SUMÁRIO

1 DECLARAÇÃO

"A Prothera está comprometida em implementar e monitorar seus controles de segurança da informação para garantir a confidencialidade, integridade, disponibilidade e privacidade de todo ativo de informação atendendo as regulamentações e requisitos contratuais de seus clientes, colaboradores e partes externas interessadas, sempre buscando a melhoria contínua de seus processos e serviços."

2 INTRODUÇÃO

A informação e os dados pessoais utilizados pela Prothera são bens que tem valor. Eles devem ser gerenciados adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade e privacidade independentemente do meio de coleta, garantindo a segurança em todo o ciclo de vida da informação, desde a coleta até o descarte seguro das informações.

A Prothera reconhece suas obrigações para proteger a informação (física e eletrônica) de ameaças internas e externas e que o gerenciamento eficaz da segurança da informação é essencial para garantir o funcionamento das tecnologias de informação e comunicação e consequentemente a entrega de seus serviços.

A Prothera possui um extenso e robusto Sistema de Gestão da Segurança e Privacidade da Informação - SGSPI - que consiste em uma vasta gama de políticas, procedimentos, controles e medidas em observância as normas NBR ISO/IEC 27001:2022 e NBR ISO/IEC 27701:2019.

O SGSPI pode ser definido como um sistema de gestão corporativo que inclui toda abordagem organizacional usada para a proteção das informações de forma a garantir a confidencialidade, integridade, disponibilidade e privacidade dos quais estão sob gestão da Prothera visando a melhoria contínua em resposta às ameaças e vulnerabilidades emergentes e mutáveis, sendo vital para a proteção de informações e reputação da Prothera.

Para garantir a implementação adequada do SGSPI, foram utilizados políticas e procedimentos separados para cada área de segurança da informação e, quando aplicável, consta a referência a essas políticas externas neste documento.

Todas as políticas e procedimentos de segurança da informação devem ser lidos e referidos em conjunto entre si, pois seus significados, controles e medidas são complementares. As políticas e documentos que fazem parte do SGSPI da Prothera serão descritos no capítulo 13 desde documento.

3 PROPÓSITO

Este documento é um conjunto de normas que tem como finalidade orientar o gerenciamento das informações, protegendo e garantindo os pilares de confidencialidade, integridade, disponibilidade e privacidade em observância as normas NBR ISO/IEC 27001:2022 e NBR ISO/IEC 27001:2019.

- **Disponibilidade**: Que os ativos e as informações estejam disponíveis e acessíveis aos usuários autorizados quando necessário.
- **Integridade**: Que as informações estejam protegidas de modificações, destruição deliberada ou acidental por usuários autorizados e não autorizados, garantindo a exatidão das informações da organização.
- **Confidencialidade**: Que as informações só possam ser acessadas e visualizadas por pessoas autorizadas evitando sua divulgação deliberada ou acidental.
- **Privacidade**: Que os dados pessoais sejam protegidos contra as consequências de falhas de integridade, interrupções na disponibilidade e violações de confidencialidade durante todo seu ciclo de vida.

4 OBJETIVOS DE SEGURANÇA DA INFORMAÇÃO

Os objetivos estabelecidos para a Prothera relacionados à segurança da informação são:

- **OBJETIVO 01:** Aumentar continuamente a conscientização sobre Segurança da Informação, Proteção de Dados e Privacidade em todas as equipes.
- **OBJETIVO 02:** Garantir que as informações pessoais sejam protegidas, de acordo com a legislação de proteção de dados pessoais.
- **OBJETIVO 03:** Estabelecer e monitorar um Sistema de Gerenciamento de Segurança e Privacidade da Informação eficaz para reduzir o risco para a Prothera, seus clientes e usuários de seus serviços.

- **OBJETIVO 04:** Estabelecer e monitorar a disponibilidade do sistema PROTHERA no ambiente de produção.
- **OBJETIVO 05:** Estabelecer e monitorar a integridade do sistema PROTHERA no ambiente de produção.

