1. OBJETIVO

A presente Política Corporativa, tem como objetivo estabelecer diretrizes que permitam a privacidade dos dados com eficiência, e eficácia, de modo seguro e transparente, garantindo a disponibilidade, integridade, autenticidade, legalidade e sigilo, de forma alinhada aos requisitos legais da LGPD (Lei Geral de Proteção de Dados) e normas internas para a FINDES e suas entidades.

Nesse contexto, esta Política de Privacidade busca explicar de maneira clara e acessível como os dados pessoais poderão ser tratados.

2. ABRANGÊNCIA

Esta Política se aplica a qualquer titular de dados que de alguma forma possua relação com alguma das entidades que compõem a FINDES, ou seja, a própria FINDES, o CINDES, o SESI-ES, o SENAI-ES, o IEL-ES, o IDEIES e o CONEF, denominadas aqui apenas "FINDES", bem como a usuários do site "www. https://findes.com.br/" e dos sites específicos das demais entidades, clientes, parceiros, candidato (a) de processos seletivos, prestadores de serviço, representantes legais de empresas parceiras, contratantes ou contratadas, empregados, colaboradores, dentre outros.

3. DOCUMENTOS COMPLEMENTARES

- Lei nº 13.709/2018 – LGPD - Lei Geral de Proteção de Dados.
- Lei nº 12.527/2011 de Acesso à Informação (LAI).
- Lei nº 12.965/2014 - Marco Civil da Internet.
- ABNT NBR ISO/IEC 27001 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
- ABNT NBR ISO/IEC 27002 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ABNT NBR ISO/IEC 27701 – Tecnologia da Informação – Técnicas de segurança – gestão da privacidade da informação — Requisitos e diretrizes.
- Código de Ética e Conduta da FINDES.
- POL-FINDES-008 - Gestão de Consequências e Medidas Disciplinares.
- POL-FINDES-005 - Política de Segurança da Informação.
- NOR-FINDES-025 - Uso dos Recursos de Tecnologia da Informação e Comunicação.
- NOR-FINDES-037 – Gestão de documentos.
- Política de Privacidade Externa.
- PRO-GETI-001 - Procedimento de Descarte de Mídia
- PRO-GETI - Procedimento de incidentes de segurança.
- PRO-GECOMP - Plano de Resposta a incidentes com dados pessoais.
- PRO-GECOMP – Procedimento de Plano de Resposta a Incidentes
- PRO-GECOMP-007 – Inventário de dados (revisar e elaborar processos).

4. DEFINIÇÕES

Para a compreensão deste documento adotam-se os seguintes termos e definições:

- **Consentimento**: Manifestação livre, informada e inequívoca pela qual o (a) titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do (a) titular.
- **Dado pessoal:** Qualquer informação relativa a uma pessoa singular identificada ou identificável, que pode ser identificada, direta ou indiretamente, por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line ou a um ou mais fatores específicos a identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.
- **Dado pessoal sensível:** Todo Dado Pessoal que pode gerar qualquer tipo de discriminação, como por exemplo os dados sobre 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.
- **Anonimização:** É o processo pelo qual as informações pessoais relativas aos indivíduos se tornam não identificáveis, considerando-se a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu processamento. Dado anonimizado não é considerado Dado Pessoal.
- **Pseudoanonimização:** É um processo pelo qual os Dados Pessoais não mais se relacionam diretamente com uma pessoa identificável (por exemplo, mencionando seu nome), mas não é anônimo, porque ainda é possível, com informações adicionais, que são mantidas separadamente, identificar uma pessoa;
- **Incidente de segurança da informação com dados pessoais:** É qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.
- **Informação:** Conjunto de dados, imagens, textos e quaisquer outras formas de representação, dotadas de significado dentro de um contexto.
- **LGPD:** Lei Geral de Proteção de Dados. Legislação brasileira nº 13.709/2018, comumente conhecida como Lei Geral de Proteção de Dados Pessoais, que regula as atividades de Tratamento de Dados Pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.
- **Titular de Dados**: Pessoa natural singular identificada ou identificável a quem se refere um Dado Pessoal específico.
- **Privacidade de dados:** Privacidade de dados é um dos pilares da segurança da informação, cujo foco é proteger a confidencialidade das informações de uma organização e seus clientes, partindo de um tratamento adequado que capacite a organização a cumprir com as normas vigentes.
- **Encarregado de Proteção de Dados ou Data Protection Officer ("DPO"):** O indivíduo designado como encarregado formal/oficial de proteção de dados, conforme previsto nas leis de proteção de dados, tais como GDPR e LGPD, para um determinado território. O DPO pode ser um integrante ou uma pessoa terceirizada.
- **Tratamento de Dados Pessoais ou Tratamento:** Qualquer operação ou conjunto de operações efetuadas sobre Dados Pessoais ou sobre conjuntos de Dados Pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a

recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o pagamento ou a destruição do dado.

- **Terceiro ou Parceiro:** Qualquer pessoa, física ou jurídica, que atue em nome, no interesse ou para o benefício da Findes, preste serviços ou forneça outros bens, assim como Parceiros comerciais que prestem serviços à Findes, diretamente relacionados à obtenção, retenção ou facilitação de negócios, ou para a condução de assuntos da Findes, incluindo, sem limitação, quaisquer distribuidores, agentes, corretores, despachantes, intermediários, Parceiros de cadeia de suprimentos, consultores, revendedores, contratados e outros prestadores de serviços profissionais.
- **Segurança da Informação:** Área responsável por proteger a integridade, disponibilidade e confidencialidade dos sistemas de TI e deve implementar as medidas adequadas para alcançar este objetivo, sendo o apoio técnico do Líder de Privacidade Corporativo e responsável pelas questões relacionadas às medidas técnicas e administrativas.

5. DIRETRIZES GERAIS

Toda informação gerada ou de responsabilidade da FINDES e suas entidades deve ser preservada de acordo com a necessidade de serviço ou determinação legal. Assim sendo, os usuários devem adotar comportamento seguro e consciente, com o objetivo de preservar e proteger as informações de propriedade e/ou responsabilidade das entidades, com destaque para as diretrizes abaixo:

- Não divulgar informações privilegiadas e/ou sigilosas sem autorização prévia;
- Evitar modificação, despersonalização ou perda da informação;
- Evitar o descarte inseguro das informações;
- Não armazenar, transmitir ou compartilhar conteúdo indevido ou ilegal nos ativos de propriedade e/ou responsabilidade das entidades;
- Obter o consentimento, quando necessário, para o tratamento de dados pessoais;
- Cumprir as normas, recomendações, orientações de segurança da informação e prevenção de incidentes de segurança da informação publicadas pelas entidades;
- Comunicar ao encarregado do tratamento de dados pessoais qualquer evento que possa colocar em risco os dados pessoais tratados pela FINDES e suas entidades;
- As informações geradas, acessadas, manuseadas, armazenadas ou descartadas pelos dirigentes, colaboradores e terceiros no exercício de suas atividades profissionais com as entidades da FINDES, bem como os demais recursos tangíveis e intangíveis disponibilizados pela instituição a esses atores, são de propriedade exclusiva das entidades e devem ser empregadas exclusivamente em atividades de interesse institucional.

5.1. PROTEÇÃO DE DADOS PESSOAIS

Para fins desta Política, considera-se a Proteção de Dados Pessoais como uma combinação de dois pilares:

- Segurança da Informação
- Privacidade de Dados

A Privacidade de dados tratada nesta política, refere-se onde são definidos os procedimentos que disciplinam o tratamento dos dados pessoais, como a coleta, retenção, processamento, compartilhamento e eliminação. Já a Segurança da informação é tratada na Política de Segurança da Informação, onde são definidos a mecanismos de preservação da integridade dos dados, seja por meio de ferramentas e procedimentos que garantam que o dado esteja em segurança.

A disciplina da proteção de dados pessoais, segundo a LGPD, tem como fundamentos:

I - O respeito à privacidade;
II - A autodeterminação informativa;
III - A liberdade de expressão, de informação, de comunicação e de opinião;
IV - A inviolabilidade da intimidade, da honra e da imagem;
V - O desenvolvimento econômico e tecnológico e a inovação;
VI - A livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A figura a seguir, ilustra como a segurança da informação em conjunto com a privacidade dos dados convergem no sentido de promover a proteção total dos dados pessoais.

