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 tratados pela Prothera são ativos valiosos e devem ser gerenciados adequadamente, visando garantir sua disponibilidade, integridade, confidencialidade e privacidade, independentemente do meio em que foram coletados. A segurança deve estar presente em todo o ciclo de vida da informação, desde a coleta até o descarte seguro das informações.

Reconhecemos nossa responsabilidade de proteger a informação (física e eletrônica) contra ameaças internas e externas. A gestão eficaz da segurança da informação é essencial para a continuidade das operações e para a qualidade na entrega de nossos serviços.

A Prothera possui um Sistema de Gestão da Segurança e Privacidade da Informação (SGSPI) robusto, composto por políticas, procedimentos, controles e medidas em conformidade com as normas NBR ISO/IEC 27001:2022 e NBR ISO/IEC 27701:2019.

O SGSPI é um sistema de gestão corporativo que abrange a abordagem organizacional para proteção das informações sob nossa responsabilidade, promovendo a melhoria contínua frente a ameaças e vulnerabilidades. Sua aplicação é essencial para a proteção dos dados e da reputação da Prothera. Para garantir sua efetiva implementação, o SGSPI é estruturado por políticas e procedimentos específicos para cada área de segurança da informação. Quando aplicável, este documento faz referência às políticas complementares.

Os documentos do SGSPI se complementam entre si, sendo importante considerá-los em conjunto para melhor compreensão. As políticas e documentos que fazem parte do SGSPI da Prothera estão referenciados na lista mestra de documentos.

3 PROPÓSITO

Este documento estabelece diretrizes para o gerenciamento da informação, visando proteger e garantir os pilares de confidencialidade, integridade, disponibilidade e privacidade, conforme as normas NBR ISO/IEC 27001:2022 e NBR ISO/IEC 27701:2019.

Definição dos pilares:

- **Disponibilidade**: Garantir que os ativos e as informações estejam acessíveis aos usuários autorizados sempre que necessário.
- **Integridade**: Assegurar que as informações estejam protegidas contra alterações indevidas, destruição ou perda, garantindo sua exatidão.
- **Confidencialidade**: Assegurar que as informações sejam acessadas apenas por pessoas autorizadas, evitando divulgações não intencionais ou maliciosas.
- **Privacidade**: Proteger os dados pessoais contra falhas de integridade, indisponibilidade e violações de confidencialidade ao longo de 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 se aplica a:

- Softwares fornecidos ou controlados pela Prothera;
- Comunicações enviadas ou recebidas;
- Dados pertencentes, controlados ou processados pela Prothera, inclusive em sistemas externos;
- Locais de acesso aos dados, incluindo ambientes domésticos ou externos;
- Ativos de informação mantidos, processados ou armazenados em instalações internas ou externas;
- Informações em trânsito por redes de voz ou dados.

Esta política deve ser conhecida por todos os colaboradores da Prothera: empregados, prestadores de serviço, representantes, subcontratados, estagiários e aprendizes. O descumprimento poderá resultar em sanções disciplinares.

6 RESPONSABILIDADES

- **Analista da qualidade:** Responsável pela manutenção deste documento e seus procedimentos associados.
- **Comitê do SGSPI**: Responsável pela governança e revisão bienal da política ou sempre que houver mudanças relevantes. Deve garantir a conformidade com requisitos legais e manter a consistência entre todas as políticas do SGSPI.
- **Coordenador de TIC/Infraestrutura:** Responsável pelas operações de segurança da informação, incluindo o recebimento de relatos sobre falhas, ameaças ou incidentes.
- **Encarregado de proteção de dados (DPO):** Responsável por assuntos relacionados à privacidade e proteção de dados pessoais, incluindo atendimento aos titulares, interações com a autoridade nacional, orientações internas e providências cabíveis.
- **Todos os usuários:** Cumprir esta política e os procedimentos, medidas e diretrizes associados à segurança da informação.

