ÍNDICE

1. INTRODUÇÃO

1.1 A Política de Gestão de Incidentes de segurança da informação complementa o documento **CDD-TI-001 Política de Segurança da Informação** e estabelece as diretrizes para registro, investigação e tomada de ação relacionada a incidentes e eventos de segurança de segurança da informação.

1.2 A Política de Gestão de Incidentes de Segurança da Informação é uma declaração formal que demonstra nosso compromisso com a proteção dos Ativos de Informações da **CDD IT SERVICE INNOVATION**. Localizada na cidade de São Paulo, Estado de São Paulo, a **CDD IT** exige que todos os colaboradores e qualquer pessoa ou empresa que tenha acesso a qualquer dado ou Ativo de Informação pertencente à **CDD IT,** cumpram e respeitem as diretrizes estabelecidas neste documento. Não importa quando, onde ou em que circunstâncias, qualquer pessoa que lide com nossas informações estará sujeita às determinações aqui presentes.

2. CONCEITOS

2.1 Para o perfeito entendimento e interpretação da presente Política**,** são adotadas as seguintes definições:

a) **Ameaça**: Causa potencial de um incidente que pode vir a prejudicar a **CDD IT SERVICE INNOVATION**;

b) **Área de TI:** setor da **CDD IT** responsável por aplicar e fiscalizar as medidas de Segurança da Informação;

c) **Ativo**: É qualquer bem (material ou imaterial) que tenha valor para a **CDD IT SERVICE INNOVATION** e precisa ser adequadamente protegido;

d) **Ativos de Informação**: conjunto de informações valiosas para a empresa, armazenadas de forma identificável e reconhecível. Esses ativos representam o patrimônio intangível da **CDD IT** e englobam informações estratégicas, técnicas, administrativas, mercadológicas, financeiras, de recursos humanos e legais;

e) **Comitê Gestor de Segurança da Informação:** grupo multidisciplinar composto por membros das diretorias executivas, com o objetivo de avaliar a estratégia e diretrizes da Segurança da Informação seguidas pela **CDD IT**;

f) **Confidencialidade**: garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário;

g) **Controle**: medida de segurança adotada pela **CDD IT**, para tratamento de um risco específico;

h) **Dados Pessoais**: informações coletadas pela **CDD IT** durante o desenvolvimento de suas atividades que possibilitam a identificação, direta ou indireta, de pessoa natural;

i) **Dados Sensíveis:** 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;

j) **Dados**: informações coletadas pela **CDD IT** durante o desenvolvimento de suas atividades;

k) **Deskwork:** Sistema ITSM gestão de serviços utilizada pela **CDD IT SERVICE INNOVATION**;

l) **Disponibilidade:** garante que a Informação esteja disponível para as pessoas ou organismos autorizados, sempre que se fizer necessária;

m) **Encarregado (Data Protection Officer - DPO**): Pessoa indicada pela **CDD IT SERVICE INNOVATION** para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

n) **Equipe de Resposta ao Incidente (CSIRT - Computer Security Incident Response Team**): Profissionais técnicos identificados pela **CDD IT SERVICE INNOVATION** para, quando acionados, receberem, analisarem e responderem aos eventos detalhados nesta Política;

o) **Evento ou Incidente de Segurança:** é qualquer ocorrência visível em uma rede ou sistema de informação;

p) **Incidente de Segurança da Informação**: é um evento adverso, de forma acidental ou dolosa, identificado que indica possível violação à Política de segurança da informação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação, capaz de dar ensejo à destruição, perda, alteração, divulgação ou ao uso ou acesso não autorizados de dados tratados pela **CDD IT SERVICE INNOVATION**;

q) **Informação**: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato;

r) **Informações da CDD IT:** Ativos de Informação que se relacionem diretamente à **CDD IT**, suas atividades, e qualquer tipo de Dado ou informação gerada ou alterada por membros da **CDD IT**, no exercício de suas funções.

