RELATÓRIO FINAL DE CONSULTORIA E APRESENTAÇÃO DE PROPOSTA DE PLANO DE ADEQUAÇÃO

IBAPE-SP

São Caetano do Sul, 12 de maio de 2022.

Apresentamos o Relatório Final de Consultoria contratada visando a identificação do nível de maturidade da organização em relação à Lei Geral de Proteção de Dados Pessoais (LGPD).

Nas páginas que seguem, demonstraremos as etapas propostas e efetivamente realizadas, uma amostragem das atividades, entrevistas e reuniões realizadas, bem como os documentos gerados com o objetivo de extrair um DIAGNÓSTICO do estado atual dos processos e procedimentos do negócio que tem relação direto com a LGPD e precisam ser adequados à diretriz de *Privace by Design e Privace by Default.*

Todas as informações colhidas e relatórios gerados serão disponibilizados por meio de Anexos ao presente relatório ou, então, por meio de compartilhamento dos arquivos, de forma que o IBAPE-SP possa manter o histórico dos relatos e poder, posteriormente, prosseguir com a gestão do programa, assim como para poder propiciar o monitoramento e revisão das atividades relacionadas ao seu Programa de Compliance em Proteção de Dados pessoais.

Na sequência, apresentaremos o Plano de Adequação, com um quadro de medidas de conformidade minimamente necessárias a comprovar a adesão do IBAPE-SP à LGPD.

À disposição para esclarecimentos.
Att.

GUIRÃO ADVOGADOS / NETCONSULTING CORP
Alexandro Guirão / Evandro Cleber Alves
a.guirao@guirao.com.br | evandro.alves@netconsulting.com.br
www.guirao.com.br | www.netconsulting.com.br

RELATÓRIO FINAL DE CONSULTORIA

DIAGNÓSTICO LGPD

ANÁLISE DOS PROCESSOS DE NEGÓCIO

1. Escopo da Consultoria

A parceria resultante da união de esforços do Guirão Advogados e da Netconsulting Corp, firmou uma proposta inicial de trabalho em favor do IBAPE-SP contemplando uma Jornada de Adequação à LGPD, iniciando pela realização do Diagnósticos dos Processos Internos e Processos de Negócio da organização, com a finalidade de apurar o grau de MATURIDADE da empresa acerca do tratamento de dados pessoais. Assim, foi proposta a realização das seguintes atividades:

Etapas do Diagnóstico

Descritivo Simplificado das Etapas
1. Levantamento de Processos e Fluxos atuais de coleta e tratamento de dados pessoais Fase de Campo: Identificação dos fluxos já existentes, relação de documentos e informações coletadas, locais de armazenamento (Físico e digital), levantamento de recursos humanos e tecnológicos disponíveis, assim como estrutura organizacional da companhia, revisão e adequação de questionários e entrevistas que serão aplicadas. Definição de documentos que confirmam e validam os questionários aplicados e confrontação de informações. Abordagem das equipes definidas pela organização que participarão prestando informações. Fase Interna: tabulação das informações coletadas, parametrização dos índices de impacto e probabilidade de risco à Proteção de Dados Pessoais, aplicando a metodologia da Análise de Risco Parametrizada.
2. Elaboração do Mapa de Risco à Proteção de Dados Pessoais Fase Interna: Elaboração da documentação que será submetida à validação da Companhia, com a identificação dos riscos críticos a serem tratados e medidas de mitigação ou tratamento de dados. Fase de Campo: apresentação para o responsável pelo projeto na companhia e aprovação, ou não, da Matriz de Risco elaborada.
3. Identificação de GAP's e Vulnerabilidades Técnicas e Jurídicas Fase Interna: enquadramento jurídico das vulnerabilidades e riscos identificados à proteção de dados. Preparação para elaboração de Relatórios. Fase de Campo: apresentação para o responsável pelo projeto na organização.
4. Elaboração do Relatório de Evidências de Tratamento de Dados Pessoais (ROPA) e/ou Relatório de Impacto à Privacidade de Dados Pessoais (DPIA).
5. Elaboração do Plano de Adequação à LGPD Elaboração e entrega de projeto de adequação com as fases posteriores, visando adequação das rotinas e processos à LGPD, contendo a indicação das etapas a serem cumpridas de acordo com o mapa de risco à proteção de dados: - documentação do projeto de adequação (Políticas e Controles, Adequação de Contratos e Cláusulas Contratuais Padrão), - Apresentação de ferramentas tecnológicas visando a efetividade dos controles, - Identificação e auxílio na escolha e capacitação do Encarregado de Proteção de Dados (DPO), - Treinamentos de equipes e comunicação do projeto, - Implantação de Mecanismo de Reporte (canal de Denúncias ou COMUNICAÇÃO disponível aos TITULARES DE DADOS) e elaboração dos planos de resposta aos titulares dos dados e autoridades - Elaboração do plano de contingenciamento de crises e continuidade de negócios (em caso de eventuais ocorrências de vazamentos ou violações de dados pessoais), - Outras atividades identificadas de acordo com as características do negócio da Organização.
6. Validação do Projeto de Adequação e Definição de Próximas Fases – Implantação e manutenção do Programa.

Inicialmente foi prevista uma dedicação aproximada em horas técnicas de atividade de consultoria, conforme tabela abaixo:

	Estimativa de Horas Técnicas			
Descritivo da Etapa	Consultor Sênior	Consultor Associado	Consultor Técnico	TOTAL de HORAS
Quantidade de Horas Previstas / Consultor	14	12	24	50

2. Atividades Desenvolvidas

2.1. Reunião de *Kick off e de* Alinhamento com Equipe de Projeto

Realizada no dia 24/03/2021, com a presença da Equipe do IBAPE-SP dedicada ao projeto:

- Paulo Magri
- Marcio Paiva
- Bruno Furtado
- Andreia
- Fernando
- Ana Paula

Nessa reunião foi esclarecida a metodologia que seria aplicada para a realização do diagnóstico, reforçada a importância do apoio dos altos gestores da organização a fim de que a equipe de projeto pudesse colaborar com o desenvolvimento da Consultoria, bem como solicitada a designação da equipe de projeto.

Ainda, nessa oportunidade foram apresentadas as áreas da organização que continham processos de negócios ou internos que tratam dados pessoais, identificando os pontos de impacto da LGPD para o negócio:

- RH – Recursos Humanos
- Cadastro de Associados
- Atendimento
- Marketing
- Cursos e Eventos
- Câmara Técnica

2.2. Identificação das Áreas de Negócio e Mapeamento dos Fluxos de Processos em que há impacto da LGPD.

Cada membro da equipe de projeto colaborou para a definição e identificação dos fluxos de processos que seriam necessários mapear, resultando no seguinte registro dos processos organizacionais:

DEPARTAMENTO/ÁREA	ASSUNTO	PROCESSO
RH	Contratação e Registro de Funcionários	***Nome do Processo:*** *CONTRATAÇÃO E REGISTRO DE FUNCIONÁRIOS* ***Objetivo do Processo****: Atender demanda por preenchimento de vagas e/ou posto de trabalho/serviços*

RH	CONTRATAÇÃO E REGISTRO DE FUNCIONÁRIOS	***Nome do Processo:*** *CONTRATAÇÃO E REGISTRO DE FUNCIONÁRIOS.* ***Objetivo do Processo:*** *Atender demanda por preenchimento de vagas e/ou posto de trabalho/serviços.*
RH	GESTÃO DE FOLHA DE PAGAMENTO	***Nome do Processo:*** *GESTÃO DE FOLHA DE PAGAMENTOS.* ***Objetivo do Processo:*** *Execução do contrato de trabalho, pagamento de salários e informações sociais aos órgãos competentes.*
RH	GESTÃO DE FOLHA DE PAGAMENTO	***Nome do Processo:*** *CONTROLE DE ACESSO E JORNADA POR BIOMETRIA.* ***Objetivo do Processo:*** *Pagamento de salários e outros benefícios trabalhistas/previdenciários decorrentes do controle de jornada.*
RH	GESTÃO DE BENEFÍCIOS *Plano de Saúde*	***Nome do Processo:*** *FORNECIMENTO DE BENEFÍCIO - PLANO DE SAÚDE.* ***Objetivo do Processo:*** *Garantir a cobertura do benefício ao funcionário que optar por este.*
RH	GESTÃO DE BENEFÍCIOS *Vale Transporte*	***Nome do Processo:*** *FORNECIMENTO DE BENEFÍCIO - VALE TRANSPORTE.* ***Objetivo do Processo:*** *Realizar o pagamento de benefício determinado por lei.*
RH	GESTÃO DE BENEFÍCIOS *Vale Refeição*	***Nome do Processo:*** *FORNECIMENTO DE BENEFÍCIO - VALE REFEIÇÃO.* ***Objetivo do Processo:*** *Realizar pagamento de benefício determinado por lei.*
CADASTRO ASSOCIADO	CADASTRO DE NOVO ASSOCIADO	***Nome do Processo:*** *CADASTRO DE ASSOCIADO.* ***Objetivo do Processo:*** *Atender os objetivos associativos da entidade.*
CADASTRO ASSOCIADO	DESLIGAMENTO DE ASSOCIADO	***Nome do Processo:*** *DESLIGAMENTO DE ASSOCIADO.* ***Objetivo do Processo:*** *Atender as exigências do estatuto.*
CADASTRO ASSOCIADO	LICENCIAMENTO DE ASSOCIADO	***Nome do Processo:*** *LICENCIAMENTO DE ASSOCIADO.* ***Objetivo do Processo:*** *Atender à solicitação do associado.*
CADASTRO ASSOCIADO	COBRANÇA DE ANUIDADE	***Nome do Processo:*** *COBRANÇA DE ANUIDADE DE ASSOCIADO.* ***Objetivo do Processo:*** *Garantir arrecadação e receita para a entidade atingir seus objetivos sociais e compromissos econômicos.*
ATENDIMENTO	ATENDIMENTO E INFORMAÇÕES GERAIS	***Nome do Processo:*** *FALE CONOSCO - SOLICITAÇÃO DE INFORMAÇÕES.* ***Objetivo do Processo:*** *Acolher pedido de informações gerais sobre o IBAPE, suas funções e finalidades, estrutura e*

		diretorias, bem como informações sobre associados.
ATENDIMENTO	ATENDIMENTO E INFORMAÇÕES GERAIS	***Nome do Processo:*** *FALE CONOSCO - FORNECIMENTO DE INFORMAÇÕES.* ***Objetivo do Processo:*** *Oferecer informações gerais sobre o IBAPE, suas funções e finalidades, estrutura e diretorias, bem como informações sobre associados, mediante solicitação.*
ATENDIMENTO	ATENDIMENTO E INFORMAÇÕES PARA POTENCIAL ASSOCIADO	***Nome do Processo:*** *PRÉ-CADASTRO.* ***Objetivo do Processo:*** *Receber solicitação de informações de potenciais associados.*
MARKETING	ESTRATÉGIA DE MARKETING	***Nome do Processo:*** *ESTRATÉGIA DE MARKETING - DISPARO DE E-MAILS MARKETING.* ***Objetivo do Processo:*** *Promover cursos, eventos e a associação.*
CURSOS E EVENTOS	CURSOS	***Nome do Processo:*** *VENDA CURSOS ON-LINE.* ***Objetivo do Processo:*** *Arrecadar receita para a associação, bem como cumprir com sua função social.*
CURSOS E EVENTOS	CURSOS	***Nome do Processo:*** *DESENVOLVIMENTO DO CURSO ONLINE.* ***Objetivo do Processo:*** *Atender ao contrato da compra do curso entre aluno e instituição IBAPE.*
CURSOS E EVENTOS	CURSOS	***Nome do Processo:*** *EMISSÃO DE NOTA FISCAL.* ***Objetivo do Processo:*** *Cumprir obrigação legal de fornecer Nota Fiscal ao adquirente do serviço (evento ou curso).*
CURSOS E EVENTOS	CONVÊNIO	***Nome do Processo:*** *Prestação de contas - CONVÊNIO - IBAPE NACIONAL.* ***Objetivo do Processo:*** *Cumprir obrigações estatuária e regimental de prestar contas à Entidade Nacional do Sistema Associativo.*
CURSOS E EVENTOS	CONVÊNIO	***Nome do Processo:*** *CONVÊNIO - CREA* ***Objetivo do Processo:*** *Cumprir obrigações legal e contratual de prestar contas par Entidade.*
CURSOS E EVENTOS	EVENTOS	***Nome do Processo:*** *ORGANIZAÇÃO DE EVENTOS/CONVITE A PALESTRANTES E PERSONALIDADES.* ***Objetivo do Processo:*** *Identificar e escolher potenciais palestrantes e participantes dos Eventos realizados pelo IBAPE-SP.*
CURSOS E EVENTOS	EVENTOS	***Nome do Processo:*** *Inscrição em EVENTOS PAGOS do IBAPE-SP (público em geral).* ***Objetivo do Processo:*** *colher inscrições de interessados em participar dos eventos do IBAPE-SP.*

