Postal Saúde
Sua vida, nossa existência

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
Unidade Administrativa Gestora do normativo	Diretoria Administrativa e Financeira (DIAFI) Gerência de Tecnologia (GETEC) Coordenação de Sistemas (COSIS) Coordenação de Infraestrutura (COINF)
Unidade Administrativa responsável pela análise normativa (interna) e padronização	Presidência (PRESI) Gerência de Estratégia e Inteligência Organizacional (GEORG) Coordenação de Estratégia e Inteligência Organizacional (COORG)
Unidade Administrativa responsável pela conformidade	Presidência (PRESI) Gerência Jurídica (GEJUR) Coordenação Consultiva e Regulatória (CONSU)
Numeração	POL/001
Versão	002
Data da Apreciação DIREX	DIREX Nº 267, de 20 de setembro de 2021
Data da Aprovação CODEL	CODEL Nº 153, de 30 de setembro 2021
Data de Publicação	29/10/2021
Advertência	Este normativo é de **uso exclusivo** da Postal Saúde. A divulgação não autorizada estará sujeita às penalidades cabíveis por lei. Toda e qualquer autorização para cópia, divulgação, apresentação ou qualquer outra finalidade deverá ser obtida junto à Postal Saúde.

Sumário

Capítulo 1
DOS OBJETIVOS 4

Capítulo 2
DA ABRANGÊNCIA 6

Capítulo 3
DOS CONCEITOS E DEFINIÇÕES 8

Capítulo 4
DOS PRINCÍPIOS 12

Capítulo 5
DAS DIRETRIZES GERAIS 14

Capítulo 6
DAS DIRETRIZES ESPECÍFICAS 17

Capítulo 7
DAS COMPETÊNCIAS 25

Capítulo 8
DAS RESPONSABILIDADES 27

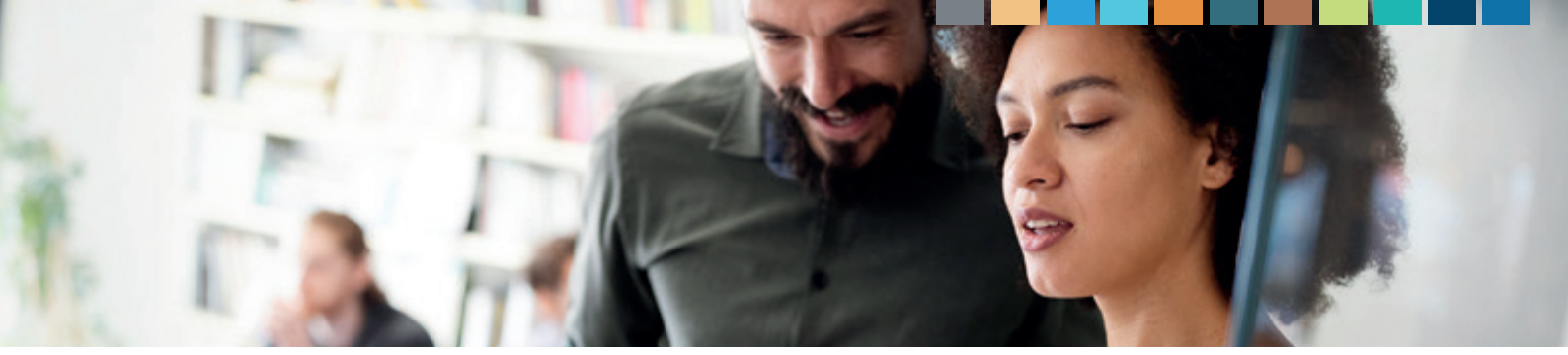
Capítulo 9
DO COMPROMISSO E PENALIDADES 33

Capítulo 10
DAS ATUALIZAÇÕES 35

Capítulo 11
DAS DISPOSIÇÕES FINAIS 37

DOS OBJETIVOS

1



Capítulo 1 - **DOS OBJETIVOS**

1.1. Objetivo Geral

1.1.1. Garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação da Postal Saúde, operadora dos planos de saúde dos empregados dos Correios.

1.1.2. A elaboração e a adoção da Política de Segurança da Informação interna evidenciam o comprometimento da Administração com a provisão de diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação na Postal Saúde.