s) **Integridade**: garante que a Informação esteja íntegra, exata e completa durante todo o seu ciclo de vida;

t) **LGPD:** Lei Geral de Proteção de Dados, definida através das disposições da Lei nº 13.709/18, alterada pela Lei nº 13.853/19;

u) **Normas:** Normas de Segurança da Informação;

v) **Resposta a incidentes**: Medidas tomadas para a preparação, detecção, resposta, contenção e recuperação de um incidente de segurança, além de todas as atividades pós- incidente e de conscientização;

w) **Risco de Segurança da Informação:** efeito da incerteza sobre os objetivos de Segurança da Informação da **CDD IT**;

x) **Risco**: combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos;

y) **Segurança da Informação:** técnicas aplicadas na utilização de recursos tecnológicos para garantir sua utilização de maneira segura;

z) **Sistemas de Informação:** sistemas computacionais utilizados pela **CDD IT** para suportar suas operações. Pode haver exceções que, mesmo não sendo sistemas informáticos, suportem operações da **CDD IT**;

aa) **Tratamento de Dados**: toda a operação realizada com Dados, 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;

bb) **Usuários**: Qualquer indivíduo com direitos de acesso remoto aprovado pela Empresa e que tenha passado por todas as etapas necessárias de provisionamento. Os usuários geralmente incluem, mas não estão limitados a usuários, consultores, fornecedores e contratados.

3. ABRANGÊNCIA

3.1 Esta Política se aplica a todos os colaboradores, prestadores de serviço, assim como, às entidades e aos órgãos que possuam acesso as informações da **CDD IT SERVICE**

INNOVATION, parceiros de Negócios, qualquer pessoa com poderes de representação da **CDD IT** direta ou indiretamente respeitando os acordos operacionais estabelecidos, que possuíram, possuem ou virão a possuir acesso físico ou lógico da empresa e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da **CDD IT.**

4. OBJETIVO

4.1 Este documento visa estabelecer diretrizes para o gerenciamento de resposta a incidentes de segurança documentada e formalizada, a fim de que os procedimentos de suporte colaborem para garantir a segurança dos recursos de sistema da **CDD IT SERVICE INNOVATION**.

5. RESPONSABILIDADES

5.1 As responsabilidades do Gestor de TI e do DPO (Data Protection Officer) são:

a) Condução do processo de Gestão de Incidentes de Segurança da Informação;
b) Investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;
c) Acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;
d) Comunicação aos Gestores responsáveis;
e) Realização de análises pós-incidentes (post mortem) para identificação e tratamento de causas raiz e aprimoramento de processos da empresa e do próprio processo de gestão de incidentes de segurança da informação.

5.2 As responsabilidades dos usuários são:

a) Devem informar imediatamente à área de Gestão de TI e ao DPO todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

5.3 As responsabilidades da área de TI são:

a) Provimento dos acessos necessários para que a área de Gestão de TI e DPO que possa realizar a identificação e investigação de incidentes de segurança;
b) Responsável pelo provimento de trilhas de auditoria e evidencias para a investigação de incidentes;
c) Suporte às investigações através do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

5.4 As responsabilidades dos Gestores são:

a) Ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e SLAs predefinidos pela área de Gestão de TI e DPO.

5.5 As responsabilidades da área Jurídica são:

a) Suporte às questões legais relacionados a incidentes de segurança da informação.

6. DIRETRIZES

6.1 DISPOSIÇÕES GERAIS

6.1.1 São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco.

6.1.2 Todos os colaboradores devem estar em capacidade de identificar incidentes de segurança da informação quando for testemunhado.

6.1.3 Todos os colaboradores devem notificar qualquer evento de segurança ou fragilidade observada que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da empresa.