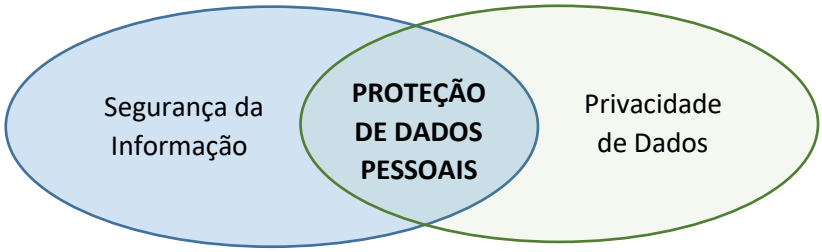

Figura 1: Conversão da Proteção de dados pessoais

5.1.1 Princípios da Proteção de Dados Pessoais

Para o uso adequado dos dados pessoais é necessário que o seu tratamento observe os seus princípios, em especial na coleta, armazenamento, compartilhamento interno e compartilhamento externo, para estar em conformidade com a legislação vigente sobre proteção de dados pessoais.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

- **Princípio da finalidade**: Realizar somente o tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. É vedado o tratamento para outras finalidades e fins discriminatórios ilícitos ou abusivos;
- **Princípio da Adequação:** O tratamento dos dados deve ser compatível com as finalidades informadas ao titular (Cliente, fornecedor, parceiro, colaborador, entre outros);
- **Princípio da Necessidade**: Limitar o tratamento dos dados ao mínimo necessário para a realização das

finalidades do tratamento de dados, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação a essas;

- **Princípio do Livre Acesso:** Garantir aos titulares de dados pessoais a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Princípio da Qualidade dos dados**: Garantir aos titulares de dados pessoais a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Princípio da Transparência**: Garantir, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Princípio da Segurança:** Utilizar medidas técnicas e administrativas adequadas ao tratamento e proteção de dados pessoais quanto aos acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Princípio da Prevenção:** adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- **Princípio da Não Discriminação**: Não realizar tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos;
- **Princípio da Responsabilização e Prestação de Contas:** Adotar medidas eficazes para o cumprimento das normas de proteção de dados pessoais.

5.2. PRINCÍPIOS DA PRIVACIDADE DE DADOS

5.2.1. Ciclo de vida da informação

O ciclo de vida da informação contém etapas e eventos como produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação. Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

- **Coleta:** é a etapa onde a informação é criada e manipulada.
- **Retenção:** consiste no armazenamento da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.
- **Processamento:** essa fase é quando o documento é alterado, consultado, classificado, utilizado, entre outros.
- **Compartilhamento:** ocorre quando a informação é compartilhada com outras unidades de dentro da FINDES ou com terceiros (fornecedor, parceiro, clientes, etc).
- **Eliminação:** essa fase refere-se à eliminação de documento impresso (depositado fragmentado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

5.2.2. Tratamento de Dados Pessoais

O tratamento de dados pessoais é qualquer ação que se faça com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, compartilhamento, armazenamento, eliminação, modificação ou comunicação.

5.2.3. Dados coletados e Finalidade

- A quantidade e o tipo de Dados Pessoais coletados podem variar de acordo com o contexto da relação firmada com a pessoa relacionada a determinado Dado Pessoal. Assim, prezando pela transparência, listamos abaixo, os Dados Pessoais que poderão ser tratados, de acordo com os diferentes contextos de tratamento, e as finalidades para as quais estes poderão ser utilizados, incluindo, mas não se limitando a: Informações de contato através do "fale conosco"- nome e e-mail;
- Processos de recrutamento e seleção e informações de colaboradores e estagiários: Dados Pessoais incluídos no currículo, ou fornecidos durante as entrevistas, testes ou avaliações (como escolaridade, detalhes de competências, qualificações, experiência, histórico de trabalho com referências dos empregadores anteriores, remuneração atual e benefícios, entre outras);
- Informações de saúde: como atestados e relatórios médicos, receitas médicas e resultados de exames;
- Informações contidas em certidões judiciais/extrajudiciais: como certidões de nada consta e de processos em andamento ou já julgados;
- Informações pessoais para participação em concursos, eventos culturais, educacionais, recreativos ou esportivos, capacitação, treinamentos, questionários ou pesquisas;
- Informações pessoais e de responsáveis legais para matrículas em cursos regulares na área de educação;
- Informações para cadastro e identificação dos prestadores de serviços e representantes de empresas prestadoras de serviços;
- Informações de saúde e de caráter profissional e ocupacional para execução dos serviços oferecidos pela FINDES e/ou suas entidades através das soluções ofertadas e contratadas;
- Execução dos deveres e obrigações da Findes em razão de contrato associativo ou outro contrato celebrado, a exemplo do contrato educacional ou similar;
- Para viabilizar a comunicação por meio de algum dos canais de atendimento, quando a informação for fornecida diretamente, através de pré-cadastro, formulário, telefone, e-mail, ou plataformas de comunicação online;