1.2. Objetivos específicos

1.2.1. Estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de rede de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional.

1.2.2. Designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação.

1.2.3. Apoiar a implantação das iniciativas relativas à Segurança da Informação.

1.2.4. Possibilitar a criação de controles e promover a otimização dos investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

DA ABRANGÊNCIA

Capítulo 2 - **DA ABRANGÊNCIA**

2.1 As diretrizes estabelecidas nesta Política de Segurança da Informação serão aplicadas em toda a Postal Saúde; deverão ser observadas por todos os conselheiros, diretores, empregados, colaboradores, fornecedores e prestadores de serviço e se aplicam à informação em qualquer meio ou suporte.

2.2 Este documento, entre outras diretrizes, dá ciência a cada envolvido de que os ambientes, os sistemas, os recursos computacionais e as redes informacionais da Postal Saúde poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

DOS CONCEITOS E DEFINIÇÕES

3

Capítulo 3 - DOS CONCEITOS E DEFINIÇÕES

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Postal Saúde.

Ativo de Informação: é o conhecimento organizado e gerenciado como uma entidade única e que, como qualquer outro recurso corporativo, tem valor financeiro que aumenta em relação direta com o número de pessoas capazes de usá-lo. São considerados, assim, os meios de armazenamento, transmissão e processamento da informação, os equipamentos e os sistemas utilizados para tal, os locais onde se encontram esses meios e os recursos humanos aos quais eles têm acesso.

Ativo: expressa os bens, valores, créditos, direitos e assemelhados que, num determinado momento, formam o patrimônio de uma pessoa singular ou coletiva e que são avaliados pelos respectivos custos, ou seja, algo que tenha valor para a Postal Saúde.

Conformidade: processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (mantenedores, patrocinadores, prestadores, empregados, credores etc.) e com aspectos legais e regulatórios, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração da Postal Saúde.

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controle de Acesso: permissões concedidas por autoridade competente da Postal Saúde após o processo de credenciamento, que habilitem determinada pessoa, sistema ou organização ao acesso mediante a assinatura ou não de termo de responsabilidade ou outro instrumento formal, podendo a credencial ser física, como crachá, cartão, token, selo ou lógica para identificação de usuários.

Custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, pela operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

Dispositivos Móveis: consiste em equipamentos portáteis dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes, *notebooks, netbooks, smartphones, tablets, pendrives*, USB *drives*, HDs externos e cartões de memória.

Capítulo 3 - DOS CONCEITOS E DEFINIÇÕES

Gestão da Continuidade de Negócios: procedimentos e informações necessárias para que as instituições mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

Incidente de Segurança da Informação: evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos princípios da segurança da informação, como a confidencialidade, a integridade, a autenticidade ou a disponibilidade.

Informação: é a reunião ou o conjunto de dados e conhecimentos resultante do processamento, manipulação ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe. Podem ser utilizadas para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

LGPD: é a Lei nº 13709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Política de mesas limpas: prática de Segurança da Informação recomendada para evitar a exposição desnecessária de informações contidas em papéis e dispositivos eletrônicos no ambiente de trabalho ou inadequadamente armazenados.

Política de telas limpas: prática de Segurança da Informação recomendada para evitar a exposição desnecessária de informações na tela dos computadores e similares.

Risco de Segurança da Informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da Empresa.

Segurança da Informação: é o conjunto de ações e controles que têm como objetivo garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da Operadora.

Serviço em Nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação, rede de

computadores, servidores, processamento, armazenamento, aplicativos e serviços, provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

SIC: Segurança da Informação e Comunicações.

TIC: Tecnologia da Informação e Comunicações.

Titular: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

Usuário: empregados, agentes públicos, terceirizados, colaboradores, consultores, auditores, estagiários e pessoas que obtiveram acesso aos Ativos de Informação da Postal Saúde.

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em riscos para um sistema ou organização, os quais podem ser mitigados por uma ação interna de segurança da informação.

