Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP: 60.130-240- Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

PSIP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

Empresa de Tecnologia da Informação do Ceará – Etice

MAIO / 2024

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP: 60.130-240- Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

SUMÁRIO

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP: 60.130-240- Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

1 Apresentação

A Empresa de Tecnologia da Informação do Ceará – Etice, no seu papel de prover soluções em Tecnologia da Informação e Comunicação – TIC, entende a importância de ter uma Política de Segurança da Informação e Proteção de Dados Pessoais que trate de forma adequada o cenário de Transformação Digital atual como essencial para o alcance da sua missão e objetivos estratégicos. Assim, a Etice, por meio desta política, declara formalmente seu compromisso com a Segurança da Informação e Proteção de Dados Pessoais.

A **Política de Segurança da Informação e Proteção de Dados Pessoais – PSIP** da Etice é o documento que orienta e define os princípios, as diretrizes, normas e procedimentos corporativos para garantir a proteção, confidencialidade, integridade e disponibilidade das informações, dos serviços e dos sistemas de TIC da organização. A Segurança da Informação e Proteção de Dados Pessoais é vital para a qualidade dos serviços e o sucesso da Empresa de Tecnologia da Informação do Ceará, bem como, para a confiança de nossos clientes e parceiros.

O presente documento alinha-se institucionalmente à Política de Segurança da Informação e Comunicação dos Ambientes de TIC do Estado do Ceará (PoSIC) e à Lei Geral de Proteção de Dados (LGPD), estando também subordinado e integrado às recomendações do Escritório de Governança Corporativa (EGC) e da Procuradoria Jurídica (Projur) da Etice, apresentando-se às diversas áreas estratégicas como apoio e cooperação para o bom desempenho da empresa. Além disso, está baseada nas recomendações propostas pelas normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013.

Devemos lembrar também que a LGPD inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais. Vale ressaltar a importância da Política de Gestão de Riscos da Etice, que desempenha um papel fundamental para esta política, pois fornece a estrutura necessária para identificar, avaliar e gerenciar os riscos relacionados à Segurança da Informação e Proteção de Dados Pessoais na Etice.

2 Justificativa

Atualmente, a Tecnologia da Informação e Comunicação – TIC é elemento-chave para qualquer negócio. Independentemente do porte ou da área de atuação das empresas, os grandes destaques do mercado operam seus principais sistemas em computadores e com grande dependência da conectividade. Esse é um dos motivos que justificam a necessidade de uma Política de Segurança da Informação e Proteção de Dados nas empresas.

Isto se deve ao fato que nas últimas décadas, houve um significativo aumento da quantidade de informações sensíveis circulando de um ponto a outro tanto dentro da organização como dela para o mundo todo, via Internet. A proliferação dos dispositivos móveis e dos serviços de *cloud computing* (computação em nuvem) também vêm impulsionando este cenário.

Desta forma, para conseguir atender seus objetivos estratégicos e prestar um serviço de qualidade à população é questão de primeira necessidade ter políticas que, documentadas, detalhem procedimentos e diretrizes para eliminar a subjetividade ao lidar com informações sensíveis. Assim, a Etice pode melhor gerenciar os riscos por meio de controles bem definidos, que ainda fornecem referências para auditorias e ações corretivas, agregando mais valor ao negócio da empresa.

Concluindo, uma Política de Segurança da Informação e Proteção de Dados Pessoais, é fundamental para a Etice, de forma a proteger seus ativos, garantir a confidencialidade dos dados, mitigar riscos, cumprir regulamentações e manter a confiança dos clientes e parceiros. Ela serve como um guia abrangente para promover a segurança em todas as operações da empresa.

3 Objetivo

O objetivo desta política é estabelecer princípios, diretrizes e responsabilidades para a Gestão da Segurança da Informação e Proteção de Dados Pessoais na Etice, visando preservar os ativos de TIC de ameaças internas e externas, garantindo a confidencialidade, integridade e disponibilidade das informações, minimizando os riscos por meio da implementação de controles apropriados e buscando a conformidade com leis, normas e padrões vigentes.