CURSOS E EVENTOS	EVENTOS	***Nome do Processo:*** *REALIZAÇÃO DO EVENTO (PAGO).* ***Objetivo do Processo:*** *Garantir a realização do evento e atingir as finalidades da entidade.*
CURSOS E EVENTOS	EVENTOS	***Nome do Processo:*** *Inscrição em EVENTO GRATUITO do IBAPE-SP (público em geral).* ***Objetivo do Processo:*** *Colher inscrições de interessados em participar dos eventos do IBAPE-SP, divulgar as atividades do IBAPE-SP e atingir as finalidades da entidade.*
CÂMARA TÉCNICA	REUNIÕES DA CÂMARA TÉCNICA	***Nome do Processo:*** *INSCRIÇÃO PARA REUNIÃO DA CÂMARA TÉCNICA (público geral).* ***Objetivo do Processo:*** *Cumprir com função social da associação, capacitando os profissionais.*
CÂMARA TÉCNICA	EXECUÇÃO DAS REUNIÕES	***Nome do Processo:*** *EXECUÇÃO DAS REUNIÕES DAS CÂMARAS TÉCNICAS (ONLINE).* ***Objetivo do Processo:*** *Cumprir com compromisso firmado entre os profissionais e o IBAPE.*
CÂMARA TÉCNICA	PUBLICAÇÃO DE ARTIGOS, MATERIAIS, NORMAS E REGULAMENTOS	***Nome do Processo:*** *PUBLICAÇÃO DE ARTIGOS, MATERIAIS, NORMAS E REGULAMENTOS.* ***Objetivo do Processo:*** *Divulgar estudos concernentes às áreas técnicas das Câmaras.*

Em resumo:

- RH – Recursos Humanos: 06 (seis) processos.
- Cadastro: 04 (quatro) processos.
- Atendimento: 03 (três) processos.
- Marketing: 01 (um) processo.
- Cursos e Eventos: 09 (nove) processos.
- Câmara Técnica: 03 (três) processos.

Totalizando 26 (vinte e seis) processos de negócio ou internos, mapeados.

3. Entrevistas e coleta de informações para elaboração do ROPA – Relatório Operacional de Tratamento de Dados Pessoais (ANEXO I)

Definida a estrutura organizacional representada pelas áreas acima identificadas, a Consultoria iniciou a atividade de ENTREVISTAS com as equipes, visando identificar, descrever e registrar os processos de negócios e internos que tinham ponto de contato e impacto da LGPD.

As atividades dessa etapa se desenvolveram ao longo de mais de reuniões/entrevistas, divididas em:

- Coleta de informações dos processos e desenho dos fluxos por processo.
- Alimentação das planilhas e sistemas.
- Validação das informações, visando a elaboração do ROPA.

Foram necessárias aproximadamente 40 (quarenta) horas de atividade. O resultado dessa etapa pode ser verificado do ROPA – Relatório de Tratamento de Dados Pessoais que integra o presente relatório, como ANEXO I e nos demais arquivos de registro e coleta de informações (Fluxograma dos Processos, Planilhas em Excel, Relatórios e eventuais arquivos em PDF) que serão disponibilizados para o IBAPE-SP.

4. Risk Assessment e Mapa de Riscos (ANEXO II)

Definidos os riscos críticos a partir das conclusões dos ROPA's de cada processo mapeado, iniciamos a atividade de entrevistas de Análise de Riscos, coletando informações e impressões da Equipe de Projetos acerca dos Impactos e Probabilidade de concretização dos referidos riscos.

O resultado dessa Análise consta do ANEXO II e dos demais arquivos em Excel disponibilizados ao final do presente trabalho, que propiciam a revisão do assessment após a implementação do Programa e de Medidas de Mitigação de Risco.

Nessa Etapa, em torno de 01 hora de atividade era necessária, por processo mapeado (totalizando aproximadamente 26 horas), para a elaboração da matriz de risco, que consta do Anexo II. Além do referido anexo, serão disponibilizadas as planilhas elaboradas para a coleta das informações necessárias para a elaboração de referida matriz de riscos.

5. Segurança da Informação e Medidas Técnicas

O art. 6°, inciso VII, combinado com o artigo 46 da LGPD cria um dever geral aos agentes de tratamento para que adotem medidas técnicas e administrativas de garantia da segurança dos dados pessoais. A LGPD adota a segurança da informação e as medidas técnicas e aptas a assegurar essa finalidade como um "Princípio", dada a importância dos recursos tecnológicos nos processos de negócio, hoje em dia.

Ainda, mais, o art. 49 da LGPD estabelece que os sistemas utilizados para tratamento de dados devem ser "*estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.*" Por fim, devem os Controladores e Operadores, além de redigir as suas políticas e normas internas de segurança da informação que atenda aos interesses dos titulares, adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados (art. 50, § 2º. I, "c").

Durante a avaliação dos processos, foi efetuado o levantamento de um Inventário de TI (Tecnologia da Informação) com vistas a registrar os ativos e soluções (Ferramentas) detidas pela organização para garantir um nível de segurança aos dados tratados pelo IBAPE-SP.

Durante o mapeamento dos processos fizemos o levantamento da infraestrutura e maturidade tecnológica do IBAPE-SP. Após esta análise detectamos pontos de melhorias que deverão ser endereçados na organização para mitigação dos riscos de perda de dados e ou informações.

O IBAPE-SP, durante a pandemia do COVID-19 (período em que foram realizados a maioria das atividades dessa consultoria), operou suas atividades no sistema home office e on-line, transformando, inclusive, seus cursos e eventos para esse formato. Hoje, pelo relatado, os funcionários retornaram às atividades na sede do Instituto.

Porém, uma característica da operação da organização é importante que seja mencionada: os membros da Diretoria do Instituto realizam muitas atividades e interações com Dados Pessoais em ambientes externos, usando seus equipamentos pessoais. Durante o processo de coleta de informações, inclusive, identificou-se a utilização de e-mails pessoais por membros da Diretoria, impedindo medidas de controle de acesso e fluxo de informações.

É bem verdade que tomamos conhecimento, também, de que o IBAPE-SP vem investindo na transformação desse cenário, estimulando que os Diretores (que se revezam em ciclos de 2 anos – tempo do mandato de cada diretoria) passem a utilizar contas de e-mail corporativos, mas não é dispensada a elaboração, de forma rápida uma "Política de BYOD" (utilização de equipamentos pessoais dos colaboradores na operação) para definir as regras e padrões mínimo de segurança para os equipamentos que acessam a rede do IBAPE-SP.

Os processos do IBAPE, mesmo utilizando sistemas acessados via Web, utiliza de forma frequente a exportação de informações, listas para um arquivo Excel salvando-os em máquinas / servidor que está no IBAPE e em máquinas pessoais, para posterior compartilhamento via e-mail. Estas ações geram um risco que poderia ser mitigado se as informações permanecessem nos sistemas web e fossem acessadas através de usuário e senha com os devidos níveis de permissão de acesso a cada função. Outro ponto a de preocupação é um sistema de acesso a rede / servidor ser via compartilhamento de pastas ao invés de termos os acessos realizados através de usuários e senhas baseados no Active Directory, este sem custo de licenciamento, apenas é necessário a configuração do ambiente.

A rotina de backup do servidor não utiliza as boas práticas para esta rotina, e entendemos que isto é um ponto crítico que dever ser corrigido o mais rápido possível.

O IBAPE precisa resolver pontos como: Controle e monitoramento de acessos, eliminar compartilhamento de usuário e senha para acesso às aplicações, definir políticas de backup para os dados que definirem críticos para a operação, aplicação de dupla autenticação (MFA) para identificação para todos que acessam o ambiente.

Como ação estruturante entendemos que a criação de uma Política de Segurança da Informação deverá ser criada para definir ações para adequação dos processos, procedimentos, tecnologias e treinamentos a serem utilizadas na operação do IBAPE-SP a fim de mitigar os riscos de perdas de dados atualmente existentes.

6. Adequação de Instrumentos

Durante a elaboração do Diagnóstico contratado, evidenciou-se a necessidade de adequação imediata do *Instrumento Particular de Instituição de Parceria Comercial e Autorização de Uso de Imagem e Conteúdo*, praticado pelo IBAPE-SP para a contratação de profissionais, professores e especialistas visando a ministração de cursos no Instituto. A Diretoria optou pela revisão do instrumento prático, considerando especialmente a transformação dessas atividades, antes quase que exclusivamente presenciais, para o formato *on-line.*

7. Conclusão

Desde o início da presente consultoria foram realizadas diversas reuniões de suma importância para a compreensão dos processos do Instituto, essenciais à demonstração de aderência do IBAPE-SP à LGPD (como é o caso do ROPA e da Matriz de Riscos), além da revisão de instrumento contratual e, ainda, análise de contratos de prestadores de serviços que atuam como operadores de dados pessoais coletados pelo IBAPE-SP.

Foram em torno de 60/70 horas de reuniões e entrevistas e dedicação à elaboração de documentos, o que revelam a superação da expectativa inicial. Sem contar o tempo dedicado à elaboração do presente relatório e do Projeto de Adequação.

Na Sequência, passamos a presentar o Projeto de Adequação, que entendemos, tornará o IBAPE-SP aderente às demandas da Lei Geral de Proteção de Dados, estabelecendo um Programa de Compliance de Privacidade e Proteção de Dados, composto por medidas de conformidade e governança da informação, medidas técnicas e de segurança da informação que objetivam o tratamento dos riscos à proteção dos dados pessoais identificados durante a elaboração do presente diagnóstico.

Optamos por fundamentar todas as medidas de conformidade e de governança, com base nos ditames da LGPD, como forma de transmitir com segurança ao Instituto o que garantirá certo nível de aderência à conformidade legal. E, ainda, listar todas as medidas necessárias, para a validação pelo IBAPE-SP, com vistas a elaborar, posteriormente, a proposta comercial de IMPLANTAÇÃO DO PROJETO DE ADEQUAÇÃO.