DOS PRINCÍPIOS

4

Capítulo 4 - DOS PRINCÍPIOS

4.1. São princípios da Segurança da Informação:

I. **Confidencialidade** - É o modo de garantir que a informação estará acessível apenas para pessoas, sistemas ou órgãos autorizados. Uma forma de mantê-la é por meio da autenticação, controlando e restringindo os acessos. Ela impõe limitações aos dados sigilosos que a Operadora possui;

II. **Integridade** - O princípio de integridade refere-se à manutenção das condições iniciais das informações, de acordo com a forma como foram produzidas e armazenadas. Somente pessoas autorizadas poderão acessar e modificar os dados do sistema. Pode-se dizer que é a propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

III. **Disponibilidade** - Os dados corporativos precisam estar seguros, acessíveis e utilizáveis sob demanda de uma pessoa, sistema ou órgão devidamente autorizado. Esse princípio diz respeito à eficácia dos recursos de TIC, para que seja possível utilizar a informação quando necessário; e

IV. **Autenticidade** - Esse processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação e ocorre quando um usuário manipula algum dado, gerando a documentação dessa ação. Visa a assegurar que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa, equipamento, sistema, órgão ou entidade.

DAS DIRETRIZES GERAIS

5

Capítulo 5 - DAS DIRETRIZES GERAIS

5.1. Toda informação produzida ou recebida pelos empregados, colaboradores, fornecedores e prestadores de serviço, em resultado da função exercida ou da atividade profissional contratada, pertence à Operadora. As exceções devem ser explícitas e formalizadas entre as partes.

5.2. Todos os recursos de informação da Postal Saúde devem ser projetados para que seu uso seja consciente e responsável. Os recursos comunicacionais e computacionais da Operadora devem ser utilizados para a consecução de seus objetivos finalísticos.

5.3. Deverão ser criados e instituídos pela Área de Tecnologia da Informação controles apropriados, trilhas de auditoria e registros de atividades, em todos os pontos e sistemas em que a Operadora julgar necessário, com vistas à redução dos riscos dos seus ativos de informação.

5.4. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade.

5.5. Todo o acesso a redes e sistemas da Operadora deverá ser feito, preferencialmente, por meio de login de acesso único, com senha pessoal e intransferível.

5.6. A Postal Saúde pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocadas na infraestrutura provida pela Operadora.

5.7. Cada usuário é responsável pela segurança das informações dentro da Postal Saúde, principalmente daquelas que estão sob sua responsabilidade.

5.8. Com o objetivo de reduzir o risco de descontinuidade das atividades da Operadora e de perda de confidencialidade, integridade, disponibilidade e autenticidade dos ativos de informação, deverá ser implantado plano de contingência pela Área de Tecnologia da Informação para os serviços e sistemas; o plano deverá ser implantado, revisado e testado periodicamente.

5.9. Todos os requisitos de segurança da informação, incluindo a necessidade de plano de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Capítulo 5 - DAS DIRETRIZES GERAIS

5.10. Deverá constar em todos os contratos da Postal Saúde, quando o objetivo for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação por empresas fornecedoras e por todos os profissionais que desempenham suas atividades na Operadora.

5.11. Deverá estar prevista, por parte das empresas e profissionais prestadores de serviço, entrega de declaração expressa de compromisso em relação à confidencialidade e de termo de ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela Operadora.

5.12. Papéis, anotações e lembretes devem ser mantidos, sempre que possível, fora da superfície da mesa de trabalho. Informações do negócio, em qualquer mídia, deve ser guardada em local seguro, com chave, quando não estiver em uso: política de mesas limpas.

5.13. Computadores e notebooks não devem ser deixados autenticados ou registrados quando não houver um operador junto dele. Telas de bloqueio protegidas por senhas e outros controles devem ser ativados quando os monitores não estiverem em uso: política de telas limpas.

5.14. Informações corporativas da Postal Saúde não podem ser transportadas em qualquer meio sem as devidas autorizações e proteções. Atenção especial deve ser aplicada no uso de dispositivos móveis.

5.15. Esta Política de Segurança da Informação será implementada no âmbito da Postal Saúde por meio de manual específico, proposto pela Área de Tecnologia da Informação, sendo obrigatória a sua observância por todos os conselheiros, diretores e empregados, independentemente do nível hierárquico ou função, bem como de vínculo empregatício temporário ou de prestação de serviço.