5 ESCOPO

Esta política de segurança da informação se aplica a:

- Quaisquer softwares fornecidos ou sob o controle da Prothera;
- Quaisquer comunicações enviadas ou recebidas;
- Quaisquer dados pertencentes, controlados ou processados, incluindo dados mantidos em sistemas externos;
- Locais a partir dos quais os dados são acessados, incluindo uso doméstico e externo;
- Ativos de informação mantidos, processados ou armazenados nas instalações ou locais externos;
- Informações em trânsito pelas redes de voz ou dados.

Todos os colaboradores da Prothera (empregados, prestadores de serviço, representantes ou subcontratados de terceiros, estagiários e aprendizes) devem conhecer esta política. A adesão a esta política é obrigatória e o não cumprimento pode levar a sanções disciplinares.

6 RESPONSABILIDADES

- **Todos os usuários:** É responsabilidade de qualquer indivíduo ou organização que tenha acesso aos sistemas e informações da Prothera cumprir esta política de segurança da informação e as diretrizes, medidas e procedimentos associados a ela.
- **Analista da qualidade:** Tem a responsabilidade global pela manutenção deste documento e seus procedimentos associados.
- **Coordenador de TIC/Infraestrutura:** Tem a responsabilidade pela coordenação das atividades operacionais associadas a segurança da informação. Cabe ao mesmo, recepcionar os relatos de qualquer suspeita ou real falha, ameaças, eventos ou incidentes de segurança da informação.
- **Comitê do SGSPI**: Tem a responsabilidade pela governança das disposições deste documento, bem como a revisão desta política bienalmente, ou quando mudanças que

afetem o SGSPI forem identificadas para garantir que ela esteja em conformidade com todos os requisitos e regras legais, estatutárias e regulamentares. É de inteira responsabilidade do comitê do SGSPI garantir que essas revisões ocorram e que o conjunto de políticas esteja e permaneça internamente consistente.

- **Encarregado de proteção de dados (DPO):** Responde pelas questões associadas a privacidade e proteção de dados pessoais. Inclui: aceitar reclamações e comunicações dos titulares de dados pessoais, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional de proteção de dados pessoais e adotar providências, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

7 POLÍTICAS E DIRETRIZES

7.1 USO ACEITÁVEL DOS ATIVOS

Todos os colaboradores têm a responsabilidade de proteger as informações e os ativos de informação sob sua responsabilidade que devem ser usados de maneira aceitável e de acordo com esta e outras políticas e processos relacionados ao SGSPI.

7.2 MESA LIMPA TELA LIMPA

Os dispositivos de computação desacompanhados ou não sendo utilizados devem ser protegidos com uma tela ou mecanismo de bloqueio controlado por senha ou mecanismo de autenticação semelhante (isso inclui laptops, tablets, smartphones e estações de trabalho).

As estações de trabalho são bloqueadas por tempo de inatividade de até 5 minutos. Ao ausentar-se bloqueie a estação de trabalho e ou laptops usando Ctrl-Alt-Del, opção “Bloquear”, ou a tecla Windows e 'L'. Isso impedirá que qualquer pessoa acesse qualquer informação a qual não esteja autorizada, enquanto o dispositivo estiver desacompanhado.

Ao visualizar informações confidenciais ou que contenham dados pessoais em uma tela, os usuários devem estar cientes de seus arredores e devem garantir que pessoas não autorizadas não consigam visualizar tais informações. As telas dos computadores nas quais informações confidenciais ou pessoais são processadas ou visualizadas devem ser posicionadas de tal forma que não possam ser visualizadas por pessoas não autorizadas.

Informações confidenciais ou de acesso restrito, independentemente da forma de armazenamento, devem ser protegidas durante e após o uso, especialmente quando o local de trabalho é desocupado após o final da jornada de trabalho. A impressão de documentos confidenciais ou de acesso restrito deve ser realizada apenas conforme a necessidade para evitar a divulgação não autorizada.

7.3 USO DA INTERNET

O uso da Internet deve ser realizado de modo consciente, segundo a necessidade para execução das atividades laborais e, eventualmente, pessoais. O uso abusivo, que possa comprometer o bom desempenho laboral, ou conscientemente colocar em risco ativos da informação da empresa, pode resultar em advertências verbais ou formais, de acordo com a gravidade. O acesso à Internet em ativos da empresa é monitorado e controlado por meio de um sistema de filtro de conteúdo (proxy), salvo se houver necessidade explícita de acesso irrestrito para a execução da atividade laboral relacionada à função. O acesso irrestrito deve ser autorizado por gestor ou diretor.