PLANO DE ADEQUAÇÃO

A partir desse momento, consideradas todas as informações coletadas durante a fase de diagnóstico e as interações com a Equipe de Projetos, apresentamos uma proposta de Plano de Adequação a fim de que o IBAPE-SP se torne aderente à Lei Geral de Proteção de Dados.

O objetivo de cada Medida de Conformidade abaixo está detalhado e, também, devidamente fundamentada, com base nos dispositivos da Lei Geral de Proteção de Dados, como forma de justificar sua real necessidade.

As Medidas de Conformidade (documentais e administrativas), conjugadas com as Medidas Técnicas e, ainda, adequação de procedimentos de negócios, permitem a mensuração do grau de adequação do IBAPE-SP à LGPD, mas precisam ser constantemente monitoradas e revisadas, de acordo com a necessidade ou, ainda, de acordo com uma periodicidade definida.

Isso significa afirmar que o Plano de Adequação ora apresentado é o que mais revela a necessidade momentânea da organização, nada impedindo que haja a necessidade de sua revisão e adequação, caso surjam novas demandas. É um PROGRAMA VIVO, em constante necessidade de avaliação e revisão, o que não pode ser negligenciado pela organização, tanto a Alta Direção, como o Encarregado de Proteção de Dados (que precisa ser identificado e nomeado) e, também, todos *heads* e colaboradores envolvidos nos processos em que há impacto da LGPD.

Abaixo, então, passamos a apresentar as MEDIDAS DE CONFORMIDADE, as MEDIDAS DE MITIGAÇÃO DE RISCOS e eventuais MEDIDAS TÉCNICAS necessárias a garantir conformidade e, ainda, assegurar o cumprimento de PRINCÍPIOS e DIRETRIZES da LGPD para os Agentes de Tratamento de Dados, bem como ASSEGURAR OS DIREITOS DOS TITULARES DE DADOS.

MEDIDAS DE CONFORMIDADE

Etapa	Descritivo de tarefas da Etapa
1. Identificar e Nomear o ENCARREGADO	***1.*** *Auxiliar a organização na escolha e qualificação do Encarregado de Proteção de Dados (recomendando curso de capacitação ou, eventualmente, promovendo seu treinamento e assessoramento).* ***2.*** *Elaborar seu descritivo de funções e responsabilidades.*

Fundamento Legal: Art. 5°, inciso VIII e art. 41 da LGPD.
Objetivo: Consoante a Lei Geral de Proteção de Dados Pessoais, o encarregado tem a função de atuar como canal de comunicação entre o controlador e o operador de dados e a Autoridade Nacional de Proteção de Dados (ANPD). Zelar pelo cumprimento interno da LGPD, tratar das demandas relacionadas aos titulares de dados.
Comentários e Considerações: A nomeação do encarregado, pessoa indicada pelo controlador e operador, é uma das primeiras coisas que devem ser realizadas ao desenvolver e implementar um programa de proteção de dados.

Além dele, sendo necessário, a organização poderá formar uma comissão/comitê de Proteção de Dados, auxiliando o Encarregado no processo decisório ou, ainda, na adoção de medidas de intervenção e gestão de crises envolvendo eventuais incidentes ou ocorrências com os dados tratados pela organização. Esse "colegiado", embora não seja obrigatório, é importante para revelar a adoção de boas práticas e de efetiva governança do IBAPE-SP no tratamento dos dados.

Etapa	Descritivo de tarefas da Etapa
2. Elaboração de Política de Direitos dos Titulares	*Customizar por direitos/segmento econômico, seguindo a LGPD e outros normativos ou regulações de mercado específicas para a organização.*

Fundamento Legal: Arts. 17, 18 ,46 e 50, § 2°, I, "a'' da LGPD.
Objetivo: Medidas e instrumentos que servem para garantir o cumprimento dos direitos dos titulares dos dados, de modo a evitar que seus dados sejam eventualmente utilizados de maneira indevida. Cumpre com o dever de TRANSPARÊNCIA e INFORMAÇÃO aos titulares de dados.
Comentários e Considerações: Essas medidas são os meios de comunicação com o titular dos dados pessoais, dessa forma, é possível informar todas as garantias, práticas e os procedimentos adotados no tratamento de dados pessoais. Bem por isso, a referida POLÍTICA necessita ser devidamente divulgada, de forma objetiva, clara e acessível ao titular dos dados. Consideradas as características da operação do IBAPE-SP (associação e venda de curso e eventos), é adequado que a essa POLÍTICA seja considerada de acordo com cada atividade e sua disponibilização nos correspondentes CANAIS DE ATENDIMENTO aos titulares dos dados.

Etapa	Descritivo de tarefas da Etapa
3. Elaborar Plano de ATENDIMENTO DE DEMANDAS DOS TITULARES.	*<u>Definir:</u>* ***3.1.*** *Planos e Padrões de respostas de acordo com a base legal de tratamento (que garanta a manutenção do tratamento dos dados, se for o caso)* ***3.2.*** *Planos e Padrões de respostas de acordo com a classificação dos dados pessoais tratados (dados pessoais propriamente ditos, dados sensíveis e dados críticos)*

Fundamento Legal: Art.18 da LGPD.
Objetivo: Facilitar e formalizar um procedimento de atendimento às demandas, dúvidas e pedidos dos titulares de dados pessoais que interagem com organização. O objetivo de fundo é garantir, ainda, o atendimento dos direitos dos titulares de dados.
Comentários e Considerações: A criação de um procedimento de atendimento às demandas dos titulares de dados revela adoção de Boas Práticas de Governança pelo IPBAPE-SP, transparência na forma de garantir esses interesses e revela o compromisso do Instituto no atendimento de seus usuários, parceiros de negócios e público em geral que, de alguma forma, interage com a entidade. Cria expectativas no titular dos dados, identificando as etapas de seu processo de atendimento, o prazo de resposta para suas demandas e, ainda, a instância responsável pelo atendimento de suas solicitações. Permite, ainda, uma pré-seleção de demandas e direcionamento para outros canais de atendimento, caso o tema a ser tratado pelo titular não tenha relação com o tratamento de seus dados pessoais. Propícia ao IBAPE-SP, ainda, a identificação de metodologia para prestação de contas à Autoridade de Proteção de Dados, acerca do cumprimento de seus deveres enquanto Agente de Tratamento de Dados Pessoais.

O Procedimento de Atendimento deve estar alinhado à solução adotada para ativação do Canal de Atendimento.

Etapa	Descritivo de tarefas da Etapa
4. Criar e ativar CANAL DE ATENDIMENTO aos Titulares de Dados	*Definir o processo interno de tratamento da demanda e responsável pelo feedback*

Fundamento Legal: Art. 18 e Art. 50, § 2º, I, "e" da LGPD.
Objetivo: Facilitar o acesso de titulares de dados pessoais para exercer seus direitos e receber informações acerca do tratamento de seus dados.
Comentários e Considerações: A ativação do CANAL DE ATENDIMENTO do titular de dados pessoais tratados pelo IBAPE-SP revela Boas Práticas de Governança no tratamento de dados pessoais, transparência e compromisso no atendimento aos interesses dos titulares de dados pessoais.
A solução deve corresponder ao procedimento de atendimento criado e garantir o registro das demandas de titulares, as respostas ofertadas e interações com ele, a fim de ser possível evidenciar o atendimento, em sendo necessário para comprovação perante a Autoridade Nacional de Proteção de Dados. O ideal é a utilização de ferramenta que propicie o registro cronológico e lógico das demandas, até a conclusão do atendimento, de forma que possa ser eventualmente auditado (cumprindo uma das diretrizes da LGPD, que é a Prestação de Contas). Ainda deve propiciar ao titular de dados o acompanhamento de suas demandas, seja por meio de acesso individual a ele assegurado, seja pela prestação de informações personalizadas em atendimentos diretos (ao telefone ou por e-mail).

Etapa	Descritivo de tarefas da Etapa
5. COMUNICADOS DE PRIVACIDADE PARA O PÚBLICO EM GERAL	*Elaboração/adequação do Termo de Privacidade para SITE e Termo de Cookies (de acordo com a interação existente no ambiente virtual) e ativar um sistema de gestão de cookies.*

Fundamento Legal: Art. 46 e Art. 50, § 2º da LGPD.
Objetivo: Transmitir com transparência, para todos os interessados, informações acerca da forma como os dados pessoais dos usuários e visitantes das plataformas do IBAPE-SP serão tratados.
Comentários e Considerações: A Política de Privacidade está relacionada com informações específicas de coleta, armazenamento e proteção de dados pessoais de usuários do site. É um documento que revela Boa Prática de Governança dos Dados, mas que precisa estar alinhada aos Processos Internos e Processos de Negócios da organização.

Etapa	Descritivo de tarefas da Etapa
6. Política de retenção e descarte de dados	*Definir acordo com a categoria de dados, interesses da organização (questões relacionadas à prescrição ou exercício de direitos e, eventualmente, deveres da organização, como os relacionados à deveres legais ou regulatórios.*

Fundamento Legal: Arts. 16, 46 e 50, § 2°, I, "a" da LGPD

Objetivo: Garantir e justificar a manutenção de dados mesmo sem consentimento ou contra eventual pretensão manifestada pelo titular e, ainda, promover o descarte seguro dos dados pessoais desnecessários ou cujo tratamento tenha sido concluído.
Comentários e Considerações: De suma importância essa política, pois define os períodos de retenção necessários para os dados pessoais e define padrões mínimos a serem aplicados ao descartar certas informações dentro do Instituto. Dá suporte, inclusive, a eventuais demandas e pedidos de titulares de dados que pretendam o descarte ou exclusão de suas informações. Leva em consideração a natureza e finalidade do tratamento dos dados, a classificação de cada elemento de dado e a relação dos dados com os processos e interesses da organização. É estruturado levando-se em consideração conceitos legais (como prescrição e decadência), assuntos de regulação de mercado, interesses do Agente de Tratamento de Dados e do próprio titular, entre outros.

Etapa	Descritivo de tarefas da Etapa
7. Adequação de contratos e revisão de termos de contratos de fornecedores e clientes.	*Ativar Cláusulas de contratos com aderência à LGPD; Revisar ou criar TERMOS DE COMPROMISSO acerca de dados pessoais tratados ou compartilhados (ex.: NDA)*

Fundamento Legal: Art. 46 da LGPD
Objetivo: Estar aderente às normas e princípios estabelecidos pela lei geral de proteção de dados pessoais.
Comentários e Considerações: Um contrato adequado à LGDP deve trazer cláusulas prevendo todo tipo de situação passível de ocorrer na gestão e tratamento de dados pessoais. Deve estabelecer os limites adequados à finalidade do tratamento do dado, o respeito às bases legais, compromissos de adesão às diretrizes do controlador e, ainda, compromisso de garantir a implementação de medidas de segurança ao tratamento dos dados. Os contratos e termos devem ser adequados para cada tipo de contratação ou negócio jurídico a que se referem, assegurar garantias de responsabilização e ressarcimento dos agentes de tratamento de dados de acordo com o nível de sua classificação (Controlador ou Operador de Dados).

Etapa	Descritivo de tarefas da Etapa
8.Política de Segurança da informação (física e Digital) BYOD	*Estabelecer Diretrizes para garantir CID – Confidencialidade, Integridade, Disponibilidade dos dados pessoais.*

Fundamento Legal: Art. 46 da LGPD e ISO 27001.
Objetivo: Regras que ditam o acesso, o controle e a transmissão da informação.
Comentários e Considerações: Entendemos que a criação de uma Política de Segurança da Informação deverá definir de forma estruturada as ações para adequação dos processos, procedimentos, tecnologias e treinamentos a serem utilizadas na operação do IBAPE-SP a fim de mitigar os riscos de perdas de dados atualmente existentes.