4 Termos e Definições

Para fins dessa política, entende-se por:

4.1 **agente de tratamento:** o controlador e o operador;

4.2 **ameaça:** qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio;

4.3 **anonimização**: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

4.4 **ativo**: qualquer coisa que represente valor para a instituição;

4.5 **ativo de TIC**: conjunto de conhecimentos e dados que tem valor para uma instituição, e seus meios de armazenamento, transmissão e processamento, equipamentos necessários a isso, sistemas utilizados para tal e locais onde se encontram esses meios e equipamentos, e recursos humanos que a eles têm acesso;

4.6 **ativo de TIC patrimonial**: subconjunto de ativos de TIC, compreendendo os meios de transmissão, armazenamento e processamento de dados, equipamentos necessários a isso, sistemas utilizados para tal e locais onde se encontram tais meios e equipamentos;

4.7 **Autoridade Nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;

4.8 **backup:** cópia de dados em meio separado do original, de forma a protegê-los de qualquer eventualidade;

4.9 **banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

4.10 **bloqueio**: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

4.11 **colaborador:** empregado, comissionado, terceirizado, estagiário ou jovem aprendiz da Etice;

4.12 **computação em nuvem:** modelo computacional que permite acesso por demanda, independente da localização geográfica, a um conjunto de recursos computacionais configuráveis, que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços;

4.13 **confidencialidade:** garantia de que a informação é acessível somente por pessoas devidamente autorizadas a ter acesso à mesma;

4.14 **consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

4.15 **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais;

4.16 **CSIP**: Comitê de Segurança da Informação e Proteção de Dados Pessoais;

4.17 **criticidade:** importância da informação para a continuidade das operações da instituição;

4.18 **custodiante:** pessoa ou instituição com atribuição fornecida pelo proprietário do ativo de TIC de guardá-lo e protegê-lo adequadamente;

4.19 **dado anonimizado**: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

4.20 **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;

4.21 **dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

4.22 **dados não aplicáveis à LGPD:** informações onde os dados são anônimos, ou que tiverem sido anonimizados, não sendo a pessoa natural assim identificada ou identificável, ou em casos em que tais dados não forem sequer relacionados à pessoa natural;

4.23 **disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

4.24 **dispositivos móveis:** equipamentos portáteis dotados de capacidade computacional ou de armazenamento, entre os quais se incluem, não se limitando a estes: *notebooks, netbooks, smartphones, tablets, pendrives, USB drives*, HDS externos e cartões de memória;

4.25 **eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

4.26 **encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

4.27 **fornecedor:** pessoa física ou jurídica que mantém contrato de prestação de serviços ou fornecimento de equipamentos, materiais e seus representantes ou empregados;

4.28 **Sistema da Gestão de Segurança da Informação e Proteção de Dados Pessoais - SGSIP**: conjunto de políticas, processos, normas e procedimentos interligados, objetivando a segurança da informação e proteção de dados pessoais na Etice, implementado de acordo com a LGPD (https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm) e a Política de Gestão de Riscos (PGR – https://www.etice.ce.gov.br/wp-content/uploads/sites/5/2024/01/Politica-de-Gestao-de-Riscos-Final-Assinada.pdf) da Etice, baseada também no ciclo PDCA e na Norma ISO 27001;

4.29 **incidente**: evento não planejado relativo à TIC que pode acarretar prejuízos à empresa ou mesmo violar as regras de segurança da informação;

4.30 **informação**: conjunto organizado de dados, que constitui uma mensagem;

4.31 **integridade**: salvaguarda da exatidão completa da informação e dos métodos de processamento;

4.32 **LGPD**: Lei Geral de Proteção de Dados Pessoais, lei nº 13.853, de 2019;

4.33 operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

4.34 **órgão de pesquisa**: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

4.35 **PoSIC**: Política de Segurança da Informação e Comunicação dos Ambientes de TIC, do Governo do Estado do Ceará, instituída pelo Decreto No 29.227, de 13 de março de 2008 e revisada pelo Decreto No 34.100, de 08 de junho de 2021;

4.36 **proprietário de ativo de TIC**: responsável primário pelo ativo de TIC;

4.37 **RIPD**: Relatório de Impacto à Proteção de Dados Pessoais, documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

4.38 **ROPA**: Registro de Operações de Tratamento de Dados Pessoais, documento exigido ao controlador e ao operador, disposto no artigo 37 da LGPD;