7.4 USO DO E-MAIL

O uso do e-mail corporativo para fins pessoais é impróprio e não é permitido em nenhum momento. Você só deve usar os sistemas de e-mail fornecidos pela Prothera para enviar e receber informações da Prothera.

Você não deve usar o sistema de e-mail de forma insultuosa ou ofensiva. Todos os e-mails são marcados automaticamente com a classificação ‘Confidencial’. Você deve considerar se precisa alterar a classificação para 'Pública', “Uso interno” ou 'Restrita'.

Se você receber um e-mail impróprio ou abusivo, deve relatá-lo imediatamente ao seu superior, que tomará as medidas cabíveis. Se o remetente for conhecido por você, informe-o de que ele deve interromper o envio do material. E-mails que parecem suspeitos, podem ser tentativas de "phishing" ou malware, devem ser relatados imediatamente como um incidente de segurança.

7.5 INTELIGÊNCIA DE AMEAÇAS PROATIVA

Entendendo que as ameaças podem acontecer a qualquer momento, bem como novas podem surgir, a Prothera terceiriza um serviço de análise contínua de vulnerabilidades, com a finalidade de examinar periodicamente seu ambiente e reportar, através da Gestão da Continuidade de Vulnerabilidades ameaças que possam comprometer a segurança da informação dos ativos da organização. Mensalmente, relatórios da empresa contratada são apresentados em reuniões, a fim de mostrar os resultados e criar ações para mitigar as vulnerabilidades que possam representar um risco para o ambiente.

7.6 USO DE MÍDIAS REMOVÍVEIS

Entende-se por mídia removível qualquer tipo de memória que pode ser removida conferindo portabilidade para os dados que foram nela armazenadas. Alguns exemplos de mídias removíveis são: CD, DVD, memória USB, entre outros.

A Prothera possui diretrizes para o uso de mídias removíveis que estão documentadas na política de uso de mídias removíveis.

7.7 DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Qualquer pessoa que armazena ou transporta dados e informações relacionadas com a Prothera, usando dispositivos móveis é considerada pela empresa como responsável pela segurança dos dados e deve tomar as medidas adequadas e apropriadas para protegê-los. Dados restritos ou confidenciais não devem ser copiados, replicados ou baixados para celular ou dispositivos remotos sem a permissão do proprietário das informações. Onde a permissão for concedida, medidas adequadas devem ser tomadas pelo usuário para proteger os dados enquanto eles existem no dispositivo móvel ou remoto.

Perda ou furto de equipamento (corporativo ou não) que foi usado para acessar os ativos de informação da Prothera ou que possam ter uma cópia ou parte de informação devem ser comunicados ao Coordenador de TIC/Infra. Se houver perda ou divulgação não autorizada de dados confidenciais, sensíveis ou pessoais da Prothera devido a práticas inadequadas ou negligência de sua parte, uma ação disciplinar pode ser tomada contra o infrator.

Os colaboradores da Prothera que exercem trabalho remoto devem seguir as medidas de segurança e proteção de dados para garantir uma comunicação com segurança e que seus

dispositivos estejam protegidos contra ameaças. Algumas medidas devem ser adotadas pelos colaboradores em trabalho remoto e estão documentadas na Política de dispositivos móveis e trabalho remoto.

7.8 RESTRIÇÕES SOBRE O USO E INSTALAÇÕES DE SOFTWARE

Os softwares são gerenciados e controlados de acordo com as políticas da empresa em relação ao gerenciamento de ativos e contratos de licença. Todos os softwares usados em dispositivos gerenciados pela empresa devem ser instalados de acordo com as diretrizes internas de licenciamento de software atuais.

A instalação, atualização e desinstalação de software somente é executada pelos profissionais do departamento de tecnologia e informação.