Etapa	Descritivo de tarefas da Etapa

9. Política de Resposta a incidentes	***9.1.*** *Definir a Equipe de Gestão de Crises* ***9.2.*** *Criar estratégias de Comunicação aos titulares e Autoridades;* ***9.2****. Tomada de Ações Corretivas* ***9.3****. Procedimento Investigação Interna*

Fundamento Legal: Art. 46 e 50, § 2°, I, "g" da LGPD

Objetivo: Preparar a empresa para lidar com a gerência de um incidente de segurança, garantindo que responda de forma mais rápida, organizada, eficiente e adequada a esse incidente, assim, minimizando suas consequências.

Comentários e Considerações: A adoção de referido instrumento revela o zelo da empresa no tratamento de intercorrências do próprio negócio, em si, ou fatores externos que possam levar à violação de segurança e afetação dos dados de pessoas físicas tratados pela organização. Em referido documento será previsto o Procedimento a ser deflagrado na hipótese de um incidente de segurança, os responsáveis por cada medida a ser adotada, os responsáveis por tomadas de decisão, entre outras. O nível de resposta dependerá do tipo de dado e da complexidade do tratamento aplicado. Considerando o dever de transparência e prestação de contas, referido procedimento indicará os meios a serem utilizados para a devida comunicação dos interessados (Titulares e Autoridades). Além disso, na medida do possível, também indicar as eventuais medidas corretivas ou, então, definir responsabilidades pela tomada de decisão acerca da medida mais adequada. Por fim, em referido documento será previsto procedimento para investigação interna a fim de apurar eventual responsabilidade de agentes e integrantes da organização e, por fim, determinar as devidas ações corretivas, se for o caso.

Etapa	Descritivo de tarefas da Etapa
10. Política para atividades em redes sociais e ferramentas de comunicação e grupos.	*10. Definir regras a serem observadas para a utilização das redes sociais da organização, relativamente à LGPD, no que se refere a coleta de dados, tratamento de dados e interação com titulares de dados.* *10.2. Definir os responsáveis e alçadas para tratamento e dados nas redes sociais.* *10.3. Estabelecer diretrizes para colaboradores acerca da utilização de suas redes sociais próprias X relação de trabalho/emprego.*

Fundamento Legal: Art. 46 e 50, § 2°, I, "a" da LGPD

Objetivo: Definição de parâmetros de uso das redes sociais da organização consoante a LGPD.

Comentários e Considerações: Referidas medidas, sendo consideradas como normas a serem respeitadas pelos colaboradores, devem servir de norte e referência para o comportamento dos colaboradores e prestadores de serviço da organização nas redes sociais próprias e da empresa, com vistas a demonstrar o comportamento zeloso com os dados de titulares com quem interagem nesse ambiente virtual.

Etapa	Descritivo de tarefas da Etapa

11. Guia de Marketing	*Orientação quando e de que forma é possível tratar Dados Pessoais com essa finalidade.* *Documento interno, orientativo para treinamento e capacitação das áreas de interesse, definindo responsabilidades da área*

Fundamento Legal: Art. 46 e Art. 10, I e II da LGPD

Objetivo: Definição de parâmetros de uso das estratégias de marketing utilizadas pelo setor, observando as regras estabelecidas pela LGPD.

Comentários e Considerações: A tomada de decisões depende de manifestação de vontade humana e as organizações adotam estratégias de Marketing para atrair interesses de pessoas aptas e capacitadas a tomar referidas decisões de contratação de produtos e serviços. Sendo assim, o dado pessoal é um ativo que pode ser utilizado para referida finalidade (apoio e promoção das atividades do agente de tratamento), desde que garantido ao titular dos dados o exercício de seus direitos, além do atendimento dos princípios e diretrizes estabelecidos na própria LGPD, como o da transparência do tratamento, adequação e necessidade e prestação de contas. Sendo assim, a organização necessita adotar um normativo que estabeleça segurança para a empresa na prática dessas atividades, determinando como eventuais prestadores de serviço de marketing (ou a área responsável) devem se comportar para que não haja desvirtuamento das finalidades para as quais os dados foram coletados. Ainda, deve adotar medidas para sempre comunicar ao titular de dados controlados e detidos para uma finalidade específica, a pretensão de passar a utilizá-lo para uma finalidade de apoio e promoção, garantindo-lhe o direito de se opor a essa nova finalidade de tratamento, embora assentindo com outra(s) finalidade(s), sem praticar qualquer espécie de retaliação ou condição para continuidade do tratamento ordinário. Esse documento deve revelar as boas práticas de marketing, levando sempre em consideração o avanço da tecnologia para a referida atividade, novas modalidades de mídias e metodologias de trabalho, concebidas sempre a partir dos princípios e diretrizes da LGPD.

Etapa	Descritivo de tarefas da Etapa
12. Política de Gestão de Terceiros em relação à LGPD	*12.1. Análise e/ou elaboração de contratos de terceiros visando adequação e aderência à LGPD;* *12.2. Elaboração dos questionários de conformidade para avaliação de maturidade da LGPD pelo terceiro.*

Fundamento Legal: Arts. 42 a 46 e Art. 50, § 2°, I, "a" da LGPD

Objetivo: Definição de práticas de relacionamento com fornecedores e demais parceiros do IBAPE-SP visando definir e prevenir responsabilidade pelo tratamento inadequado dos dados pessoais.

Comentários e Considerações: As interações entre Agentes de Tratamento de dados, sejam Controladores ou Operadores de dados, devem estar devidamente documentadas e monitoradas, pois a LGPD, no art. 42 define a responsabilidade objetiva dos Agentes de Tratamento de Dados (pressupondo o risco inerente a essa atividade) e, ainda, a solidariedade entre Controladores e Operadores no tratamento dos dados pessoais. Para isso, a organização Controladora dos dados (como é o caso do IBAPE-SP) deve evidenciar que efetua uma adequada gestão de seus prestadores de serviços contratados para darem cabo a operações de tratamento de dados pessoais, estabelecendo mecanismos de monitoramento periódico das atividades do operador, revisando ou criando termos e contratos definindo regras de tratamento e limites de compartilhamento de dados Coletados pelo controlador (ou para o controlador), contendo ainda regras de responsabilização por eventuais intercorrências ou incidentes envolvendo dados pessoais e, por fim, estabelecendo parâmetros de segurança mínimos a serem adotados pelo operador que asseguram o mesmo nível (ou similar) de segurança que o Controlador adota para suas operações de tratamento de dados.

Etapa	Descritivo de tarefas da Etapa
13. Política de Recursos Humanos	*Elaborar as Políticas de:* ***1.*** *Recrutamento e Seleção,* ***2.*** *Gestão de Dados de Empregados e* ***3.*** *Gestão de Dados de Ex-Empregados*

Fundamento Legal: Art. 46 e 50, § 2°, I, "a" da LGPD
Objetivo: Definição de normas e diretrizes que determinam como os colaboradores de uma empresa devem se portar frente à relação de trabalho e aos dados pessoais dos colaboradores da organização. Ou seja, definir um padrão de comportamento de todos os colaboradores e, dessa forma, assegurar o devido tratamento dos dados das pessoas físicas.
Comentários e Considerações: A fonte mais comum de coleta de dados pessoais para todas as organizações certamente é a Relação de Emprego ou de Trabalho, o que impacta diretamente a área de Recursos Humanos das empresas. O tratamento de dados pessoais, por essa área, se inicia mesmo antes de (ou independentemente de) se concluir a Relação de Emprego ou de Trabalho. Portanto, essa política tem o papel de esclarecer, a todos que lidam com essas informações, qual é a conduta adequada em cada uma das situações especificadas pela gestão. Considerada a base legal de tratamento dos dados e a finalidade definida é importante, ainda, esclarecer ao titular dos dados, em políticas específicas, como será o tratamento dos dados dele, pela organização, a fim de limitar as expectativas dele quanto a consentimento ou não acerca do tratamento.

Etapa	Descritivo de tarefas da Etapa
14. Plano de Treinamento de Funcionários e Terceiros de Interesse.	*Estabelecer estratégias de comunicação assertiva visando adesão espontânea dos colaboradores e terceiros às diretrizes de proteção de dados da organização.*

Fundamento Legal: Art. 46 e Art. 50, I e II da LGPD
Objetivo: Funcionários e terceiros interessados capacitados para estar alinhados com a lei geral de proteção de dados.
Comentários e Considerações: O treinamento é um mecanismo fundamental para capacitar os colaboradores e adequá-los à lei geral de proteção de dados pessoais. Demonstra qual a conduta esperada pelo sujeito, conforme as regras estabelecidas (na lei, no código de conduta ou mesmo nas políticas específicas de Compliance e Proteção de Dados). A empresa deve adotar estratégias de treinamento e comunicação que sejam facilmente evidenciáveis, que possuam a linguagem adequada para cada nível corporativo, levando ao conhecimento do máximo de colaboradores possíveis os riscos de não serem adotadas as medidas determinadas pela empresa. Para aqueles que lidam mais diretamente com o tratamento dos dados pessoais, objeto da LGPD, é necessária uma abordagem diferente, de capacitação mais apropriada.

Etapa	Descritivo de tarefas da Etapa

15. Elaboração do DPIA – Relatório de Impacto à Proteção de Dados	*Documento exigido pela legislação quando há tratamento de dados de acordo com certas bases de dados e, especialmente, quando há tratamento de dados sensíveis e dados de crianças e adolescentes.*

Fundamento Legal: Art. 5º, inciso XVII e Art. 38
Objetivo: O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Comentários e Considerações: Neste Relatório, o objetivo é avaliar o potencial discriminatório dos DADOS SENSÍVEIS (LGPD, art. 5º, II - dados biométricos/fotografia de Titulares Usuários, Beneficiários e Colaboradores da organização) e o impacto aos direitos e interesses dos titulares. Deve ser revisado periodicamente, especialmente após a adoção de medidas específicas de mitigação ou tratamento de riscos.

Etapa	Descritivo de tarefas da Etapa
16. Elaboração do LIA – Análise de Legítimo Interesse	*Assessment que leva em consideração os dados cuja base legal de tratamento é o legítimo interesse da organização Controladora/Operadora*

Fundamento Legal: Art. 10, § 2° da LGPD
Objetivo: Auferir consistência na definição da base legal do "legítimo interesse" nos dados pessoais que serão tratados, ou seja, instrumento de avaliação de risco que deverá ser elaborado sempre que haja utilização da base legal do legítimo interesse.
Comentários e Considerações: A base legal do legítimo interesse é uma das diversas bases legais elencadas no artigo 7° da LGPD para o tratamento de dados pessoais. Como é uma das bases de tratamento utilizada pelo IBAPE-SP, executar o LIA reforçará sua conformidade e permitirá o alinhamento junto ao princípio da responsabilidade, previsto na lei. Dessa forma, para cada processo em que o legítimo interesse esteja pré-definido como base legal, faz-se necessária a realização do LIA. Essa análise é uma espécie de um teste de PONDERAÇÃO, a fim de garantir, pelo confronto entre o ônus e o bônus, a continuidade do tratamento dos dados pessoais com essa base legal ou, então, a reclassificação para garantir melhor adesão à LGPD e garantir os interesses dos titulares de dados.