4.39 **segurança física**: proteção dos ativos físicos de uma empresa contra furto, roubo, dano ou acesso não autorizado;

4.40 **segurança lógica**: proteção de dados e sistemas contra ameaças internas e externas;

4.41 **suboperador**: pessoa natural ou jurídica, de direito público ou privado, contratada pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador;

4.42 **termo de uso e privacidade**: comunicação enviada ao titular dos dados ou usuário de serviço com a finalidade de esclarecer a política de tratamento de dados, explicitando os dados coletados e a forma de sua utilização, em observância às disposições da LGPD;

4.43 **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

4.44 **transferência internacional de dados**: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

4.45 **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;

4.46 **uso compartilhado de dados**: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

4.47 **usuário**: pessoa que acessa ou utiliza de forma legítima e autorizada um serviço ou informação.

5 Abrangência

5.1 Abrangência Geral

As ações referentes à Segurança da Informação e Proteção aos Dados Pessoais abrangem todos os ativos de TIC gerenciados pela Etice, independentemente da titularidade de propriedade ou localização geográfica, bem como os processos de todas as unidades organizacionais, extensivas, no que couber, aos serviços e produtos oferecidos aos clientes, devendo ser seguidas, dentro de suas responsabilidades, por todos os colaboradores e fornecedores.

5.2 Abrangência específica à proteção de dados pessoais

As ações específicas ao tratamento de dados pessoais abrangem os seguintes tipos de dados:

5.2.1 Dados dos empregados, comissionados, conselheiros, estagiários ou jovens aprendizes da Etice, para fins de gerenciamento de recursos humanos, incluindo contratação, remuneração, gestão de benefícios, gestão de desempenho, disciplina e rescisão, bem como para fins de contatos de emergência.

5.2.2 Dados de titulares cujos dados são controlados pelos clientes da Etice, para fins de atendimento às especificações dos serviços contratados, enquanto operador, de acordo com as especificações exigidas pelo cliente para o tratamento de dados em observância à LGPD.

5.2.3 Dados de usuários dos sítios e aplicativos móveis da Etice, para fins de habilitar as principais funções, garantir a segurança, melhorar a funcionalidade, aprimorar e personalizar a experiência de navegação e analisar o tráfego e uso do sítio ou aplicativo.

5.2.4 Dados dos representantes de clientes e fornecedores da Etice, para fins de relacionamentos de negócio.

5.2.5 Dados de visitantes e público em geral, para fins de segurança durante o acesso às dependências físicas da Etice.

5.2.6 Dados de todos os colaboradores da Etice, para fins de operacionalização de seus processos.

5.2.7 Dados de pessoas naturais em situações diversas, não previstas expressamente nessa política, mas de acordo com a LGPD.

6 Responsabilidades

As responsabilidades relativas às ações de Segurança da Informação e Proteção aos Dados Pessoais são as seguintes:

6.1 CSIP – Comitê de Segurança da Informação e Proteção de Dados Pessoais

6.1.1 Atuar no planejamento e coordenação da segurança da informação e proteção de dados pessoais, discutindo e organizando as ações inerentes ao tema.

6.1.2 Ajustar e propor melhorias à PSIP e ao SGSIP.

6.1.3 Estabelecer as responsabilidades complementares e adjacentes à PSIP.

6.1.4 Acompanhar, monitorar e avaliar a execução da PSIP, bem como o SGSIP.

6.1.5 Formular, revisar e estabelecer normas, procedimentos, planos, processos e demais ações, de acordo com os princípios e as diretrizes estabelecidas na

PSIP.

6.1.6 Orientar e estimular a governança e adoção de boas práticas quanto aos aspectos relacionados à Segurança da Informação e Proteção aos Dados Pessoais.

6.1.7 Gerenciar os riscos da Segurança da Informação e Proteção aos Dados Pessoais.

6.1.8 Cumprir outras responsabilidades estabelecidas em ato próprio de criação ou alteração do CSIP.

6.2 Encarregado

6.2.1 Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

6.2.2 Receber comunicações da Autoridade Nacional (ANPD) e adotar providências.

6.2.3 Orientar os funcionários e os contratados da Etice a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

6.2.4 Executar as demais atribuições determinadas pela Presidência da Etice ou estabelecidas em normas complementares.

6.3 Presidência

6.3.1 Estimular a adoção de práticas de Segurança da Informação e Proteção de Dados Pessoais, inclusive disponibilizando os recursos necessários para tanto.

