invenções. A quebra da confidencialidade ou uso impróprio das informações é inaceitável. É vedado o uso das informações sobre atividades, assuntos do ISV ou pacientes para favorecimento próprio ou de terceiros. As senhas de acesso às informações são mecanismos de proteção das informações, devendo ser individual e intransferível, e seu compartilhamento será considerado inaceitável

09| O Auditoria Interna e externa

O ISV e os funcionários cooperarão com auditorias internas e externas assistenciais e administrativas.

O ISV e os funcionários deverão resguardar os registros ou documentos relacionados com colaboradores, saúde ocupacional, segurança, meio ambiente, financeiro e contábil, projetos de responsabilidade social e de pacientes, seguindo a temporalidade prevista pelos órgãos normatizadores.

10| Manutenção de registros e contabilização precisa

É obrigação do ISV manter livros, registros e contas que reflitam, de forma detalhada, precisa e correta, todas as suas transações. As transações do ISV são transparentes, totalmente documentadas e codificadas para contas que refletem de maneira precisa a sua natureza.

O ISV mantém controles internos que oferecem razoável segurança de que:

Todas as operações executadas sejam aprovadas conforme as alçadas e limites estabelecidos;

Todas as operações sejam registradas conforme necessário para permitir a elaboração das demonstrações financeiras de acordo com os princípios contábeis geralmente aceitos ou qualquer critério aplicável a estas demonstrações e para manter o controle dos ativos;

Todo pagamento deverá conter uma justificativa, ainda que breve, de forma a ficar incorporado a que se refere e qual a necessidade deste pagamento para o ISV e a sua adequação com o preço de mercado. Assim, serão evitados eventuais pagamentos de suborno, por meio de empresas de fachada, facilitando a detecção de ilícitos;

Os acessos aos ativos somente sejam permitidos de acordo com a aprovação geral ou específica da diretoria executiva do ISV;

Os ativos registrados sejam confrontados com os ativos existentes em intervalos razoáveis e que medidas apropriadas sejam tomadas em relação a quaisquer diferenças.

11 | Conscientização e treinamento

O ISV manterá um programa permanente de conscientização e treinamento anticorrupção para os colaboradores da sede e de suas unidades.

São ministrados treinamentos que apresentam as políticas e normas anticorrupção e o Código de Ética.

12 |Certificados

Todos os empregados indicados, pela Superintendência de Compliance, para participar obrigatoriamente, de treinamento anticorrupção deverão, como parte da conclusão bem-sucedida de seu treinamento, certificar, por escrito:

Que receberam, entenderam e cumprirão as políticas e procedimentos relacionados ao compliance anticorrupção;

Que agiram e continuarão a agir em cumprimento de tais políticas e procedimentos;

Que imediatamente relatarão quaisquer alegações, violações ou questões relacionadas à compliance de que tomem conhecimento.

13| Comunicação e declaração à imprensa

As declarações a imprensa serão realizadas exclusivamente pela assessoria de comunicação, com prévio alinhamento com a Diretoria Executiva do ISV.

O ISV se compromete em transmitir as informações necessárias com transparência e veracidade.

Informações sobre produtos e serviços prestados devem ser verdadeiras, completas, atualizadas e, sempre que aplicável e necessário, devem ser baseadas por evidências científicas.

14| Redes e mídias sociais

Não é permitido o uso de redes e mídias sociais pelos colaboradores durante o expediente de trabalho, exceto em áreas em que o escopo de trabalho exige esse acesso (como marketing e outras) ou em campanhas institucionais.

É importante que o profissional esteja ciente que seu dever é estar disponível para o trabalho e não para passar o tempo em outras atividades.

Os colaboradores e profissionais do ISV devem respeitar as recomendações em relação ao uso de mídia social pessoal, fazendo referência às unidades geridas pelo ISV como objetivo de preservar as informações e o sigilo do paciente, colaboradores e estagiários:

Não divulgar ou compartilhar imagens, vídeos ou informações internas do ISV que não tenham sido divulgadas nas páginas oficiais do ISV e das unidades geridas.

Não manifestar opiniões dando entender que se trata de um posicionamento oficial do ISV.

Não expor imagens e/ou informações de clientes, usuários, parceiros e fornecedores.

15| Propriedade intelectual e proteção da marca

Instituto São Vicente = ISV

Deve-se proteger a marca e a propriedade intelectual do mau uso, desvio ou benefício próprio e também ter cuidado em relação à propriedade intelectual de terceiros.

A marca do ISV e o conhecimento produzido internamente pelo desenvolvimento de suas atividades ou em parceria são patrimônios institucionais e devem ser sempre protegidos por todos que esta política se aplica.

A propriedade intelectual do ISV se aplica ao seu direito de proteção às ideias de criações desenvolvidas internamente ou em parceria e inclui sua marca, patente, registro de software, direitos autorais.

16| Gestão do Aprendizado e Ensino.

A parceria de ensino entre o ISV e instituições conveniadas é pautada pela ética e profissionalismo, devendo ser declarado qualquer conflito de interesse existente. Algumas recomendações devem ser seguidas:

Nas exposições de aulas e/ou palestras, os vínculos institucionais devem ser declarados.

A escolha do material apresentado sempre deve ser feita baseada nos critérios técnicos e científicos.

Apoios e patrocínios não podem estar condicionados à interferência na programação, nos objetivos, local ou seleção de palestrantes.

Colaboradores e profissionais que forem convidados a ministrar palestras de temas inerentes à Instituição, em eventos externos, devem comunicar o convite ao ISV por meio do gestor imediato da área de ensino, para avaliação e aprovação.

17| Canal para Denúncias.

É dever de todos os colaboradores, fornecedores, prestadores de serviços e clientes, sempre que tiverem conhecimento ou vivenciarem uma situação que possa caracterizar uma conduta que viole o código de ética, as demais políticas e os princípios éticos do ISV e/ou a legislação e regulamentação vigente ou quando suspeitar ou souber de fatos que possam prejudicar a empresa, comunicar a Instituição via Canal de Denúncias.

A comunicação de suspeitas ou violações será reportada através do Canal de Denúncias, acessível aos colaboradores, fornecedores, prestadores de serviços e clientes, ficando garantida, ao denunciante, de boa-fé, a inocorrência de qualquer represália ou punição em decorrência da sua atitude.

O canal de denúncias é confidencial, neutro e independente, garantindo a isenção em relação a qualquer das partes, seja a que está denunciando ou a que está sendo denunciada sem levar em consideração o nível hierárquico dos envolvidos.

Além disso, através do Canal de Denúncias, as dúvidas ou preocupações podem ser submetidas de forma anônima.

Encontram-se disponibilizados os seguintes canais de comunicação:

INTERNET: https://www.institutosaovicente.com.br - FALE CONOSCO

18| Sanções

É responsabilidade de todos os colaboradores comunicar qualquer violação e suspeita de violação aos requisitos das leis anticorrupção. Às sanções aplicadas em casos de infrações deste código de ética podem ser:

1. Advertência verbal;
2. Advertência por escrito;
3. Suspensão;
4. Dispensa sem justa causa; e
5. Dispensa por justa causa.

Além das punições acima mencionadas, as violações às leis anticorrupção podem resultar em severas penalidades civis e criminais para o ISV e para seus colaboradores e/ou representantes envolvidos.

As penalidades criminais podem ser impostas tanto às pessoas físicas como às pessoas jurídicas.

Quando da comunicação das violações, deverá ocorrer a pronta interrupção de irregularidades ou infrações detectadas, cabendo, à Comissão de Ética Institucional do ISV, a tempestiva tratativa e remediação dos danos gerados, com a aplicação de suspensão cautelar do funcionário que possa atrapalhar a apuração.

O ISV não vai permitir ou tolerar qualquer tipo de retaliação contra qualquer pessoa que apresente uma denúncia de boa-fé ou a queixa de violação desta política.

Qualquer colaborador que se envolver em retaliação está sujeito a atos disciplinares.

As penalidades a serem aplicadas deverão ser sugeridas, após análise e comprovação do dolo, pela Comissão de Ética Institucional do ISV, com homologação pelo Diretor Presidente do ISV.

19| Revisão de Programa Anticorrupção

A Comissão de Ética Institucional do ISV avaliará periodicamente a eficácia do Programa de Integridade e relatará os resultados à Diretoria Executiva do ISV.

Esta revisão ocorrerá, pelo menos, uma vez ao ano, com equipe interna ou por meio de contratação de empresa de auditoria independente, diante dos resultados obtidos por meio do mapeamento de riscos, que deverá ser realizado com a mesma periodicidade mencionada neste item.

20| Documentação e manutenção

A Superintendência de Compliance documentará regularmente as iniciativas de compliance anticorrupção do ISV, para comprovar que a instituição disseminou, implantou e fez cumprir seu Programa de Integridade, conforme expectativa dos órgãos reguladores brasileiros.

Adicionalmente, é sua responsabilidade o arquivamento de Relatórios de Revisões de Compliance e relatos de atividades suspeitas.

Certificados de treinamentos relacionados à Compliance serão mantidos no dossiê do colaborador, sob a supervisão da Superintendência de Desenvolvimento Humano Organizacional.

21| Disposições gerais

As diretrizes contidas neste CÓDIGO DE ÉTICA são baseadas no propósito, na missão, nos valores e na visão do INSTITUTO SÃO VICENTE, refletindo assim o compromisso com um modo de agir ético, consciente, sustentável e equilibrado.

A responsabilidade e o cumprimento das normas, políticas e práticas estabelecidas no Código são dever e obrigação de cada colaborador.

Todos os colaboradores deverão ler o presente Código.

22| Termo de conhecimento e compromisso

Eu, matrícula nº , declaro, para os devidos fins de direito, que estou ciente dos termos do Código de Ética do ISV, na sua integralidade, comprometendo-me a cumprir todas as suas disposições, sob pena de incorrer nas punições estabelecidas.

De acordo,

(Local) /(UF)

Assinatura

23| Anexo | Modelo de declaração

DECLARO, nos termos do item 6.13 do Código de Ética Institucional do ISV, que a entidade inscrita no CNPJ sob o n. , sediada na Rua, beneficiada com a doação, ora realizada, não tem relação com familiares até segundo grau ou sócios de servidores públicos que tenham vínculo com a atividade do Instituto São Vicente – ISV.

INSTITUTO
SÃO VICENTE

código de Ética

(88) 3536-1280

www.institutosaovicente.com.br

Instituto São Vicente

REGULAMENTO DE AQUISIÇÃO DE BENS E SERVIÇOS

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA
CNPJ: 07.609.365/0001-67

Art. 1º. Este Regulamento tem por objetivo definir os critérios e as condições a serem observados pelo ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA doravante denominado ISV, para a realização de compras e contratações de quaisquer bens ou serviços destinados ao regular atendimento das necessidades organizacionais e operacionais da entidade na execução dos seus objetivos institucionais,inclusive na execução de Contratos de Gestão firmados com o Poder Público, regidas pelos princípios da moralidade, probidade, economicidade, impessoalidade, isonomia, bem como pela busca permanente da qualidade, boa-fé, isonomia, publicidade, dinamicidade, motivação das decisões, julgamento objetivo das propostas, vinculação ao instrumento convocatório e prevalência do interessepúblico.

Parágrafo único - O presente regulamento é de aplicação obrigatória quando as compras, contrataçõesde obras e serviços decorrerem dos recursos públicos repassados por meio de contratos de gestão, em conformidade com a Lei Federal 9.637/98;

Art. 2º. O Setor de Compras e/ou Diretor Administrativo-Financeiro do ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA tem como finalidade cuidar de toda e qualquer aquisição de bens, produtos ou serviços destinados, direta ou indiretamente, a serem empregados na prestação dos serviços, nos contratos e convênios celebrados com o Instituto.

Parágrafo único. Considera-se compra toda aquisição remunerada de bens de consumo e medicamentos, equipamentos, gêneros alimentícios, materiais permanentes e outros, além da prestação de serviços por pessoas físicas e jurídicas com a finalidade de suprir as necessidades do Instituto paradesenvolvimento de suas atividades.

Art. 3º. Constituem objetivos fundamentais deste Regulamento:

I. Garantir a impessoalidade na seleção da melhor proposta;

II. Fornecer regras objetivas para escolha e contratação;

III. Promover a transparência na gestão da Organização Social;

IV. Buscar a eficiência, celeridade e economicidade;

Art. 4º. Nos procedimentos descritos neste regulamento serão observados, dentre outros princípios, ficará igualmente vinculado ao instrumento convocatório e prevalência do interesse público.

Art. 5º. É garantido, em qualquer caso deste Regulamento, o direito de revogar o procedimento

escolha, ou recusar-se em proceder na contratação com o vencedor, quando este, emcontrato anterior com a Administração Pública ou com a própria Organização Social, se enquadrar emnas hipóteses abaixo:

I. Demonstrou falha ou má-qualidade na prestação do serviço;

II. Incapacidade técnica devidamente comprovada;

I. Estiver em período de suspensão temporária de participação em licitação e impedimento de contratar com a Administração Pública;

II. Sofreu penalidade de declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

Parágrafo único. O disposto no caput não gera qualquer direito de indenização ao fornecedor excluído, devendo ser fundamentado pelo responsável do Setor de Compras e/ou Diretor Administrativo-Financeiro, em relatório que será parte integrante do procedimento.

Art. 6º - Para efeito deste regulamento, considera-se:

I. **Obra:** toda construção, reforma, fabricação, recuperação ou ampliação realizada por execução diretaou indireta;

II. **Serviço:** a prestação de atividade de qualquer natureza por pessoas físicas e/ou jurídicas, necessárias ao funcionamento da Organização Social e das obrigações assumidas no Contrato de Gestão;

Compra: toda aquisição remunerada de bens e materiais de consumo para fornecimento de uma só vez ou parceladamente;

III. **Fornecedor:** não somente o fabricante do material, mas também seus representantes, grupo de compras, e distribuidores autorizados.

Art. 7º. O procedimento interno para aquisição de bens e contratação de obras ou serviços será iniciadocom a abertura de TERMO FORMALIZADO e numerado, pelo Setor de Compras e/ou Diretor Administrativo-Financeiro, contendo:

I. Solicitação com a indicação de seu objeto;

II. Autorização da despesa pelo responsável;

III. Relatório do Setor de Compras;

IV. **Parágrafo único.** Em todas as modalidades previstas nesse Regulamento, a empresa vencedora deve comprovar sua regularidade jurídico-fiscal para prestação do objeto contratado.