6.1.4 Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

6.1.5 A seguir exemplos, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

a) Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;
b) Indisponibilidade do ambiente tecnológico em virtude de ataque maliciosos interno e externo;
c) Vazamento de informações confidenciais (informações de clientes, informações estratégicas, outros);
d) Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI;
e) Ato de violar uma política de segurança, explícita ou implícita;
f) Uso ou acesso não autorizado a um sistema;
g) Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;

h) Compartilhamento de senhas.

6.1.6 O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida.

6.1.7 Os eventos de incidente de segurança da informação devem ser categorizados e classificados através de uma matriz de severidade com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão.

6.1.8 Os eventos abaixo não são considerados eventos de segurança da informação:
a) Eventos acidentais (falhas de hardware ou sistêmicas) não intencionais;
b) Eventos não maliciosos (erro humano ou descuido que não infrinja as regras de segurança da informação).

6.1.9 Todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento.

6.1.10 Devem ser implementados sistemas de proteção e mecanismos de controle para proteção dos recursos de sistema em toda a empresa, reforçando os sistemas críticos quanto à segurança da informação.

6.1.11 Os usuários autorizados devem adotar as devidas diligências para detectar um incidente ou anormalidades no sistema.

6.1.12 O plano de ação e resposta a incidentes, estabelecido pelo **CDD IT SERVICE INNOVATION**, deve ser seguido para minimizar o impacto do incidente na infraestrutura crítica de rede e sistema da **CDD IT SERVICE INNOVATION**, devendo ser testado anualmente.

6.1.13 Uma vez que o sistema afetado é restabelecido, deve ser realizada uma análise técnica para examinar detalhadamente a integridade dos dados.

6.1.14 Apenas incidentes que afetem serviços considerados relevantes, de acordo com a cadeia de valor estabelecida em estudo interno, são abrangidos pela Resolução CMN 4658/18.

6.1.15 O incidente classificado como de “risco alto” deve ser comunicado de acordo com procedimentos internos, podendo envolver instituições do setor e reguladores externos de acordo com a categorização do incidente.

Comentado [DG1]: Informar SUSEP/BACEN/ANS e Santander

6.1.16 Após a resolução do incidente, um Relatório de Resposta a Incidentes (IRR) deverá ser elaborado e disponibilizado para gerenciamento.

6.1.17 Devem ser estabelecidos processos, testes, métricas, indicadores, identificação, avaliação e correção de eventuais deficiências, com base no Procedimento de Contratação de

Fornecedores, para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

6.1.18 A Gestão de Incidentes de Segurança da Informação deve contemplar processos que atendam aos seguintes objetivos:

6.2 PREVENÇÃO

6.2.1 Os incidentes de segurança devem ser prevenidos pela **CDD IT SERVICE INNOVATION** por meio da fiscalização da conformidade frente à legislação aplicada, dos princípios éticos, bem como das regras e restrições estabelecidas pelas diretrizes internas.

6.2.2 É de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP) para que não haja disparidades na correlação de eventos, logs e outros dados.

6.2.3 A **CDD IT SERVICE INNOVATION** deve realizar o monitoramento das vulnerabilidades existentes por meio de ferramentas de supervisão de atividades, registro, monitoramento e análise de trilhas de auditoria e controle de acesso em ambientes físicos e lógicos.

6.3 GESTÃO DE INCIDENTES

6.3.1 O plano de resposta a incidentes deve ser visto como um conjunto de procedimentos para avaliação de um incidente de segurança, que inclui identificação, triagem, mitigação, resposta e atividades pós-incidente necessárias, incluindo treinamentos e testes.

6.3.2 A gestão dos incidentes de segurança da informação deve ser realizada com base nas seguintes etapas:

6.3.3 Identificação

6.3.3.1 Consiste em detectar ou identificar de fato a existência de um incidente de segurança. A equipe de resposta ao incidente baseia-se na identificação de incidentes internos ou externos, seja na detecção de alertas provenientes dos sistemas de monitoramento da rede da **CDD IT SERVICE INNOVATION** ou por notificações realizadas por qualquer pessoa relatando ser de seu conhecimento ou mesmo vítima de atividade suspeita ou em desacordo com a Política de Segurança da Informação.