MEDIDAS TÉCNICAS (Sistemas e Soluções Tecnológicas)

Com base no mapeamento tecnológico realizado, mesmo antes da formalização da Política de Segurança da Informação, entendemos que as ações abaixo deveriam ser priorizadas para mitigar os riscos de perdas de dados e informações:

- Implementação de gestão de acessos a sistemas de TI;
- Implementação de solução de segurança para os computadores, celulares, servidor e aplicações;
- Implementação de solução de backup conforme boas práticas de mercado;
- Eliminar/limitar o compartilhamento de dados pessoais via e-mail pessoal no caso dos diretores e trabalhar para ajustar os processos para evitar a troca de informações pessoais que são exportados dos sistemas web e encaminhá-los por e-mail.
- Evitar troca de informações via WhatsApp, Telegram, Redes Sociais etc.;

O IBAPE-SP deve elaborar planos para trabalhar com o mínimo acesso necessário para cada colaborador. Em razão disso, é necessário integrar a Política de Segurança da Informação a Processos e Soluções/Aplicações que garantam a ativação dos controles nos níveis determinados pela organização.

Como complemento dessa estratégia, em breve a IBAPE-SP deve reforçar essa proteção ampliando o uso de um agente de segurança nos dispositivos que são de propriedade da empresa, e em caso de o IBAPE definir que os colaboradores irão continuar a utilizar equipamentos pessoais, o mesmo nível de proteção definida para os equipamentos internos deverão ser aplicadas nos pessoais.

MEDIDAS DE MITIGAÇÃO DE RISCOS

Ao longo do trabalho de Análise de Riscos (*Risk Assessment*), a organização deve identificar os agentes de risco e suas origens. Vulnerabilidades que, se tratadas de forma satisfatória, podem impactar ou evitar a concretização do risco avaliando, ainda, os indicadores de IMPACTO e PROBABILIDADE da concretização de determinado risco em cada processo de negócios.
Adotando a metodologia de Análise de Risco Parametrizada, com a coleta de impressões (não estatísticas) de colaboradores das áreas de negócios, é possível estabelecer uma série de riscos que podem afetar os interesses da empresa e estabelecer a MATRIZ DE RISCOS, definindo aqueles mais críticos que merecem tratamento mais imediato ou determinado.
No ANEXO III foi definida a matriz de riscos. A seguir, seguem as medidas de mitigação sugeridas para uma adequada GESTÃO DOS RISCOS da organização, no que se refere à LGPD:

RISCO	MEDIDAS DE MITIGAÇÃO
Retenção prolongada dos dados - sem exigência legal ou regulatória	Política de retenção e descarte de dados, e treinamentos.
Acesso não autorizado	Gestão de Controle de acesso lógico (Gestão de Identidade), desenvolvimento lógico e segurança em redes e política de controle identidade e acesso e treinamento.
Ataque cibernético	Política de segurança da informação – deverá ser criada para a definição de estratégias de governança e segurança dos dados.
Perda	Política de segurança da informação – deverá ser criada para a definição de estratégias de governança e segurança dos dados, definição de Políticas de Backup para os dados considerados críticos para a operação, incluindo ambiente do Google Drive, e-mails, sistemas de terceiros utilizados.
Roubo	Política de segurança da informação – deverá ser criada para a definição de estratégias de governança e segurança dos dados.
Falha em considerar os direitos dos titulares	Treinamento e controle interno.
Desvio da finalidade de tratamento	Treinamento e controle interno.
Compartilhamento com terceiros essenciais para a execução do contrato sem consentimento do titular	*Due Diligence*, tomada de decisão e controle interno
Modificação não autorizada (intencional ou acidental)	Aplicar regra de mínimo acesso (restrição de acessos), Dupla autenticação (MFA) e controle interno.
Remoção não autorizada	Treinamento

Coleta excessiva	Treinamento e controle interno.
Informação insuficiente ao titular sobre a finalidade do tratamento	Política de divulgação de informações.
Inexistência de indicação de finalidade de tratamento	Treinamento e controle interno.
Responsabilidade civil por ato de terceiro que recebe o dado por compartilhamento	Treinamento e controle interno.
Vinculação indevida de dados pessoais do titular coletado em razão de um serviço e utilizado para outro serviço	Treinamento e controle interno.
Dados armazenados em documentos físicos – arquivos in loco/ acesso indevido/ cópia indevida/ transferência indevida/ sinistro no local do armazenamento	Treinamento e controle interno.
Retenção prolongada - sem exigência legal ou regulatória	Política de retenção e descarte de dados, e treinamentos.

PLANO DE ADEQUAÇÃO

Etapa	Descritivo de tarefas da Etapa	Validação
1. Identificar e Nomear o ENCARREGADO	***1.*** *Auxiliar a organização na escolha e qualificação do Encarregado de Proteção de Dados (recomendando curso de capacitação ou, eventualmente, promovendo seu treinamento e assessoramento).* ***2.*** *Elaborar seu descritivo de funções e responsabilidades.* ***3****. Designação e composição do comitê de privacidade e proteção de dados*	
Etapa	Descritivo de tarefas da Etapa	
2. Elaboração de Política de Direitos dos Titulares	*Customizar por direitos/segmento econômico, seguindo a LGPD e outros normativos ou regulações de mercado específicas para a organização.*	
Etapa	Descritivo de tarefas da Etapa	
3. Elaborar Plano de Atendimento de Demandas dos Titulares.	*<u>Definir:</u>* ***3.1.*** *Planos e Padrões de respostas de acordo com a base legal de tratamento (que garanta a manutenção do tratamento dos dados, se for o caso)* ***3.2.*** *Planos e Padrões de respostas de acordo com a classificação dos dados pessoais tratados (dados pessoais propriamente ditos, dados sensíveis e dados críticos)*	
Etapa	Descritivo de tarefas da Etapa	
4. Criar e ativar CANAL DE ATENDIMENTO aos Titulares de Dados	• *ativação da ferramenta ou solução de atendimento às demandas dos titulares de dados* • *definir o processo interno de tratamento da demanda (fluxo de andamento das demandas) e responsável pelo feedback*	
Etapa	Descritivo de tarefas da Etapa	
5. COMUNICADOS DE PRIVACIDADE PARA O PÚBLICO EM GERAL (Site/APP)	*Elaboração/adequação do Termo de Privacidade para SITE e Termo de Cookies (de acordo com a interação existente no ambiente virtual) e ativar um sistema de gestão de cookies.*	
Etapa	Descritivo de tarefas da Etapa	
6. Política de retenção e descarte de dados	*Definir acordo com a categoria de dados, interesses da organização (questões relacionadas à prescrição ou exercício de direitos e, eventualmente, deveres da organização, como os relacionados à deveres legais ou regulatórios.* *Criar Processo de Classificação de dados pessoais e definir a Política de Retenção de acordo com a natureza e classificação de dados, por exemplo:* ● *Dados de Usuários* ● *Dados de Funcionários e Prestadores de Serviços*	

	● *Dados de Representantes Legais de Clientes/Fornecedores etc.*	
Etapa	Descritivo de tarefas da Etapa	
7. Adequação de contratos e revisão de termos de uso fornecedores e clientes.	*Ativar Cláusulas de contratos com aderência à LGPD;* *Revisar ou criar TERMOS DE USO (contratos de serviços) TERMOS DE COMPROMISSO acerca de dados pessoais tratados ou compartilhados com terceiros (ex.: NDA).* *Obs.: A quantidade de documentos criados/revisados dependerá do volume de negócios jurídicos que demandarem adequação à LGPD.*	
Etapa	Descritivo de tarefas da Etapa	
8. Política de Segurança da informação (física e digital)	● *Estabelecer Diretrizes para garantir CID – Confidencialidade, Integridade, Disponibilidade dos dados pessoais.* ● *Estabelecer políticas e procedimentos para uso de dispositivos particulares na organização (BYOD)* ● *Definir Políticas e Controles de Acesso aos dados da organização.*	
Etapa	Descritivo de tarefas da Etapa	
9. Política de Resposta a incidentes de Segurança	***9.1.** Definir a Política de Gestão de Crises e Criar o Comitê de Gestão de Crises* ***9.2.** Criar estratégias de Comunicação aos titulares e Autoridades;* ***9.2**. Procedimento Investigação Interna para dar suporte às demandas e incidentes e minimizar consequências*	
Etapa	Descritivo de tarefas da Etapa	
10. Política para atividades em redes sociais e ferramentas de comunicação e grupos.	*10.1. Definir regras a serem observadas para a utilização das redes sociais da organização, relativamente à LGPD, no que se refere a coleta de dados, tratamento de dados e interação com titulares de dados.* *10.2. Definir os responsáveis e alçadas para tratamento e dados nas redes sociais.* *10.3. Estabelecer diretrizes para colaboradores acerca da utilização de suas redes sociais próprias X relação de trabalho/emprego.* *Considerar Processos de:* ● Relacionamento/atendimento a clientes ● Marketing ● Cyber segurança a partir dos contatos via redes sociais (engenharia social)	
Etapa	Descritivo de tarefas da Etapa	
11. Guia de Marketing	*Orientação quando e de que forma é possível tratar Dados Pessoais com essa finalidade.* *Documento interno, orientativo para treinamento e capacitação das áreas de interesse, definindo responsabilidades da área*	
Etapa	Descritivo de tarefas da Etapa	

12. Política de Gestão de Terceiros em relação à LGPD	*12.1. Análise e/ou elaboração de contratos de terceiros visando adequação e aderência à LGPD;* *12.2. Elaboração dos questionários de conformidade (Due Diligence) para avaliação de maturidade da LGPD pelo terceiro.* *12.3. Acompanhamento da Adequação do Terceiro.*	
Etapa	Descritivo de tarefas da Etapa	
13. Política de Recursos Humanos	*Elaborar as Políticas de:* ***1.** Recrutamento e Seleção,* ***2.** Gestão de Dados de Empregados e* ***3.** Gestão de Dados de Ex-Empregados*	
Etapa	Descritivo de tarefas da Etapa	
14. Plano de Treinamento de Funcionários e Terceiros de Interesse.	*Estabelecer estratégias de comunicação assertiva visando adesão espontânea dos colaboradores e terceiros às diretrizes de proteção de dados da organização.*	
Etapa	Descritivo de tarefas da Etapa	
15. Elaboração do DPIA – Relatório de Impacto à Proteção de Dados	*Documento exigido pela legislação quando há tratamento de dados de acordo com certas bases de dados e, especialmente, quando há tratamento de dados sensíveis e dados de crianças e adolescentes.*	
Etapa	Descritivo de tarefas da Etapa	
16. Elaboração do LIA – Análise de Legítimo Interesse	*Assessment que leva em consideração os dados cuja base legal de tratamento é o legítimo interesse da organização Controladora/Operadora*	
Etapa	Descritivo de tarefas da Etapa	
17. MEDIDAS TÉCNICAS (Sistemas e Soluções Tecnológicas)	*Assessoramento na definição das medidas necessárias à garantia de implementação da Política de Segurança da Informação*	
Etapa	Descritivo de tarefas da Etapa	
18. GESTÃO DE RISCOS À PROTEÇÃO DE DADOS	*Assessoramento e acompanhamento visando implantação de medidas de tratamento do risco, dimensionadas de acordo com as características da organização.*	
Etapa	Descritivo de tarefas da Etapa	
19. PLANO DE REVISÃO DO PROGRAMA	*Adequação de Processos e Procedimentos de acordo com os indicadores do Programa de Compliance de Proteção de Dados Pessoais.*	