Violar os direitos de qualquer pessoa ou empresa protegida por direitos autorais, segredo comercial, patente ou outra propriedade intelectual, ou leis ou regulamentos semelhantes, incluindo, mas não se limitando a, instalação ou distribuição de produtos "pirateados" ou outros produtos de software que não sejam apropriadamente licenciados podem deixar o colaborador sujeito a ação disciplinar.

7.9 SENHAS

Senhas e outras formas de autenticação secreta, tais como chaves criptográficas e padrões de desenho, utilizadas para acessos a dispositivos, redes e sistemas, devem ser de uso exclusivo do usuário, portanto não devem ser compartilhadas. Da mesma forma, o usuário não deve utilizar a senha de outra pessoa. As senhas devem ser trocadas no primeiro login após a emissão de uma senha temporária segura.

As senhas e outras formas de autenticação secreta devem ter complexidade suficiente para serem difíceis de serem adivinhadas. Para atender a este requisito, a senha deve ser composta de no mínimo 8 caracteres, e sempre que possível, de números, caracteres especiais, letras maiúsculas e minúsculas; e devem ser alteradas num prazo máximo de 120 dias. Senhas padrões devem ser evitadas, bem como informações pessoais, como nomes e datas. Sempre que aplicável criar mecanismos de dupla autenticação com ferramentas de e-mail ou telefone corporativo. Nos sistemas onde for possível, o responsável pelo sistema deve configurá-lo para que a complexidade de senha seja obrigatória.

O colaborador é responsável por todas as transações atribuídas ao seu identificador de usuário, confirmado por senha ou outra forma de autenticação secreta.

Não anotar senhas em blocos de anotação, post-it ou similares, ressalvo locais com segurança, como softwares que atuam como cofre de senha, exemplo KeePass. O uso de cofre de senhas é recomendado para armazenar as senhas de forma segura. Senhas não devem ser enviadas através de dispositivos de mensagens, tais como celulares ou e-mails, exceto em casos em que o reset da senha seja necessário para atendimento aos usuários devidamente validados e que não caracterize tentativas de phishing. Não se deve responder e-mails ou telefonemas solicitando senhas, mesmo que pareçam ser de uma fonte confiável. Essas solicitações costumam ser tentativas de roubar as credenciais dos usuários.

Ao suspeitar de que uma senha ou outra forma de autenticação secreta possa ter sido comprometida, o colaborador deve alterá-la imediatamente em todos os dispositivos, redes e sistemas em que ela esteja sendo utilizada e comunicar, também imediatamente, à área responsável pela gestão de incidentes de segurança e privacidade da informação.

7.10 SEGURANÇA DA INFORMAÇÃO NO GERENCIAMENTO DE PROJETOS

A segurança da informação deve estar presente em todo o ciclo de vida do desenvolvimento de software, inclusive na aquisição ou contratação de sistemas e/ou plataformas que operem informações de responsabilidade da Prothera. Uma análise junto ao coordenador de infra TIC deve ser realizada, observando pontos obrigatórios voltados à segurança e privacidade da informação. Caso algum sistema e/ou plataforma seja reprovado e sua utilização seja necessária, uma autorização formal da direção deverá ser emitida, podendo ser registrada pela abertura de um chamado via ferramenta de workflow.

7.11 CONTRATOS DE TRABALHO

Os requisitos de segurança devem ser tratados na fase de recrutamento e todos os contratos de trabalho devem conter uma cláusula de confidencialidade e uma cláusula de privacidade. Os requisitos de segurança, proteção de dados e privacidade estão incluídos nas definições de trabalho.

7.12 PROTEÇÃO CONTRA MALWARE

Todas as estações de trabalho da empresa possuem software antivírus instalado e configurado para atualizar as assinaturas antivírus automaticamente. As estações de trabalho são verificadas periodicamente em busca de malware, programas maliciosos ou indesejados.

Todos os sistemas serão protegidos por várias camadas de segurança envolvendo firewall, segmentação de rede, AntiSpam e proteção contra malware em todas as estações de trabalho na rede da empresa.

O uso de máquina pessoal na execução de atividades laborais, é permitido apenas quando o colaborador alocado remotamente, optar por esta modalidade, no entanto deve-se utilizar licença paga de antivírus, caso o colaborador não tenha, a empresa poderá fornecer.

