REPRODUÇÃO: cópia de dado preexistente obtido por meio de qualquer processo;

TRANSFERÊNCIA: mudança de dados de uma área de armazenamento para outra, ou para terceiro;

TRANSMISSÃO: movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

UTILIZAÇÃO: ato ou efeito do aproveitamento dos dados.

Exemplos de dados pessoais são lista de emails, dados de funcionários e fornecedores, dados biométricos, dados para compra, negociação, cadastro e cookies em sites (coletar e armazenar por exemplo, as páginas que foram visitadas no site, o tempo gasto e o IP do usuário, entre outras informações de navegação).

Finalidade da Operação: A ENGLEVI usará os dados necessários dos titulares para cadastramentos como clientes e fornecedores, fornece as cotações necessárias, realizar contratos de consultoria, realizar produção de bens e serviços e armazenar relatórios de lições aprendidas.

6. Como Realizar o Tratamento de Dados Pessoais

Os dados pessoais sensíveis, cabe destacar que a lei autoriza o tratamento de dados sensíveis apenas em situações indispensáveis. Isso traz para o controlador o ônus da prova da alegada indispensabilidade, e por isso, são sujeitos a proteção mais rígida.
Na medida do possível, ENGLEVI não necessitará destes dados.
As identificações das hipóteses de tratamento, usa-se o "Guia_LGPD" em anexo para esta identificação de hipótese.

6.1. Coleta

A coleta é uma das operações de tratamento referenciadas pelo art. 5º, inciso X da LGPD.
Coletar os dados que serão utilizados nas atividades de contrato, portanto dados pessoais de representantes da empresa, dados da própria empresa e nossos dados pessoais e da nossa empresa.

Antes da fase de contrato, também existe a troca de dados pessoais e da empresa, para cadastramento como fornecedor e cliente, para ser possível emitir nota fiscal correta e os serviços prestados.
A informação continua sendo um bem muito precioso e, portanto, iremos coletar apenas o necessário para os tramites necessários para a negociação.
A forma de coleta de dados será online e através de formulários personalizados para atender as demandas das empresas.

6.2. Anonimização e Pseudonimização

Segundo a LGPD, dado anonimizado é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta. A partir do momento em que o dado é considerado anonimizado, e não permite mais qualquer identificação do seu titular, esse dado sai do escopo da legislação, por não mais se tratar de um dado pessoal, conforme previsto no art. 12 da LGPD.
Pseudonimização é a técnica de tratar dados pessoais de uma forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos, desde que essas informações sejam mantidas em ambiente separado, controlado e seguro. A título ilustrativo, criptografia é um método de Pseudonimização, quando os dados somente podem ser atribuídos a um titular mediante o conhecimento da chave criptográfica. Sem conhecer a chave, os dados são ininteligíveis.

6.3. Publicidade

O inciso I do art. 23 da LGPD impõe às pessoas jurídicas de direito público obrigações de transparência ativa. Isto é, de publicar informações sobre os tratamentos de dados pessoais por elas realizados em seus sítios eletrônicos de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos.

6.4. Relatório de Impacto à Proteção de Dados Pessoais

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

A ENGLEVI usará como sugestão o modelo de elaborar o RIPD do anexo "Guia_LGPD" adaptado para cada caso em estudo mas envolvendo os procedimentos da figura 3.

Figura 1 - Criar o RIPD

Apostila GUIA_LGPD – gov.br

Se o titular dos dados concluir junto com a ENGLEVI que deve existir um RIPD, templates já usados pelo titular pode ser usado ou criar-se templates e necessidades específicos para o titular com sua aprovação.

6.5. Término do Tratamento

Nos termos da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

a) Exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;
b) Fim do período de tratamento;
c) Revogação do consentimento ou a pedido do titular, resguardado o interesse público;
d) Determinação da autoridade nacional em face de violação do disposto na Lei.

Na incidência de qualquer uma das hipóteses acima, a Lei determina que os dados sejam eliminados, a não ser nos casos em que:

a1) Remanesça o cumprimento de obrigação legal ou regulatória pelo controlador;
a2) Sejam necessários para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;
a3) Ocorra a transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em Lei;
a4) GUIA DE BOAS PRÁTICAS - LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) 43 (iv) seja utilizado exclusivamente pelo controlador, vedado seu acesso por terceiro, e desde que anonimizados.