- Por meio de **cookies** ou outras tecnologias semelhantes.

5.2.4. Cookies e Links para outros sites

5.2.4.1. Cookies são pequenos arquivos de texto que são gravados em seu computador, telefone ou qualquer outro dispositivo com acesso à internet, contém informação sobre a sua navegação nesse site e retêm apenas informações relacionadas à suas preferências.

Para garantir que o usuário tenha uma experiência agradável enquanto visita o website das entidades, utilizaremos Cookies Permanentes e Cookies de Sessão.

Cookies permanentes: são cookies que permanecem no dispositivo do usuário durante um período determinado ou até que ele os exclua.

Cookies de sessão: são cookies que expiram assim que o usuário fecha o seu navegador, encerrando a sessão.

Ao acessar o site e **consentir** com o uso de Cookies, o usuário manifestará conhecer e aceitar a utilização de um sistema de coleta de dados de navegação com o uso de Cookies em seu dispositivo.

Caso o titular dos Dados Pessoais não aceite alguns cookies das páginas das entidades da FINDES, alguns serviços poderão não funcionar de maneira ideal.

Links para outros sites

Os sites das entidades poderão conter links para sites ou aplicativos de terceiros. No entanto, uma vez que o usuário use estes links para sair dos nossos sites, deverão observar que não teremos mais controle sobre tais plataformas, devendo ser verificadas as políticas de privacidade e os termos que se aplicam a estas.

5.2.5. Privacidade de dados: Classificação da informação e critérios de utilização

Todas as informações da FINDES e suas entidades devem ter um responsável designado. Recomenda-se que as informações sejam classificadas conforme grau de sensibilidade e confidencialidade, garantindo o acesso pelos profissionais devidamente autorizados.

A classificação da informação deve seguir os critérios da tabela a seguir:

Classificação	Critério
Confidencial	A informação confidencial deve ser mantida em sigilo e repassada somente às pessoas que irão utilizá-las em suas atribuições. Estas informações devem ser armazenadas em diretórios auditáveis para assegurar seu controle.
Interna	A informação interna é restrita às áreas internas da FINDES, podendo ser compartilhada entre todos os colaboradores e prestadores de serviço, porém não pode ser repassada a indivíduos que não pertençam às instituições, isto é, não deve ser divulgada publicamente.
Pública	A informação pública não possui restrições de divulgação, podendo ser repassada a qualquer indivíduo, dentro ou fora da FINDES, podendo ser publicada na internet, jornais, televisão, etc.

- O conhecimento da informação deve ser usado apenas para os propósitos de interesse da FINDES e suas entidades.
- Toda informação deve possuir um proprietário, responsável por sua classificação que deverá ser determinada no momento de criação.
- Alterações de classificação devem ser providas preferencialmente por quem a classificou originalmente e na sua ausência, por colaboradores que assumiram a sua função ou possuem nível hierárquico superior ao exigido para a sua classificação.
- O descarte de informações classificadas como confidenciais deve ser feito de forma que impossibilite a recuperação.
- Toda informação corporativa, não classificada será considerada por padrão como interna.