O tráfego de entrada e saída da rede é monitorado para identificar qualquer atividade anômala que possa ser uma ameaça à segurança da rede.

7.13 CONTROLE DE ACESSOS

A equipe de Infraestrutura e TIC deve manter um procedimento formal para concessão e revogação do acesso a todos os sistemas e serviços de informação. O acesso às informações é restrito a usuários autorizados que tenham uma necessidade de acessar as informações. Todos os ativos de informação são protegidos de forma a garantir sua confidencialidade, integridade, privacidade e disponibilidade.

O acesso às informações deve ser restrito ao mínimo necessário para realizar atividades de negócios autorizada. A Prothera adota o princípio de que "o acesso é proibido a menos que tenha sido especificadamente e formalmente autorizado".

Procedimentos para o registro e cancelamento de registro de usuários para o acesso a todos sistemas de informação devem ser estabelecidos para garantir que todos os direitos de acesso do usuário correspondem à sua autorização. Esses procedimentos devem ser implementados pelo coordenador de TIC/Infra. O acesso aos sistemas operacionais deve ser controlado por um procedimento de login seguro e todos os usuários devem ter uma identidade de usuário única, que possibilite rastrear as atividades até o indivíduo responsável.

Contas de administradores só devem ser concedidas e utilizadas em situações de necessidade. O acesso administrativo deve ser associado à autenticação de 2 fatores, sempre que houver a opção, e deve ser habilitado a opção de exigir usuário e senha em atividades de

níveis privilegiados. Os direitos de acesso aos aplicativos e funções de aplicativos devem ser limitados ao mínimo necessário para execução das atividades.

As contas padrões e desnecessárias do sistema devem ser removidas, desativadas ou de outra forma protegidas.

7.14 CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES

As informações devem ser classificadas em diferentes níveis de sensibilidade considerando seu valor para a Prothera, requisitos legais e impacto devido à perda de confidencialidade, disponibilidade, integridade e privacidade e devem ser protegidas de acordo com o seu nível de sensibilidade.

As informações são classificadas nas seguintes categorias: confidencial, restrito, interno, público ou sigiloso. Os critérios de classificação estão documentados na política de classificação da informação.

7.15 SEGURANÇA FÍSICA E DO AMBIENTE

Todas as instalações de processamento de informações devem ser protegidas por controles físicos apropriados de acordo com requisitos relativos à criticidade, sensibilidade e conformidade regulamentar e riscos para os sistemas ou serviços operados nesses locais.

O acesso de visitantes e prestadores de serviços deverá ser acompanhado de um colaborador com acesso autorizado ao ambiente. É proibido o acesso de visitantes e prestadores de serviço, em áreas restritas, sem o devido registro de entrada realizado na recepção.

As definições dos controles, assim como outras informações estão documentadas no procedimento de controle de acesso para recepção.

7.16 BACKUP

A Prothera realiza backup e testa regularmente as informações essenciais, estejam elas armazenados em servidores locais ou nuvem. A periodicidade, retenção, abrangência e tipo de backup são definidos de acordo com a criticidade da informação ou sistema para a organização. Os colaboradores devem armazenar as informações no servidor de arquivos que é

salvaguardado por backup. As definições relacionadas a backup estão documentadas na política de backup e recovery.

7.17 TRANSFERÊNCIA DE INFORMAÇÕES

A transferência de informações para uma organização externa deve ser regida por acordos de transferência de informações para garantir a confidencialidade e integridade dos dados de propriedade institucional.

Os critérios para realização da troca de informação são estabelecidos nos contratos com a organização externa e na política de controle criptográficos.

7.18 GERENCIAMENTO DE VULNERABILIDADES TÉCNICAS

O Coordenador de Infra/TIC é responsável pela gestão de vulnerabilidade técnica, incluindo monitoramento, avaliação de risco, correção e rastreamento de ativos.