7. Ciclo de Vida dos dados Pessoais

O dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados (LGPD, art. 18, IV), ao cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (LGPD, art. 52, VI) ou ao término de seu tratamento (LGPD, art. 16).
A configuração de um ciclo que se inicia com a coleta e que determina a "vida" (existência) do dado pessoal durante um período, de acordo com

certos critérios de eliminação.

Existem algumas fases de acordo com o "Guia_LGPD".

A LGPD considera como tratamento toda operação realizada com os dados pessoais, como as que se referem 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.

Nesse cenário, o ciclo de vida do tratamento tem início com a coleta do dado e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento definidas na LGPD.

A figura a seguir sintetiza as fases do ciclo de vida do tratamento de dados pessoais:

Figura 2 - Ciclo de vida do tratamento dos dados pessoais

Apostila *GUIA_LGPD – gov.br*

Coleta: Obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.).

Retenção: Arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc.).

Os dados são armazenados em nuvem, com senha para acesso deles, sendo que somente os engenheiros responsáveis, por manipulá-los durante o desenvolvimento do projeto, possuem a senha para acessá-los.

Figura 3 - Armazenamento na nuvem

Internet

Processamento: Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

Compartilhamento: Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.

Eliminação: qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

No contexto da gestão de documentos, o ciclo de vida dos documentos de arquivo compreende três fases, a saber: produção, utilização e destinação final (eliminação ou guarda permanente). Em cada uma dessas fases são realizados os procedimentos e operações de gestão de documentos, conforme figura abaixo:

Figura 4 - Ciclo de vida dos documentos de arquivos

Apostila *GUIA_LGPD – gov.br*

Produção: operações referentes à elaboração de documentos em razão da execução das atividades de um órgão ou entidade.
Utilização (uso e manutenção): operações referentes ao fluxo percorrido pelos documentos para o cumprimento de sua função administrativa, assim como de sua guarda, após cessar o seu trâmite.
Destinação final: operações referentes ao ato de decidir quais documentos devem ser eliminados (mediante autorização, conforme legislação vigente), bem como quais documentos devem ser mantidos por razões administrativas, legais ou fiscais. Para tal, envolve as atividades de análise, seleção e fixação de prazos de guarda dos documentos.

7.1. Ativos Organizacionais

É importante identificar quais ativos organizacionais estão envolvidos em cada fase do ciclo de vida do tratamento dos dados pessoais. Os principais ativos são: bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais.

Figura 5 - Ativos envolvidos no ciclo de vida do tratamento de dados

Apostila *GUIA_LGPD – gov.br*

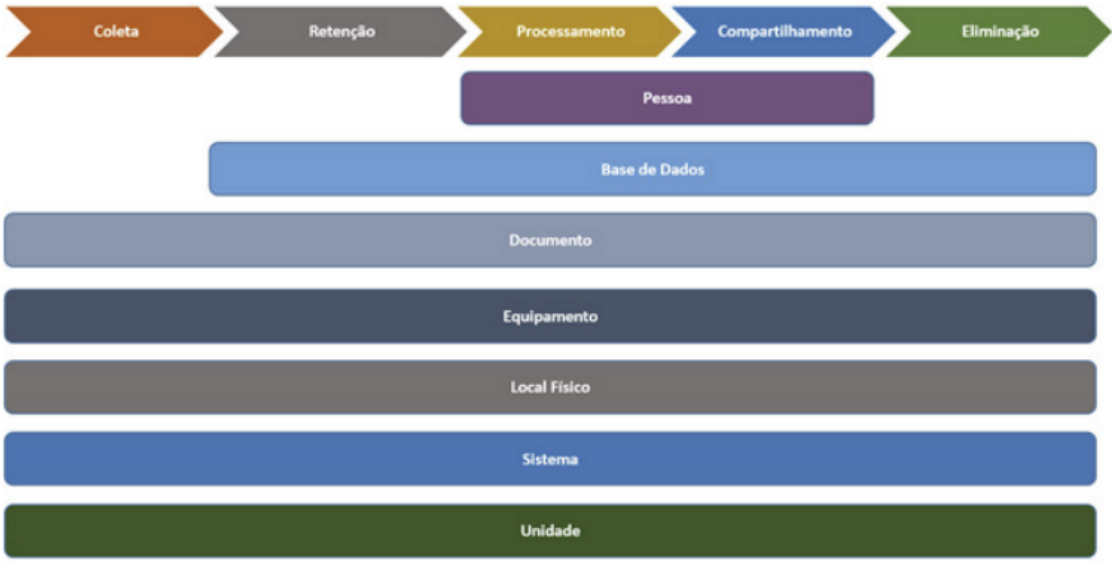
Base de dados: é uma coleção de dados logicamente relacionados, com algum significado. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico.
Documento: unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005).
Equipamento: objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.
Local físico: determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal. Por exemplo, uma sala, um arquivo, um prédio, uma mesa etc.
Pessoa: qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais, como as que se referem 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.
Sistema: qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais.
Unidade organizacional: órgãos e entidades da Administração Pública.