V. **Art. 8º.** Para efeito de monitoramento e condução do processo de compra de bens e serviços deve estar minimamente com as seguintes especificações:

INSTITUTO SÃO VICENTE
Folha Nº 14
07.609.365/0001-67

I. Solicitação de Compras: deve ser realizado pelo Requisitante, previamente definido pelo gestor local do projeto; contendo a devida justificativa da necessidade da aquisição, bem como as especificações dos produtos e;/ou serviços a serem adquiridos.

II. Mapa de Cotação: deve ser realizado pelo setor de compras, que após efetuado a cotação, será homologado pelo Diretoria Administrativa Financeira;

III. Pedido de compra: será concluído com base no mapa de cotação, sendo considerado para efeitode escolha, a melhor oferta apresentada pelo fornecedor, devendo ser validado pelo Setor de Comprase/ou Diretor Administrativo-Financeiro.

Art. 9º. O Setor de Compras e/ou Administrativo, selecionarão criteriosamente os fornecedores/prestadores que participarão do processo de cotação, considerando idoneidade, avaliaçãodo fornecedor, qualidade e menor custo quando cabível.

Parágrafo único. Para fins do disposto neste capítulo, considera-se menor custo aquele que resulta da matória de fatores utilizados, envolvendo entre outros os seguintes aspectos:

I. Custo de transporte e seguro até o local de entrega;

II. Forma de pagamento;

III. Prazo de entrega;

IV. Custos para operacionalização do produto, eficiência e compatibilidade com as especificações exigidas;

V. Durabilidade do produto;

VI. Credibilidade mercadológica do proponente;

VII. Disponibilidade do produto;

VIII. Eventual necessidade de treinamento de pessoal;

IX. Qualidade do material.

X. Art. 10º. O processo de seleção ou aquisição será por consulta/cotação de preços.

XI.

XII.

XIII. Art. 11º. A cotação de preços é a modalidade de aquisição realizada para compras ou contratações que tenham valor estimativo global indeterminado, e consistirá na consulta de no mínimo 03 (três) orçamentos provenientes de diferentes fornecedores e também com o devido registro em mapa de cotações dos preços obtidos.

XIV. Parágrafo primeiro. Quando não for possivel realizar as cotações mínimas estabelecidas no presente regulamento, a Diretoria do Instituto autorizará a compra com o número de cotações existente, mediante justificativa.

XV. Parágrafo segundo. As propostas recebidas devem ser formalizadas por escrito através de papel timbrado e assinado pelo fornecedor/prestador, e enviada diretamente pelo mesmo ou através de meio eletrônico, ficando mantidas em arquivo pelo Setor Compras e/ou Diretoria Administrativa Financeira,por no mínimo 05 (cinco) anos.

INSTITUTO SÃO VICENTE Folha Nº

Art. 12º. As cotações de preços deverão ser elaboradas mediante relatório constando:

I. Nome do bem, serviço ou produto a ser adquirido com as respectivas especificações técnicas;

II. Forma de apresentação e prestação;

III. Preço e condições comerciais ofertadas;

IV. Prazo de entrega e forma de pagamento;

V. Prazo de garantia;

Parágrafo primeiro. A melhor oferta será apurada considerando-se o disposto nos artigos do presente Regulamento e será apresentada à Diretoria Administrativa Financeira para verificação de viabilidade financeira do projeto, a quem competirá aprovar a concretização da Compra.

Parágrafo segundo. Após aprovação do mapa de cotação, o Setor de Compras e/ou Diretoria Administrativa Financeira emitirá o pedido de Compra, disponibilizando vias para:

I. Fornecedor;

II. Arquivo de Compras;

III. Setor recebedor do Material.

IV. **Parágrafo terceiro.** Caso haja divergência na entrega de produtos em número superior ao solicitado pela contratante, será considerado para fins de pagamento o valor unitário orçado, exceto em caso de adequações de recipientes/embalagens.

V. **Art. 13º.** Para os fins deste Regulamento, constituem-se as seguintes modalidades de compras, obras e serviços:

VI. **Compras, obras e serviços de pequeno valor:** são compras, obras e serviços de valor não superiora um salário-mínimo vigente na data da compra, esse tipo de compra dispensa as demais formalidadesdeste regulamento, e deverá ser autorizada e justificada pelo Diretoria ou Gerência beneficiada / responsável, diretamente no respectivo comprovante fiscal.

VII. **Compras, obras e serviços de valor inferior:** são compras, obras e serviços de valor superior a um salário-mínimo vigente na data da compra e de até R$ 5.000,00 (cinco mil reais), inclusive, que serão realizados mediante pesquisa simples de preços no mercado envolvendo, no mínimo, 03 (três) cotações com fornecedores, feita por telefone, internet, fax ou qualquer outro meio de apuração de preços.

VIII. **Compras, obras e serviços de valor médio:** são compras, obras e serviços de valor superior a R$ 5.000,00 (cinco mil reais) e de até R$ 50.000,00 (cinquenta mil reais), inclusive, que serão realizados mediante coleta de no mínimo 03 (três) propostas orçamentárias de diferentes fornecedores.

IX. **Compras, obras e serviços de valor superior:** são compras e serviços de valor acima de R$ 50.000,00 (cinquenta mil reais), que serão realizados mediante publicação de ato convocatório no website do ISV, com a participação de no mínimo 03 (três) propostas orçamentárias de diferentes fornecedores.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

Art. 14º. As compras de pequeno valor estão dispensadas da triplice cotação, prevista no artigo 11º, não desobrigando do fiel cumprimento das exigências do processo administrativo.

Art. 15º. As compras de materiais prestação de serviços exclusivos fornecidos e prestados por um único fornecedor/prestador, estão dispensadas da triplice cotação, prevista no artigo 11º; não desobrigando do fiel cumprimento das exigências do processo administrativo.

Parágrafo único: A previsão do caput desse artigo compreende-se igualmente aos periféricos, componentes e suprimentos dos equipamentos comprados que não funcionam sem os referidos adicionais exclusivos.

Art. 16º. A condição do fornecedor exclusivo será comprovada por carta de exclusividade apresentadapelo fornecedor/prestador e renovada a cada 06 (seis) meses.

Art. 17º. As compras relativas às diárias de hotéis, passagens áreas e compras via e-commerce, incluindo as compras internacionais de livros e material utilizado e aluguel de carro, poderão ser realizadas utilizando cartão de crédito em nome do ISV, como forma de pagamento.

Art. 18º. As despesas a serem a realizadas por meio do uso de cartão de crédito deverão ser aprovadas anteeipadamente pela Diretoria Administrativa Financeira, independentemente do valor envolvido.

Art. 19º. O cartão de crédito será utilizado exclusivamente para compras tipificadas no artigo 17º deste procedimento sendo, portanto, vedada a utilização do cartão de crédito de forma diversa da aqui prevista;

I. A responsabilidade pela guarda do cartão será da Diretoria Administrativa Financeira;

II. Os comprovantes e notas fiscais emitidas em nome ISV, deverão ser anexados à fatura que comporá o processo para pagamento.

Art. 20º. Será desnecessário (dispensado) o procedimento formal de realização de pesquisa de preços previsto nos incisos do caput dos art. 10º e 11º, para as seguintes modalidades de compras econtratações:

I. Em caráter de emergência, quando caracterizada a urgência de atendimento de situação que possa ocasionar prejuizos ao ISV ou comprometer a segurança de pessoas, obras, serviços ou equipamentos.

II. Quando, em razão da natureza do objeto, não houver pluralidade de opções.

III. Para a contratação de serviços técnico-profissionais especializados.

IV. Nos casos em que não houver dispêndio de recursos financeiros por parte do Instituto de Planejamento de Gestão, como o recebimento de doações ou comodatos, permutas, celebração de parcerias, convênios, termos de cooperação, locações, cessões de espaço, entre outros.

INSTITUTO SÃO VICENTE
Folha Nº
CNPJ 07609.365/0001-67

V. Nos casos de grave perturbação da ordem, calamidade pública, epidemias, pandemias ou alertas emitidos pela Agência Nacional de Saúde;

VI. Para a locação de imóvel destinado ao serviço desenvolvido pela Organização Social, cujas características de instalação ou localização condicionem a sua escolha;

VII. Quando não acudirem interessados ao procedimento anterior, e esta não puder ser repetida sem prejuízo à Organização Social, mantidas, neste caso, as condições preestabelecidas;

Parágrafo primeiro. Entende-se por serviços técnico-profissionais especializados aqueles exercidos por profissionais e empresas cujo conhecimento especifico ou conceito no campo de sua especialidade,decorrente de desempenho anterior, estudos, experiências, publicações, organização, aparelhamento, equipe técnica ou outros requisitos relacionados à sua atividade, permitam inferir que o seu trabalho éo mais adequado à plena satisfação do objeto a ser contratado, exemplificando-se, mas não se limitando, aos seguintes serviços e produtos:

a) Pareceres, perícias e avaliações em geral;

a) Assessorias ou consultorias técnicas, jurídicas, auditorias financeiras, contábeis e folha de pagamento;

b) Coordenação, fiscalização, supervisão ou gerenciamento de obras ou serviços;

c) Patrocínio ou defesa de causas judiciais ou administrativas;

d) Recrutamento, treinamento e aperfeiçoamento de pessoal;

e) Informática, inclusive quando envolver aquisição de programas;

f) Serviços que envolvam criação artística, tais como desenhos, pinturas, gravuras, esculturas,fotografia e outros.

Parágrafo segundo. Em quaisquer dessas ocorrências (dispensas), deve ser realizado o registro e assegurada a necessária transparência dos atos de compras e contratações.

Art. 21º. O Setor de Compras do ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA adotará o Processo deCadastramento Sumário, em que o fornecedor/prestador apresentará as seguintes informações;

I. Pessoa Jurídica:

a) Nome do Fornecedor;

b) Nome Fantasia;

c) Endereço (Rua, Número, Bairro, CEP, Cidade, Estado);

d) Número de Inscrição no CNPJ;

e) Informar qual o Regime de apuração de impostos – simples nacional/lucro presumido, lucroreal, imune ou isenta;

f) Inscrição Estadual ou Municipal;

g) Telefone e e-mail para contato;

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

h) Informações Bancárias;

i) Condições usuais de pagamento;

j) Outros dados julgados oportunos.

II. Pessoa Física:

a) Nome Completo;

b) RG;

c) CPF;

d) Certidão de Casamento ou Nascimento;

e) Número de PIS;

f) Endereço (Rua, Número, Bairro, CEP, Cidade, Estado);

g) Telefone, e – mail para contato;

h) Informações bancárias;

i) Condições usuais de pagamento;

j) Outros dados julgados oportunos.

Parágrafo único. Além das informações prestadas conforme caput, o fornecedor/prestador deverá apresentar os seguintes documentos:

III. Pessoa Jurídica:

a) Ficha Cadastral (conforme modelo);

b) Cartão de CNPJ;

c) Consulta do Quadro de Sócios Administradores – QSA;

d) Contrato Social originário e última alteração;

e) Cópia do RG, CPF e comprovante de endereço dos sócios administradores;

f) Cadastro Nacional de Empresas Idôneas e Suspensas;

g) Cadastro Informativo dos Créditos Não Quitados e Órgãos e Entidades Estaduais (CADIN);

h) Certidão Negativa de Débitos Federais e Dívida Ativa da União;

i) Certidão Negativa de Débitos Tributários Estaduais;

j) Certidão Negativa de Débitos Tributários Municipais;

k) Certidão Negativa de Débitos Trabalhistas;

l) Certidão de Regularidade do FGTS;

m) Licença de funcionamento ou documento equivalente (conforme categoria).

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

IV. Pessoa Física:

a) Cópia do RG

b) Cópia do CPF

c) Cópia do Número de PIS

d) Cópia do Endereço, Número, CEP, Cidade, Estado

e) Cópia de Inscrição Municipal (Se Profissional Autônomo)

f) Certidão de Casamento ou Nascimento;

g) Carteira de Trabalho e Previdência Social – CTPS;

Art. 22º. A coleta de dados ou envio de informações ou documentos do fornecedor/prestador poderá ser efetuada, por e-mail disponibilizado no site do Instituto de Planejamento e Gestão.

Art. 23º. É de responsabilidade do fornecedor/prestador a atualização dos documentos perante o Setor competente do ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA a cada 06 (seis) meses ou a qualquer mudança no quadro.

Art. 24º. Quando for necessário, solicitação deverá conter elementos técnicos, projeto básico ou projeto executivo do objeto a ser contratado.

Art. 25º. Considera-se autorizada a despesa com a manifestação positiva do Setor de Compras e/ou Diretoria Financeira, contendo indicação do valor estimado para futura operação.

Art. 26º. Os contratos firmados com base neste Regulamento estabelecerão, com clareza e precisão, as condições para sua execução, expressas em cláusulas que definam os direitos, as obrigações e responsabilidades das partes, em conformidade com os termos do ato convocatório e da proposta a quese vinculam.

Art. 27º - Os contratos deverão conter, minimamente:

I. Qualificação completa das partes.

II. Seu objeto.

III. Prazo de entrega do bem e/ou serviço.

IV. Vigência.

V. Preço e forma de pagamento.

VI. Deveres e responsabilidades das partes.

VII. Cláusula penal contendo sanções pelo descumprimento das obrigações.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

VIII. Hipótese de rescisão

IX. Foro.

Art. 28º. Exige-se a celebração de contrato formal para os serviços continuados ou quando houver entrega parcelada de bens ou a exigência de fornecimento de garantias.

Art. 29º. O Diretor Presidente em conjunto com a Diretoria da área interessada, se necessário, deverão selecionar criteriosamente, o prestador de serviço técnico profissional especializado, que poderá ser pessoa jurídica ou física, considerando a idoneidade, a experiência e a especialização do contrato, dentro da respectiva área.

Art. 30º. Todos os contratos deverão ser aprovados por assessoria jurídica ou, na falta desta, pelo dirigente máximo do ISV, a fim de garantir a adequada formalização dos termos avençados.

Art. 31º. No caso de contratos celebrados com pessoas jurídicas, deverão ser apresentados a cópia deseu ato constitutivo e alterações, ou ato constitutivo consolidado, bem como atas de eleição dos dirigentes, além de outros documentos que o ISV julgar necessários, de acordo com o tipo de contrato a ser celebrado.

Art. 32º. Todos os contratos deverão ser numerados e rubricados em todas suas páginas.

