PSI- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DIRETRIZES E NORMAS ADMINISTRATIVAS

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

FUNDAÇÃO REGIONAL DE SAÚDE - FUNSAÚDE

DIRETORIA EXECUTIVA

Manoel Pedro Guedes Guimarães

Diretor-Presidente

André Luis Coutinho de Araújo Macêdo

Diretor de Atenção à Saúde

Melissa Soares Medeiros

Diretora de Pesquisa, Negócios e Inovação Tecnológica

Yara Ribeiro de Senna Souza

Diretora de Gestão e Desenvolvimento de Pessoas

Iluska de Alencar Salgado Barbosa

Diretor Administrativo-Financeiro

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

1. LISTA DE ABREVIATURAS E SIGLAS

CGSI - Comitê Gestor de Segurança da Informação
DDOS - Distributed Denial of Service (também conhecido como ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores.
HD – Disco Rígido
LGPD – Lei Geral de Proteção de Dados
P2P - Peer to Peer (O serviço P2P cria uma rede virtual entre as máquinas conectadas no momento e vasculha o HD do usuário atrás da música, vídeo ou qualquer outro documento que a pessoa esteja baixando.)
PSI – Política de Segurança da Informação
SI – Segurança da Informação
TI – Tecnologia da Informação
TIC – Tecnologia da Informação e Comunicação
VPN – acrônimo de Rede Privada Virtual (Virtual Private Network)

2. INTRODUÇÃO

2.1. A informação consiste em um dos bens mais valiosos de uma organização, por isso precisa ser bem protegida. Afinal, é por meio do uso de informações que decisões estratégicas podem ser tomadas dentro de uma instituição. Assim, a adoção de uma Política de Segurança da Informação – PSI no âmbito das atividades da Funsaúde torna-se essencial para assegurar que os dados sejam tratados conforme os preceitos legais assegurando assim, efetividade, lisura e *compliance* para a atuação da Funsaúde.
2.2. Os procedimentos, regras e normas devem ser cumpridos por todos que atuam na fundação, independente do cargo que exerçam.
2.3. Toda e qualquer ação que venha a comprometer efetividade, lisura e *compliance* atentará contra os valores definidos na Funsaúde, bem como violando o Código de Conduta, Ética e Integridade da Instituição.
2.4. As diretrizes estabelecidas nesta Política devem estar alinhadas ao Planejamento Estratégico, ao Plano Diretor de TI, ao Manual de Padronização de documentos e atos oficiais da Funsaúde, à Lei Geral de Proteção de Dados (Lei n° 13.709/2018), à Política de Segurança da Informação do Estado do Ceará (Decreto n° 29.227/2008) e em consonância com os valores institucionais.
2.5. Integram também a PSI as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

3. OBJETIVO GERAL

3.1. Orientar a utilização das Tecnologias de Informação e Comunicação – TICs, estabelecendo diretrizes e normas gerais para a gestão da segurança da informação, autenticidade dos dados, sistemas, documentos, correspondências, publicações e comunicações de maneira a preservá-las quanto à integridade, confidencialidade e disponibilidade. Este documento descreve procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas, vulnerabilidades e acessos não autorizados, preservando assim a imagem institucional da Funsaúde.

4. OBJETIVOS ESPECÍFICOS

4.1.Estabelecer diretrizes estratégicas, responsabilidades, competências, normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, sistemas, documentos, correspondências e publicações, bem como seus repositórios ou meios de armazenamento, reconhecidamente necessários ao desempenho das atribuições da instituição, contra ameaças que possam comprometer seus ativos ou sua imagem institucional.
4.2.Garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações processadas pela organização. Estes aspectos estão intimamente relacionados ao controle de acesso.

5. CONCEITOS E DEFINIÇÕES

5.1. **Acesso** – ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
5.2. **Agentes públicos –** os colaboradores a serviço da Funsaúde ou profissionais com outras relações laborais em instituições com vínculo com a Funsaúde.
5.3. **Assinatura eletrônica** – nome dado aos mecanismos que permitem a assinatura de documentos virtuais com validade jurídica. A legislação brasileira disciplinou a assinatura eletrônica, de forma ampla, através da Medida Provisória 2002-2/2001;
5.4. Ataque – ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível;
5.5. Ativo – qualquer coisa que tenha valor para a organização [ISSO/IEC 13335-1:2004];
5.6.**Ativos de Informação** – bases de dados e arquivo, contratos e acordos, documentação de sistemas, informações sobre pesquisas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas [ISSO/IEC 13335-1: 2004];
5.7. **Ativos de Software** – aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