DAS DIRETRIZES ESPECÍFICAS

6

Capítulo 6 - DAS DIRETRIZES ESPECÍFICAS

6.1. Do Tratamento da Informação

6.1.1. O tratamento da informação envolve ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação, em qualquer grau de sigilo, exigindo, sempre, zelo em seu manuseio.

6.1.2. O tratamento deve ser feito de forma a viabilizar e assegurar confidencialidade, integridade, disponibilidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

6.1.3. O tratamento de dados pessoais deve nortear-se pelo objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Considerando as atividades da Postal Saúde, devem-se observar os procedimentos previstos na LGPD, em especial o tratamento de dados sensíveis, desde o consentimento dos titulares.

6.1.4. Diretrizes específicas e procedimentos próprios de tratamento da informação corporativa deverão ser fixados no Manual de Segurança da Informação.

6.2. Monitoramento e Auditoria do Ambiente

6.2.1. Para garantir a aplicação das diretrizes mencionadas nesta Política, além de fixar no Manual de Segurança da Informação procedimentos complementares sobre o tema, a Postal Saúde poderá:

I. Implantar sistemas de monitoramento nas estações de trabalho, servidores, e-mail, conexões com a internet, dispositivos móveis e outros componentes de rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como o material manipulado;

II. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, nos casos previstos na LGPD e outros normativos;

III. Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade ou sob sua responsabilidade;

IV. Instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso; e

V. Desinstalar, a qualquer tempo, software ou sistema que represente risco ou esteja em desconformidade com as políticas, as normas e os procedimentos vigentes.

6.3. Tratamento de incidentes em redes computacionais

6.3.1. A Equipe Técnica de Segurança da Informação deverá:

I. Monitorar o ambiente e recursos de TIC, a fim de identificar possíveis incidentes de segurança da informação;

II. Registrar todos os incidentes notificados ou detectados, com a finalidade de assegurar registro histórico das atividades desenvolvidas e avaliações estatísticas;

III. Realizar a investigação do incidente de segurança da informação, executando medidas de contenção; e

IV. Realizar a análise do incidente de segurança da informação, de forma a propor medidas para eliminar ou solucionar os problemas que causaram o incidente.

6.4. Do e-mail funcional

6.4.1. O correio eletrônico é um recurso de comunicação corporativa da Postal Saúde. As regras de acesso e utilização de e-mail devem atender a todas as orientações deste documento e das Normas Internas Complementares a esta Política de Segurança da Informação.

6.4.2. O correio eletrônico fornecido pela Postal Saúde é um instrumento de comunicação interna e externa para a realização do negócio da Postal Saúde. As mensagens devem ser escritas em linguagem profissional, e não devem comprometer a imagem da Operadora, não podem ser contrárias à legislação vigente e nem aos princípios éticos da Postal saúde.

6.4.3. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. Para incluir um novo usuário no correiso eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão.

6.5. Uso e acesso à internet

6.5.1. O acesso à rede mundial de computadores - Internet, no ambiente de trabalho, deve ser regido por Normas Internas Complementares, atendendo às determinações desta Política, demais orientações governamentais e legislação em vigor.

6.5.2. Embora a utilização da internet seja de grande importância nas atividades da Operadora, faz-se mister o uso de sistemas de monitoramento, a fim de conceder melhor acesso aos que a utilizam corretamente.

6.5.3. O uso da Internet será monitorado pela GETEC, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou. A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição do Gestor imediato, com base em Normas Internas.

6.5.4. A GETEC fica responsável, via ferramenta de *firewall*, bloquear e gerenciar o acesso a site maliciosos contidos em *BlackList* Internacional. Verificando e aplicando suas atualizações rotineiramente.

6.6. Uso de mídias sociais

6.6.1. As mídias sociais podem otimizar a comunicação. É importante que as mídias sociais sejam usadas adequadamente e mantidas nesse contexto. Caso contrário, pode levar à perda de produtividade, distrações ou, até mesmo, infrações.

6.6.2. O uso das redes sociais, disponíveis internamente e na Internet, objetiva prestar atendimento e serviços púbicos, divulgando ou compartilhando informações da Postal Saúde; deve ser regido por Norma Complementar, observando as determinações desta Política, demais orientações governamentais e a legislação em vigor.