Art. 33º. Todos os procedimentos estipulados neste regulamento poderão ser suprimidos ou ampliados, sempre de forma motivada e com aprovação do Departamento Jurídico, objetivando melhoradequação às particularidades do caso e garantia do interesse público.

Art. 34º. A disciplina estabelecida neste Regulamento poderá ser complementada por adendospublicados no site do ISV, que será parte integrante deste.

Art. 35º. O presente regulamento entrará em vigor na data de sua aprovação pelo Conselho de Administração, nos termos expostos pelo Estatuto Social.

Art. 36º. Os casos omissos ou duvidosos na interpretação do presente Regulamento serão resolvidospelas Diretorias do Instituto, com base nos princípios gerais de administração.

Art. 37º. Os valores estabelecidos no presente Regulamento serão revistos e atualizados pela Diretoria Administrativa Financeira sempre que necessário.

Art. 38º. O presente Regulamento entrará em vigor a partir da data da sua publicação.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

Lavaras da Mangabeira – CE, 25 de Setembro de 2023

PRESIDENTE DO CONSELHO DE ADMINISTRAÇÃO

DIRETOR PRESIDENTE

institutosaovicente@gmail.com

Telefone: (088) 3536 – 1280

BR 230 – BAIRRO VIRGILIO DE AGUIAR GURGEL – CEP 63300-000 – LAVRAS DA MANGABEIRA – CEARÁ - CNPJ 07609 365/0001-67

REGIMENTO INTERNO

CAPÍTULO I
DA ORGANIZAÇÃO E FUNCIONAMENTO

Art. 1°. Para o cumprimento do conjunto de diretrizes e princípios previstos no Estatuto Social e demais documentos da entidade, ficam estabelecidos as seguintes regras de organização e funcionamento, aplicáveis ao conjunto de associados:

Art. 2°. São instâncias consultivas e deliberativas do ISV:

I. A Assembleia Geral;
II. A Diretoria;
III. O conselho fiscal;
IV. O conselho de administração;

§1° As instâncias deliberativas são a Assembleia Geral e a Diretoria ;

§2° As instâncias de caráter consultivo são o Conselho Fiscal, o Conselho de Administração.

Art. 3º. A Assembleia Geral será coordenada pelo Diretor Presidente ou, na ausência deste, pelo Diretor Vice-Presidente ou, estando também ausente, pelo Diretor Financeiro.

Art. 4º. Os trabalhos na Assembleia Geral obedecerão à seguinte ordem:

I. Aprovação e discussão da Pauta do dia;
II. Eleição e destituição dos membros da Diretoria e do Conselho Fiscal;
III. Aprovação dos planos e planejamento do ISV;
IV. Aprovação de alteração e reforma do Estatuto Social;
V. Aprovação de alteração do Regimento Interno;
VI. Revisão ou anuência, conforme o caso, das deliberações da Diretoria ;
VII. Fixação do valor das contribuições habituais a serem pagas pelos associados

mantenedores;

VIII. Deliberação sobre assuntos não previstos no Estatuto Social ou qualquer outro assunto de relevância para o ISV que lhe seja submetido;

§1° As decisões serão tomadas pela maioria simples dos membros presentes, salvo nos casos em que haja previsão diversa no Estatuto;

§2° As votações poderão ser simbólicas ou nominais, abertas ou secretas, a critério dos presentes em cada reunião, devendo ser consignado em ata a forma de votação adotada, bem como o resultado de cada deliberação;

§3° Sob responsabilidade do Secretário, deverá ser lavrada e registrada em livro próprio a Ata de cada Assembleia Geral, assinada pelos integrantes da mesa, nos termos do Estatuto Social;

§4° As matérias constantes da pauta poderão ser transferidas para a próxima reunião ordinária, quando terão preferência para discussão e votação;

§5° Poderão ser incluídas na pauta do dia, matérias consideradas de urgência pela Plenária;

§6° As questões de ordem terão preferência sobre quaisquer outras, não podendo o Presidente negar a palavra ao associado que a solicitar para esse fim;

§7° O associado que assim desejar, poderá requerer ao Presidente que conste em ata seu pronunciamento, bem como seu voto, quando este for diverso da deliberação dos membros presentes.

Art. 5°. Para o exercício de suas competências estatutárias, a Assembleia Geral poderá:

I. Requisitar informações a qualquer Associado ou membro da Diretoria , Conselho de Administração e Conselho Fiscal;

II. Determinar a continuidade, suspensão ou a conclusão de estudos ou atividades de interesse da entidade;

III. Analisar recursos e pedidos de reconsideração;

IV. Solicitar a petição de demandas perante os órgãos públicos ou privados;

Art. 6º A Diretoria , sempre que reunida, deliberará sobre questões previamente estabelecidas.

Art. 7º. O Conselho Fiscal e o Conselho de Administração reunir-se-ão, ordinária ou extraordinariamente, conforme determinação do Estatuto ou a critério de seus integrantes, e suas atividades poderão ser registradas em livro próprio.

Art. 8º. Para o exercício de suas funções o Conselho Fiscal poderá:

I. Requerer a qualquer tempo à apresentação dos relatórios, balancetes, extratos e ou contratos bancários e demais documentos financeiros necessários à elaboração de seu relatório de análise das contas;

II. Requerer a participação do Diretor Presidente, do Diretor Administrativo Financeiro ou de qualquer outro integrante da diretoria para obter esclarecimentos acerca de omissões, obscuridades ou contradições dos documentos financeiros da associação.

Dos Associados

Art. 09. Os Associados, além de se submeterem a este regimento deverão ter ciência de seus direitos e deveres conforme Estatuto.

Art. 10. São considerados associados ausentes os associados Integrantes que em 6 (seis) meses consecutivos ou 9 (nove) meses alternados em um período de 2 (dois) anos, por vontade própria, deixaram de participar da vida ativa da Associação, assim compreendendo, de forma global ou isolada as seguintes situações:

I. não participação nas reuniões da Assembleia Geral;

II. Outras situações reconhecidas por decisão de maioria absoluta dos Órgãos deliberativos do ISV.

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E
INFA:07609365000167

Assinado de forma digital por ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFA:07609365000167
Dados: 2021.05.25 14:58:28 -03'00'

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

Parágrafo único – Fica o associado Integrante com residência e domicilio fora da sede do Instituto, em um raio de 100 km (cem quilômetros), desobrigado das demais condições estabelecidas neste artigo, devendo, todavia, pelo menos 1 (uma) vez por ano manter contato com a Associação através de participação de 1 (uma) de suas reuniões e de 1 (uma) visita a sede.

Art. 11. São considerados dependentes dos associados aqueles reconhecidos pela legislação vigente ou, em caso excepcional, os admitidos pelos Órgãos Deliberativos.

Parágrafo único – São deveres dos dependentes, no que for cabível, todos os deveres da categoria do associado do qual é dependente.

CAPÍTULO II
DOS COLABORADORES

Art. 12. O quadro de colaboradores do ISV deverá ser composto de pessoas jurídicas e profissionais especializados, contratados para a execução de suas diferentes atividades técnicas e administrativas, em número compatível com a necessidade dos trabalhos, desde que os encargos decorrentes não prejudiquem o seu equilíbrio financeiro.

§1° Nas contratações de colaboradores realizadas pelo ISV, a Diretoria observará critérios de transparência, impessoalidade, igualdade e publicidade;

§2° É de responsabilidade dos colaboradores zelar pelo cumprimento da legislação, do Estatuto, deste Regimento Interno e das demais normas oriundas dos órgãos deliberativos do ISV.

Do processo de seleção

Art. 13. O processo de seleção de colaboradores deve ser requisitado por meio de adequado dimensionamento das necessidades do ISV, encaminhado à Diretoria , a qual compete deliberar sobre a contratação.

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E
INFA:07609365000167

Assinado de forma digital por ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E
INFA:07609365000167
Dados: 2023.05.31 14:57:49 -03'00'

INSTITUTO SÃO VICENTE
07.609.365/0001-67

Art. 15. Quando se tratar de pessoas jurídicas, compete ainda demonstrar o atendimento aos seguintes critérios, sem prejuízo dos demais que porventura sejam exigidos pela legislação vigente, Estatuto social e demais normas internas do ISV:

I. Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);
II. Registro na Junta Comercial, quando exigido pela legislação;
III. Possuir capacidade econômica compatível com a sua execução.

Art 15. Quando se tratar de profissionais colaboradores pessoas físicas, compete demonstrar o critério de especialização na área de atuação por meio de certificação que comprove o grau (graduação e/ou pós-graduação) exigido para o exercício das atividades, sem prejuízo dos demais critérios que porventura sejam exigidos pelo Estatuto social e pela legislação vigente, sendo os contratados nesta modalidade regidos pelas normas da Consolidação das Leis do Trabalho – CLT.

Parágrafo único – Excluem-se dos critérios acima os membros da Diretoria , do Conselho de Administração e do Conselho Fiscal, uma vez que são cargos eletivos providos na forma do Estatuto Social e por este regido, não incidindo sobre esses quaisquer das hipóteses de contratação tratadas anteriormente.

CAPÍTULO III
DOS PROCEDIMENTOS DISCIPLINARES

Art. 16. Na hipótese de descumprimento das obrigações sociais, administrativas ou éticas definidas no Estatuto Social e no Código de Ética do ISV, bem como na legislação vigente, por decisão da Assembleia Geral ou da Diretoria, serão iniciados procedimentos disciplinares com o objetivo de apurar o fato determinado e aplicar a sanção adequada aos respectivos associados e/ou colaboradores.

Art. 17. Nos casos envolvendo associados, os procedimentos disciplinares serão conduzidos por comissões criadas especificadamente para apurar a ocorrência de qualquer das infrações mencionadas no Estatuto Social e no Código de Ética do ISV, bem

como na legislação vigente, devendo, ao final, ser remetido relatório devidamente motivado e fundamentado à Assembleia Geral para que sejam tomadas as providências cabíveis.

Parágrafo único – Nos casos envolvendo colaboradores, o procedimento disciplinar será conduzido pela Diretoria, com o objetivo de apurar o fato determinado e aplicar a penalidade adequada, de acordo com as infrações e penalidades previstas no Estatuto Social, no Código de Ética do ISV, bem como na legislação vigente.

Art. 18. Os atos praticados por Associado e/ou Colaborador que sejam considerados infrações apresentam penalidades com a seguinte classificação:

I. Advertência, podendo ser verbal ou escrita, aplicando-se nos casos de descumprimento das normas internas, desrespeito ao estatuto, ao código de ética, ao regimento interno e à legislação vigente;

II. Suspensão, aplicando-se nos casos de reincidência de infração já punida com advertência;

III. Exclusão ou Desligamento, aplicando-se às infrações consideradas graves, nos casos de descumprimento das normas internas, do estatuto, do código de ética, do regimento interno e da legislação vigente incluindo-se a reincidência em suspensão e a tentativa ou participação em conluio para lesar os interesses do ISV.

Parágrafo único – As penalidades serão aplicadas pela Assembleia Geral no caso de associados ou pela Diretoria no caso de colaboradores da Instituição, sendo em ambas as situações observados o direito ao contraditório e ampla defesa.

Art. 19. Após a abertura de procedimento disciplinar, deverá ocorrer comunicação escrita ao associado envolvido, onde conste a infração que lhe é atribuída, o prazo – nunca inferior a 03 dias - e o local onde deverá apresentar sua defesa;

§1° A recusa ao recebimento, a não apresentação de defesa, a apresentação de defesa genérica ou relativa a fato diverso do contido na comunicação, implica em confissão e nos efeitos da revelia;

§2° As decisões serão materializadas em pareceres, que poderão determinar a aplicação ou não da sanção, sua natureza, bem como o prazo de sua vigência.

§3° As sanções de advertência e suspensão poderão ser aplicadas liminarmente pelo Presidente, cabendo recurso de sua decisão - cujo efeito será meramente devolutivo - à diretoria ou à primeira assembleia geral subsequente.

§4° A sanção de exclusão poderá ser aplicada pela diretoria, cabendo recurso de sua decisão - cujo efeito será meramente devolutivo - à primeira assembleia geral subsequente.

Do processo eleitoral

Art. 20. A Eleição para a diretoria será convocada pelo Diretor Presidente ou seu substituto legal, nos termos do Estatuto, antes do término do mandato da diretoria;

Art. 21. A convocação será realizada através de edital e afixada na sede da entidade e nos pontos onde haja afluência de associados.

Art. 22. Concluída a apuração ou processo de votação, a critério da Assembleia Geral poderá dar posse à nova Diretoria.

Art. 23. Concluído o processo eleitoral, os resultados deverão ser registrados no livro da Entidade ou em Atas para subsequente registro.

Disposições gerais

Art. 24. Compete privativamente ao Conselho de Administração aprovar o regimento interno, bem como suas posteriores aprovações, sendo esta condição suficiente e necessária para que se possa remeter à aprovação da assembleia geral, nos termos do Estatuto do ISV.

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E
INFA:07609365000167

Assinado de forma digital por ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E
Dados: 2023.09.25 14:56:16 -03'00'

INSTITUTO SÃO VICENTE
Folha Nº 1
CNPJ 07.609.365/0001-67

Art. 25. Os casos omissos, controversos e as dúvidas surgidas na aplicação deste Regimento, serão solucionados por deliberação da diretoria, em qualquer de suas reuniões, por maioria dos membros presentes, ad referendum da primeira Assembleia Geral subsequente.

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFA:07609365000167

Assinado de forma digital por ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFA:07609365000167
Dados: 2023.09.25 14:45:45 -03'00'

ASSOCIAÇÃO DE PROTEÇÃO E ASSISTENCIA À MATERNIDADE E A INFANCIA DE LAVRAS DA MANGABEIRA – CE

CNPJ 07609.365/0001-67

BR 230 – BAIRRO VIRGILIO DE AGUIAR GURGEL – CEP 63300-000 – LAVRAS DA MANGABEIRA – CEARA

Presidente: Mirialdo Linhares Garcia,

Primeiro Secretário: Júlia Maria Linhares de Sá Torres

Primeiro Tesoureiro: João Vieira da Silva

Vice-Presidente: Gustavo Belchior Linhares

Segundo Secretário: Maria Sizenita Venâncio Gonçalves

Segundo Tesoureiro: Ieda Torquato Lobo Vieira

Data da Revisão: 01/11/2023

Versão: 1.0

SUMÁRIO

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

APRESENTAÇÃO

Associação de Proteção e Assistência a Maternidade e a Infância de Lavras da Mangabeira - Ceará, constituída sob forma de Associação, sem fins lucrativos, que terá duração por tempo indeterminado, localizada na ROD BR 230, S/N, Bairro Virgílio de Aguiar Gurgel, CEP 63.300-000, sede e foro na município de Lavras da Mangabeira, Estado de Ceará.