5.2.6. Descarte de informações físicas e digitais

Todas as informações em papel ou em qualquer outra mídia que não serão mais utilizadas, devem ser destruídas antes de serem colocadas no lixo. Além disso, é preciso tomar alguns cuidados ao apagar arquivos no computador porque existem técnicas de recuperação de dados previamente apagados. O descarte de informações deve seguir as seguintes regras:

- Documentos impressos que contenham informações pessoais, financeiras ou outros dados importantes para a FINDES e suas entidades devem ser destruídos e não podem ser reutilizados.
- Periodicamente os usuários devem realizar uma avaliação no conteúdo dos diretórios de rede sob sua responsabilidade com o objetivo de manter no ambiente corporativo apenas informações relevantes.

- Dispositivos de armazenamento (CDs, DVDs, discos rígidos, memórias "flash" e outros meios de armazenamento) devem seguir o procedimento de Descarte de Mídia PRO-GETI-001. Em caso de dúvidas ou necessidade de suporte, a TI está à disposição através de abertura de chamado via Service Desk.

5.3. TRATAMENTO DE DADOS SENSÍVEIS

Dados sensíveis são aqueles que, podem gerar discriminação ou causar constrangimento, por revelarem, por exemplo, a origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa. O tratamento desses dados só poderá ocorrer nas seguintes hipóteses:

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

II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

g) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

h) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

5.4. TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

Inicialmente para este item trazemos a diferença entre as definições de criança e de adolescente, estabelecidas pelo ECA - Estatuto da Criança e do Adolescente:

- **Adolescente**: Pessoa entre doze e dezoito anos de idade (Art. 2º do ECA).
- **Criança**: Pessoa até doze anos de idade incompletos (Art. 2º do ECA).

O tratamento de dados de crianças (pessoa até 12 anos de idade incompletos) e adolescentes (pessoa entre 12 e 18 anos de idade) somente poderá ocorrer nas hipóteses seguintes:

- O tratamento dados pessoais de crianças e adolescentes, é obrigatório o **consentimento específico** e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
- Dados pessoais de crianças poderão ser coletados **sem o consentimento do responsável apenas em duas situações:**
    - Quando a coleta for necessária para contatar os pais ou responsável legal; ou
    - Para a proteção da criança e adolescentes.

5.5. COMPARTILHAMENTO DE DADOS

Segundo a LGPD, o **uso compartilhado de dados** pode ser entendido como qualquer comunicação, difusão, transferência internacional, interconexão de dados pessoais.

A lei estipula que a comunicação ou compartilhamento de dados deve acontecer somente com o consentimento do titular, deixando claro a ele de que forma eles serão utilizados.

Em tais casos, medidas apropriadas serão adotadas para garantir a segurança das informações pessoais e evitar a sua alteração, perda, tratamento ou acesso não autorizado. Cláusulas contratuais específicas e outros mecanismos de transferência legalmente aceitáveis estão adequados e implementados em nossos procedimentos para proteção dos Dados Pessoais.

Contudo, existem situações previstas que dispensam tal autorização, as quais a lei chama de **hipótese para o tratamento de dados.** São elas:

- Os dados em questão estão atrelados ao cumprimento de obrigações legais ou regulatórias;
- Os dados estão vinculados a execução de contratos e processos judiciais, e administrativos;
- A segurança física do titular dos dados ou de terceiros ou proteção à vida;
- Para a proteção de créditos;
- Existe o **legítimo interesse** da Findes;
- Ou ainda, o titular tornou os próprios dados públicos.

5.6. DO TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

De acordo com a LGPD, o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- Fim do período de tratamento;
- Comunicação do titular quanto à revogação do consentimento, resguardado o interesse público; ou
- Determinação pela autoridade nacional, quando houver violação à proteção de dados pessoais.

A Findes e suas entidades realiza o tratamento de dados pessoais pelo tempo necessário para cumprir a finalidade

para os quais foram coletados, de acordo com sua base legal. Quando no término do tratamento, os dados pessoais serão eliminados, sendo autorizada a conservação nas situações previstas na legislação vigente.

5.7. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

Todos os incidentes com dados pessoais devem ser notificados ao Encarregado de Dados Pessoais (DPO) através do e-mail LGPD@findes.org.br

No caso de incidentes envolvendo dados pessoais, deverá ser adotado o procedimento PRO-GECOMP-Procedimento de plano de resposta a incidentes com dados pessoais.