6.6.3. A definição dos funcionários que terão permissão para uso de mídias sociais através de ativos da Postal Saúde para desempenharem suas funções é atribuição do Gestor imediato, justificando a solicitação.

6.7. Do serviço em nuvem

6.7.1. O uso dos serviços em nuvem apresenta vantagens como escalabilidade e redução de investimentos em infraestrutura, porém um dos principais fatores identificados como risco em sua utilização é a segurança da informação.

6.7.2. O uso de recursos desse serviço para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias, deve ser regido por Normas Complementares, atendendo às determinações desta Política, demais orientações governa-

mentais e a legislação em vigor, visando a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

6.8. Do Teletrabalho

6.8.1. Diretrizes específicas e procedimentos próprios de controle deverão ser fixados no Manual de Segurança da Informação.

6.8.2. Dentre alguns requisitos a serem observados para o uso do teletrabalho, destacam-se: a segurança física do local de trabalho remoto, incluindo o trânsito de outras pessoas; as proteções de acesso ao equipamento utilizado; e a classificação das informações, os sistemas internos e os serviços que o usuário esteja autorizado a acessar.

6.9. Do Sistema de Gestão Eletrônica de Documentos

6.9.1. Diretrizes específicas e procedimentos próprios de controle deverão ser fixados no Manual de Segurança da Informação.

6.9.2. O Sistema de Gestão Eletrônica de Documentos é uma ferramenta de elevada importância, contribuindo acentuadamente para a gestão do conhecimento da Operadora. Embora a acessibilidade, a facilidade de consultas e a otimização dos fluxos de trabalho, entre outras possibilidades desses sistemas, sejam notórias, a segurança é requisito fundamental para a seleção de um produto com essa finalidade.

6.10. Do Controle de Acesso

6.10.1. As regras de controle de acesso aos sistemas corporativos, à Intranet, à Internet, às informações, aos dados e às instalações da Postal Saúde deverão ser definidas e regulamentadas, por meio de Normas Complementares, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da Operadora.

6.10.2. Quando da necessidade de cadastramento ou atualização de um novo usuário para utilização da “rede”, dos sistemas ou dos equipamentos de informática, o setor de origem do usuário deverá comunicar esta necessidade à Gerência de Tecnologia, por meio de chamado, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos. A Gerência de Tecnologia fará o cadastramento e informará apenas ao usuário qual será a sua senha, solicitando troca de mesma ao primeiro acesso. Essa solicitação é de responsabilidade do Gestor imediato do colaborador.

Capítulo 6 - DAS DIRETRIZES ESPECÍFICAS

6.11. Sala de Servidores

6.11.1. Os procedimentos para administração da sala de servidores deverão ser fixados no Manual de Segurança da Informação.

6.11.2. Os controles do restrito acesso a esse ambiente são de vital importância para o atendimento dos princípios de segurança da informação. E de responsabilidade da Gerência de Tecnologia.

6.12. Gestão de Riscos da Segurança da Informação

6.12.1. A gestão de riscos da segurança da informação deverá considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da Operadora, direta e indiretamente, além de estarem alinhadas a esta Política de Segurança da Informação.

6.12.2. O processo deverá ser contínuo e aplicado na implementação e na operação da Gestão de Segurança da Informação, contemplando inclusive as contratações de soluções de TIC, para as quais deverá ser elaborado um Plano de Tratamento de Riscos, a cargo da Área de Tecnologia da Informação.

6.13. Gestão da Continuidade de Negócios

6.13.1. A Gestão da Continuidade de Negócios de TIC é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da Postal Saúde e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem.

6.13.2. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional capaz de responder, efetivamente, aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da Postal Saúde. Permite, ainda, recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, objetivando salvaguardar os interesses da Operadora e da sociedade.

6.13.3. As áreas da Postal Saúde deverão manter processo de gestão de continuidade de negócios, visando a não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

6.13.4. Todas as áreas internas que dependam de recursos de TIC deverão criar Planos de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros. O Plano deve contemplar um conjunto de estratégias e de procedimentos que deverão ser adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

6.14. Serviço de Backup

6.14.1. Os procedimentos próprios ao serviço de backup (cópia de segurança) deverão ser fixados no Manual de Segurança da Informação.