A Associação de Proteção e Assistência a Maternidade e a Infância de Lavras da Mangabeira - Ceará adotará o nome fantasia de Instituto São Vicente.

A Associação de Proteção e Assistência a Maternidade e a Infância de Lavras da Mangabeira - Ceará, tem por finalidade:

I - prestar serviços médicos hospitalar e ambulatorial, com atendimento em pequena, média e alta complexidade;

II - realizar exames laboratoriais, de imagem e eletrocardiograma;

III - realizar a gestão e operação de unidades e serviços voltados para a promoção de saúde, assistência social e áreas afins, públicos ou privados.

Visando ao seguimento dos serviços não exclusivos no qual o Estado atua simultaneamente com outras organizações públicas não-estatais e privadas na oferta de serviços estes que envolvem direitos humanos fundamentais, como no caso específico a saúde. O Instituto São Vicente, tem plena noção da sua responsabilidade tanto perante a gestão pública quanto a sociedade.

O Instituto São Vicente é uma Organização Social, planejada e efetivada em consonância com as diretrizes da Lei Federal nº 9.637, de 15 de maio de 1998, leis estaduais e municipais vigentes que dispõem sobre a qualificação de entidades, sendo composta por uma equipe administrativa, assistencial e multidisciplinar qualificada em prestação de serviços de Gestão e tecnologia nas áreas de saúde, Educação e Projetos Sociais.

Observa-se que a integridade pública é composta por estruturas institucionais que contribuem para a realização dos objetivos desejados pela sociedade. Nesse contexto, a predominância da transparência desempenha um papel fundamental no interesse público, fortalecendo a confiança dos cidadãos em suas instituições.

Na prática, esse sentimento se reflete no escrutínio de todos os aspectos das ações dos gestores, incluindo decisões, planos, orçamentos, despesas, contratos, transferências e metas. Isso

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

permite determinar se a organização está cumprindo sua missão. A ampla fiscalização e o cerco dessa questão, e a integridade e a garantia desse processo.

Com a efetiva implementação deste programa, a instituição reforça seu compromisso com a sua missão institucional e convoca todos os colaboradores a adotar comportamentos íntegros e éticos como parte integrante de seu DNA organizacional. Essa iniciativa destaca o papel da instituição como um modelo de conduta exemplar para a sociedade a qual ela se dedica. Além disso, é importante ressaltar que, ao seguir esses princípios de integridade e ética, a instituição não apenas serve como referência, mas também contribui para o fortalecimento de laços de confiança com seus stakeholders, promovendo um ambiente de respeito e responsabilidade em todas as suas operações.

O programa não só estabelece diretrizes claras, mas também fornece os recursos e o suporte necessários para que todos os colaboradores possam desempenhar um papel ativo na promoção desses valores em todas as interações da organização com a sociedade.

O Instituto São Vicente é uma Organização Social que atua nas áreas da saúde, educação e projetos sociais. Com o objetivo de promover uma cultura de integridade e compliance em todo a sua organização, o Instituto São Vicente estabelece o presente Programa de Integridade e Compliance.

Este Programa tem como objetivo:

Garantir que o Instituto São Vicente opere de forma ética e em conformidade com as leis, normas e regulamentos aplicáveis;

Proteger os interesses da organização, de seus colaboradores, parceiros e beneficiários;

Prevenir e combater a corrupção, fraudes e outras irregularidades.

Princípios

O Programa de Integridade e Compliance do Instituto São Vicente é baseado nos seguintes princípios:

Transparência: Todas as atividades do Instituto São Vicente devem ser realizadas de forma transparente, com acesso público às informações relevantes.

Responsabilidade: Todos os colaboradores do Instituto São Vicente são responsáveis por agir de forma ética e em conformidade com as leis, normas e regulamentos aplicáveis.

Equidade: Todas as pessoas devem ser tratadas de forma justa e imparcial, independentemente de sua posição ou cargo.

Responsabilidade social: O Instituto São Vicente deve atuar de forma responsável com a sociedade e o meio ambiente.

Áreas de aplicação

INSTITUTO SÃO VICENTE
Folha Nº
CNPJ 07.609.365/0001-67

O Programa de Integridade e Compliance do Instituto São Vicente aplica-se a todas as atividades da organização, incluindo:

Operações administrativas: O Instituto São Vicente deve adotar políticas e procedimentos que garantam a integridade e conformidade de suas operações administrativas, como compras, contratações, finanças e contabilidade.

Atividades operacionais: O Instituto São Vicente deve adotar políticas e procedimentos que garantam a integridade e conformidade de suas atividades operacionais, como prestação de serviços de saúde, educação e projetos sociais.

Relações externas: O Instituto São Vicente deve adotar políticas e procedimentos que garantam a integridade e conformidade de suas relações externas, como com fornecedores, parceiros e beneficiários.

Mecanismos de controle

O Instituto São Vicente implementará os seguintes mecanismos de controle para garantir a eficácia do Programa de Integridade e Compliance:

Código de Conduta: O Instituto São Vicente adotará um Código de Conduta que estabelece os princípios e valores que devem orientar o comportamento de todos os colaboradores.

Treinamento: O Instituto São Vicente oferecerá treinamentos periódicos a todos os colaboradores sobre os princípios e valores do Programa de Integridade e Compliance.

Canal de denúncia: O Instituto São Vicente disponibilizará um canal de denúncia anônimo para que os colaboradores possam relatar irregularidades.

Investigação e apuração: O Instituto São Vicente investigará e apurará todas as denúncias recebidas, tomando as medidas cabíveis.

Comitê de Integridade e Compliance

O Instituto São Vicente criará um Comitê de Integridade e Compliance responsável por supervisionar a implementação e o funcionamento do Programa de Integridade e Compliance. O Comitê será composto por representantes da alta administração da organização, bem como por colaboradores de diferentes áreas.

Responsabilidades

As responsabilidades pelo compromisso do Programa de Integridade e Compliance são as seguintes:

Alta administração: A alta administração do Instituto São Vicente é responsável por garantir o apoio e a liderança do Programa de Integridade e Compliance.

Colaboradores: Todos os colaboradores do Instituto São Vicente são responsáveis por cumprir os princípios e valores do Programa de Integridade e Compliance.

Comitê de Integridade e Compliance: O Comitê de Integridade e Compliance é responsável por supervisionar a implementação e o funcionamento do Programa de Integridade e Compliance.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

PRINCIPAIS REFERÊNCIAS NORMATIVAS

O Programa de Integridade do Instituto São Vicente se baseia em um arcabouço de legislações do ambiente externo e normativas internas que estabelecem as diretrizes para a conduta ética de todos os envolvidos, sejam dirigentes, colaboradores, parceiros ou terceiros da instituição. Essas orientações éticas orientam as interações e ações da organização em consonância com os mais elevados padrões de integridade.

O programa concentra-se na promoção de exemplos éticos e, simultaneamente, na prevenção e combate a atos de fraude e corrupção. Atualmente, a eficácia do programa é avaliada através dos canais de monitoramento designados, garantindo que as práticas e políticas de integridade estejam sendo adequadamente implementadas e ajustadas conforme necessário. Além disso, a avaliação contínua do programa contribui para a constante melhoria das práticas da instituição, reforçando seu compromisso com a integridade e a ética em todas as esferas de atuação. Abaixo, seguem os principais instrumentos que mobilizam o sistema de integridade corporativo:

1) Código de Ética e Conduta;

2) Regulamento de Seleção de Pessoal;

3) Regulamento de compras e aquisições;

4) Ouvidoria

institutosaovicente@gmail.com

Telefone: (088) 3536 – 1280

BR 230 – BAIRRO VIRGILIO DE AGUIAR GURGEL – CEP 63300-000 – LAVRAS DA MANGABEIRA – CEARÁ - CNPJ 07609 365/0001-67

GESTÃO DA INTEGRIDADE NO INSTITUTO SÃO VICENTE - ISV

A cultura da integridade permeia integralmente a estrutura de governança e gestão do Instituto São Vicente (ISV). O objetivo primordial é assegurar que todos os colaboradores compreendam plenamente suas responsabilidades e desfrutem do apoio incondicional da Alta Administração ao executarem suas funções.

O Programa de Integridade do ISV aborda essa temática por meio de um conjunto de elementos fundamentais, incluindo:

Liderança: Definindo claramente o comportamento da alta liderança com a integridade e a ética, estabelecendo um exemplo inspirador para todos os colaboradores.

Padrões de Conduta: Estabelecendo diretrizes e normas rígidas que delineiam os princípios éticos pelos quais todos os envolvidos devem se orientar em suas atividades.

Correção: Enfatizando a importância do retidão e da conformidade estrita com leis e regulamentos em todas as ações da organização.

Denúncias: Oferecendo canais seguros e confidenciais para denúncias de irregularidades, garantindo um ambiente onde as preocupações possam ser expressas sem medo de retaliação.

Capacitação: Proporcionando treinamento contínuo para que os colaboradores compreendam plenamente os princípios éticos e as políticas de integridade da instituição.

Comunicação: Garantindo que a mensagem de integridade seja disseminada amplamente e de maneira compreensível para todos os públicos envolvidos.

Monitoramento: Estabelecendo processos de acompanhamento para avaliar a eficácia das práticas de integridade e tomar medidas corretivas quando necessário.

Riscos e Controle Interno: Identificando e gerenciando proativamente os riscos relacionados à integridade e mantendo controles internos eficazes para prevenir e detectar irregularidades.

A gestão da ética é um dos pilares fundamentais desse programa e inclui ferramentas reconhecidas, como detecção, investigação e a aplicação de sanções que variam de ações disciplinares a processos criminais, conforme a gravidade das infrações.

Este documento apresenta o Programa de Integridade de forma transparente e acessível, não apenas para os colaboradores, mas também para a sociedade em geral e os órgãos de controle. O ISV tem o firme propósito de ser um exemplo de integridade e ética, representando um

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

exemplo a ser seguido pela sociedade. Nossa equipe acredita firmemente que a integridade é um valor transcendental que vai além das questões governamentais e serve ao bem-estar do Estado e da comunidade como um todo.

Compromisso da Alta Administração

O compromisso da alta administração é o alicerce de uma política de integridade eficaz. Isso envolve a liderança da organização demonstrando, por meio de palavras e ações, seu comprometimento inabalável com a integridade e a ética. Eles estabelecem um exemplo claro para todos os colaboradores, parceiros e partes interessadas.

A alta administração deve:

- Comunicar e reforçar consistentemente os valores e princípios éticos da organização.
- Definir as expectativas de comportamento ético e conformidade com leis e regulamentos.
- Apoiar a implementação de políticas de integridade e tomar medidas corretivas em caso de violações.
- Participar ativamente de iniciativas de integridade e promover um ambiente onde a ética seja priorizada.

Código de Ética e Conduta

O Código de Ética e Conduta é um documento essencial que estabelece os princípios éticos pelos quais todos os envolvidos na organização devem se guiar. Ele descreve as diretrizes e normas que definem o comportamento esperado e os valores da organização.

As premissas do Código de Ética e Conduta incluem:

- Estabelecer regras claras e compreensíveis que abordem situações éticas comuns.
- Proporcionar orientações sobre como os colaboradores devem agir em situações éticas complexas.
- Definir consequências para o não cumprimento das normas éticas.
- Ser amplamente comunicado e facilmente acessível a todos os envolvidos.

Gestão de Riscos e Controles Internos

A gestão de riscos e controles internos é fundamental para identificar, avaliar e mitigar riscos relacionados à integridade.

A forma de atuação envolve:

- Identificar possíveis riscos éticos e de conformidade em todas as áreas da organização.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

- Implementar controles internos eficazes para prevenir e detectar violações éticas.
- Realizar avaliações regulares de riscos para manter os controles atualizados.
- Desenvolver planos de contingência para gerenciar crises éticas ou violações.

Capacitação e Treinamento

A capacitação e treinamento são vitais para garantir que todos compreendam plenamente os princípios éticos da organização e como aplicá-los em situações práticas.

A forma de trabalho de capacitação e treinamento inclui:

- Fornecer treinamento regular sobre integridade e ética para todos os colaboradores.
- Abordar tópicos como o Código de Ética, políticas de integridade e práticas de conduta.
- Assegurar que os colaboradores estejam cientes das implicações legais e éticas de suas ações.
- Oferecer oportunidades para tirar dúvidas e buscar orientações sobre situações éticas.

Canais de Denúncia e Investigação

Os canais de denúncia e investigação são mecanismos críticos para identificar e lidar com violações éticas. Tendo como objetivos:

- Estabelecer canais seguros e confidenciais para relatar preocupações éticas.
- Garantir que as denúncias sejam tratadas de maneira imparcial e justa.
- Realizar investigações completas em resposta a denúncias de violações éticas.
- Tomar medidas corretivas apropriadas, incluindo a aplicação de sanções, quando necessário.

Cada um desses elementos desempenha um papel vital na promoção de uma cultura de integridade e ética dentro da organização, protegendo-a de riscos éticos e fortalecendo a confiança dos colaboradores, parceiros e partes interessadas. Eles devem trabalhar em conjunto de maneira coordenada para garantir a eficácia da política de integridade.

Revisão e atualização

O Programa de Integridade e Compliance do Instituto São Vicente será revisado periodicamente para garantir sua adequação às necessidades da organização.

O Instituto São Vicente está comprometido com a promoção de uma cultura de integridade e compliance em toda a sua organização. O presente Programa estabelece os princípios, diretrizes e mecanismos de controle necessários para alcançar esse objetivo.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

1. Fundamentos e Conceitos de Política de Segurança da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

Para a implementação de controles de segurança faz-se necessária a criação de um processo de gestão da segurança da informação. Este processo deve considerar o incentivo à definição de políticas de segurança, cujos escopos devem abarcar o gerenciamento de riscos baseado em análise quantitativa e qualitativa, como análises de custo benefício e programas de conscientização.