7 POLÍTICAS E DIRETRIZES

7.1 USO ACEITÁVEL DOS ATIVOS

Todos os colaboradores são responsáveis por proteger as informações e os ativos de informação sob sua responsabilidade. Esses ativos devem ser usados de forma adequada, em

conformidade com esta política e com os demais documentos e processos relacionados ao SGSPI.

7.2 MESA LIMPA TELA LIMPA

Dispositivos de computação não acompanhados ou fora de uso devem estar protegidos por bloqueio de tela controlado por senha ou outro mecanismo de autenticação (incluindo laptops, tablets, smartphones e estações de trabalho).

As estações de trabalho são configuradas para bloqueio automático após até 5 minutos de inatividade. Ao se ausentar, bloqueie o dispositivo manualmente utilizando Ctrl-Alt-Del > “Bloquear”, ou a tecla Windows e 'L'.

Durante o uso de informações confidenciais ou que contenham dados pessoais, o usuário deve estar atento ao ambiente ao redor, garantindo que pessoas não autorizadas não possam visualizar tais informações. As telas devem ser posicionadas de forma a impedir a visualização por pessoas não autorizadas.

Informações confidenciais ou restritas devem ser protegidas durante e após o uso, especialmente ao final do expediente. Impressões devem ocorrer somente quando estritamente necessárias, a fim de evitar divulgação não autorizada.

7.3 USO DA INTERNET

O uso da Internet deve ser consciente e alinhado às necessidades das atividades laborais. O uso excessivo ou que comprometa o desempenho profissional, bem como coloque em risco os ativos da informação, pode resultar em advertências, conforme a gravidade.

O acesso à Internet em ativos da empresa é monitorado e controlado por um sistema de filtro de conteúdo (proxy), salvo em casos de necessidade de acesso irrestrito previamente autorizado por gestor ou diretor.

7.4 USO DO E-MAIL

O uso do e-mail corporativo para fins pessoais não é permitido. Os sistemas de e-mail fornecidos pela Prothera devem ser utilizados exclusivamente para assuntos da empresa. É proibido utilizar o e-mail de forma ofensiva ou inadequada. Todos os e-mails são classificados automaticamente como ‘Confidencial’.

Caso você receba uma mensagem imprópria ou abusiva, comunique imediatamente a equipe de Infraestrutura/TIC, que tomará as medidas necessárias. Se o remetente for conhecido, oriente-o a interromper o envio desse tipo de material. Mensagens suspeitas, como possíveis tentativas de phishing ou malware, devem ser reportadas de imediato à equipe de Infraestrutura/TIC como incidentes de segurança.

7.5 INTELIGÊNCIA DE AMEAÇAS PROATIVA

A Prothera contrata serviço especializado de análise contínua de vulnerabilidades, com o objetivo de identificar e reportar ameaças que possam comprometer a segurança da informação. Relatórios mensais são apresentados em reuniões para definição de ações corretivas e mitigação de riscos identificados durante a análise.

7.6 USO DE MÍDIAS REMOVÍVEIS

Considera-se mídia removível qualquer dispositivo que permita o transporte de dados (Ex: CD, DVD, pen drive, HD Externo, entre outros). O uso de mídias removíveis é orientado pela política de uso de mídias removíveis da Prothera, a qual deve ser consultada pelos colaboradores.

7.7 DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

Qualquer pessoa que armazena ou transporta dados da Prothera em dispositivos móveis é responsável por protegê-los adequadamente. Informações confidenciais não devem ser copiadas para dispositivos remotos sem a autorização prévia do proprietário das informações.

Em caso de perda ou furto de dispositivos com acesso aos ativos da Prothera, o ocorrido deve ser comunicado imediatamente ao Coordenador de Infraestrutura/TIC.

O trabalho remoto deve seguir as diretrizes da Política de Dispositivos Móveis e Trabalho Remoto, garantindo a segurança dos dados e dos sistemas acessados.

7.8 RESTRIÇÕES SOBRE O USO E INSTALAÇÕES DE SOFTWARE

Todos os softwares utilizados devem estar em conformidade com as políticas de licenciamento e gestão de ativos da empresa. A instalação, atualização e remoção de software são de responsabilidade exclusiva da equipe de Infraestrutura/TIC.