6.3.3.2 Detectar um Incidente de forma rápida e eficiente é essencial para uma resolução bem-sucedida. São várias as formas de detecção, de modo que é impossível desenvolver uma metodologia que contemple cada uma. Desta forma, todos devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um Incidente, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, phishing, malware, instabilidades sistêmicas etc.

6.3.3.3 Uma vez detectado um Incidente ou detectada a mera suspeita de um Incidente, deverá comunicar imediatamente a Equipe de Resposta a Incidentes

6.3.3.4 As notificações internas ou externas poderão ser geradas pelos seguintes meios:
a) Interno: Ferramenta Deskwork (Help Desk da **CDD IT);**
b) Externo: E-mail - suporte@**CDD IT**.com.br

6.3.3.5 A comunicação sobre a suspeita de um incidente é vital para a empresa, assim, caso haja suspeita de um incidente e não haja comunicação sanções disciplinares poderão ser aplicadas, a depender da gravidade e da comprovação de eventual negligência.

6.3.3.6 Toda notificação ou denúncia deve ser formalmente registrada pela Área de Segurança da Informação. Este registro deve estar associado a alguma referência numérica (ID único) para que possa ser gerenciado pela Equipe de Resposta ao Incidente.

6.3.4 Triagem

6.3.4.1 Etapa onde a Equipe de Resposta a Incidentes deve realizar a análise inicial do evento, notificação ou denúncia visando a sua confirmação como incidente e classificando a sua relevância sobre as atividades da **CDD IT SERVICE INNOVATION**. Nesta etapa devem ser identificados os sintomas do evento, suas características e os potenciais danos causados.

6.3.4.2 Após a confirmação de detecção de um incidente, ele deverá ser minuciosamente analisado antes da tomada de qualquer ação, principalmente para poder confirmar a validade do incidente.

6.3.4.3 A análise realizada pela Equipe de Resposta a Incidentes consiste na coleta, aquisição e análise de dados, informações e demais evidências sobre o incidente para investigar o ativo de rede ou sistema de informação que gerou o incidente detectado ou denunciado.

6.3.4.4 Essa investigação passa pela identificação de ativos compreendendo endereços IP, endereços MAC da interface de rede, nomes, switches e portas de acesso, bem como prédio, departamento, salas e usuários. Essas informações devem ser levantadas pelas trilhas de auditoria dos diversos sistemas e serviços disponíveis pela **CDD IT SERVICE INNOVATION**.

6.3.4.5 Confirmado o incidente, Equipe de Resposta a Incidentes deve categorizar e priorizar com base:
a) O impacto potencial conforme avaliação de risco em segurança da informação;
b) No tempo e recursos necessários para recuperar ativos impactados;

6.3.4.6 Todo incidente categorizado como sendo de severidade crítica deve ser notificado imediatamente à Área de Tecnologia da Informação, que pode realizar a escalação deste incidente e realizar a alocação dos profissionais necessários para resolução do incidente.

6.3.4.7 Caso o incidente detectado envolva ou tenha a suspeita de envolver o tratamento não autorizado de dados pessoais, a Equipe de Resposta ao Incidente deve notificar imediatamente o Encarregado de privacidade pelo Tratamento de Dados Pessoais para avaliar se o incidente informado se trata de uma violação de dados pessoais, conforme procedimento específico.

6.3.4.8 Confirmado que o incidente é uma violação de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais deve ser adicionado à equipe responsável por monitorar e responder ao incidente para orientar e acompanhar as medidas a serem tomadas.

6.3.5 Mitigação

6.3.5.1 Etapa que busca a solução do incidente por meio de um ciclo básico composto pelas seguintes fases:

a) Análise dos dados;
b) Pesquisa de solução;
c) Ação proposta e realizada (contenção);
d) Comunicação;
e) Solução efetiva ou de contorno e recuperação do ambiente.