A gestão da segurança da informação inicia-se com a definição de políticas, procedimentos, guias e padrões. As políticas podem ser consideradas como o mais alto nível de documentação da segurança da informação, enquanto nos níveis mais baixos podemos encontrar os padrões, procedimentos e guias. Isto não quer dizer que as políticas sejam mais importantes que os guias, procedimentos e padrões.

O primeiro documento a ser definido deve conter o comprometimento da alta administração, deixando clara a importância da segurança da informação e dos recursos computacionais para a missão institucional. É uma declaração que fundamenta a segurança da informação na totalidade da instituição. Deve conter ainda a autorização para a definição dos padrões, procedimentos e guias de mais baixo nível.

As políticas de alerta não são mandatórias, mas são fortemente incentivadas, normalmente incluindo as consequências da não conformidade com as mesmas. A política informativa é aquela que existe simplesmente para informar aos usuários de um determinado ambiente. Não implica necessariamente em requisitos específicos, e seu público alvo pode ser determinados setores somente ou até mesmo parceiros externos. Possuindo caráter genérico, pode ser distribuída para parceiros externos, como fornecedores, por exemplo, que acessam a rede do local, sem que isso acarrete o comprometimento da informação interna.

Os regulamentos de segurança são políticos que uma instituição deve implementar em conformidade com legislação em vigor, garantindo aderência a padrões e procedimentos básicos de setores específicos.

Os padrões especificam o uso uniforme de determinadas tecnologias. Normalmente são mandatórios e implementados através de toda a instituição, a fim de proporcionar maiores benefícios.

Os fundamentos ou princípios são semelhantes aos padrões, com pequena diferença. Uma vez que um conjunto consistente de fundamentos seja definido, a arquitetura de segurança de uma instituição pode ser planejada e os padrões podem ser definidos. Os fundamentos devem levar em conta as diferenças entre as plataformas existentes, para garantir que a segurança seja implementada uniformemente em toda a instituição. Quando adotados, são mandatórios. Os guias são similares aos padrões, embora mais flexíveis, se referindo a metodologias para os sistemas de segurança, contendo apenas ações recomendadas e são mandatórias. Consideram a natureza distinta de cada sistema de informação.

Podem ser usados para especificar a maneira pela qual os padrões devem ser desenvolvidos, como quando indicam a conformidade com certos princípios da segurança da informação.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

Os procedimentos contêm os passos detalhados que devem ser seguidos para a execução de tarefas específicas. São ações detalhadas que as partes interessadas pertinentes e não pertinentes devem seguir. São considerados como inseridos no mais baixo nível em uma cadeia de políticas.

O seu propósito é fornecer os passos detalhados para a implementação das políticas, padrões e guias. Também podem ser chamados de práticas. As responsabilidades devem estar relacionadas com o perfil de cada envolvido no processo, como nos exemplos listados a seguir:

a. Gerentes de mais alto nível: Estão envolvidos com toda a responsabilidade da segurança da informação. Podem delegar a função de segurança, mas são vistos como o principal ponto quando são consideradas as responsabilizações por eventos relacionados com a segurança;

b. Profissionais de segurança dos sistemas de informação: Recebem da gerência de mais alto nível a responsabilidade pela implementação e manutenção da segurança. Estão sob sua responsabilidade o projeto, a implementação, o gerenciamento e a revisão das políticas, padrões, guias e procedimentos;

c. Possuidores de dados: São responsáveis pela classificação da informação. Podem também ser responsabilizados pela exatidão e integridade das informações;

d. Usuários: Devem aderir às determinações definidas pelos profissionais de segurança da informação;

e. Auditor de sistemas de informação: São responsáveis pelo fornecimento de relatórios para gerência superior sobre a eficácia dos controles de segurança, consolidados através de auditorias independentes e periódicas. Também analisam se as políticas, padrões, guias e procedimentos são eficazes e estão em conformidade com os objetivos de segurança definidos para a instituição.

2. Recomendações Gerais da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

2.1. Recomendações para o uso aceitável dos recursos de TI

O uso correto e responsável dos recursos de TI deve ser aplicado a todos os usuários da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA, inclusive as partes interessadas pertinentes, que utilizam esses recursos e a infraestrutura disponível.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo usuário, no âmbito da infraestrutura de TI, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

Os sistemas de TI deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer pessoa ou da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA, como marcas e patentes, nome comercial, segredo empresarial, domínio na Internet, desenho industrial ou qualquer outro material, que não tenha autorização expressa do autor ou proprietário dos direitos, relativos à obra artística, científica ou literária.

As informações da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA devem ser utilizadas apenas para os propósitos definidos na sua missão institucional.

2.2. Recomendações para o uso seguro dos recursos de TI

O envolvimento do usuário é importante no processo da segurança dos recursos de TI, pois é na adequada utilização destes recursos, como instrumento de trabalho, que se inicia a formação de uma sólida cultura de segurança da informação. Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

a. Manter registro das cópias de segurança;

b. Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original;

c. Utilizar um método de senhas que garante a segurança do usuário;

d. Alterar periodicamente suas senhas;

e. Utilizar um método de segurança que garanta o atendimento com o Art. 46 e Art. 47, de acessos não autorizados;

f. Certificar a procedência do site e a utilização de conexões seguras ao realizar transações via web;

g. Certificar que o endereço apresentado no navegador corresponde ao site que realmente se quer acessar, antes de realizar qualquer ação ou transação;

h. Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;

i. Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus;

j. Não utilizar o formato executável em arquivos compactados, pois estes tipos são propícios à propagação de vírus.

2.3. Recomendações sobre atividades permitidas

a. Utilizar programas de computador licenciados para uso da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA;

b. A instalação de programas e sistemas homologados é atribuição da administração de sistemas e TI;

c. Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente àqueles referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade.

2.4. Recomendações sobre atividades não permitidas

a. Introduzir códigos maliciosos nos sistemas de TI;

b. Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;

c. Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;

d. Tentar interferir sem autorização em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;

e. Alterar registro de evento dos sistemas de TI;

f. Modificar cabeçalho de qualquer protocolo de comunicação de dados;

g. Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;

h. Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;

i. Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;

j. Fornece informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;

k. Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente;

l. Armazenamento ou uso de jogos em computador ou sistema informacional;

m. Uso de recurso informacional da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;

n. Uso de aplicativos não homologados nos recursos informacionais;

3. Recomendações Específicas da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

3.1. Recomendações para controle de acesso à:

a. O acesso a informações rotuladas como públicas e uso interno não é restringido com controles de acesso que discriminam o usuário. Por outro lado, o acesso às informações confidenciais ou restritas serão permitidas apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pela unidade responsável. Da mesma forma, o acesso a alguns equipamentos de hardware e/ou software especiais (como equipamentos de diagnóstico de rede chamados "sniffers") deve ser restrito a profissionais competentes, com uso registrado e baseado nas necessidades do local.

b. Recursos automáticos: Será dado a todos os usuários, automaticamente, o acesso aos serviços básicos como correio eletrônico, aplicações de produtividade e browser WEB. Estas facilidades básicas irão variar de acordo com os cargos. Todos os outros recursos dos sistemas serão providos via perfis de trabalho ou por uma solicitação especial feita ao proprietário da informação envolvida. A existência de acessos privilegiados, não significa por si só, que um indivíduo esteja autorizado a usar esses privilégios.

c. Solicitação de acesso: As solicitações para novas identificações de usuários e alterações de privilégios devem ser feitas por escrito e aprovadas pela chefia imediata do usuário antes que um administrador de sistema realize tal solicitação. Os usuários devem declarar, claramente, porque são necessárias alterações em seus privilégios e a relação de tais alterações com as atividades exercidas;

d. O processo de aprovação do acesso deve ser iniciado pelo superior do usuário e os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe-as. Se um desses dois eventos

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-57

ocorrer, o superior hierárquico tem que notificar imediatamente a unidade responsável. Todos aqueles que não são usuários diretos (contratados, consultores, temporários, etc.) têm que se submeter a um processo semelhante através de seus gerentes de projetos. Os privilégios destas pessoas deverão ser imediatamente revogados quando da finalização do projeto. O mesmo deverá ser observado no desligamento antecipado, considerando ainda a responsabilização pelas atividades e atos cometidos durante a sua permanência no local.

e. Os privilégios para todos os usuários dos serviços da rede deverão ser revistos a cada seis meses.

f. Termo de Responsabilização e Sigilo: Todos os usuários que desejam usar os sistemas devem assinar este termo antes de acessar as dependências do local. Nos casos em que o usuário já possua a identificação e acesso ao local, mas que ainda não tenha assinado tal termo, a assinatura do termo deve ser obtida em caráter de urgência. A assinatura deste termo indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA relacionados ao ambiente de TI (incluindo as instruções contidas neste documento), bem como as implicações legais decorrentes do não cumprimento do disposto.

g. Senha de Acesso: As senhas de acesso são controles de segurança essenciais para os sistemas de segurança do ambiente de TI. Para garantir que os sistemas de segurança façam a parte do trabalho para o qual eles foram desenvolvidos, os usuários devem escolher senhas que sejam difíceis de serem deduzidas.

h. Proibição de Senhas de Acesso Cíclicas: Os usuários dos recursos de TI devem utilizar sempre novas senhas e o histórico das senhas já utilizadas deve ser mantido pelo banco de dados. Os usuários podem escolher senhas de fácil memorização, mas que sejam ao mesmo tempo difíceis de serem descobertas por outras pessoas.

i. Encadear várias palavras formando o que é conhecido como "frases de acesso". Combinar números e pontuação em uma palavra regular.

j. Criar acrônimos a partir de palavras de música, um poema ou outra sequência de palavras conhecidas.

k. Em caso de suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

l. Os usuários devem possuir orientação sobre a manutenção sigilosa das suas senhas de acesso e as responsabilidades envolvidas com o mal uso das mesmas. Independente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

m. Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas. Nestes eventos uma versão segura do sistema operacional assim como dos softwares de segurança deverá ser baixada novamente. Da mesma forma, sob uma dessas circunstâncias, todas as alterações recentes de usuários e privilégios do sistema devem ser revisadas a fim de detectar modificações não autorizadas de dados.

n. Todos os usuários têm que ser corretamente identificados antes de estarem aptos a utilizar qualquer atividade em computador ou recursos do ambiente de TI.

INSTITUTO SÃO VICENTE Folha Nº 07.609.365/0001-6

o. Quaisquer computadores que tenham comunicação remota em tempo real com os sistemas de TI, devem se submeter ao mecanismo de controle de acesso definido pela unidade competente, levando-se sempre em consideração os privilégios necessários ao acesso a cada tipo de informação.

p. Os computadores com informações sensíveis e/ou classificadas deverão, obrigatoriamente, ser desligados ou bloqueados na ausência do usuário.

q. Quando os equipamentos ou contas de usuário não estiverem em uso deverão ser imediatamente bloqueados ou desligados.

4. Recomendação para a Utilização do Correio Eletrônico Corporativo da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

Deve ser vedado o acesso não autorizado às caixas postais de terceiros e as tentativas de acesso deverão ser registradas em log, inclusive acessos feitos indevidamente por administradores de sistemas;

Deve ser vedado o envio de informações críticas para pessoas ou organizações não autorizadas observando quando for o caso, orientações para o tratamento de informações classificadas;

Deve ser vedado o envio de material obsceno, ilegal ou não ético, envio de propaganda, mensagem do tipo corrente e de entretenimento, relacionadas com nacionalidade, raça, orientação sexual, religiosa, convicção política ou qualquer outro assunto que possa vir a difamar o usuário como cidadão e que não tenha relação com o serviço a que o usuário é destinado no ambiente do TI.

Deve ser vedado o envio de mensagens simultâneas aos usuários da rede, exceto por intermédio da administração desta;

É necessário o registro por parte do usuário, enquanto funcionário, nas listas de discussão em que se encontra inserido, para fins de controle e possível cancelamento quando houver necessidade;

É recomendada a utilização de Assinatura Digital, para o envio de mensagens internas via Correio Eletrônico Corporativo quando do trâmite de informações classificadas, seguindo sempre a legislação vigente que trata deste assunto.

5. Recomendação para a Utilização de Aplicações Corporativas e Software de Terceiros da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

Deve ser vedado aos usuários que fazem uso de sistemas de informação o acesso não autorizado a qualquer outro sistema que não possua permissão de uso, assim como a danificação, a alteração a interrupção da operação de qualquer sistema do ambiente de TI. Da mesma maneira deve ser vedado aos usuários a obtenção indevida de senhas de acesso, chaves criptográficas ou qualquer outro mecanismo de controle de acesso que possa possibilitar o acesso não autorizado a recursos informacionais;

A classificação ou reclassificação da informação deve seguir as orientações da legislação vigente;

Deve ser vedado aos usuários o acesso, modificação, a remoção ou a cópia de arquivos que pertençam a outro usuário sem a permissão expressa do mesmo;

A ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA deve reservar o direito de revogar os privilégios de usuário de qualquer sistema e a qualquer momento. Não sendo permitidas condutas que

INSTITUTO SÃO VICENTE Folha Nº 07.609.365/0001-57

interfiram com a operação normal e adequada dos sistemas de informação e que adversamente afetam a capacidade de outras pessoas utilizarem esses sistemas de informação, bem como condutas que sejam prejudiciais e ofensivas;

Deve ser vedada aos usuários a execução de testes ou tentativas de comprometimento de controles interno, este tipo de prática somente pode ser permitido a usuários técnicos, em situações nas quais esteja ocorrendo monitoramento e análise de riscos, com a autorização da unidade competente;

Deve ser exigido a assinatura de termo de confidencialidade antes que seja fornecido o acesso aos sistemas relacionados com a cadeia de privilégios do usuário.

As configurações e atribuição de parâmetros em todos os computadores conectados à rede devem estar de acordo com as políticas e normas de gerenciamento internas.

\ ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA quanto ao desligamento do usuário, seus arquivos armazenados em estação de trabalho ou em qualquer servidor de rede, também, seus documentos em papel devem ser imediatamente revisados pela chefia imediata para determinar quem tornará curador das informações relacionadas, assim como nos casos devidos, identificar o método mais adequado para a eliminação das mesmas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente. Todas as atividades dos usuários que podem afetar os sistemas de informação da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA devem ser possíveis de reconstituição a partir dos logs de maneira a evitar ou dissuadir o comportamento incorreto. Estes procedimentos devem contar inclusive com mecanismos de responsabilização claros e amplamente divulgados nos meios de comunicação internos.

A divulgação das regras e orientações de segurança aplicadas aos usuários finais deverão ser objeto de campanhas internas permanentes, seminários de conscientização e quaisquer outros meios de maneira a criar uma cultura de segurança da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA.