A Prothera subcontrata serviço de GCV (Gestão Continuada de Vulnerabilidade), com a finalidade de avaliar e gerenciar vulnerabilidades. Além disso realiza mensalmente com o fornecedor, reunião de alinhamento para apresentação dos resultados obtidos e criação de plano de tratamento se necessário. A avaliação da vulnerabilidade e a correção do sistema devem ser realizadas apenas por colaboradores ou terceiros designados e sobre o acompanhamento do Coordenador de Infra/TIC.

7.19 CONTROLES CRIPTOGRÁFICOS

A Prothera assegura a utilização efetiva e adequada de criptografia para proteger a confidencialidade, autenticidade e a integridade das informações. As diretrizes para o gerenciamento de chaves e algoritmos criptográficos estão documentados na política de controle criptográficos.

7.20 SEGURANÇA NAS COMUNICAÇÕES

A redes da empresa são segmentadas por departamento e todo tráfego e acesso é monitorado. A segregação da rede é baseada nos princípios de segurança da “segregação de funções” e “menor privilégio”.

Todos os colaboradores devem possuir um ID e senha único, que não deve ser compartilhado, para acessar sua estação de trabalho.

A Prothera possui um firewall que monitora e bloqueia ataques, vírus e atua como filtro de conteúdo. O setor de infra/TIC monitora rotineiramente o tráfego da rede, incluindo o tráfego da Internet, para utilização da largura de banda e para fins de segurança. Ao se deparar com o uso inadequado de recursos de rede, essa ocorrência será levada ao conhecimento do coordenador de TIC/Infra para a ação corretiva necessária.

7.21 PROTEÇÃO E PRIVACIDADE DA INFORMAÇÃO DE IDENTIFICAÇÃO PESSOAL

A Prothera controla e limita o tratamento de informação de identificação pessoal àquilo que atenda a sua função e propósito.

Os dados pessoais são mantidos em sistemas de informação protegidos através da implementação de controles de segurança apropriados. O uso de informações de identificação pessoal deve ser restrito ao propósito para o qual foram coletadas.

A Prothera protege e trata os dados de acordo a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e a norma ABNT NBR ISO/IEC 27701:2019.

Os principais pontos de entrada do site devem incluir acessos para a política de privacidade da instituição.

7.22 RELACIONAMENTO NA CADEIA DE SUPRIMENTOS

Qualquer fornecedor que colete, armazene, manuseie, transmita, processe, comunique, gerencie ou descarte as informações da Prothera devem estabelecer, implementar e manter políticas razoáveis e um programa de medidas de segurança organizacional, operacional, administrativa, física e técnica e organizacional adequadas para impedir qualquer acesso às informações da Prothera de uma maneira não autorizada.

O fornecedor deve garantir que sua equipe de segurança da informação tenha experiência necessária em segurança da informação e rede.

A relação com fornecedores que envolve coleta, armazenamento, manuseio, transmissão, processamento, comunicação, gerenciamento ou descarte das informações, sistemas de informação ou recursos de processamento de informações da Prothera deve ser baseada em um contrato formal contendo cláusula de confidencialidade e penalidades.

7.23 INVENTÁRIO DE ATIVOS

Um inventário de ativos é mantido com base no impacto à organização, devido à perda de sua confidencialidade, disponibilidade e integridade. O inventário de ativos atribuiu um proprietário nomeado para cada ativo, que compreenderá totalmente suas responsabilidades para a proteção do ativo.

7.24 DESENVOLVIMENTO SEGURO

Os colaboradores da Prothera, membros da equipe de desenvolvimento de software, devem seguir as diretrizes da política de desenvolvimento seguro estabelecida.

8 DISTRIBUIÇÃO E IMPLEMENTAÇÃO

8.1 DISTRIBUIÇÃO

Este documento será disponibilizado a todos os colaboradores por meio dos canais de comunicações internos da Prothera. Um aviso global será enviado a todos os colaboradores notificando-os sobre a liberação deste documento e sempre que uma revisão significativa for realizada. Um link para este documento será fornecido no site do SharePoint da Prothera.

9 GERENCIAMENTO DE FALHAS DE SEGURANÇA

A definição da Prothera de violação de segurança da informação e violação da proteção de dados pessoais para fins deste e de outros documentos relacionados, é uma divergência de qualquer procedimento operacional estabelecido pela empresa, que causa uma falha no cumprimento das normas de conformidade exigidas, conforme estabelecido pelos objetivos do próprio sistema de conformidade e ou os de qualquer órgão regulador.