7.2. Relacionamento do Ciclo Vida do Tratamento dos Dados Pessoais com Ativos Organizacionais

Para cada fase do ciclo de tratamento de dados é importante identificar os ativos organizacionais que estarão envolvidos.
Na figura abaixo apresenta o relacionamento entre as fases do ciclo de tratamento de dados pessoais e os ativos que podem ser utilizados em cada etapa. É importante registrar, assim, que existem ativos presentes em todas as fases do ciclo (ex.: Documento) e outros que estarão em

apenas algumas delas (ex.: Pessoa).

Figura 6- Ativos e fases do ciclo de vida dos dados pessoais



Apostila *GUIA_LGPD – gov.br*

8. Boas Práticas em Segurança da Informação

8.1. Privacidade desde a concepção

Os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, pois ambas estão relacionadas. Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas.

Os agentes de tratamento devem implementar medidas adequadas para garantir que, por padrão, apenas serão processados os dados pessoais necessários para cumprimento da(s) finalidade(s) específica(s)

definida(s) pela instituição que desempenha o papel de controlador dos dados pessoais. Essa obrigação de implementação significa que a instituição deve limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Essa medida deve garantir, por exemplo, que nem todos os usuários dos agentes de tratamento tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pela instituição.

Detalhes de as atividades rever o "Guia_LGPD" em anexo a este documento.

8.2. Padrões Frameworks e Controles de Segurança da Informação

É importante ter e seguir um conjunto de documentos para melhorar o gerenciamento de riscos de segurança cibernética. Um framework, por exemplo, apresenta condutas e recomendações para que sejam aplicados princípios e práticas recomendadas de gerenciamento de riscos para melhorar a segurança e a resiliência.

8.2.1. e-ping: A arquitetura e-PING define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral, informações: http://eping.governoeletronico.gov.br/

8.2.2. ABNT NBR ISO/IEC 27001:2013: É uma norma do comitê técnico formado pela ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), aprovada e traduzida pela Associação Brasileira de Normas Técnicas (ABNT) - e

transformada em uma Norma Brasileira (NBR) - de gestão de segurança da informação. São apresentados os requisitos para estabelecer, implementar, manter GUIA DE BOAS PRÁTICAS - LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) 55 e melhorar continuamente um Sistema de gestão da Segurança da Informação (SGSI), **bem como** os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização.

8.2.3. ABNT NBR ISO/IEC 27002: 2013: Estipula melhores práticas para apoiar a implantação do SGSI, com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

8.2.4. ABNT NBR ISO/IEC 27005:2019: Esta norma apresenta diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um SGSI, conforme a NBR ISO/IEC 27001.

8.2.5. ABNT NBR ISO/IEC 31000:2018: É um documento com recomendações para gerenciar riscos enfrentados pelas organizações, podendo ser personalizado para qualquer contexto. A versão do ano de 2018 apresenta um guia mais claro e conciso, com o intuito de ajudar as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

8.2.6. ABNT NBR ISO/IEC 27701:2019: Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Visa a gestão da privacidade no contexto da organização.

8.2.7. CONARQ- Conselho Nacional de Arquivos: é um órgão colegiado, vinculado ao Arquivo Nacional do Ministério da Justiça e Segurança Pública, que tem por finalidade definir a política nacional de arquivos públicos e privados, como órgão central de um Sistema Nacional de Arquivos, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo. No que se refere aos aspectos tecnológicos de gestão arquivísticas de documentos, o CONARQ editou as resoluções indicadas a seguir:

a) Resolução Nº 25, de 27 de abril de 2007: Resolução que dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

b) Resolução Nº 39, de 29 de abril de 2014: Resolução que estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR). [Redação dada pela Resolução nº 43 de 04 de setembro de 2015].