Deve ser vedada a utilização de software da Internet ou de qualquer outro sistema externo. Esta proibição é necessária porque tal software pode conter vírus, worms, Cavalos de Tróia e outros podem comprometer o ambiente de TI. Caso haja uma legítima necessidade de obtenção de aplicações de terceiros o fato deve ser comunicado à unidade competente para que a mesma estabeleça os procedimentos de segurança necessários. Deve ser vedada a utilização de dispositivos de armazenamento de origem externa, nas estações de trabalho ou nos servidores de rede antes de serem submetidos a um software antivírus. Todos os softwares e arquivos transferidos de fontes que não sejam próprias, via Internet (ou qualquer outra rede Pública) devem ser examinados com o software de detecção de vírus. Este exame deve acontecer antes que o arquivo seja executado ou aberto por um outro programa, como por exemplo, por um processador de texto e também, antes e depois que o material tenha sido descompactado.

O usuário do ambiente de TI da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA não deve executar ou desenvolver qualquer tipo de programa ou processo externo às suas atividades.

Os usuários não devem desenvolver, gerar, compilar, copiar, coletar, propagar, executar ou tentar introduzir qualquer código projetado para se auto replicar, danificar ou de outra maneira obstruir o acesso ou afetar o desempenho de qualquer computador, rede ou sistema de TI. Deve ser vedado aos usuários e visitantes fumar, comer ou beber próximo aos equipamentos de TI.

INSTITUTO SÃO VICENTE
Folha Nº: 1
07.609.365/0001-03

6. Recomendação para a Manipulação das Informações da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

A palavra "usuário" será utilizada para designar todos utilizadores do ambiente de TI, independente do cargo ocupado;

Instruções claras e bem divulgadas sobre normas existentes sobre a manipulação de informações;

Todos os usuários têm que observar as exigências para manipulação da informação, baseadas no tipo de informação considerada e que será definida pelo seu proprietário (ou responsável) seguindo as orientações encontradas no documento de Política de Segurança. Os proprietários podem atribuir controles adicionais para maior restrição de acesso ou para ampliar a proteção a suas informações.

A divulgação de informações CONFIDENCIAIS ou RESTRITA, para qualquer pessoa (usuário ou não do ambiente de TI) da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA, é proibida, a menos que este acesso tenha sido previamente autorizado pelo proprietário da informação. Todas as pessoas que não forem usuários diretos, devem assinar um termo de confidencialidade antes de terem acesso a esses tipos de informação. Os curadores dessas informações devem verificar a existência deste termo, devidamente assinado, antes de divulgá-las para pessoas que não pertençam ao quadro funcional. O acesso a este tipo de informação deve ser sempre devidamente registrado.

A reprodução da informação CONFIDENCIAL e/ou RESTRITA, incluindo a impressão de cópias adicionais, não é permitida a menos que seja explicitamente autorizada por seu proprietário. Da mesma forma, trechos, resumos, traduções ou qualquer material derivado de informações sensíveis ou resguardadas por direitos autorais, não poderão ser feitos a menos que o proprietário da informação tenha aprovado previamente.

O transporte físico das informações CONFIDENCIAIS e/ou RESTRITAS requer a observação no disposto em legislação relacionada.

Quando as informações são CONFIDENCIAIS e/ou RESTRITAS não forem mais necessárias e quando exigências legais ou regulatórias para sua retenção não se aplicarem mais, elas deverão ser destruídas de acordo com os métodos aprovados. É proibida a eliminação em latas de lixo ou em depósitos de papel que serão encaminhados para reciclagem. A informação sensível em forma de papel deve ser eliminada com o uso de picotador de papel. A informação sensível armazenada em disquetes, fitas magnéticas ou outras mídias magnéticas computacionais deve ser destruída via reformatação ou apagando-se a informação caso a mídia seja reutilizada por outros sistemas do da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA. A simples "remoção" de uma informação sensível armazenada em uma mídia magnética não é suficiente porque a informação pode ser definitivamente destruída com cortadores ou colocada em um recipiente especialmente destinado a armazenagem de informação sensível que será destruída.

7. Responsabilidade da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

É de competência de cada unidade e responsabilidade para assinatura de seus usuários, objetivando a declaração de conhecimento de suas normas de segurança. As transgressões a tais normas deverão ser apuradas em conformidade com a legislação aplicável.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-67

Anexo I

Glossário de Termos Técnicos

A

Ambiente do Site - Infraestrutura computacional, de rede e lógica, que compõe a base para o provimento do serviço Web.

Arquitetura de Rede - É uma definição de alto nível do comportamento e das conexões entre nós em uma rede, suficiente para possibilitar a avaliação das propriedades da rede.

Atacante - Indivíduo responsável pela realização de um ataque. Ataque - Ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema não confiável, ou indisponível, violando assim a política de segurança. Um ataque bem-sucedido que resulte no acesso ou manipulação de informações, de forma não autorizada, é chamado de invasão.

Ataque de Negação de Serviço - Ataque que consiste em impedir o acesso autorizado a recursos de um sistema, seja através de uma grande sobrecarga no processamento de dados de um sistema computacional, da saturação de um ponto de acesso através de um grande tráfego de dados para uma rede, ou da indisponibilização de um ou mais serviços desse sistema.

Atividade Maliciosa - Qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema computacional.

Autenticação - Procedimento utilizado na identificação de usuários, dispositivos ou processos, e que é pré-requisito para o acesso aos recursos de um sistema.

Autorização - É o direito ou permissão de acesso a um recurso de um sistema.

B

Backdoor - Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

C

Capacidade de Sobrevivência (Survivability) - É a capacidade de um sistema de cumprir a sua missão, no momento certo, na presença de ataques, falhas ou incidentes.

Cavalo de Tróia - É um Programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Cenário de Uso - É uma instância do uso de um sistema, tanto o uso legítimo como o uso em uma invasão. O organismo utilizador, normalmente caracterizada por um processo ou programa de computador, que requisita e utiliza recursos/informações e interage com um serviço fornecido por um sistema computacional, como por exemplo um servidor Web (ver Servidor Web, Serviço Web).

Código Malicioso - Programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente através de exploração de alguma vulnerabilidade desse sistema.

Comprometimento de segurança - É uma violação de segurança na qual os recursos do sistema são expostos, ou potencialmente expostos, a um acesso não autorizado.

Confiança - Atributo de um sistema de informação que provê a base para ter a confiança de que o sistema opera de forma a cumprir a política de segurança.

Confiança (Assurance) - Medida de confiança garantida pela arquitetura ou pelas características de segurança implementadas em um sistema de informação automatizado.

Confidencialidade - É o requisito que diz que uma informação não é disponibilizada ou revelada para partes não autorizadas.

Contato Técnico de Segurança - Pessoa ou equipe a ser acionada em caso de incidente de segurança envolvendo um sítio governamental, com atribuições eminentemente técnicas sobre a questão.

Correção de Segurança - Software que têm por finalidade corrigir os problemas de segurança referentes a vulnerabilidades conhecidas. Também chamado de patch, hot fix ou service pack.

Criptografia - É a disciplina que trata dos princípios, meios e métodos para a transformação de dados, tornando-os ininteligíveis, de forma a possibilitar a detecção de modificações no conteúdo da informação e/ou prevenir seu uso não autorizado.

Controle de Acesso - Mecanismo utilizado para proteger os recursos de um sistema de acesso não autorizado. Deve permitir, de acordo com uma política de segurança, o acesso somente às entidades autorizadas, como usuários, processos, programas ou outros sistemas.

D

Desfiguração de Site - Ataque que consiste em desfigurar, ou seja, substituir ou alterar o conteúdo de uma ou mais páginas Web em um site. A desfiguração normalmente é consequência da exploração bem-sucedida de uma vulnerabilidade no servidor Web que hospeda as páginas do sítio.

Detecção de Intrusão - Consiste no monitoramento e análise de eventos em sistemas computacionais, com o propósito de detectar e prover alertas sobre tentativas de acesso não autorizado a recursos destes sistemas.

Direito de Acesso - É a permissão dada a uma pessoa para acessar e manipular informações presentes em um sistema.

Disponibilidade - É o requisito que diz que os recursos de um sistema estarão disponíveis para acesso, por pessoas autorizadas, sempre que venham a ser solicitados.

Firewall - Um sistema, constituído pela combinação de software e hardware, que intermedia o acesso a uma rede, permitindo ou proibindo certos tipos de acesso, de acordo com uma política de segurança pré-estabelecida.

Firewall Pessoal - Um sistema utilizado para proteger um único computador contra acessos não autorizados. Constitui um tipo específico de firewall.

I

Incidente de Segurança - Um incidente de segurança é caracterizado por qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas computacionais ou de redes de computadores. Tentativas de obter acesso não autorizado a sistemas ou dados, ataques de negação de serviço, uso ou acesso não autorizado a um sistema e desrespeito à política de segurança ou à política de uso aceitável de uma instituição são exemplos de incidentes de segurança.

Informação de Autenticação - Informação apresentada e utilizada para confirmar a identidade de alguém, como usuários, processos, programas ou sistemas.

Integridade - É o requisito que diz que uma informação não é modificada ou destruída de maneira não autorizada ou acidental.

Intrusão - Ver Invasão. Intruso - Ver Invasor.

Invasão - Evento ou combinação de eventos que constituem um incidente de segurança em que um invasor ou um código malicioso obtém acesso a um sistema, ou a recursos de um sistema, de forma não autorizada.

Invasor - Indivíduo responsável pela realização de uma invasão.

Irretratabilidade - Garantia de que o emissor de uma mensagem não irá negar posteriormente a sua autoria ou participação em uma transação. É controlada pela existência de uma assinatura digital que somente o emissor pode gerar.

M

Mecanismo de Controle de Acesso (Access Control Mechanism) - São mecanismos de hardware ou software, procedimentos operacionais ou gerenciais usados para detectar e prevenir os sistemas computacionais contra acessos não autorizados.

Modelo de Uso (Usage Model) - É a definição de todos os cenários de utilização possíveis de um ambiente de sistemas, incluindo o uso legítimo e aquele possível de ser explorado por um intruso.

Mecanismos de Controle de Acesso - São mecanismos de hardware ou software, ou procedimentos operacionais ou gerenciais, usados para proteger os sistemas computacionais contra acessos não autorizados.

Modo seguro - É o conjunto que envolve configurações, procedimentos e diretrizes de segurança recomendados por entidades notoriamente reconhecidas na área de segurança da informação.

N

Negação de Serviço - É o ataque à segurança feito a partir da saturação de um ponto de acesso de forma que este não disponha de banda passante para o atendimento dos seus usuários legítimos.

O

Órgãos Conveniados - São aquelas entidades que não fazem parte das estruturas organizacionais da Administração Pública Federal (APF), e, mediante convênio, utilizam os serviços oferecidos por meio dos

Sistemas de TI destas. Órgão Proprietário do Sítio Governamental - Entidade governamental proprietária do domínio onde se encontram armazenadas as informações e serviços prestados.

P

Plug-in - Módulo constituído por um dispositivo de hardware ou software, que adiciona uma característica, funcionalidade ou serviço específico a um sistema.

Política de Segurança - Atribui direitos e responsabilidades aos indivíduos que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Define as atribuições de cada indivíduo em relação à segurança dos recursos com os quais trabalha. Qualquer evento que resulte no descumprimento da política de segurança é considerado um incidente de segurança.

Política de Uso Aceitável - Documento que define como os recursos computacionais de uma instituição podem ser utilizados. Também define os direitos e responsabilidades dos usuários destes recursos.

R

Recursos da Infraestrutura de TI - Os recursos da infraestrutura de TI incluem equipamentos, utilitários, aplicativos, sistemas operacionais, mídias de armazenamento, contas em servidores, contas de correio eletrônico, navegação na Internet e intranet, serviço de transferências de dados, terminal virtual, comunicação interativa e sistemas de gestão.

Rede Sem Perímetro - É uma rede caracterizada por tipologia e funcionalidade que não podem ser determinadas, assim como pela ausência de controle centralizado.

Registro de Evento - Conjunto de informações armazenadas e que estão relacionadas aos eventos ocorridos em um determinado contexto, como serviços Web, autenticação de usuários, etc.

Requisitos de Sobrevivência de Serviços - É a definição dos serviços essenciais assim como das funcionalidades relacionadas com a resistência, reconhecimento, recuperação e adaptação, e evolução que são suficientes para satisfazer os requisitos necessários à garantia da sobrevivência do sistema.

S

Script - Um script consiste em uma lista de comandos que podem ser executados sem a interação do usuário. Normalmente é escrito em uma linguagem de programação simples, que facilita o seu desenvolvimento. É bastante utilizado, por exemplo, em serviços Web, para a realização de buscas, processamento e fornecimento de informações em páginas Web.

Serviços de Adaptação e Evolução - São funções que melhoram continuamente a capacidade do sistema de fornecer os serviços essenciais, melhorando sua resistência, capacidade de reconhecimento e recuperação.

Serviços Subsidiários - São serviços adicionais à emissão dos certificados que suportam a assinatura digital e outros serviços relacionados ao comércio eletrônico como criptografia de dados. Como exemplo deste tipo de serviços pode-se citar serviços de diretoria e serviços de geração de pares de chaves. O serviço de diretório possibilita que os usuários recuperem certificados e outras informações sobre pessoas, como nomes distintos e endereços de e-mail. Serviços de geração de pares de chaves fornecem aos usuários pares

de chaves pública/privada de alta qualidade apropriadas para um algoritmo criptográfico particular. As chaves privadas são seguramente destruídas após a sua geração de forma a evitar potenciais comprometimentos.

institutosaovicente@gmail.com
Telefone: (85) 3536-1240
Rua Osvaldo Cruz 1 Meireles
Sala 1707 Fortaleza - CE

Anexo II

Referências de Legislação 3.2 Decreto Nº 8.183, de 11 de abril de 1991 dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional. 3.3 Decreto Nº 1.048, de 21 de janeiro de 1994 dispõe sobre a estrutura e o funcionamento do SISP 3.4 Decreto 3505, de 14 de junho de 2000 atualiza o código penal e dá outras providências 3.6 Decreto 4553 Define procedimentos para a classificação de informações sensíveis.

institutosaovicente@gmail.com
Telefone: (88) 3536-1290
Rua Conselho Cruz 1, Messejana,
CEP 1707, Fortaleza - CE

Anexo III

Exemplo de Termo de Confidencialidade e Sigilo

Eu, _____, Portador do documento de identidade nº _____, comprometo-me a manter sigilo sobre dados, processos, informações, documentos e materiais que eu venha a ter acesso ou conhecimento no âmbito da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA, em razão das atividades profissionais a serem realizados e ciente do que preceituam a Lei 10.406, de 10 de janeiro de 2002 (Código Civil), no seu art. 229, inciso I; o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), nos arts. 153, 154, 314, 325 e 327; o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), no art. 207; a Lei nº 5.689, de 11 de janeiro de 1973 (Código de Processo Civil), nos arts. 116, 117, 132 e 243; a Lei nº 8.159, de 8 de janeiro de 1991 (Lei de Arquivos), nos arts. 4, 6, 23 e 25; a Lei nº 9.983, de 14 de julho de 2000 (Alteração do Código Penal); e o Decreto nº 4.553, de 27 de dezembro de 2002 (Salvaguarda de dados, informações, Documentos e materiais sigilosos).