É proibida a utilização de softwares piratas ou sem licença válida. Violação de direitos autorais ou de propriedade intelectual pode resultar em sanções disciplinares.

7.9 SENHAS

Senhas e demais formas de autenticação secreta (como chaves criptográficas ou padrões de desenho) são de uso pessoal e intransferível.

As senhas devem ser alteradas no primeiro acesso após a emissão e trocadas a cada 120 dias. Sempre que possível, devem conter no mínimo 8 caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais, de modo a dificultar sua adivinhação. Senhas padrão ou que utilizem informações pessoais, como nomes e datas, devem ser evitadas. Sempre que aplicável, deve ser habilitada a autenticação em duas etapas, utilizando ferramentas como e-mail ou telefone corporativo. Nos sistemas que permitirem, o responsável deve configurá-los para exigir a complexidade mínima de senha.

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.

Diante de suspeita de comprometimento, a senha deve ser alterada imediatamente em todos os dispositivos, redes e sistemas, e a equipe de Infraestrutura/TIC deve ser comunicada.

7.10 SEGURANÇA DA INFORMAÇÃO NO GERENCIAMENTO DE PROJETOS

A segurança da informação deve estar integrada a todo o ciclo de vida de projetos e sistemas contratados ou desenvolvidos.

Antes da implementação de sistemas, deve-se realizar análise de segurança com o Coordenador de Infraestrutura/TIC.

Sistemas reprovados só poderão ser utilizados mediante autorização formal da direção, registrada via ferramenta de workflow.

7.11 CONTRATOS DE TRABALHO

Requisitos de segurança devem ser abordados desde a fase de recrutamento. Todos os contratos de trabalho devem conter cláusulas de confidencialidade e privacidade, alinhado com os princípios do SGSPI.

7.12 PROTEÇÃO CONTRA MALWARE

Todas as estações de trabalho contam com antivírus instalado e atualizado automaticamente. A proteção do ambiente envolve firewalls, segmentação de rede, AntiSpam e antivírus.

O uso de equipamentos pessoais em regime remoto exige antivírus com licença paga. Caso o colaborador não possua, a empresa poderá fornecer. O tráfego de rede é monitorado para identificar comportamentos suspeitos e prevenir acidentes.

7.13 CONTROLE DE ACESSOS

A Prothera adota o princípio de que todo acesso é proibido, exceto quando houver autorização específica. O acesso às informações é restrito a usuários autorizados e deve estar alinhado com a necessidade de acesso para a execução de atividades de negócio.

Cabe à equipe de Infraestrutura e TIC manter um procedimento formal para concessão, revisão e revogação de acessos a todos os sistemas e serviços de informação, assegurando que os direitos de acesso estejam sempre compatíveis com as autorizações concedidas. Todos os ativos de informação devem ser protegidos de forma a garantir sua confidencialidade, integridade, disponibilidade e privacidade. O acesso deve ser limitado ao mínimo necessário, considerando o perfil e as responsabilidades de cada usuário.

Cada colaborador deve possuir uma identificação de usuário única, permitindo a rastreabilidade de suas ações. O acesso aos sistemas operacionais deve ser realizado por meio de procedimentos seguros de login.

Contas administrativas devem ser utilizadas apenas quando estritamente necessário e associadas à autenticação de dois fatores sempre que disponível. Para atividades com privilégios elevados, deve ser obrigatório o uso de usuário e senha.

7.14 CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÕES

As informações devem ser classificadas conforme seu nível de sensibilidade, levando em conta seu valor para a Prothera, os requisitos legais aplicáveis e o impacto que uma eventual perda de confidencialidade, integridade, disponibilidade ou privacidade poderia causar. A proteção de cada informação deve ser proporcional ao seu nível de classificação.