6.3.5.2 Devem ser realizados procedimentos iniciais para contenção do incidente visando evitar a sua propagação e posteriormente em restabelecer o ativo, mesmo que com uma solução temporária, até que a solução definitiva seja implementada.

6.3.5.3 A Equipe de Resposta ao Incidente deve assegurar que as comunicações com Partes Internas e Externas Interessadas (parceiros, prestadores e terceiros) ocorram no momento oportuno e estejam coordenadas de acordo com as diretrizes de gestão de crises da **CDD IT SERVICE INNOVATION**. As Partes Interessadas Internas devem ser informadas sobre as ações que precisarão ser realizadas durante o estágio de recuperação.

6.3.5.4 A Equipe de Resposta ao Incidente deve buscar a solução definitiva, ou seja, identificar a causa raiz de um incidente e eliminá-lo para assegurar que o ativo esteja seguro e confiável para que os procedimentos de recuperação sejam iniciados. A Equipe de Resposta ao Incidente pode solicitar o envolvimento e suporte das demais Áreas da **CDD IT SERVICE INNOVATION** afetadas para assegurar que os vetores do incidente sejam solucionados.

6.3.5.5 A Equipe de Resposta ao Incidente deve acompanhar os processos de recuperação dos ativos até o pleno funcionamento.

6.3.5.6 Os sistemas relevantes a **CDD IT SERVICE INNOVATION** devem retomar a funcionalidade básica de modo prioritário. As interdependências sistêmicas também devem ser conhecidas, já que alguns sistemas só podem ser recuperados após outros.

6.3.5.7 Durante a recuperação, os sistemas devem ser reconstruídos, reinstalados ou restaurados pela Área de Tecnologia da Informação usando dados de backup e sistemas e patches atualizados, se necessário com apoio da Equipe de Resposta ao Incidente. Os sistemas recuperados devem ser testados e monitorados para assegurar que não ocorra novamente o incidente e que os ativos estejam funcionando de modo adequado.

6.3.6 Resposta ao incidente

6.3.6.1 A Equipe de Resposta ao Incidente deve documentar e arquivar as conclusões do tratamento do incidente, descrevendo:

a) Detalhadamente o ocorrido;
b) Como o incidente foi detectado, ou seja, foi relatado por pessoa natural ou por meio de alerta de sistema automatizado;
c) As etapas tomadas pela Equipe de Resposta ao Incidente a partir da detecção do evento até o estágio de recuperação dos ativos;
d) O status do incidente à medida que ele se move ao longo do processo de solução;
e) Qualquer dado que seja coletado durante o processo de solução que possa ser usado como evidência;
f) Definir a categorização final do incidente;
g) Comentários e sugestões da Equipe de Resposta ao Incidente.

6.3.6.2 Esta documentação deve servir como referência para pós-incidente.

6.3.6.3 A coleta e preservação de provas, sejam digitais ou não, na etapa de solução do incidente, bem como dados e informações que possibilitaram a identificação do incidente são importantes e devem ser documentadas no registro final do incidente. A coleta de provas deve ser avaliada, conforme a necessidade pela Equipe de Resposta ao Incidente, devendo acionar o Departamento Jurídico, em caso de dúvidas quanto à sua necessidade.

6.3.6.4 Quando a severidade de um incidente for categorizada como crítica, deverá ser realizada a coleta e preservação das provas envolvidas.

6.3.7 Pós incidente

6.3.7.1 A etapa de pós incidente tem o seu início após a resolução e encerramento do incidente, onde serão analisadas pela Equipe de Resposta ao Incidente as causas que motivaram a sua ocorrência e quais são as medidas que podem ser tomadas com objetivo de evitar que o fato ocorra novamente.