E por estar de acordo com o presente Termo, assino-o na presença das testemunhas abaixo mencionadas.

_____

Colaborador

_____

Diretoria

RELATÓRIO DE DIAGNÓSTICO LGPD ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

1. O QUE É O DIAGNÓSTICO LGPD?

Este relatório de diagnóstico tem como propósito avaliar a conformidade da organização com os requisitos da LGPD (Lei Geral de Proteção de Dados) e identificar áreas que precisam ser aprimoradas. O objetivo é estabelecer um plano de ação claro para assegurar o cumprimento das diretrizes de privacidade e proteção de dados estipuladas pela legislação.

A equipe de especialistas da INTUIX irá realizar uma análise comparativa entre o nível atual de conformidade e o estado desejado após a implementação completa da LGPD. Essa avaliação irá destacar tanto as discrepâncias presentes quanto os elementos essenciais que demandam atenção para efetuar as mudanças necessárias.

Com base nesta análise, iremos fornecer diretrizes sólidas e as ferramentas adequadas para que a sua empresa alcance os objetivos desejados em termos de conformidade com a LGPD. Nosso enfoque está em tornar a implementação das

mudanças necessárias eficaz, assegurando que as práticas relacionadas à privacidade e proteção de dados estejam em total conformidade.

Através da análise criteriosa e de uma abordagem estratégica da INTUIX, a sua organização estará preparada para enfrentar os desafios e aproveitar as oportunidades que a LGPD oferece. Juntos, estabeleceremos um futuro mais seguro e responsável para a sua empresa e seus clientes, garantindo o cumprimento das regulamentações e a devida salvaguarda dos dados.

2. LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que foi aprovada em 2018 e entrou em vigor em setembro de 2020. Essa Lei estabelece as regras sobre como as empresas devem realizar o tratamento de dados pessoais no país. Esta lei tem como objetivo principal proteger a privacidade e os direitos dos indivíduos em relação aos seus dados pessoais, estabelecendo princípios, diretrizes e obrigações para as empresas que lidam com esses dados. Ela se baseia em conceitos como consentimento, finalidade, necessidade, transparência, segurança e responsabilidade.

LGPD

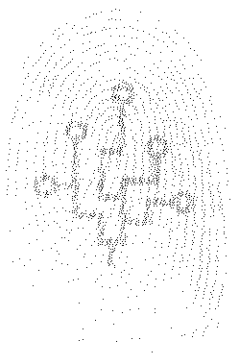
A abrangência da LGPD é ampla, aplicando-se a todas as empresas e organizações que realizam o tratamento de dados pessoais no território brasileiro, independentemente do seu porte ou setor de atuação. A lei se aplica tanto a empresas privadas como a entidades governamentais.

No que diz respeito às multas, a LGPD prevê sanções administrativas para casos de descumprimento das suas disposições. As multas podem chegar a até 2% do faturamento da empresa no último exercício fiscal, limitadas a um total de R$ 50 milhões por infração. Além das multas, a ANPD (Autoridade Nacional de Proteção de Dados) também pode aplicar advertências, bloqueio ou eliminação dos dados tratados de forma irregular, entre outras medidas.

2.1 Benefícios da LGPD

Entre os benefícios trazidos pela LGPD estão:

- **Maior proteção dos direitos dos indivíduos:** A lei fortalece a privacidade e dá aos titulares dos dados maior controle sobre suas informações pessoais, garantindo direitos como acesso, retificação, exclusão, portabilidade e revogação do consentimento.



- **Melhoria na segurança dos dados:** A LGPD estabelece requisitos e medidas para a segurança e proteção dos dados pessoais, incentivando as empresas a adotarem práticas e tecnologias adequadas para evitar incidentes de segurança e vazamentos.
- **Fortalecimento da confiança dos clientes:** O cumprimento da LGPD demonstra um compromisso com a proteção da privacidade dos clientes, contribuindo para a construção de uma relação de confiança e fidelidade.
- **Harmonização com padrões internacionais:** A LGPD alinha a legislação brasileira com os padrões internacionais de proteção de dados, facilitando o fluxo de dados entre o Brasil e outros países.

3. PRINCIPAIS NOMENCLATURAS DA LGPD

A LGPD possui algumas nomenclaturas específicas, estas precisam ser plenamente entendidas pelos colaboradores, para que o processo de implementação do Compliance LGPD ocorra de uma maneira adequada e a empresa mitigue os riscos relacionados à inadimplência com a Lei.

Dados pessoais: São informações relacionadas a uma pessoa física identificada ou identificável. Esses dados referem-se a qualquer informação que permita a identificação direta ou indireta de uma pessoa, como nome, CPF, RG, endereço, telefone, e-mail, dados biométricos, entre outros.

Dados pessoais sensíveis: São categorias especiais de dados pessoais que requerem um nível mais elevado de proteção devido ao seu potencial de discriminação ou risco. Isso inclui informações sobre origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, dados genéticos, dados biométricos, entre outros.

Titular dos dados: É a pessoa física a quem os dados pessoais se referem, ou seja, o indivíduo que é dono dos dados. É importante distinguir claramente o titular dos dados pessoais das pessoas jurídicas, que não possuem os mesmos direitos e proteções.

Tratamento de dados: Refere-se a qualquer operação realizada com dados pessoais, como coleta, armazenamento, uso, compartilhamento, exclusão, entre outras ações.

Controlador: É a pessoa física ou jurídica que toma as decisões sobre o tratamento de dados pessoais. É o responsável por determinar as finalidades e os meios de processamento dos dados.

Operador: É a pessoa física ou jurídica que realiza o tratamento de dados pessoais em nome do controlador, seguindo suas instruções.

Encarregado de Proteção de Dados (DPO): É o profissional designado pela empresa para atuar como ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO é responsável por garantir o cumprimento das obrigações da LGPD.

Consentimento: É a manifestação livre, informada e inequívoca do titular dos dados concordando com o tratamento de seus dados pessoais para uma finalidade específica. O consentimento deve ser obtido de forma clara e específica, não podendo ser presumido.

INSTITUTO SÃO VICENTE
Folha Nº
CNPJ 23.[illegible]/0001-69

Autoridade Nacional de Proteção de Dados (ANPD): É a autoridade responsável por fiscalizar e regulamentar a aplicação da LGPD no Brasil, bem como receber denúncias, aplicar sanções e orientar empresas e titulares de dados.

Anonimização: É o processo pelo qual os dados pessoais são modificados de forma a não mais serem associados a um titular identificado ou identificável, de modo que não seja possível reidentificar os indivíduos a partir desses dados.

Transferência internacional de dados: Refere-se ao envio de dados pessoais para fora do território brasileiro, podendo envolver países ou organizações internacionais. A transferência de dados só é permitida para países que possuam um nível adequado de proteção ou mediante a adoção de garantias apropriadas, como cláusulas contratuais ou regras corporativas vinculantes.

Incidente de segurança: Refere-se a qualquer evento que comprometa a segurança dos dados pessoais, como acesso não autorizado, vazamento, perda ou destruição acidental dos dados. A LGPD estabelece a obrigação de notificar incidentes de segurança às partes envolvidas e à ANPD, quando aplicável.

Período de retenção de dados: refere-se ao tempo durante o qual os dados pessoais são armazenados e mantidos por uma empresa ou organização. É o intervalo de tempo em que os dados são considerados necessários para cumprir a finalidade original da sua coleta ou para atender a obrigações legais ou regulatórias.

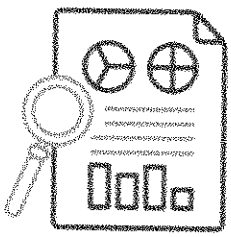
Sanções e penalidades: A LGPD prevê sanções administrativas em caso de não conformidade com as disposições da lei. As penalidades podem incluir advertências, multas de até 2% do faturamento da empresa (limitado a R$ 50 milhões por infração) e a proibição parcial ou total do exercício das atividades relacionadas ao tratamento de dados.

Essas nomenclaturas podem ser complexas e exigir um entendimento claro para garantir a conformidade com a LGPD. É importante que os colaboradores da organização ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA estejam familiarizados com esses termos e suas definições para evitar confusões e garantir uma aplicação adequada da legislação de proteção de dados.

INSTITUTO SÃO VICENTE
Folha Nº
07.609.365/0001-57

4. DADOS GERAIS DA ORGANIZAÇÃO

Manter conformidade com a LGPD é crucial por várias razões: respeito à privacidade dos titulares dos dados, evitar multas e penalidades, construir confiança, minimizar riscos cibernéticos, acessar novos mercados, evitar litígios e demonstrar profissionalismo ético. Isso protege tanto os dados dos indivíduos quanto a reputação e operações das organizações.



Segmento da organização: associação

Estado: Ceará

Denominação do negócio: entidade

Público do negócio: parceiros

5. DATA PROTECTION OFFICER - DPO

O DPO (Data Protection Officer), ou Encarregado de Proteção de Dados, é uma figura fundamental na implementação e manutenção da conformidade com a LGPD (Lei Geral de Proteção de Dados). O DPO desempenha um papel crucial como um ponto focal para todas as questões relacionadas à proteção de dados dentro de nossa organização.

Nome do DPO: Brenda Silveira Ruivo

E-mail: compras@institutosaovicente.com.br

Telefone comercial: 85 3021-0044

5.1 Deveres do DPO

I - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

O DPO é responsável por receber reclamações e comunicações dos titulares dos dados pessoais. Isso significa que qualquer pessoa cujos dados estejam sendo processados pela organização pode entrar em contato com o DPO para expressar preocupações, fazer perguntas ou apresentar queixas relacionadas ao tratamento de seus dados. O DPO deve estar preparado para fornecer explicações e esclarecimentos sobre como os dados estão sendo tratados e, se necessário, tomar medidas para resolver problemas ou violações de segurança.

II - Receber comunicações da autoridade nacional e adotar providências:

A autoridade nacional mencionada é a Autoridade Nacional de Proteção de Dados (ANPD) no contexto brasileiro. O DPO deve estar pronto para receber comunicações e orientações da ANPD. Se a autoridade nacional emitir diretrizes, regulamentos ou pedidos relacionados ao tratamento de dados pessoais, o DPO é responsável por garantir que a organização adote as providências necessárias para cumprir essas orientações. Isso inclui tomar ações corretivas ou ajustar procedimentos conforme exigido pela ANPD.

III - Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais:

Uma das funções cruciais do DPO é educar e orientar os funcionários e contratados da organização sobre as práticas adequadas de proteção de dados. Isso inclui fornecer treinamento para garantir que todos os colaboradores compreendam as políticas de privacidade, procedimentos internos e regulamentações relevantes relacionadas à proteção de dados pessoais. O DPO deve garantir que os funcionários saibam como lidar com os dados, como minimizar riscos e como cumprir as obrigações legais relacionadas à privacidade.

IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares:

O DPO é obrigado a realizar outras tarefas específicas conforme determinadas pelo controlador (a organização que decide como os dados pessoais serão processados) ou conforme definido em normas complementares, como regulamentos específicos ou diretrizes emitidas pela ANPD. Isso pode envolver tarefas adicionais relacionadas à proteção de dados pessoais e à conformidade com a LGPD.

INSTITUTO SÃO VICENTE
Folha Nº
09.509.365/0001-57

6. DIAGNÓSTICO LGPD

A equipe de especialistas da INTUIX realizou uma análise e identificou áreas essenciais que demandam aprimoramentos para garantir a conformidade plena da organização ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA com a Lei Geral de Proteção de Dados (LGPD). Esses pontos de aperfeiçoamento foram criteriosamente selecionados com base nos processos envolvidos na coleta, processamento e armazenamento de dados pessoais:

Pontos de Melhoria Identificados

Entendimento da LGPD e Cultura de Compliance:

A organização precisa melhorar seu conhecimento sobre as regras e termos da LGPD. Também precisa melhorar sua cultura de compliance e privacidade dos dados pessoais.

Avaliação: Fraco

Coleta de Consentimento e Segurança dos dados Pessoais:

A organização está evoluindo na coleta de consentimento e segurança dos dados pessoais.

Avaliação: Razoável

Mapeamento do Fluxo de Dados e Período de Retenção:

A organização precisa aprimorar o mapeamento do fluxo de dados e ser mais criteriosa na formulação de seu período de retenção.

Avaliação: Fraco

Níveis da Avaliação	Ruim	Fraco	Razoável	Bom	Excelente

Uma análise mais detalhada e instruções específicas para superar cada desafio estão disponíveis na seção subsequente. A INTUIX se empenha em oferecer um diagnóstico abrangente, destinado a auxiliar a organização na implementação de práticas sólidas de conformidade com a LGPD, assegurando o respeito à privacidade dos dados e a prevenção de possíveis implicações legais.

6.1 Medidas Gerais para Melhorias

Na lista abaixo, encontre os pontos de melhorias identificados e implemente as medidas sugeridas para aprimorar seu processo de compliance com a LGPD.