A Prothera tem objetivos e controles robustos para prevenir falhas de segurança e para gerenciá-las se ocorrerem. Devido à natureza do negócio, a Prothera processa e armazena informações pessoais e dados confidenciais de clientes e, portanto, requer um sistema estruturado e documentado de incidentes de violação para mitigar o impacto de quaisquer violações. Embora tome todos os cuidados com sistemas, segurança e informação, os riscos ainda existem ao usar a tecnologia e depender da intervenção humana, necessitando de medidas e protocolos definidos para lidar com quaisquer violações.

A empresa realiza avaliações de riscos e auditoria uma vez ao ano para garantir que processos, funções e procedimentos estejam em conformidade e que as ações para reduzir os riscos estejam em vigor quando necessário. No entanto, caso haja alguma violação, está totalmente preparada para identificar, investigar e mitigar imediatamente e assim reduzir os impactos.

Consultar a política de incidentes de segurança da informação e o plano de respostas a incidentes envolvendo dados pessoais para mais informações.

10 SANSÕES

A falha de contratados, funcionários temporários, públicos, parceiros ou organizações terceirizadas em cumprir a política de segurança da informação da Prothera pode resultar na rescisão dos contratos e relações, suspensão de serviços e ou instauração de processo judicial.

Aos colaboradores que desrespeitarem as normas estabelecidas neste documento, serão aplicadas as seguintes sanções, imediatamente à ocorrência do ato faltoso:

- 2 advertências verbais;
- 2 advertências por escrito;
- 1 suspensão de 3 dias;
- 1 suspensão de 5 dias;
- Dispensa por justa causa.

Objetiva-se que o referido rol de penalidades seja aplicado de forma gradativa, porém, e conforme permite a legislação vigente, quando a gravidade do ato assim demandar, a penalidade será mensurada e aplicada proporcionalmente ao ato faltoso cometido, ainda que a medida anterior não tenha sido levada a efeito.

10.1 ADVERTÊNCIA ESCRITA E SUSPENSÕES

- A suspensão do direito de uso de serviços oferecidos pela rede da empresa por tempo indeterminado poderá ser aplicada além da suspensão do comparecimento ao trabalho;
- No caso de falta considerada leve, penas de advertência e suspensão serão aplicadas nos casos legais e imediatamente após a regular apreciação do ato faltoso, sendo que no caso da suspensão, o funcionário sofrerá o desconto salarial correspondente ao número de dias em que perdurar a penalidade e, conforme legislação vigente (art. 130,

CLT), referido período será considerado como falta injustificada para o cômputo das férias.

10.2 PROCEDIMENTO EM CASO DE FALTA GRAVISSIMA

- Nos casos de falta gravíssima a pena de demissão por justa causa será aplicada nos casos legais e, imediatamente, após regular apreciação através de processo administrativo disciplinar;
- Aos colaboradores enquadrados no regime de trabalho CLT, ditos “empregados”, a pena de demissão por justa causa será aplicada nas hipóteses previstas no artigo 482 e parágrafo único da Consolidação das Leis do Trabalho - DECRETO-LEI N.º 5.452, de 1º de maio de 1943 e recente alteração promovida pela Lei nº 13.467/17;
- Aos colaboradores terceirizados, será solicitado à empresa prestadora da respectiva mão-de-obra, o afastamento temporário ou definitivo do funcionário, conforme a falta cometida podendo em último caso a organização solicitar a rescisão do contrato de prestação de serviço.

De acordo com a gravidade analisada e de posse dos registros comprobatórios, o assunto será encaminhado à direção para tomar as medidas cabíveis para o caso em questão.

Conforme a legislação trabalhista vigente, além da aplicação das penalidades disciplinares, o funcionário estará sujeito a desconto salarial para pagamento do prejuízo a que tiver dado causa à organização, o qual será incluído na próxima folha de pagamento a ser gerada após a ocorrência e apuração do ato faltoso, consoante permite o art. 462, § 1º da CLT. No caso de prestador de serviço de qualquer natureza, estará sujeito ao desconto no valor a ser pago na(s) próxima(s) fatura(s) gerada(s) após a ocorrência e apuração do ato faltoso, para ressarcimento do prejuízo que tiver causado.