6.14.2. As garantias de rápida recuperação do material contido nos repositórios devem ser buscadas a fim de capacitar a Postal Saúde ao enfrentamento de ataques e panes.

6.14.3. Cópias de segurança dos sistemas integrados e servidores de rede, hospedados fisicamente na Postal Saúde, são de responsabilidade da Gerência de Tecnologia e deverão ser feitos diariamente.

6.15. Uso de dispositivos móveis

6.15.1. As diretrizes gerais de uso de dispositivos móveis para acesso às informações, aos sistemas, às aplicações e ao correio eletrônico da Postal Saúde devem considerar, prioritariamente, os requisitos legais e a estrutura da Operadora, atendendo a esta Política de Segurança da Informação e regidas por Normas Complementares, as quais contemplarão as recomendações sobre o uso desses dispositivos.

6.16. Admissão/Demissão de Funcionários/Temporários/Estagiários

6.16.1. A Gerência de Pessoal deverá informar à Gerência de Tecnologia toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos. Cabe ao setor solicitante da contratação a comunicação Gerência de Tecnologia sobre as rotinas às quais o novo contratado terá direito de acesso. No caso de demissão, a Gerência de Pessoal deverá comunicar o fato o mais rapidamente possível, para que o funcionário demitido seja excluído do sistema. Cabe ao

setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação ao Manual da Segurança da Informação. Nenhum funcionário, estagiário ou temporário poderá ser contratado sem ter expressamente concordado com este Manual.

6.17. Equipamentos de Impressão e reprografia

6.17.1. O uso de equipamento de impressão e reprografia devem ser feitos exclusivamente para serviços de interesse da Postal Saúde ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

6.17.2. Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais da Postal Saúde ou de beneficiários.

DAS COMPETÊNCIAS

7

Capítulo 7 - DAS COMPETÊNCIAS

7.1. Estão envolvidos na gestão de segurança da informação da Postal Saúde:

I. Área de Tecnologia da Informação (GETEC): unidade organizacional responsável pela gestão e operação dos recursos de TIC na Postal Saúde e custodiante da informação;

II. Equipe Técnica de Segurança da Informação: equipe composta pelos gestores da área de TIC da Postal Saúde, responsável por implementar e administrar as soluções de segurança da informação;

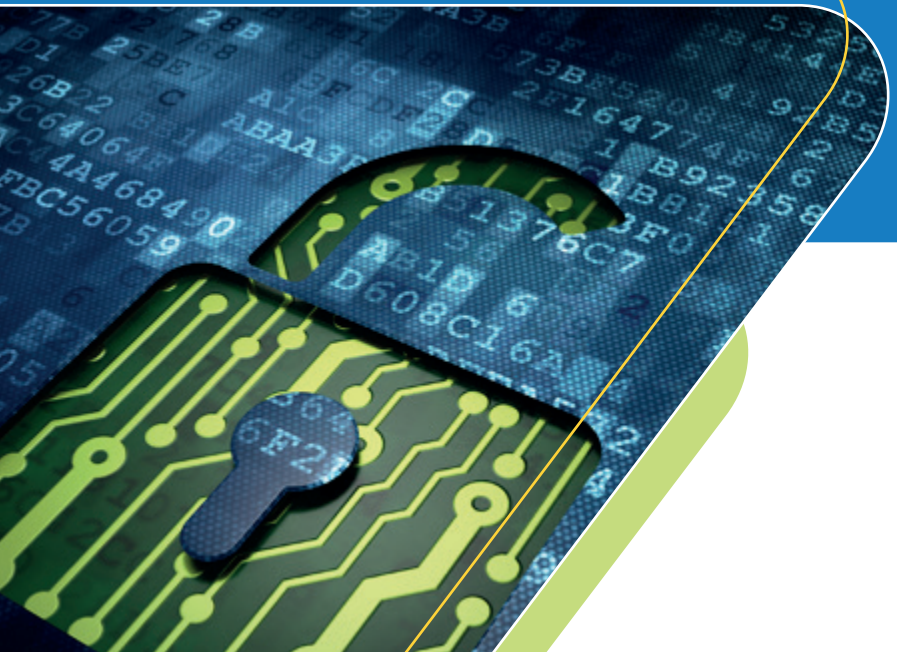
III. Gestor de Segurança da Informação: empregado responsável pela gestão da segurança da informação em todos os seus aspectos, designado pelo Diretor-Presidente;