Ponto de aprimoramento	Medidas
Melhorar a definição dos prazos para descarte de dados	Determinar prazos para a retenção e o posterior descarte de dados pessoais é essencial para atender aos requisitos da LGPD. Manter dados por mais tempo do que o necessário pode aumentar riscos e violar a privacidade dos titulares. Recomenda-se: • Realizar uma análise dos tipos de dados coletados e das finalidades para definir prazos adequados de retenção. • Estabelecer políticas de retenção claras e detalhadas, garantindo que os dados sejam excluídos após o período de retenção. • Implementar processos automatizados para identificar e remover dados que excedam o prazo de retenção.
A organização precisa implementar e divulgar melhor a Política de Privacidade e Cookies	Uma política de privacidade clara e completa é fundamental para informar os titulares de dados sobre como suas informações pessoais são coletadas, processadas, usadas e protegidas. Além disso, a política de cookies deve explicar como são utilizados os cookies e outras tecnologias de rastreamento. Recomenda-se:

	• Verificar se a política de privacidade detalha os tipos de dados coletados, a finalidade da coleta, as bases legais para o processamento, os direitos dos titulares e os procedimentos para exercer esses direitos. • Verificar se a política inclui informações sobre cookies e outras tecnologias de rastreamento, explicando como os visitantes podem gerenciar suas preferências de consentimento. • Disponibilizar a política de privacidade e cookies de forma acessível em seu site e em outros canais de coleta de dados.
Entender e melhorar as formas de segurança para proteção dos dados.	A implementação de medidas de segurança robustas é fundamental para proteger os dados pessoais contra acesso não autorizado e violações de segurança. • Utilizar criptografia para proteger dados pessoais em trânsito e em repouso. • Implementar controle de acesso para garantir que apenas pessoal autorizado possa acessar dados sensíveis. • Realizar auditorias regulares de segurança para identificar vulnerabilidades e corrigi-las prontamente. • Manter sistemas e software atualizados com as últimas correções de segurança.
A organização precisa melhorar seu conhecimento sobre as regras e termos da LGPD.	Muitas empresas têm dificuldade em entender os detalhes da lei e como ela se aplica às suas operações. Recomenda-se: • Realizar treinamentos e workshops sobre a LGPD para funcionários em todos os níveis. • Contratar consultorias especializadas em privacidade e proteção de dados para orientar as etapas de conformidade.
A organização precisa	Identificar quais dados pessoais são coletados, processados e armazenados em toda a organização pode ser desafiador.

aprimorar o mapeamento do fluxo de dados.	Recomenda-se: • Realizar um inventário de dados pessoais, documentando os processos e finalidades de cada tipo de dado. • Designar responsáveis por cada categoria de dados para gerenciar sua conformidade.
A organização precisa avançar na implementação das Políticas e Procedimentos da LGPD.	Elaborar políticas e procedimentos eficazes para lidar com o tratamento de dados pessoais pode ser complexo. Recomenda-se: • Desenvolver políticas claras de privacidade e proteção de dados, abordando coleta, processamento, armazenamento, compartilhamento e exclusão de dados. • Criar procedimentos para lidar com solicitações de titulares de dados, como acesso, retificação e exclusão de informações.
A organização necessita aprimorar a coleta de consentimento e garantir os direitos dos titulares de dados.	Garantir que a coleta e o processamento de dados pessoais sejam baseados em consentimento válido e que os direitos dos titulares sejam respeitados é um desafio. Recomenda-se: • Obter consentimento explícito para coleta e processamento de dados sempre que necessário. • Implementar processos para atender às solicitações de titulares, como acesso a dados e exclusão.
A organização precisa aumentar a segurança e a proteção de dados.	Manter a segurança dos dados pessoais e prevenir violações de segurança é uma preocupação constante. Recomenda-se: • Implementar medidas de segurança robustas, como criptografia, autenticação multifator e monitoramento contínuo de ameaças. • Estabelecer um plano de resposta a incidentes de segurança, caso ocorram violações de dados.
É recomendável que a organização adeque seu	Gerenciar o compartilhamento de dados com terceiros de forma segura e em conformidade pode ser complicado.

processo de realização de contratos com terceiros e parceiros.	Recomenda-se: • Revisar contratos com terceiros para garantir que eles atendam aos requisitos da LGPD. • Incluir cláusulas específicas de proteção de dados nos acordos com fornecedores e parceiros.
A organização precisa desenvolver uma cultura de privacidade.	Promover uma cultura organizacional que valorize a privacidade e proteção de dados pode ser desafiador. • Integrar a conscientização sobre privacidade nos treinamentos regulares para funcionários. • Nomear um encarregado de proteção de dados (DPO) para supervisionar a conformidade e atuar como ponto de contato para questões relacionadas à privacidade.

institutosaovicente@gmail.com
Telefone: (88) 3538-1260
Rua Oswaldo Cruz 1, Meireles,
Sala 1707, Fortaleza - CE

POLÍTICA INTERNA DE PROTEÇÃO DE DADOS

ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA

1. Definições

Para fins da Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais, de acordo com o Capítulo 1 – Disposições preliminares, o Art. 5º especifica as principais informações determinantes:

Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Dado pessoal sensível: qualquer dado pessoal que contenha informação sobre:

- Origem racial ou étnica.
- Convicção religiosa.
- Opinião política.
- Filiação a sindicato ou organização de caráter religioso, filosófico ou político.
- Saúde.
- Vida sexual.
- Genética ou biometria.

Titular: Pessoa natural (física) a quem se referem os dados. Tratamento: qualquer operação com os dados pessoais, incluindo armazenamento.

Consentimento: manifestação livre e inequívoca pela qual o titular concorda com o tratamento dos seus dados pessoais para uma finalidade específica.

Operador: pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador. São operadores os empregados, prestadores de serviço e demais parceiros que participam do tratamento de dados pessoais dentro da empresa.

Controlador: pessoa física ou jurídica, de direito público ou privado, que administra e toma decisões sobre o tratamento de dados pessoais.

Agentes de tratamento: o controlador e o operador.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Encarregado de Dados (DPO): pessoa indicada pelo controlador para ser responsável pela comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANDP).

institutosaovicente@gmail.com
Telefone: (88) 3536-1240
Rua Oswaldo Cruz 1, Meireles, Sala 1707, Fortaleza - CE

Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

2. Objetivo da política interna de proteção de dados

A ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA deve orientar a todos os membros acerca das boas práticas em proteção de dados pessoais, visando conformidade com a Lei nº 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais.

3. Contexto da LGPD

A LGPD foi promulgada em 2018 com o objetivo de trazer ao ordenamento jurídico brasileiro uma preocupação que já tem lugar em todos os países desenvolvidos: a proteção de dados pessoais. No mundo todo, a legislação de proteção a dados de pessoas naturais é um instrumento necessário para garantir maior segurança jurídica e respeitabilidade aos direitos humanos fundamentais. Assim sendo, a conformidade com tais leis tem sido um fator importante na ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA.

4. Princípios da LGPD

São os princípios norteadores da Lei Geral de Proteção de Dados e também os desta política interna:

Adequação: o tratamento dos dados tem que ser compatível com a finalidade informada ao titular.

Necessidade: o tratamento deve ser limitado ao mínimo necessário para atingir a finalidade proposta.

Livre acesso: os titulares têm o direito de acessar a qualquer tempo as informações referentes ao tratamento que seus dados recebem.

Qualidade dos dados: o tratamento dos dados deve mantê-los exatos, claros, relevantes e atualizados, sem discrepâncias ou distorções.

Transparência: o tratamento dos dados deve ser explicado aos titulares de maneira transparente e acessível, observado o segredo comercial e industrial necessário.

Segurança: os dados pessoais devem ser protegidos pelo controlador, para que não sejam perdidos, alterados, destruídos ou acessados indevidamente.

Prevenção: cabe ao controlador tomar medidas para prevenir danos provenientes do tratamento de dados pessoais.

Não discriminação: o tratamento de dados pessoais não deve ser realizado com finalidades discriminatórias, ilícitas ou abusivas.

Responsabilização e prestação de contas: demonstração, aos titulares, das medidas utilizadas para garantir conformidade com a Lei Geral de Proteção de Dados Pessoais.

5. Responsabilidade compartilhada

A responsabilidade pelo correto tratamento dos dados pessoais dentro da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA é compartilhada entre todos aqueles que atuam como operadores, sendo fundamental a cooperação de todos para que a empresa esteja sempre em conformidade com a lei, oferecendo segurança a todos os titulares de dados pessoais sob seu controle.

Nos termos dos art. 42 e seguintes da Lei Geral de Proteção de Dados (Lei 13.709 de 14 de agosto de 2018), o operador de dados pessoais que descumprir as diretrizes lícitas de proteção de dados do controlador responderá como se também fosse controlador dos dados em questão, estando assim sujeito à responsabilidade civil, administrativa e criminal sobre o tratamento inadequado dos dados.

Segundo art. 23, a violação de segredos da organização, concepção que inclui dados pessoais sob seu controle, poderá a critério exclusivo da Direção ser motivo para embasar a demissão por justa causa de colaboradores ou a rescisão de contrato de prestadores de serviços envolvidos na violação, sem prejuízo das ações de regresso cabíveis judicialmente.

6. Tratamento dos dados pessoais

A ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA no seu tratamento de dados, deve seguir os princípios definidos nesta política, devendo ser estritamente voltado às finalidades às quais a coleta dos dados se destina, respeitando os princípios desta política e os critérios de compartilhamento e de segurança das informações.

Os dados pessoais devem ser manipulados apenas por pessoas que precisem lidar com eles. Assim, reduzem-se os riscos de falhas humanas propiciando um vazamento ou uso inadequado da informação. Para garantia, é necessário dividir os dados por setores e por responsabilidades específicas dentro de cada setor. Assim se saberá em cada situação quem são os operadores dos dados e os riscos de um incidente na segurança da informação diminuem.

Para garantir este tratamento setorizado dos dados, cada acesso ao banco de dados da empresa é individual e intransferível. Assim, somente pessoas autorizadas poderão ter acesso.

O mero acesso e/ou a utilização indevida de quaisquer dados pessoais armazenados ou processados pela empresa são terminantemente proibidos, sob pena de demissão por justa causa (ou rescisão do contrato de prestação de serviços) sem prejuízo da responsabilização cível e criminal cabível em âmbito judiciário.

7. Critérios de coleta dos dados pessoais.

As informações referentes a pessoas físicas somente devem ser coletadas na medida da necessidade para a prestação de serviços, e em todas as hipóteses cabíveis o consentimento para o tratamento dos dados deverá ser obtido em conformidade com a Lei Geral de Proteção de Dados.

O consentimento é requerido ao solicitar os dados aos titulares, quando necessário, através do aceite no campo apropriado do sistema, ou um e-mail resposta com o qual a solicitação dos serviços for concluída, na fase comercial, ou ao solicitar assinatura de termos de consentimento.

8. Critérios de armazenagem dos dados pessoais.

Quanto à armazenagem, devem seguir as seguintes diretrizes:

Quando armazenados fisicamente, os dados devem ficar em local protegido, fora do alcance de outras pessoas que não são expressamente autorizadas a acessá-los.

Quando armazenados digitalmente, devem ficar em pasta protegida por criptografia e restrição de acesso por senha pessoal.

Eventuais cópias de dados pessoais somente devem ser feitas em caso de necessidade para cumprimento da finalidade proposta ao tratamento, todas as cópias devem ser administradas internamente e protegidas para que não ocorra vazamento de dados.

9. Critérios de compartilhamento interno de dados pessoais.

Os dados pessoais somente podem ser compartilhados com pessoas cuja função dentro da empresa exija que elas tenham acesso. Por exemplo: dados referentes a saúde ocupacional, como atestados médicos, exames admissionais, entre outros, só podem ser compartilhados dentro da empresa com pessoas responsáveis pelo tratamento dessas informações, como o responsável pelo RH, não podendo ser compartilhados com alguém da área técnica que não precise ter acesso a esses dados para o cumprimento de suas funções.

10. Critérios de compartilhamento externo de dados pessoais.

O compartilhamento de dados pessoais com pessoas ou entidades externas à empresa deve ser restrito ao mínimo necessário para a execução dos contratos e prestações de serviços nos quais os titulares estão envolvidos, ou para o cumprimento de qualquer obrigação legal. Mesmo quando o tratamento envolver diretamente a prestação de serviços, o consentimento para este tratamento e compartilhamento deverá ter sido previamente obtido.
É vedado o compartilhamento externo de dados pessoais de parceiros ou qualquer parte pertencente da ASSOCIACAO DE PROTECAO E ASSISTENCIA A MAT E INFANCIA, por qualquer meio, como por exemplo, telefônico, digital ou por escrito, sem autorização destes, sendo dada a ciência devida ao titular sempre que os dados forem compartilhados em um novo contexto, não previsto no consentimento recolhido.

11. Critérios de eliminação dos dados pessoais.

Quando atingida a finalidade do tratamento dos dados pessoais, e eles não mais precisarem ser armazenados para satisfazer quaisquer exigências legais, estes deverão ser devidamente eliminados física e digitalmente, com a comunicação desta eliminação ao titular nos casos em que ela se dê de maneira diversa àquela prevista no termo de consentimento aplicável.

12. Prestação de informações e transparência.

Os operadores de dados pessoais deverão prover todas as informações requeridas pelos titulares acerca do tratamento de seus dados pessoais, respeitando o direito da empresa de manter sigilo comercial quando cabível. A finalidade do tratamento deve ser sempre evidenciada e transparente.

Quando houver solicitação da prestação de informações sobre os dados pessoais pelo titular destes, os operadores deverão informar ao Encarregado da Proteção de Dados Pessoais sobre a solicitação e então prestar as informações solicitadas ao titular.

13. Encarregado da Proteção de Dados Pessoais (DPO).

O encarregado da proteção de dados pessoais ou DPO, é a pessoa responsável, nos termos da LGPD, pela comunicação entre os titulares.

São atribuições do encarregado verificar os riscos existentes, apontar as medidas corretivas e avaliar periodicamente a segurança de dados pessoais dentro da empresa, devendo também realizar eventuais comunicações necessárias com os titulares ou com o poder público. Quaisquer questionamentos que surgirem no dia a dia da empresa acerca da proteção de dados pessoais devem ser levados ao encarregado para que este possa orientar de imediato o operador ou buscar junto à ANPD e demais entidades especializadas uma orientação adequada ao questionamento levantado.

14. Relatório de Impacto à Proteção de Dados Pessoais.

O Encarregado da Proteção de Dados Pessoais manterá relatório de avaliação de riscos e impactos à proteção de dados pessoais, por meio do qual as medidas necessárias à segurança da informação de dados pessoais poderão ser estruturadas, implementadas e avaliadas.

Quando necessário é realizada a elaboração de um relatório de impacto e o encarregado de dados ficará responsável por informar os riscos e procedimentos necessários quando ocorre o vazamento de dados.