Controlador: Instituto Brasileiro de Avaliações e Perícias de

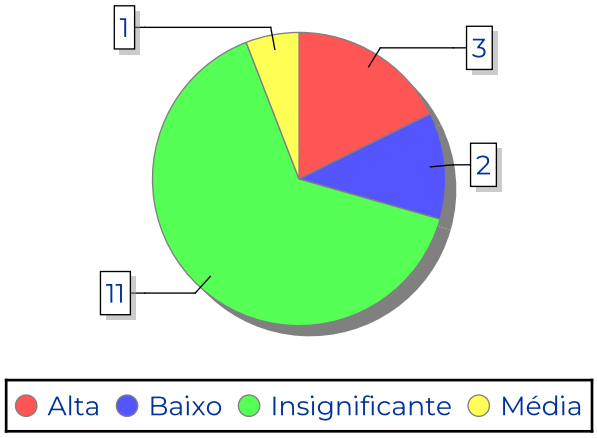
CPF/CNPJ: 65.714.784/0001-65

MONITORAMENTO E GESTÃO DE RISCOS

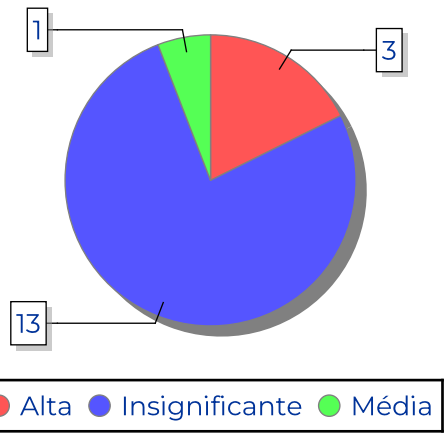
INSTITUTO BRASILEIRO DE AVALIAÇÕES E PERÍCIAS DE

18/05/2022

Riscos por Severidade

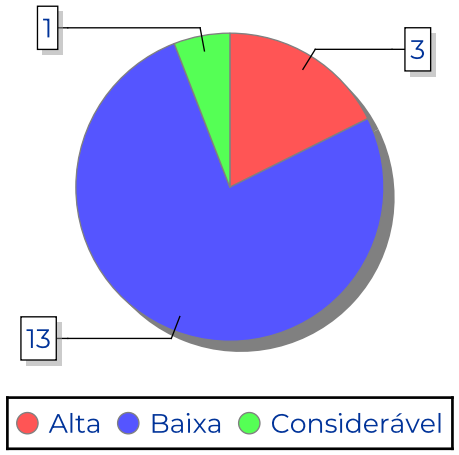


Riscos por Probabilidade



Riscos por Status

Riscos por Classe de Risco



		PROBABILIDADE			
		Insignificante	Baixa	Média	Alta
SEVERIDADE	Insignificante	11	0	0	0
	Baixa	2	0	0	0
	Média	0	0	1	0
	Alta	0	0	0	3

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Acesso não autorizado

RESPONSÁVEL: -

Acesso não autorizado aos dados pessoais.

AMEAÇAS	DANOS
O processo de compartilhamento das informações dentro da Instituição, entre colaboradores, é informal e não regulamentado.	Vazamento de dados pessoais; Imagem da empresa abalada; Processos cíveis e Multas.

FONTES DO RISCO

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Contratação e registro de funcionário
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Venda de Cursos ON-LINE
Processos de Negócio	Inscrição em evento gratuito do IBAPE/SP (público em geral)
Processos de Negócio	Organização de eventos/Convite a palestrantes e personalidades

Alta

SEVERIDADE: ALTA - PROBABILIDADE: ALTA - STATUS: NULL

Ataque cibernético

RESPONSÁVEL: -

Ataque cibernético de agente externo à empresa.

AMEAÇAS	DANOS
Dados pessoais são compartilhados em grande volume via e-mail.	Paralisação da operação por um período até normalização; Acesso dos dados por terceiro; Sanção aplicada pela ANPD e chance de

fiscalização e Abalo na confiança do cliente final com relação ao serviço

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Contratação e registro de funcionário
Processos de Negócio	Cobrança de anuidade do associado
Processos de Negócio	Atendimento e informações para potencial associado (Pré-cadastro)
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Venda de Cursos ON-LINE

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Coleta excessiva

RESPONSÁVEL: -

A coleta dos mesmos dados em processos distintos e registro/armazenamento em vários sistemas e plataformas pode trazer maior vulnerabilidade durante o tratamento destes. Há registro de dados coletados excessivamente, não se adequando ao princípio da necessidade.

AMEAÇAS	DANOS
Maior vulnerabilidade durante o tratamento dos dados pessoais.	Reclamação dos titulares e, caso, não solucionada, eventual sanção pela ANPD.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Emissão de Nota Fiscal
Processos de Negócio	Inscrição em evento gratuito do IBAPE/SP (público em geral)

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Compartilhamento com terceiros essências para a execução do contrato sem consentimento do titular

RESPONSÁVEL: -

Não há informação se o IBAPE deixa claro ao aluno, no momento da inscrição, que seus dados serão compartilhados com o CREA-SP para cumprimento, pelo CREA-SP, de execução de política pública.

AMEAÇAS	DANOS
Não há disposição clara nas políticas do IBAPE sobre quais dados serão compartilhados, como e com quem, com a finalidade única de garantir o fornecimento do serviço; Não há informação clara e inequívoca para o titular dos dados, haja vista que este não sabe com quem seus dados estão sendo compartilhados.	Reclamação por parte do titular; Denúncia junto à ANPD.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Fale conosco - solicitação de informações
Processos de Negócio	Convênio - CREA

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Dados armazenados em documentos físicos

RESPONSÁVEL: -

Arquivos físicos na sede do IBAPE.

AMEAÇAS	DANOS
Há registro de Arquivos Físicos na sede do IBAPE. Os armários possuem chave, porém, qualquer membro de qualquer departamento poderá ter acesso aos documentos. Não há processo de gestão desses documentos físicos e de acesso a eles.	Acesso indevido, cópia indevida, transferência indevida, sinistro no local do armazenamento

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Cadastro de Associado

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Desvio de finalidade de tratamento (dados compartilhados com terceiro)

RESPONSÁVEL: -

Não há um procedimento de gestão de finalidade dos dados.

AMEAÇAS	DANOS
Ausência de due dilligence e adequações contratuais para verificar se as disposições estão de acordo com a LGPD. Os dados coletados são utilizados para finalidades diversas dentro da organização, embora destinadas eventualmente ao cumprimento das finalidades sociais. Ausência de transparência quando ocorre a alteração de finalidade	Desvio de finalidade e responsabilização do IBAPE por eventual lesão ao direito do titular, Sanções por parte da ANPD

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	EVENTOS PAGOS do IBAPE/SP (público em geral)
Processos de Negócio	Convênio - CREA
Processos de Negócio	Cadastro de Associado
Processos de Negócio	Fornecimento de benefício - Plano de saúde
Processos de Negócio	Contratação e registro de funcionário
Processos de Negócio	Fornecimento de benefício - Vale refeição

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Controle de acesso e jornada por biometria
Processos de Negócio	Realização de Evento (PAGO)
Processos de Negócio	Cobrança de anuidade do associado
Processos de Negócio	Desenvolvimento de curso online
Processos de Negócio	Fornecimento de benefício - Vale transporte
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Inscrição em eventos pagos do IBAPE/SP (público geral)
Processos de Negócio	Venda de Cursos ON-LINE

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Falha em considerar o direito dos titulares

RESPONSÁVEL: -

A organização não tem processos de garantia de privacidade e proteção de dados para atendimento dos direitos dos titulares.

AMEAÇAS	DANOS
Ausência de Política, processo e controles para compartilhamento das informações dentro da Instituição, entre colaboradores; Ausência de Política, processo e controles de identificação dos níveis de acesso e alçada adequados ao tratamento das informações e dados pessoais de trabalhadores; não há política de retenção sobre dados quando for concluída a finalidade de seu tratamento, para eliminar dados que não são mais necessários; Não há um canal de atendimento para as demandas de titulares de dados tratados pela organização.	Reclamações do titular e denúncia junto à ANPD.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Atendimento e informações para potencial associado (Pré-cadastro)
Processos de Negócio	Estratégia de marketing - Disparo de e-mails marketing
Processos de Negócio	Venda de Cursos ON-LINE

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Inexistência de indicação de finalidade de tratamento

RESPONSÁVEL: -

Falta de transparência na indicação de finalidade de tratamento dos dados pessoais dos usuários.

AMEAÇAS	DANOS
Em certos processos, não há indicação da finalidade para a qual o dado pessoal coletado será tratado.	Reclamação de titular dos dados por retenção indevida.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Atendimento e informações para potencial associado (Pré-cadastro)
Processos de Negócio	Inscrição em eventos pagos do IBAPE/SP (público geral)

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Informação insuficiente ao titular sobre a finalidade do tratamento

RESPONSÁVEL: -

Ausência de informação aos titulares dos dados acerca da finalidade do tratamento.

AMEAÇAS	DANOS

Coleta de muitas informações e dados pessoais sem a devida comunicação/transparência da finalidade do tratamento. Principalmente quando os dados são usados para a finalidade informada e outra não informada.	Reclamação de titular dos dados e Sanção ANPD.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Inscrição em evento gratuito do IBAPE/SP (público em geral)
Processos de Negócio	Convênio - CREA
Processos de Negócio	Organização de eventos/Convite a palestrantes e personalidades
Processos de Negócio	Cadastro de Associado
Processos de Negócio	Fale conosco - solicitação de informações
Processos de Negócio	Controle de acesso e jornada por biometria
Processos de Negócio	Desenvolvimento de curso online
Processos de Negócio	Execução das reuniões das câmaras técnicas (online)
Processos de Negócio	Prestação de contas - Convênio - Ibape nacional
Processos de Negócio	Emissão de Nota Fiscal
Processos de Negócio	Estratégia de marketing - Disparo de e-mails marketing
Processos de Negócio	Inscrição em eventos pagos do IBAPE/SP (público geral)

Baixa

SEVERIDADE: BAIXO - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Modificação não autorizada (acidental ou intencional)

RESPONSÁVEL: -

O processo de compartilhamento das informações dentro da Instituição, entre colaboradores, é informal e não regulamentado.

AMEAÇAS	DANOS

Ausência de Política, processo e controles para compartilhamento das informações dentro da Instituição, entre colaboradores; Ausência de Política, processo e controles de identificação dos níveis de acesso e alçada adequados ao tratamento das informações e dados pessoais; Ausência de um processo que minimize a utilização de trocas de e-mails / exportar as informações dos sistemas utilizados. Verificar a possibilidade de todas as consultas serem diretamente nas plataformas e possibilidade de integração entre elas para uma gestão mais produtiva.	Lesões ao direito do titular e, caso não solucionado, podendo evoluir para fiscalização e sanções aplicadas pela ANPD.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Cadastro de Associado
Processos de Negócio	Contratação e registro de funcionário
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Venda de Cursos ON-LINE
Processos de Negócio	Inscrição em evento gratuito do IBAPE/SP (público em geral)

Alta

SEVERIDADE: ALTA - PROBABILIDADE: ALTA - STATUS: NULL

Perda

RESPONSÁVEL: -

A Organização armazena dados em ambientes físicos e virtuais, sem controle sobre o acesso.