6.3.7.2 O objetivo desta etapa é melhorar os procedimentos e aprimorar os ativos para protegê-los de futuros incidentes.

6.3.7.3 A Equipe de Resposta ao Incidente deve comunicar ao Comitê de SI da **CDD IT SERVICE INNOVATION** quanto ao resultado da análise realizada. A necessidade dessa comunicação deve ocorrer sempre que a classificação quanto ao grau de severidade.

6.3.7.4 Com base no relatório e nas informações obtidas durante a resolução do incidente, a Equipe de Resposta ao Incidente deverá elaborar um plano de ação que inclua os responsáveis, as datas de vencimento e as entregas para garantir que todas as partes interessadas saibam o que se espera delas.

6.4 ELABORAÇÃO DO PLANO DE AÇÃO PARA RESOLUÇÃO

6.4.1 De acordo com a severidade do incidente de segurança da informação, este terá os seguintes status estipulados para o seu início de atendimento e elaboração do plano de ação para resolução:

7. NÃO CONFORMIDADE E CASOS OMISSOS

7.1 A não conformidade está definida na presente Política como a violação, omissão, tentativa não consumada, ou ausência de cumprimento com quaisquer das definições, diretrizes, normas, procedimentos ou conceitos definidos nesta Política, voluntária ou involuntariamente, por parte de um Colaborador, estagiário, visitante, fornecedor ou prestador de serviços.

7.2 As regras que estabelecem o Controle e o tratamento de situações de não conformidade relativas à Política da **CDD IT** devem ser tratadas conforme as leis vigentes no país, que regulamentem as punições correspondentes ao evento. Na ocorrência de violação desta Política ou das Normas, a Diretoria Executiva poderá adotar, com apoio das Gerências Jurídicas e de Recursos Humanos, sanções administrativas e/ou legais, conforme os parágrafos a seguir.

7.3 As sanções serão aplicadas conforme análise do Comitê Gestor da Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência, e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho.

7.4 O presente documento, e a totalidade dos responsáveis citados, devem considerar que a tecnologia e as Ameaças à Segurança da Informação se intensificam e se atualizam todos os dias. Portanto, não se constitui rol enumerativo, sendo obrigação do colaborador da **CDD IT** adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir a proteção às informações da **CDD IT**.

7.5 Os eventuais casos que não estejam contemplados neste documento, ou nos documentos auxiliares que o compõem, devem ser analisados, em primeira instância, pelo gestor de Segurança da Informação, e, caso ele não tenha uma solução ou medida plausível para o evento, caberá ao Comitê Gestor de Segurança da Informação, decidir o procedimento para cada caso específico.

8. DOCUMENTO(S) DE REFERÊNCIA

8.1 Esta diretriz é baseada nas seguintes normas, leis e documentos internos:

a) Resolução CMN 4.658/18;
b) Lei 13.709/2018 – LGPD Lei Geral de Proteção de Dados Pessoais;
c) CDD-TI-001 Política de Segurança da Informação.

9. ALTERAÇÕES E REVISÕES

9.1 Esta Política poderá conter eventuais erros de tipografia, ortografia ou gramática. Em tais casos, o responsável pela elaboração e manutenção poderá elaborar novas versões deste documento, com as devidas correções, sem a necessidade de nenhuma comunicação prévia aos interessados. Demais alterações serão aplicadas à novas versões, sendo que novos acordos, reconhecimentos ou compromissos assumidos com respeito a este documento, farão sempre referência à versão mais recente dele.

9.2 Histórico de revisões:

Controle Revisão	Item alterado	Resumo da atividade	Responsável	Departamento	Data aprovação
0.0	-	Elaboração	Aline Santos	Processos & Governança	07/09/2023
0.1		Revisão/Aprovação	Daniel Gonzales	Cood. Infra -Operações	15/09/2023
1.3		Revisão/Aprovação	Rodrigo Candido	Diretoria Operações	22/11/2023
1.4		Revisão/Aprovação	Naiara Delfino	Diretoria Administrativa	22/11/2023
2.0		Publicação	Julio Argento	Recursos Humanos	27/11/2023