As informações são classificadas nas seguintes categorias: Publico, interno, restrito, confidencial e 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, conforme os requisitos relativos à criticidade, sensibilidade, conformidade regulamentar e riscos para os sistemas ou serviços operados nesses locais.

O acesso de visitantes e prestadores de serviços deverá ser acompanhado por um colaborador com acesso autorizado ao ambiente. É proibido o acesso de visitantes e prestadores de serviço a 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 armazenadas em servidores locais ou na nuvem. A periodicidade, retenção, abrangência e tipo de backup são definidos conforme 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.

7.17 TRANSFERÊNCIA DE INFORMAÇÕES

A transferência de informações para uma organização externa deve ser regida por acordos que garantam 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 Infraestrutura/TIC é responsável pela gestão de vulnerabilidades técnicas, incluindo monitoramento, avaliação de risco, correção e rastreamento de ativos.

A Prothera subcontrata serviço de Gestão Continuada de Vulnerabilidade (GCV), com a finalidade de avaliar e gerenciar vulnerabilidades. Além disso, realiza reuniões mensais com o fornecedor para alinhamento, apresentação dos resultados obtidos e criação de plano de tratamento quando necessário.

A avaliação das vulnerabilidades e a correção dos sistemas devem ser realizadas apenas por colaboradores ou terceiros designados e sob o acompanhamento do Coordenador de Infraestrutura/TIC.

7.19 CONTROLES CRIPTOGRÁFICOS

A Prothera assegura a utilização efetiva e adequada de criptografia para proteger a confidencialidade, autenticidade e 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 são monitorados. 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 devem ser compartilhados, para acessar sua estação de trabalho.

A Prothera possui firewall que monitora e bloqueia ataques, vírus e atua como filtro de conteúdo. O setor de Infraestrutura/TIC monitora rotineiramente o tráfego da rede, incluindo o tráfego da Internet, para utilização da largura de banda e para fins de segurança.

Ao detectar uso inadequado dos recursos de rede, a ocorrência deve ser comunicada ao coordenador de Infraestrutura/TIC para a ação corretiva necessária.

7.21 PROTEÇÃO E PRIVACIDADE DA INFORMAÇÃO DE IDENTIFICAÇÃO PESSOAL

A Prothera controla e limita o tratamento de informações de identificação pessoal àquilo que atende à sua função e propósito.

Os dados pessoais são mantidos em sistemas protegidos por 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 à 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 e programas de medidas de segurança organizacional, operacional, administrativa, física e técnica adequadas para impedir o acesso não autorizado às informações da Prothera.

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

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

7.23 INVENTÁRIO DE ATIVOS

Um inventário de ativos é mantido considerando o impacto à organização, decorrente da perda de confidencialidade, disponibilidade e integridade.

Cada ativo possui um proprietário nomeado, que compreende integralmente 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 geral será enviado notificando os colaboradores sobre a publicação do documento e sempre que houver uma revisão significativa. Este documento será disponibilizado no site do Sharepoint da Prothera.

9 GERENCIAMENTO DE FALHAS DE SEGURANÇA

Para fins deste e de outros documentos relacionados, a Prothera define violação de segurança da informação e violação da proteção de dados pessoais como qualquer divergência em relação aos procedimentos operacionais estabelecidos pela empresa, que resulte em descumprimento das normas de conformidade exigidas, conforme os objetivos do sistema de gestão ou de qualquer órgão regulador.

A Prothera estabelece controles robustos para prevenir falhas de segurança e está preparada para gerenciá-las caso ocorreram. Devido à natureza de suas atividades, a empresa processa e armazena informações pessoais e dados confidenciais de clientes, exigindo, portanto, um sistema estruturado e documentado para o tratamento de incidentes de violação, com o objetivo de mitigar seus impactos.

Apesar dos cuidados aplicados aos sistemas e à segurança da informação, os riscos permanecem, considerando o uso de tecnologias e a atuação humana. Por isso, são mantidas medidas e protocolos específicos para tratamento de violações.