AMEAÇAS	DANOS
Ausência de aderência dos Fornecedores de serviços e soluções tecnológicas que recebem dados em compartilhamento, estabelecendo compromissos e responsabilidades. Compartilhamento via e-mail. Ausência de Política de Segurança da informação. Vulnerabilidade dos sistemas e instrumentos informáticos.	Paralisação da operação por um período até normalização; Acesso dos dados por terceiro; Sanção aplicada pela ANPD e chance de fiscalização e Abalo na confiança do cliente

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Cadastro de Associado
Processos de Negócio	Contratação e registro de funcionário
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Venda de Cursos ON-LINE

Baixa

SEVERIDADE: BAIXO - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Remoção não autorizada

RESPONSÁVEL: -

O processo de compartilhamento das informações dentro da Instituição, entre colaboradores, é informal e não regulamentado.

AMEAÇAS	DANOS
Ausência de Política, processo e controles para compartilhamento das informações dentro da Instituição, entre colaboradores; Ausência de Política, processo e controles de identificação dos níveis de acesso e alçada adequados ao tratamento das informações e dados pessoais; Ausência de um processo que minimize a utilização de trocas de e-mails / exportar as informações dos sistemas utilizados. Verificar a possibilidade de todas as consultas serem diretamente nas plataformas e possibilidade de integração entre elas para uma gestão mais produtiva.	Lesão ao direito do titular e eventual fiscalização ou sanção aplicada pela ANPD.

FONTES DO RISCO	
Tipo de Fonte	Fonte do Risco
Processos de Negócio	Cadastro de Associado
Processos de Negócio	Contratação e registro de funcionário

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Venda de Cursos ON-LINE
Processos de Negócio	Inscrição em evento gratuito do IBAPE/SP (público em geral)

Considerável

SEVERIDADE: MÉDIA - PROBABILIDADE: MÉDIA - STATUS: NULL

Responsabilidade civil por ato de terceiro que recebe o dado

RESPONSÁVEL: -

Há registro de processos conduzidos por Operadores que assumem a condição de CO-CONTROLADORES dos dados completados e tratados pelo IBAPE (coleta, extração, organização de banco de dados, atendimento e acompanhamento durante as aulas).

AMEAÇAS	DANOS
Ausência de contrato entre o IBAPE e o OPERADOR firmando TERMO DE RESPONSABILIDADE DE CO-CONTROLADOR DE DADOS, especialmente por conta dos níveis de acesso que alguns prestadores de serviços possuem(revisar responsabilidades assumidas no contrato de prestação de serviços).	Reclamação do titular e Sanção aplicada pela ANPD

FONTES DO RISCO

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Venda de Cursos ON-LINE
Processos de Negócio	EVENTOS PAGOS do IBAPE/SP (público em geral)
Processos de Negócio	Convênio - CREA
Processos de Negócio	Cadastro de Associado
Processos de Negócio	Fornecimento de benefício - Plano de saúde
Processos de Negócio	Contratação e registro de funcionário

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Fale conosco - solicitação de informações
Processos de Negócio	Realização de Evento (PAGO)
Processos de Negócio	Fornecimento de benefício - Vale refeição
Processos de Negócio	Controle de acesso e jornada por biometria
Processos de Negócio	Cobrança de anuidade do associado
Processos de Negócio	Desenvolvimento de curso online
Processos de Negócio	Fornecimento de benefício - Vale transporte
Processos de Negócio	Gestão de Folha de Pagamento

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Retenção prolongada dos dados com exigência legal ou regulatória

RESPONSÁVEL: -

Os dados que são coletados dos usuários para uma finalidade específica, já informada aos usuários, mesmo após cessada essa finalidade, são mantidos pelo IBAPE. Não há um processo nem gestão do prazo para retenção e descarte.

AMEAÇAS	DANOS
Ausência de política de retenção de dados com prazo para exclusão dos dados do titular da plataforma; Ausência de política de prazo de retenção dos dados do funcionário acerca da contratação de plano de saúde;	Reclamação dos titulares e denuncia à ANPD

FONTES DO RISCO

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Contratação e registro de funcionário

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Controle de acesso e jornada por biometria
Processos de Negócio	Fornecimento de benefício - Vale transporte
Processos de Negócio	Emissão de Nota Fiscal
Processos de Negócio	Gestão de Folha de Pagamento

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Retenção prolongada dos dados sem exigência legal ou regulatória

RESPONSÁVEL: -

O IBAPE realiza o tratamento de dados pessoais por fundamento legal ou interesse legítimo, mas sem dever ou exigência legal ou regulatória, em alguns casos. Para esse conjunto de dados, nos processos analisados, não há uma diretriz sobre o prazo de manutenção ou critérios para descarte dos dados desnecessários.

AMEAÇAS	DANOS
Ausência de política de retenção de dados com prazo para exclusão dos dados do titular da plataforma; Ausência de política de prazo de retenção dos dados do funcionário acerca da contratação de plano de saúde;	Ausência de política de retenção de dados com prazo para exclusão dos dados do titular da plataforma; Ausência de política de prazo de retenção dos dados do funcionário acerca da contratação de plano de saúde.

FONTES DO RISCO

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Fale conosco - solicitação de informações
Processos de Negócio	Desenvolvimento de curso online
Processos de Negócio	Cobrança de anuidade do associado
Processos de Negócio	Atendimento e informações para potencial associado (Pré-cadastro)

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Execução das reuniões das câmaras técnicas (online)
Processos de Negócio	Estratégia de marketing - Disparo de e-mails marketing
Processos de Negócio	Desligamento de associado
Processos de Negócio	Inscrição em eventos pagos do IBAPE/SP (público geral)
Processos de Negócio	Venda de Cursos ON-LINE
Processos de Negócio	Convênio - CREA

Alta

SEVERIDADE: ALTA - PROBABILIDADE: ALTA - STATUS: NULL

Roubo

RESPONSÁVEL: -

A Organização armazena dados em ambientes físicos e virtuais, sem controle sobre o acesso. No caso do armazenamento físico, além dos arquivos localizados na sede da organização, há terceirização do serviço de armazenagem. É recomendado elaborar / repensar a política de acessos aos sistemas e diretórios dos arquivos considerando uma política de acesso mínimo.

AMEAÇAS	DANOS
Ausência de aderência dos Fornecedores de serviços e soluções tecnológicas que recebem dados em compartilhamento. Compartilhamento via e-mail pode ensejar em maior vulnerabilidade do IBAPE com relação à incidentes de segurança. Ausência de Política de Segurança da informação.	1 - Paralisação da operação por um período até normalização; 2 - Acesso dos dados por terceiro; 3 - Sanção aplicada pela ANPD e chance de fiscalização; 4 - Abalo na confiança do cliente

FONTES DO RISCO

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Cadastro de Associado

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Contratação e registro de funcionário
Processos de Negócio	Gestão de Folha de Pagamento
Processos de Negócio	Venda de Cursos ON-LINE

Baixa

SEVERIDADE: INSIGNIFICANTE - PROBABILIDADE: INSIGNIFICANTE - STATUS: NULL

Vinculação indevida

RESPONSÁVEL: -

Nos contratos de cursos, divulgações de eventos e outras atividades, não há informação clara sobre o uso de e-mail disponibilizado pelo titular para fins de marketing.

AMEAÇAS	DANOS
Nos materiais de inscrição para cursos, eventos ou demais atividades, ausência de cláusula específica solicitando autorização para utilização dos dados com finalidade de divulgação de atividades realizadas pelo IBAPE (e-mail marketing);	Reclamação por parte do titular; Denúncia junto à ANPD

FONTES DO RISCO

Tipo de Fonte	Fonte do Risco
Processos de Negócio	Estratégia de marketing - Disparo de e-mails marketing

Relatório de Tratamento de Dados Pessoais

Controlador: Instituto Brasileiro de Avaliações e Perícias de

CPF/CNPJ: 65.714.784/0001-65

TRATAMENTO DE DADOS DE PALESTRANTES E PERSONALIDADES

Responsável:

Diretoria de Eventos - Fabiana Albano

Dados Sensíveis?

Sim

Finalidade:

Organização de eventos

-

DADOS PESSOAIS			
Nome	Foto	Dado biométrico	Escolaridade
Formação acadêmica	Empresa	Cargo	Telefone Celular
E-mail			

CATEGORIA DE PESSOA
Palestrantes e personalidades

CATEGORIA DE DADOS		
Dados de identificação direta do titular	Dados de contato do titular	Dados profissionais
Dados de formação acadêmica		

SISTEMAS

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DEV	Diretoria de Eventos	Organização de eventos/Convite a palestrantes e personalidades
DEV	Diretoria de Eventos	Realização de Evento (PAGO)
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Interesses legítimos	
Contrato	

TRATAMENTO DE DADOS DE PARTICIPANTES DO EVENTO

Responsável:

Diretoria de Eventos - Fabiana Albano

Dados Sensíveis?

Não

Finalidade:

Organizar evento e cumprir obrigação assumida perante terceiros

-

DADOS PESSOAIS			
Nome	CPF	Telefone Celular	E-mail

CATEGORIA DE PESSOA
Participantes do Evento

CATEGORIA DE DADOS	
Dados de identificação direta do titular	Dados de contato do titular

SISTEMAS
ERP TRD

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DCULT	Diretoria Cultural	Prestação de contas - Convênio - Ibape nacional
DEV	Diretoria de Eventos	Inscrição em evento gratuito do IBAPE/SP (público em geral)
DEV	Diretoria de Eventos	Inscrição em eventos pagos do IBAPE/SP (público geral)
DEV	Diretoria de Eventos	Realização de Evento (PAGO)
DI	Diretoria Institucional	Convênio - CREA
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Interesses legítimos	IX - QUANDO NECESSÁRIO PARA ATENDER AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO, EXCETO NO CASO DE PREVALECEREM DIREITOS E LIBERDADES FUNDAMENTAIS DO TITULAR QUE EXIJAM A PROTEÇÃO DOS DADOS PESSOAIS; OU
Contrato	V - QUANDO NECESSÁRIO PARA A EXECUÇÃO DE CONTRATO OU DE PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO DO QUAL SEJA PARTE O TITULAR, A PEDIDO DO TITULAR DOS DADOS;

COMPARTILHAMENTO DE DADOS PESSOAIS		
COMPARTILHAMENTO/ FINALIDADE	PROCEDIMENTOS/POSSUI CONSENTIMENTO?	AGENTE/RESPONSÁVEL
Plataforma B2B Colher inscrição dos cadastrados em eventos	Não	
TRD Armazenamento de dados	Não	

TRATAMENTO DE DADOS COLABORADORES

Responsável:

Coordenador Administrativo - Fernando Aguiar

Dados Sensíveis?