IV. Gestores: aqueles que exercem funções de gerência no âmbito da Operadora, administrando pessoas ou processos;

V. Usuários externos: prestadores de serviços contratados, direta ou indiretamente, pela Postal Saúde e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais; e

VI. Usuários internos: todos os empregados, diretores e conselheiros que fazem uso dos recursos informacionais e computacionais da Postal Saúde.

DAS RESPONSABILIDADES



Capítulo 8 - DAS RESPONSABILIDADES

8.1. Responsabilidades gerais

8.1.1. São responsabilidades de todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais da Postal Saúde:

I. Manter-se atualizado em relação a esta Política e aos manuais e procedimentos relacionados, buscando informação junto à Área de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à obtenção, o uso ou o descarte de informações;

II. Promover a segurança de seu usuário corporativo, setorial ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

III. Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais da Postal Saúde; e

IV. Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da Postal Saúde.

8.2. Responsabilidades específicas

8.2.1. Usuários internos e externos:

I. Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, as normas e os procedimentos vigentes. A Postal Saúde poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da Política de Segurança da Informação ou das normas e dos procedimentos específicos dela decorrentes; e

II. Será de inteira responsabilidade de cada usuário todo prejuízo ou dano que vier a sofrer ou causar à Postal Saúde em decorrência da não obediência às diretrizes referidas nesta Política de Segurança da Informação e nas normas e procedimentos específicos decorrentes.

8.2.2. Gestores:

I. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, às normas e aos procedimentos específicos de segurança da informação da Postal Saúde, tomando todas as ações necessárias para cumprir tal responsabilidade;

II. Classificar as informações tratadas em sua área e avaliar os riscos que podem afetá-las; e

III. Os gestores da Postal Saúde devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão.

8.2.3. Área de Tecnologia da Informação:

I. Zelar pela eficácia dos controles de segurança da informação e informar aos gestores e demais interessados os riscos residuais;

II. Negociar e acordar com os gestores níveis de serviço relacionados à segurança da informação, incluindo os procedimentos de reposta a incidentes;

III. Configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pelos procedimentos, pelas normas e pela Política de Segurança da Informação;

IV. Gerar e manter trilhas para auditoria com nível de dados suficientes para rastrear possíveis falhas e fraudes; para as trilhas geradas ou mantidas em meio eletrônico, devem ser implantados controles de integridade, de modo a torná-las juridicamente válidas como evidências;

V. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria e investigação;

VI. Zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e eliminar a existência de pessoas que possam excluir logs e trilhas de auditoria das suas próprias ações;

VII. Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para a Postal Saúde;

VIII. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias que contenham informações custodiadas pela TIC, nos ambientes totalmente controlados por ela;

IX. Nas movimentações internas dos ativos de TIC, assegurar-se de que as informações de determinado usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário;

X. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessária para garantir a segurança e a manutenção dos serviços requeridos pelas áreas internas da Postal Saúde;

XI. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável. A responsabilidade pela gestão dos logins de usuários externos é do gestor do contrato de prestação de serviços ou do gestor da área em que o usuário externo desempenha suas atividades;

XII. Proteger continuamente todos os ativos de informação da Postal Saúde contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejável;

XIII. Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades nos ambientes de desenvolvimento, teste, homologação ou produção de sistemas. Quando tais ambientes forem acessados por terceiros, a responsabilização dever ser explicitada nas cláusulas contratuais;

XIV. Definir, exigindo seu cumprimento, as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente dedicado à visitação externa;

XV. Definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos;

XVI. Garantir, de forma mais rápida possível, com recebimento de solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento, incidente, investigação ou outra situação que exija medida restritiva, a fim de salvaguardar os ativos da Postal Saúde;