8.2.8. Empresas Especializadas: A ENGLEVI contratam serviços de empresas especializadas a tratarem dados digitais e garantir a segurança deles, como serviços do Google, DocuSign, GoDaddy. Os dados coletados em planilhas de papel, serão digitalizadas e armazenadas com segurança e se necessário for, manter o papel armazenado em cofre ou gaveta trancada com acesso limitado até quando eles perdem o valor de armazenamento e são picotados e eliminados.

9. Responsabilidades

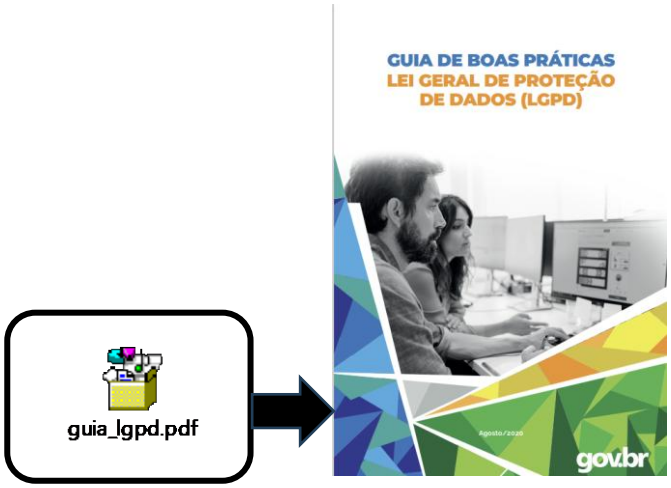
Todo colaborador da ENGLEVI possui a responsabilidade de:

- Prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção);
- Não realizar o tratamento do dado para fins discriminatórios, ilícitos ou abusivos (princípio da não discriminação);
- Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas);
- Garantir que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação).
- Eliminar os documentos físicos após o uso, como, por exemplo, cópias de documentos de clientes, fornecedor ou qualquer colaborador (CPF, RG, CNH, comprovante de residência etc.);
- Fazer revisão periódica dos arquivos que estão no computador para eliminar documentos que foram digitalizados dos clientes, fornecedor ou qualquer colaborador (CPF, RG, CNH, comprovante de residência etc.);
- Cuidar especial dos documentos dos clientes enquadrados como Tarifa Social, além dos documentos de CPF, RG, comprovante de residência, comprovantes de renda e de benefício social;
- Nunca compartilhar arquivos que contenham dados pessoais para terceiros estranhos à atividade da ENGLEVI sem autorização prévia;
- Verificar seus arquivos digitais que contenham dados pessoais dos clientes armazenados em planilhas e eliminá-los;
- Não utilizar rascunhos que contenham dados pessoais; não utilizar ordens de serviço ou registro de atendimento que contenha dados dos clientes como rascunho;

- Na eliminação de documentos físicos, rasgar e picotar antes de jogar no lixo;
- Sempre que um colaborador for remanejado para outra área ou unidade, lembre-se que os acessos de sistemas devem ser revisados;
- Não mantenha contracheques de pagamentos no computador;
- Não utilizar aplicativos de mensagens através de números corporativos ou pessoais para tramitação de arquivos;
- Verificar se há dados armazenados de forma física no ambiente de trabalho e em caso afirmativo, questione: preciso manter esses arquivos? Se positivo, deverá ser discutido com o Controlador de Dados para seu armazenamento em nuvem. Se negativo, eliminá-los;
- Realizar regularmente revisões das permissões de acesso aos dados pessoais que garantam o acesso somente a pessoas que realmente precisam ter acesso;
- Questione: há procedimento na minha unidade para prevenir pessoas que se desliguem da empresa de acesso a dados? Sejam colaboradores terceirizados ou próprios;
- Não descartar documentos contendo dados pessoais em local inapropriado;
- Não deixar documentos que contenham dados pessoais nas máquinas de xerox nem em cima de mesas;
- Não manter no computador lista de clientes, lista de empregados ou lista contendo nomes, endereços e CPF;
- Não guardear atestado médico no computador ou em meio físico.
- Feche sempre seu computador se não estiver próximo dele e sempre mantenha os arquivos com dados na nuvem, assim a empresa estará protegida.

10. Anexos

Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD) – Gov.br



11. Controle das Revisões

Nº da Revisão	Data da Revisão	Conteúdo	Aprovador
A	25/02/2025	Emissão inicial	Levi
B	03/03/2025	Atualização ENGLEVI	Levi