A aplicação destas sanções não isenta o colaborador de sofrer outras penalidades previstas em regulamentos internos (contratos) ou mesmo de sofrer processos penais por crimes de peculato, de extravio, sonegação e inutilização de livro ou documento, de condescendência criminosa, de violação de sigilo funcional entre outros, estabelecidos no código penal, sem prejuízo, ainda da responsabilização civil, também aplicada aos colaboradores que não se enquadrem como funcionários, inclusive a título de indenização por danos morais, quando cabível, nos termos dos arts. 186 c/c 927 do Código Civil.

11 CONSIDERAÇÕES FINAIS

A utilização das informações pelos colaboradores da Prothera deve estar de acordo com as políticas da empresa. Todos os usuários devem conhecer e entender esses documentos. A segurança e proteção da informação é uma responsabilidade contínua de cada colaborador da entidade em relação às informações que acessa e gerencia. Todos os colaboradores devem utilizar a informação da entidade, de acordo com as determinações desta política de segurança da informação.

O não cumprimento desta política e ou dos demais instrumentos normativos que complementarão o processo de segurança constitui em falta grave e o colaborador está sujeito a penalidades administrativas e ou contratuais. Situações não previstas, dúvidas, informações adicionais e sugestões devem ser encaminhadas ao coordenador de TIC/Infra por meio do e-mail ciso@prothera.com.br ou telefone (48) 3302-1115, ao comitê do SGSPI ou à direção da Prothera, de acordo com o grau de relevância e urgência da questão.

12 NATUREZA DAS ALTERAÇÕES

Tabela 1 – Histórico de revisões

Data	Revisão	Descrição	Alterado por	Aprovado por
21/10/2020	000	Emissão inicial	Baschirotto, C., Matos, V.	Fontana, M., Fontana, R.
01/06/2021	001	Alteração em nomenclatura de documentos relacionados	Vargas, K. N.	Fontana, R.
18/11/2021	002	Alteração ano ISO/IEC 27018	Baschirotto, C.	Fontana, R.
07/10/2022	003	Alterado os tópicos de senhas e controle de acesso e unificado os procedimentos, nesta única política	Scremin, L.M.	Fontana, R.
27/09/2023	004	Remoção da menção da política de senhas, uso de máquina pessoal com antivírus pago, remoção da citação de política de controle de acesso, alteração em usuários com privilégio administrador, gerenciamento de vulnerabilidades, remoção de ênfase no analista de segurança	Felisberto, R.B.	Fontana, R.
20/05/2024	005	Inclusão do item 4. Objetivos da segurança da informação, alteração do termo “dados pessoais” para “sigiloso”, mudança de concordância no item 6.2	Bezerra, A. S.	Fontana, R.
15/07/2024	006	Remoção da norma 27018, alteração da versão 27001:2022, inclusão de	Felisberto, R.B.	Fontana, R.

		atendimento de novos controles tais como: Inteligência de ameaças e segurança da informação no gerenciamento de projetos, alteração do e-mail de comunicação com o coordenador de infra, alteração de dias para alteração de senhas para 120 dias.		

13 DOCUMENTOS RELACIONADOS

Tabela 2 – Lista de documentos relacionados nesta política.

Tipo documento	Código	Título
Política	POL-0002	Política de classificação da informação
Política	POL-0003	Política de desenvolvimento seguro
Política	POL-0005	Política de dispositivos móveis e trabalho remoto
Política	POL-0006	Política de backup
Procedimento	PI-0013	Gerenciamento de mídias removíveis
Procedimento	PI-0014	Procedimento de controle de acesso para recepção
Política	POL-0013	Política de controle criptográficos
Política	POL-0014	Política de privacidade
Política	POL-0015	Política de incidentes de segurança da informação
Procedimento	PI-0021	Plano de respostas a incidentes envolvendo dados pessoais
Política	POL-0022	Política código de ética e conduta para fornecedores