6.3.2 Nomear o encarregado, dando-lhe recursos e condições necessárias para o desempenho de suas atividades.

6.3.3 Garantir a disseminação e o cumprimento dessa política, inclusive disponibilizando recursos necessários para tanto.

6.3.4 Comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

6.3.5 Criar o Comitê de Segurança da Informação e Proteção de Dados Pessoais – CSIP.

6.4 Todas as unidades organizacionais

6.4.1 Adotar as normas e procedimentos relativos à Segurança da Informação e Proteção aos Dados Pessoais, associados a ativos de TIC e processos de cada área de atuação.

6.4.2 Participar da análise de riscos de ativos de TIC e processos, dentro de sua área de atuação.

6.4.3 Colaborar na elaboração de normas e procedimentos relativos à Segurança da Informação e Proteção aos Dados Pessoais.

6.4.4 Cumprir as responsabilidades específicas estabelecidas pelo CSIP.

6.5 Colaboradores e fornecedores

6.5.1 Realizar a proteção e salvaguarda dos ativos de TIC, de que sejam usuários ou que tenham acesso, independente das medidas de segurança implementadas.

6.5.2 Registrar e informar incidentes relativos à Segurança da Informação e Proteção aos Dados Pessoais, de modo que possam ser avaliados e tratados.

6.5.3 Manter o sigilo dos dados manipulados, quando necessário, inclusive quanto a dados pessoais tratados na Etice.

6.5.4 Especificamente para os fornecedores e no papel de suboperador, realizar o tratamento de dados seguindo as instruções fornecidas pela Etice e pelo controlador.

6.6 Proprietário de ativo de TIC

6.6.1 Classificar os ativos de TIC de acordo com seu grau de criticidade e sigilo.

6.6.2 Autorizar o acesso ao ativo de TIC, de acordo com as normas de controle de acesso.

6.6.3 Definir o custodiante, se necessário.

6.7 Custodiante de Ativo de TIC

6.7.1 Realizar controles de segurança com base no valor do ativo que o proprietário determinar.

7 Princípios

7.1 Princípios Gerais

Os princípios orientadores das ações de Segurança da Informação e Proteção de Dados Pessoais da Etice estão alinhados com aqueles descritos na PoSIC estadual, sendo os seguintes:

7.1.1 **Alinhamento estratégico:** A Etice deverá alinhar a segurança da informação com sua missão institucional e o seu planejamento estratégico, de forma a construir as ações de acordo com os objetivos e metas da instituição.

7.1.2 **Diversidade organizacional:** As ações relativas à segurança da informação devem levar em consideração a diversidade das suas atividades, respeitando sua natureza e finalidade.

7.1.3 **Garantia da Segurança das Informações:** Deve-se sempre buscar a implantação de ações que busquem garantir os princípios da segurança da informação: a confidencialidade, a integridade e a disponibilidade das informações.

7.1.4 **Propriedade da informação:** Toda informação produzida na Etice é de sua propriedade e não de seus colaboradores ou fornecedores, exceto os casos onde a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição.

7.1.5 **Alinhamento com os aspectos legais (Conformidade):** Devem ser cumpridas as normas legais e regulamentares de abrangência estadual e federal, as políticas e as diretrizes estabelecidas para o negócio e para as atividades do Estado, bem como se deve evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

7.2 Princípios específicos à proteção de dados pessoais

Os princípios específicos, orientadores das ações de proteção de dados pessoais na Etice estão alinhados à LGPD, sendo os seguintes:

7.2.1 A proteção aos dados pessoais tem como fundamentos:

7.2.1.1 o respeito à privacidade;
7.2.1.2 a autodeterminação informativa;
7.2.1.3 a liberdade de expressão, de informação, de comunicação e de opinião;
7.2.1.4 a inviolabilidade da intimidade, da honra e da imagem;
7.2.1.5 o desenvolvimento econômico e tecnológico, bem como a inovação;
7.2.1.6 a livre iniciativa, a livre concorrência e a defesa do consumidor; e
7.2.1.7 os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