A empresa realiza avaliações de riscos e auditoria periódicas, no mínimo uma vez ao ano, para garantir a conformidade de seus processos, funções e procedimentos, e assegurar que ações corretivas estejam implementadas sempre que necessário.

Em casos de violação, a Prothera está preparada para identificar, investigar e mitigar rapidamente o incidente, minimizando seus impactos.

Para mais informações, consultar a política de incidentes de segurança da informação e o plano de respostas a incidentes envolvendo dados pessoais.

10 SANÇÕES

O descumprimento da Política de segurança da informação por contratados, funcionários temporários, públicos, parceiros ou organizações terceirizadas poderá resultar na rescisão contratual, suspensão de serviços e/ou instauração de processo judicial.

Para os colaboradores da Prothera, o desrespeito às normas estabelecidas neste documento poderá acarretar as seguintes sanções, aplicadas gradativamente conforme a gravidade da infração:

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

O objetivo é aplicar essas penalidades de forma escalonada. No entanto, conforme a legislação vigente, atos de maior gravidade poderão ser punidos de forma proporcional, ainda que as etapas anteriores não tenham sido cumpridas.

10.1 ADVERTÊNCIA ESCRITA E SUSPENSÕES

- A suspensão do direito de uso de serviços de rede da empresa poderá ser aplicada juntamente à suspensão do comparecimento ao trabalho, por tempo indeterminado.

- Em casos de infrações leves, advertências e suspensões serão aplicadas conforme a legislação, após análise da ocorrência.
- Nos casos de suspensão, haverá desconto proporcional no salário, e o período será considerado como falta injustificada para fins de férias, conforme o art. 130 da CLT.

10.2 PROCEDIMENTO EM CASO DE FALTA GRAVISSIMA

- Nos casos de falta gravíssima, a demissão por justa causa será aplicada após a apuração por meio de processo administrativo disciplinar, nos termos da lei.
- Para colaboradores em regime CLT, a justa causa será aplicada conforme o 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;
- Para colaboradores terceirizados, será solicitado à empresa prestadora a substituição ou afastamento do profissional, podendo ser solicitada a rescisão do contrato de prestação de serviço.

Conforme a gravidade e mediante registro comprobatório, o caso será encaminhado à direção para tomar as medidas cabíveis.

Conforme o art. 462, §1º da CLT, o colaborador poderá ter desconto em folha de pagamento para ressarcimento de prejuízos causados. Para prestadores de serviço, o desconto será aplicado na(s) próxima(s) fatura(s) emitida(s), após apuração da ocorrência.

A aplicação de penalidades administrativas não isenta o colaborador de responder civil ou criminalmente por infrações como:

- Peculato;
- Extravio, sonegação ou inutilização de documento;
- Violação de sigilo funcional;
- Condescendência criminosa, entre outras previstas no Código Penal.

Colaboradores que não estejam sob regime CLT também poderão responder por danos morais ou materiais, nos termos dos arts. 186 e 927 do Código Civil.

11 CONSIDERAÇÕES FINAIS

O uso das informações pelos colaboradores da Prothera deve seguir as políticas da empresa. Todos os usuários são responsáveis por conhecer este documento e os demais normativos relacionados.

A segurança e proteção da informação é uma responsabilidade contínua de cada colaborador em relação às informações que acessa e gerencia.

O descumprimento desta política e ou dos documentos que a complementam será considerado falta grave e poderá acarretar penalidades administrativas e ou contratuais.

Situações não previstas, dúvidas, informações adicionais e sugestões devem ser encaminhadas ao coordenador de Infraestrutura/TIC por meio do e-mail ciso@prothera.com.br ou telefone (48) 3302-1115, ao comitê do SGSPI ou à direção da Prothera, conforme a gravidade e urgência do assunto.

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 atendimento de novos controles tais como: Inteligência de ameaças e segurança da	Felisberto, R.B.	Fontana, R.

		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.		
07/10/2025	007	Revisão geral do documento, ajuste de fluidez nos textos e resumido alguns tópicos	Vargas, K.N.	Fontana, R.

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