Sim

Finalidade:

Registro de funcionários; gestão de folha de pagamento e fornecimento de benefícios como plano de saúde, vale transporte e vale refeição

-

DADOS PESSOAIS			
Matrícula	Nome	Foto	CPF
Carteira de Identidade	Título de eleitor	Carteira de trabalho	Número do PIS
Dado biométrico	Naturalidade	Nacionalidade	Data de nascimento
Escolaridade	Estado Civil	Sexo	Exame médico
Atestado médico	Controle de presença	Formação acadêmica	Empresa
Cargo	Renda	Endereço residencial	Endereço comercial
Telefone residencial	Telefone comercial	Telefone Celular	E-mail
Conta corrente	Transações bancárias	Nome do cônjuge	CPF do cônjuge
RG do cônjuge	Nome dos filhos	CPF do filho	RG do filho

CATEGORIA DE PESSOA	
Colaboradores	

CATEGORIA DE DADOS		
Dados de identificação direta do titular	Dados de contato do titular	Dados de saúde do titular
Dados profissionais	Dados de formação acadêmica	Dados de licenças e ausência
Dados bancários	Dados de transação financeira	

SISTEMAS		
Outlook (e-mails corporativos)	Sistema de ponto	ERP TRD
CONTMATIC		

INFRAESTRUTURA DE TI		
Servidor do sistema de ponto	Estações de trabalho corporativas	Nuvem do ERP

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
RH	Recursos Humanos	Contratação e registro de funcionário
RH	Recursos Humanos	Controle de acesso e jornada por biometria
RH	Recursos Humanos	Fornecimento de benefício - Plano de saúde
RH	Recursos Humanos	Fornecimento de benefício - Vale refeição
RH	Recursos Humanos	Fornecimento de benefício - Vale transporte
RH	Recursos Humanos	Gestão de Folha de Pagamento

DOCUMENTOS FÍSICOS		
DOCUMENTO/TIPO/DIGITALIZADO/DESCRIÇÃO	LOCAL/TIPO ARMAZENAMENTO	RESPONSÁVEL
null: Arquivos físicos dos associados Não	IBAPE SP Arquivos Físico no IBAPE	
null: Arquivos físicos de associados Não	ArquivoNET Arquivo NET	

PERMISSÕES DE ACESSO			
RAZÃO	PERMISSÃO	ACESSADO POR	CONCEDIDO POR
Administrar a gestão de colaboradores.	Administrar	Gerente de Recursos Humanos	Diretor Administrativo
Realizar as atividade de gestão de colaboradores.	Ler e Gravar	Analista de RH	Gerente de Recursos Humanos

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Obrigação Legal	http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452compilado.htm

BASE LEGAL	EVIDÊNCIAS
Contrato	Contrato de trabalho.

COMPARTILHAMENTO DE DADOS PESSOAIS		
COMPARTILHAMENTO/ FINALIDADE	PROCEDIMENTOS/POSSUI CONSENTIMENTO?	AGENTE/RESPONSÁVEL
Plano de saúde Disponibilizar plano de saúde aos colaboradores.	Ficha de cadastro preenchida em formulário online no site da operadora do plano. Não	AMIL Fernando Aguiar
Vale refeição e alimentação Disponibilizar vale refeição e alimentação aos colaboradores.	Ficha de cadastro preenchida em formulário online no site da empresa. Não	Alelo Fernando Aguiar
Folha de pagamento Rodar a folha de pagamento dos funcionários.	Troca de e-mail com a contabilidade. Não	Empresa de Contabilidade Fernando Aguiar

TRANSFERÊNCIA INTERNACIONAL		
TRANSFERÊNCIA FINALIDADE	LOCALIDADE/PROCEDIMENTOS	AGENTE/RESPONSÁVEL
Nuvem Microsoft Armazenar contrato de trabalho e documentos na nuvem da Microsoft.	Estados Unidos Utilização do Onedrive e Sharepoint corporativos.	Nome do Gerente de RH Microsoft

POLÍTICA DE RETENÇÃO		
TEMPORALIDADE PERIODICIDADE	CRITÉRIO	JUSTIFICATIVA PROCEDIMENTOS

POLÍTICA DE DESCARTE		
DISPOSIÇÃO FINAL	RESPONSÁVEL	PROCEDIMENTOS
-	-	

TRATAMENTO DE DADOS INTERESSADOS EM INFORMAÇÕES SOBRE A ENTIDADE

Responsável:

Coordenador Administrativo - Fernando Aguiar

Dados Sensíveis?

Não

Finalidade:

Prestar informações ao solicitante

-

DADOS PESSOAIS		
Nome	Telefone Celular	E-mail

CATEGORIA DE PESSOA
Interessados em informações sobre a Entidade

CATEGORIA DE DADOS	
Dados de identificação direta do titular	Dados de contato do titular

SISTEMAS		
Outlook (e-mails corporativos)	Agenda no celular coorporativo	Whatsapp coorporativo

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DADM	Diretoria Administrativa	Fale conosco - solicitação de informações
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Consentimento	

TRATAMENTO DE DADOS ALUNOS - CURSOS IBAPE

Responsável:

Diretoria Cultural - Paulo Magri

Dados Sensíveis?

Não

Finalidade:

Arrecadar receita para a associação; fornecer o curso adquirido; realizar a emissão de notas fiscais; prestar contas ao convênio com o Ibape Nacional.

-

DADOS PESSOAIS			
Nome	CPF	Data de nascimento	Endereço residencial
Telefone Celular	E-mail		

CATEGORIA DE PESSOA
Alunos - Cursos IBAPE

CATEGORIA DE DADOS	
Dados de identificação direta do titular	Dados de contato do titular

SISTEMAS
IBAPE CONECTA EAD

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DCULT	Diretoria Cultural	Desenvolvimento de curso online
DCULT	Diretoria Cultural	Emissão de Nota Fiscal
DCULT	Diretoria Cultural	Prestação de contas - Convênio - Ibape nacional
DCULT	Diretoria Cultural	Venda de Cursos ON-LINE
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Interesses legítimos	
Contrato	
Obrigação Legal	

TRATAMENTO DE DADOS ASSOCIADO - ESTUDANTE

Responsável:

-

Dados Sensíveis?

Não

Finalidade:

Garantir o cumprimento das exigências associativas da Entidade, bem como garantir ao associado acesso aos serviços e benefícios fornecidos pela Entidade

-

DADOS PESSOAIS			
Nome	Foto	CPF	Carteira de Identidade
Naturalidade	Nacionalidade	Data de nascimento	Escolaridade
Estado Civil	Sexo	Formação acadêmica	Endereço residencial
Telefone residencial	Telefone Celular	E-mail	

CATEGORIA DE PESSOA
Associados - estudantes

CATEGORIA DE DADOS		
Dados de identificação direta do titular	Dados de contato do titular	Dados de formação acadêmica

SISTEMAS

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DFIN	Diretoria Financeira	Cobrança de anuidade do associado
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing
SC	Setor de Cadastro	Cadastro de Associado
SC	Setor de Cadastro	Desligamento de associado
SC	Setor de Cadastro	Licenciamento de associado

DOCUMENTOS FÍSICOS		
DOCUMENTO/TIPO/DIGITALIZADO/DESCRIÇÃO	LOCAL/TIPO ARMAZENAMENTO	RESPONSÁVEL
null: Arquivos físicos dos associados Não	IBAPE SP Arquivos Físico no IBAPE	
null: Arquivos físicos de associados Não	ArquivoNET Arquivo NET	

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Contrato	

COMPARTILHAMENTO DE DADOS PESSOAIS		
COMPARTILHAMENTO/ FINALIDADE	PROCEDIMENTOS/POSSUI CONSENTIMENTO?	AGENTE/RESPONSÁVEL
Registro de informações no sistema TRD Armazenamento em nuvem	Não	
ArquivoNET Armazenamento de documentos fisicos	Não	

TRATAMENTO DE DADOS ASSOCIADOS - EMPRESA E/OU PATROCINADOR

Responsável:

-

Dados Sensíveis?

Não

Finalidade:

Garantir o cumprimento das exigências associativas da Entidade, bem como garantir ao associado acesso aos serviços e benefícios fornecidos pela Entidade

-

DADOS PESSOAIS			
Nome	Telefone residencial	Telefone comercial	Telefone Celular
E-mail			

CATEGORIA DE PESSOA
Associado - Empresa e/ou Patrocinador

CATEGORIA DE DADOS	
Dados de identificação direta do titular	Dados de contato do titular

SISTEMAS		
Outlook (e-mails corporativos)	ERP TRD	CONTMATIC
Serviço de e-mail da Localweb		

INFRAESTRUTURA DE TI	
Servidor de Arquivos	Nuvem do ERP

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DFIN	Diretoria Financeira	Cobrança de anuidade do associado
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing
SC	Setor de Cadastro	Cadastro de Associado
SC	Setor de Cadastro	Desligamento de associado
SC	Setor de Cadastro	Licenciamento de associado

DOCUMENTOS FÍSICOS		
DOCUMENTO/TIPO/DIGITALIZADO/DESCRIÇÃO	LOCAL/TIPO ARMAZENAMENTO	RESPONSÁVEL
null: Arquivos físicos dos associados Não	IBAPE SP Arquivos Físico no IBAPE	
null: Arquivos físicos de associados Não	ArquivoNET Arquivo NET	

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Contrato	

COMPARTILHAMENTO DE DADOS PESSOAIS		
COMPARTILHAMENTO/ FINALIDADE	PROCEDIMENTOS/POSSUI CONSENTIMENTO?	AGENTE/RESPONSÁVEL
Registro de informações no sistema TRD Armazenamento em nuvem	Não	
ArquivoNET Armazenamento de documentos fisicos	Não	

TRATAMENTO DE DADOS ASSOCIADOS - TITULARES

Responsável:

-

Dados Sensíveis?

Sim

Finalidade:

Os dados são tratados para garantir o cumprimento das exigências associativas da Entidade, bem como garantir ao associado o acesso aos serviços e benefícios fornecidos pela Entidade.

-

DADOS PESSOAIS			
Nome	Foto	CPF	Carteira de Identidade
Naturalidade	Nacionalidade	Data de nascimento	Escolaridade
Estado Civil	Formação acadêmica	Endereço residencial	Endereço comercial
Telefone residencial	Telefone comercial	Telefone Celular	E-mail

CATEGORIA DE PESSOA
Associados - Titulares

CATEGORIA DE DADOS		
Dados de identificação direta do titular	Dados de contato do titular	Dados profissionais
Dados de formação acadêmica		

SISTEMAS

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DFIN	Diretoria Financeira	Cobrança de anuidade do associado
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing
SC	Setor de Cadastro	Cadastro de Associado
SC	Setor de Cadastro	Desligamento de associado
SC	Setor de Cadastro	Licenciamento de associado

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Contrato	

COMPARTILHAMENTO DE DADOS PESSOAIS		
COMPARTILHAMENTO/ FINALIDADE	PROCEDIMENTOS/POSSUI CONSENTIMENTO?	AGENTE/RESPONSÁVEL
Registro de informações no sistema TRD Armazenamento em nuvem	Não	
ArquivoNET Armazenamento de documentos fisicos	Não	

TRATAMENTO DE DADOS DE PARTICIPANTES DOS CURSOS

Responsável:

-

Dados Sensíveis?

Não

Finalidade:

Arrecadar receita para a associação e qualificar os alunos e associados

-

DADOS PESSOAIS			
Nome	CPF	Data de nascimento	Endereço residencial
Telefone Celular	E-mail		

CATEGORIA DE PESSOA
Participante do Curso

CATEGORIA DE DADOS	
Dados de identificação direta do titular	Dados de contato do titular

SISTEMAS	
ERP TRD	IBAPE CONECTA EAD

INFRAESTRUTURA DE TI

ÁREAS E PROCESSOS DE NEGÓCIO		
SIGLA	ÁREA	PROCESSO DE NEGÓCIO
DCULT	Diretoria Cultural	Desenvolvimento de curso online
DCULT	Diretoria Cultural	Emissão de Nota Fiscal
DCULT	Diretoria Cultural	Prestação de contas - Convênio - Ibape nacional
DCULT	Diretoria Cultural	Venda de Cursos ON-LINE
DI	Diretoria Institucional	Convênio - CREA
DI	Diretoria Institucional	Estratégia de marketing - Disparo de e-mails marketing

BASES LEGAIS	
BASE LEGAL	EVIDÊNCIAS
Obrigação Legal	
Contrato	
Interesses legítimos	