7.2.2 São princípios da proteção de dados pessoais:

7.2.2.1 **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
7.2.2.2 **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
7.2.2.3 **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
7.2.2.4 **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
7.2.2.5 **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
7.2.2.6 **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
7.2.2.7 **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
7.2.2.8 **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
7.2.2.9 **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
7.2.2.10 **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

8 Diretrizes

8.1 Diretrizes Gerais

A Etice deverá cumprir as seguintes diretrizes relativas à segurança da informação, de forma geral:

8.1.1 **Planejamento Estratégico**: Incluir no planejamento estratégico da Etice diretrizes e metas relacionadas à Segurança da Informação e Proteção de Dados Pessoais, para fortalecer o alinhamento entre a TIC e os planejamentos da instituição e do Governo do Estado, com o objetivo de promover e motivar a criação de uma cultura de Segurança da Informação e Proteção de Dados Pessoais, conforme disposto na PoSIC do Ceará.

8.1.2 **Padrões a serem adotados**: Fundamentar a elaboração de normas e procedimentos da segurança da informação e proteção de dados pessoais de acordo com as normas técnicas ABNT NBR ISO/IEC 27001 e 27002.

8.1.3 **Gerenciamento de Riscos**: ativar a gestão de riscos para os ativos de TIC (processos, produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados) na Etice.

8.1.4 **Seleção de mecanismos de segurança:** selecionar os mecanismos de segurança considerando-se os fatores de riscos, tecnologias e custos.

8.1.5 **Comunicação, conscientização e capacitação:**

8.1.5.1 implementar um sistema de conscientização sobre Segurança da Informação e Proteção de Dados Pessoais de forma que todos sejam informados sobre as obrigações legais e potenciais riscos a que estão expostos os ativos de TIC, proporcionando assim, maior cooperação para o cumprimento das orientações;

8.1.5.2 informar e capacitar regularmente todos os colaboradores sobre as normas e procedimentos da segurança da informação, de acordo com suas funções, inclusive publicando-os na intranet corporativa, garantindo assim maior efetividade e eficácia das ações.

8.1.6 **Linhas de defesa**: implementar o modelo de três linhas de defesa como base para as ações de segurança da informação e proteção de dados pessoais;

8.1.6.1 primeira linha: todos os colaboradores e fornecedores;

8.1.6.2 segunda linha: governança

8.1.6.3 terceira linha: auditoria.

8.1.7 **Monitoramento e Auditoria:** seguir a legislação ao efetuar o monitoramento e auditoria relativa à segurança da informação e tratamento de dados pessoais.

8.1.8 **Conformidade com a política estadual:** Efetuar a verificação de conformidade com a PoSIC do Ceará, sempre que necessário, sendo documentada em relatório de avaliação de conformidade, o qual será encaminhado ao CSIP (Comitê de Segurança da Informação e Proteção de Dados Pessoais).

8.1.9 **Limite e compartilhamento de responsabilidades:** definir e acordar junto a clientes e fornecedores os limites e compartilhamentos de responsabilidades nas ações de segurança da informação e proteção de dados pessoais, considerando inclusive a interdependência das operações efetuadas por estas, como, por exemplo, entre o transporte de dados, serviços de

disponibilização de infraestrutura de processamento e armazenamento de dados, e a implementação e operacionalização de sistemas aplicativos.

8.1.10 **Segurança e privacidade "by design"**: adotar ações de segurança da informação e proteção de dados pessoais em todas as etapas dos projetos e processos, desde sua concepção inicial, permeando o ciclo de vida dos serviços da organização, com o objetivo de agregar e garantir integridade e privacidade aos seus projetos, processos e produtos finais.

8.1.11 **Produtos e serviços**: Cada produto ou serviço deve ser disponibilizado aos clientes com um mínimo de controle de segurança, analisado e projetado caso a caso, considerando-se os requisitos de segurança e proteção de dados pessoais do cliente e a conveniência da própria Etice, em relação aos riscos legais ou de imagem e enquanto agente de modernização do governo do estado, sem descartar a possibilidade de customização específica a determinado cliente ou projeto.