O processo é composto pelas seguintes etapas:

- **Detecção e registro:** compreende a detecção, recebimento, registro e autorizações necessárias para o encaminhamento da investigação;
- **Investigação e contenção:** compreende a investigação e o tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias;
- **Comunicação:** Comunicar à ANPD e ao titular de dados em caso de risco ou dano relevante aos titulares (Art. 48 da LGPD);
- **Avaliação de incidentes:** Compreende a avaliação do histórico de incidentes, com consolidação de informações e indicadores, bem como a verificação das oportunidades de melhoria e lições aprendidas.
- **Documentação:** Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas.

6. RESPONSABILIDADES

6.1. CABE A ALTA ADMINISTRAÇÃO

- Cabe aos executivos das entidades estabelecer as diretrizes constantes nesta política, alocar os recursos necessários à sua execução e zelar pelo seu cumprimento.

6.2. CABE A TODOS OS USUÁRIOS

- Zelar pelo cumprimento da políticas, normas e procedimentos do sistema de segurança da informação;
- Garantir a proteção das informações físicas e eletrônicas, evitando a exposição de dispositivos de armazenamento removíveis, documentos impressos sobre mesas e impressoras, etc;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Relatar todo e qualquer incidente percebido;
- Participar dos treinamentos desenvolvidos pela organização.

6.3. CABE AO COMITÊ INTERNO DE PRIVACIDADE DE DADOS

- Ofertar parecer sobre privacidade e proteção de dados pessoais nos casos em que for consultado pelo (a) encarregado (a);
- Propor, revisar e supervisionar as políticas e normas corporativas, referente a Segurança e Privacidade de Dados;
- Propor ações de capacitação e conscientização em segurança da informação, definindo o conteúdo, periodicidade e público-alvo;
- Encaminhar ao comitê de ética os incidentes ocorridos afim de avaliar violações e resultados de auditorias do sistema de segurança da informação e propor ações para tratá-las;
- Monitoramento das ações dos incidentes de segurança da informação.

6.4. CABE AO ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Manter registro de incidentes e fragilidades de segurança da informação para apresentação periódica ao Comitê Interno de Privacidade de Dados;
- Reportar quando necessário ao Comitê Interno de Privacidade de Dados incidente de segurança da informação, para análise e tomada de decisão;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

6.5. CABE AOS GESTORES DAS ÁREAS/UNIDADES

- Classificar todas as informações pertinentes à sua área/unidades;
- Difundir a Política de Segurança da Informação e viabilizar, no âmbito de sua área de atuação, o treinamento e a conscientização de sua equipe, garantindo o cumprimento de todas as diretrizes e controles definidos.

6.6. CABE A GERÊNCIA DE COMPLIANCE E INTEGRIDADE

- **Guardar** os originais desta Política e suas revisões;
- **Divulgar** em canal corporativo a versão atual desta Política.

7. COMPETÊNCIA

Compete ao Conselho de Administração da FINDES aprovar esta Política Corporativa.

8. DISPOSIÇÕES FINAIS

Os casos omissos, bem como ajustes na presente Política Corporativa devem ser submetidos à apreciação e aprovação do Conselho de Administração da FINDES.

O descumprimento desta Política de Segurança da Informação poderá implicar em penalidades, conforme descrito na Política Findes 008 - Gestão de Consequências e Medidas Disciplinares, se necessário o Comitê Interno de Privacidade de Dados deverá ser envolvido no processo de análise.

Esta versão substitui e revoga as versões anteriores.

9. ELABORADORES / REVISORES

Área	Responsável	Cargo
Gerência de Compliance e Integridade	Viviane Dias de Lima	Gerente de Compliance e Integridade
Gerência Executiva de Infraestrutura	Reginaldo Alberto Scheffer	Analista de Infraestrutura SR
Gerência Executiva Jurídica	Luciana Spelta Barcelos	Especialista

10. CONTROLE DE REVISÕES

Revisão	Data	Descrição
00	22/01/2021	Emissão da Política
01	07/04/2021	Revisão do Formulário fale conosco
02	02/09/2024	Revisão geral do texto
03	22/01/2025	Revisão geral do texto e formalização