XVII. Garantir que todos os servidores, as estações e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo Brasileiro;

XVIII. Monitorar o ambiente de TIC, gerando indicadores e histórico de: uso da capacidade instalada da rede dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos; períodos de indisponibilidade no acesso à internet e aos sistemas críticos; incidentes de segurança; e atividade de todos os usuários durante os acessos às redes externas, inclusive internet;

XIX. Elaborar, propor e atualizar o manual de operacionalização desta Política e os Planos relacionados; e

XX. Designar a Equipe Técnica de Segurança da Informação.

8.2.4. Gestor de Segurança da Informação:

I. Promover cultura de segurança da informação e comunicações no âmbito de suas atribuições dentro da Postal Saúde;

II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor recursos necessários às ações de segurança da informação;

IV. Acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

V. Assessorar a Diretoria-Executiva da Postal Saúde na implementação das ações de segurança da informação;

VI. Propor a constituição de grupos de trabalho para tratar de temas e propor soluções sobre segurança da informação;

VII. Propor alterações e revisar periodicamente a Política de Segurança da Informação da Postal Saúde, em conformidade com a legislação existente sobre o tema; e

VIII. Revisar e propor a alteração de normas complementares e procedimentos internos de segurança da informação.

8.2.5. Equipe Técnica de Segurança da Informação:

I. Propor à GETEC manuais, normas internas e planos relativos à segurança da informação;

II. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Postal Saúde;

III. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

IV. Atuar na mitigação ou resolução dos incidentes, analisando-os criticamente, em conjunto com a GETEC e o Gestor de Segurança da Informação;

V. Manter comunicação efetiva com o Gestor de Segurança da Informação sobre assuntos relacionados ao tema segurança da informação que afetem ou tenham potencial para afetar a Operadora; e

VI. Buscar alinhamento das práticas de segurança da informação com as diretrizes corporativas da Postal Saúde.

DO COMPROMISSO E PENALIDADES

Capítulo 9 - DO COMPROMISSO E PENALIDADES

9.1. Todas as garantias necessárias ao cumprimento desta Política devem ser estabelecidas formalmente com os colaboradores da Postal Saúde, por meio de Termo de Compromisso constante de normativos sobre o tema.

9.2. O descumprimento desta Política é considerado infração disciplinar e poderá acarretar a aplicação de sanções previstas em regramentos corporativos e disposições contratuais.

DAS ATUALIZAÇÕES

10

Capítulo 10 - **DAS ATUALIZAÇÕES**

10.1. Fica estabelecida a periodicidade de um ano para a revisão desta Política, sendo encaminhada ao CODEL, via relatório técnico, suas possíveis alterações ou ausência delas, no contexto da Segurança da Informação para aprovação.

10.2. Esta Política de Segurança da Informação, juntamente com o Código de Conduta Ética e de Integridade, com a Política de Pessoal, a Política de Privacidade e Proteção de Dados, o Manual Disciplinar, e outros, compõe o conjunto de normativos da Postal Saúde que tratam de atitudes e comportamentos exigidos dos colaboradores, devendo ser rigorosamente observados.

DAS DISPOSIÇÕES FINAIS

11

Capítulo 11 - **DAS DISPOSIÇÕES FINAIS**

11.1. O conteúdo desta Política é amplo e regularmente atualizado e divulgado. A releitura desta Política, mesmo que não seja diretamente solicitada, deverá ser feita periodicamente para integral compreensão.

DOCUMENTOS ASSOCIADOS

DOS DOCUMENTOS EXTERNOS

ABNT NBR ISO/IEC 17788:2016 Tecnologia da Informação – Computação em nuvem – Visão Geral e vocabulário;

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;

Decreto nº 9.637/18 - Política Nacional de Segurança da Informação;

Instrução Normativa nº ½020 – GSI-PR;

Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD); e

Lei 9.609/98 – Lei do Software.

DOS DOCUMENTOS INTERNOS

Código de Conduta Ética e Integridade;

Estatuto Social; e

Regimentos Internos dos órgãos de governança.

Postal Saúde
Sua vida, nossa existência

Caixa de Assistência e Saúde dos Empregados dos Correios

SBN, Quadra 1, Bloco F - 5º e 6º andares, Edifício Palácio da Agricultura

Asa Norte - Brasília/DF

CEP: 70040-908

ANS - nº 41913-3

www.**postalsaude**.com.br