8.1.12 **"Cybersecurity Framework" (NIST)**: utilizar como referência o paradigma NIST para segurança da informação e privacidade de dados, o qual estabelece relação entre riscos de cibersegurança e de proteção de dados.

8.1.13 **Normas e procedimentos**: definir controles para efetuar o tratamento de riscos gerais e comuns à segurança da informação e proteção de dados pessoais, através da revisão e definição de normas e procedimentos, não desconsiderando, no âmbito do SGSIP, o uso de controles adicionais p/o tratamento de riscos específicos a determinados ativos de TIC.

8.2 Diretrizes Específicas à Proteção de Dados Pessoais

A Etice deverá cumprir as seguintes diretrizes específicas à proteção de dados pessoais:

8.2.1 **Hipóteses de tratamento:** seguir as hipóteses de tratamento de dados pessoais e dados pessoais sensíveis previstas na LGPD, em especial nos artigos 7º e 11.

8.2.2 **Finalidade e hipóteses legais:** identificar, especificar e documentar as finalidades, hipóteses de tratamento e bases legais que fundamentam as atividades de tratamento de dados pessoais e dados pessoais sensíveis.

8.2.3 **Minimização**: limitar a quantidade de dados pessoais tratados ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

8.2.4 **Anonimização dos dados:** anonimizar, sempre que possível, os dados pessoais utilizados para fins de estudos por órgão de pesquisa.

8.2.5 **Direitos dos titulares:** atender, a pedido do titular, em relação aos seus dados tratados pela Etice, a qualquer momento e mediante requisição:

8.2.5.1 A confirmação da existência de tratamento.
8.2.5.2 O acesso aos dados.
8.2.5.3 A correção de dados incompletos, inexatos ou desatualizados.
8.2.5.4 A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.

8.2.6 **Compartilhamento, transferência e divulgação:** seguir estritamente a legislação ao efetuar o compartilhamento, a transferência ou a divulgação de dados pessoais.

8.2.7 **Operação e suboperação**: Efetuar as seguintes ações, enquanto operador:

8.2.7.1 seguir as instruções de tratamento de dados determinadas pelo controlador;

8.2.7.2 solicitar ao controlador as instruções de tratamento de dados, com as respectivas hipóteses legais de tratamento;

8.2.7.3 obter autorização do controlador, através de contratos, convênios ou assemelhados, para obter auxílio nas operações de tratamento de dados a eventuais suboperadores, explicitando a cadeia de responsáveis pelo tratamento dos dados;

8.2.7.4 garantir que toda a cadeia de suboperadores tratem os dados seguindo as instruções fornecidas pelo controlador.

8.2.8 **Transparência**: dar publicidade, enquanto controladora, sobre a finalidade e a forma como os dados pessoais serão tratados, através da elaboração e divulgação de termo de uso e privacidade.

8.2.9 **Transferência Internacional:** praticar a transferência internacional de dados, quando necessário, nos termos das leis vigentes.

8.2.10 **Instrução a operadores**: instruir os operadores, por meio de instrumentos adequados, quanto ao tratamento dos dados por ela controlados.

8.2.11 **Comercialização:** não comercializar, na qualidade de operadora, os dados que trata, salvo mediante prévia autorização formal do controlador.

8.2.12 **Divulgação de dados pessoais:** não divulgar os dados pessoais que trata, exceto nos casos previstos em lei.

8.2.13 **Guarda de dados pessoais:** estabelecer e manter uma tabela de temporalidade de dados pessoais, observando o período mínimo necessário para alcançar o objetivo para o qual tais dados foram coletados e a legislação específica, em cada caso.

8.2.14 **Proteção de dados e privacidade:** respeitar a privacidade dos dados pessoais, não devendo se condicionar às exigências ou opções de uso específicos, devendo-se garantir que, em caso de dúvida, a exigência de consentimento expresso do titular dos dados prevaleça sobre outros fatores.

8.2.15 **Consentimento e finalidade:** garantir, enquanto controladora, que a devida permissão do titular, quando necessária, se dará a partir de uma clara explicitação da finalidade quanto ao uso dos dados concedidos. Nos casos de existência ou surgimento de finalidades diversas, deve-se obter novo consentimento, mediante adequada e explícita informação ao titular dos dados quanto a sua(s) nova(s) finalidade(s).

8.2.16 **Identificação de agentes de tratamento:** estabelecer norma para identificar os agentes de tratamento de dados pessoais.

8.2.17 **Avaliação de *"gap analysis"***: criar regras para análise de não conformidade aos princípios legalmente estabelecidos.

8.2.18 **Vínculos contratuais de proteção de dados pessoais**: estabelecer regras para a elaboração dos compromissos legais existentes nos contratos, relativos à proteção de dados pessoais.

8.2.19 **Elaboração do RIPD e ROPA:** criar norma para elaboração do RIPD e ROPA, de acordo com as operações de tratamento de dados pessoais efetuadas por sistemas, produtos, processos ou serviços da Etice, o seu papel exercido nestas operações e os seus limites de responsabilidades legais e contratuais.

9 Disposições Finais

9.1 A alta gestão da empresa deverá dar conhecimento dessa política a todas as partes interessadas, assim compreendidas, mas não limitadas aos seus colaboradores, clientes e fornecedores, inclusive com o compromisso contratual explícito em conformidade com a LGPD.

9.2 Quaisquer contratações de serviços pela Etice deverão considerar as premissas e critérios da segurança da informação e proteção aos dados pessoais, nos termos desta política.

9.3 A presente política contempla os modelos atuais de governança e de gestão da segurança da informação e proteção de dados pessoais, devendo o CSIP ser criado de forma a orientar e auxiliar todos da empresa no que se refere ao cumprimento das orientações dessa política.

10 Casos Omissos

10.1 Os casos omissos, não previstos nessa política e seus documentos complementares, deverão ser submetidos ao CSIP, que avaliará a necessidade de encaminhamento à gestão superior para deliberação.

11 Sanções

11.1 Em caso de violação ou descumprimento dessa política, poderá ser instaurada sindicância para averiguação dos fatos, quando houver indícios de ocorrência de infração, sem prejuízo de responsabilização penal, administrativa e civil do suposto infrator, respeitando os primados da ampla defesa e do contraditório.

11.2 No caso de empregado, comissionado, estagiário e jovem aprendiz, poderá acarretar a aplicação de advertência, suspensão ou desligamento formal, de acordo com a legislação aplicada.

11.3 No caso de usuários contratados pela Etice ou que sejam vinculados a determinado fornecedor, a violação ou não cumprimento dessa política poderá resultar em suspensão, rescisão contratual e aplicação de multa a contratada, sem prejuízo de responsabilização pessoal do infrator pelos atos praticados ou para os quais tenha participado ou facilitado.

11.4 Para fins de aplicação das sanções e das punições, será considerada a gravidade da infração, o efeito alcançado e a sua recorrência.

11.5 Em caso de violações que impliquem atividades ilegais que possam provocar danos à instituição, o infrator será responsabilizado pelos prejuízos na esfera cível, penal e administrativa.

12 Revisão

12.1 A presente política passa a vigorar a partir da data de sua publicação, devendo ser revisada em um período mínimo de 2 (dois) anos, podendo ser editada ou atualizada sempre que houver necessidade.

13 **Aprovação**

Aprovada na 57ª Reunião do Conselho de Administração em 06/06/2024.

LUIS EDUARDO FONTENELLE BARROS:03175626300

Assinado de forma digital por LUIS EDUARDO FONTENELLE BARROS:03175626300

Luís Eduardo Fontenelle Barros
CONSELHEIRO PRESIDENTE

José Juarez Diógenes Tavares
CONSELHEIRO

ALFREDO JOSE PESSOA DE OLIVEIRA:29385520334

Assinado de forma digital por ALFREDO JOSE PESSOA DE OLIVEIRA:29385520334
Dados: 2024.06.13 14:51:52 -03'00'

Alfredo José Pessoa de Oliveira
CONSELHEIRO

gov.br

Documento assinado digitalmente
DEBORAH VANESSA RIBEIRO BARBOSA CAMARA
Data: 12/06/2024 15:15:28 -0300
Verifique em https://validar.iti.gov.br

Déborah Vanessa Ribeiro Barbosa Câmara
CONSELHEIRA