5.8. Ativos físicos – equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
5.9. Ativos Serviços – serviços de computação e comunicações, utilidades gerais, por exemplo: aquecimento, iluminação, eletricidade e refrigeração. **5.10. Auditoria** – processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;
5.11. Autenticação – processo que busca verificar a identidade digital de uma entidade de um sistema no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;
5.12. Banco de dados – coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam de forma a criar algum sentido (informação) e dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;
5.13. Banco de Dados Pessoais – conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
5.14. Bloqueio – suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
5.15. Bloqueio de acesso – processo que tem por finalidade suspender temporariamente o acesso;
5.16. **Classificação da Informação:**
5.16.1. Confidenciais – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar ao desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante os usuários externos;
5.16.2. Internas – informações de caráter setorial pertencentes a um órgão. O acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;
5.16.3. Secretas – informação crítica para as atividades da Funsaúde, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital;
5.16.4. Públicas – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da Funsaúde, e cuja integridade não é vital.
5.17. **Comitê Gestor de Segurança da Informação – CGSI** – grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Estadual;
5.18. **Conformidade em Segurança da Informação e Comunicações** – cumprimento das legislações, normas e procedimentos relacionados à SI da organização;
5.19. Controles de Segurança – medidas adotadas para evitar ou diminuir o risco de um ataque;
5.20. Dado Pessoal – informação relacionada a pessoa natural identificada ou identificável;

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

5.21. Dado Pessoal Sensível – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
5.22. Dispositivos móveis – equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, drives USB, HD / SSD externo, e cartões de memória;
5.23. Documento – unidade de registro de informações, qualquer que seja o suporte ou o formato;
5.24. **Documentos Classificados** – documentos que contenham informação classificada em qualquer grau de sigilo;
5.25. **Documentos controlados** – documentos que contenham informação classificada em qualquer grau de sigilo e que, a critério da autoridade classificadora, requerem medidas adicionais de controle;
5.26. E-mail – acrônimo de electronic mail (correio eletrônico);
5.27. Firewall - Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
5.28. Gestão de Segurança da Informação – ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;
5.29. Incidente – eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
5.30. Informação – dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
5.31. Intranet – rede privada, acessível apenas aos membros da organização que atende. Utiliza os mesmos recursos e protocolos da Internet, mas é comumente separada desta através de firewalls;
5.32. **Medidas de Segurança** – medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;
5.33. Mirror – Uma cópia exata de um conjunto de dados;
5.34. Níveis de Segurança – especificam quanto de cada recurso ou sistema o usuário pode utilizar;
5.35. **PDTI Funsaúde**: Plano Diretor de Tecnologia da Informação e Comunicações da Funsaúde;
5.36. **Perfil de Acesso** – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
5.37. Phishing – ataque virtual que usa um e-mail, um site malicioso ou um perfil em rede social (Facebook, Twitter, Youtube, Instagram, etc.) para fazer você clicar e, assim, dar acesso para a coleta de informações pessoais ou infecção de sua máquina por programas maliciosos.
5.38. Política de Segurança da Informação – PSI – instrumento que visa complementar a segurança da informação, assegurando assim, efetividade, lisura e compliance na atividade Funsaúde.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

5.39. Prestador de Serviço – pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;
5.40. Proxy - Um servidor proxy é uma ponte entre o usuário e o resto da internet. Normalmente, ao usar o navegador na internet, o usuário será conectado diretamente ao site acessado. Proxies comunicam-se com sites em nome do usuário.
5.41. Redes Sociais – estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

6. PRINCÍPIOS

6.1. As ações relacionadas à PSI na Funsaúde são norteadas pelos seguintes princípios:
6.1.1. **Autenticidade:** garantir a veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.
6.1.2. **Celeridade:** as ações de Segurança da Informação devem prover respostas tempestivas e eficientes a falhas de segurança.
6.1.3. **Confidencialidade:** garantir que a informação seja acessada somente por pessoas autorizadas.
6.1.4. **Disponibilidade:** garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
6.1.5. Ética: O valor institucional que busca promover os atos considerados os melhores e mais justos, sem distinção ou discriminação de qualquer natureza, com base nos princípios morais da Administração Pública.
6.1.6. Integridade: garantir a exatidão da informação e dos métodos de processamento, ou seja, de que a informação não foi modificada, alterada ou destruída sem autorização.
6.1.7. Impessoalidade: a PSI visará ao interesse público no tratamento das informações, buscando evitar que estas sejam utilizadas para finalidades particulares ou para a obtenção de benefícios pessoais;
6.1.8. Legalidade: levará em consideração as leis, as normas, instruções, procedimentos e as políticas administrativas, organizacionais, técnicas e operacionais formalmente estabelecidas pela Funsaúde;
6.1.9. Moralidade: a elaboração da PSI, bem como sua posterior aplicação, deverá observar os preceitos da boa administração pública, pautando-se pela atuação ética e nos ideais de honestidade e justiça;
6.1.10. Privacidade: os dados pessoais de pessoas naturais, quando tratados pela Funsaúde no âmbito de suas atividades, devem estar consoantes com o interesse público ou com o consentimento do titular para assegurar-lhe a inviolabilidade da intimidade, da honra e da imagem.
6.1.11. Proporcionalidade: a aplicação da PSI, no que abrange o nível, a complexidade e o custo das ações deverá ser adequada ao entendimento administrativo e aos valores dos ativos a serem protegidos;
6.1.12. Publicidade: as diretrizes, normas e procedimentos da PSI definidos pela Funsaúde devem ser publicados e amplamente divulgados para o balizamento dos agentes públicos no pleno desempenho de suas atribuições;
6.1.13. Responsabilidade: a PSI deverá ser seguida pelos agentes públicos no exercício de suas atividades, pautando-se por atitudes e comportamentos condizentes com as diretrizes, normas e procedimentos de Segurança da Informação.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

7. ABRANGÊNCIA

7.1. A Política de Segurança da Informação – PSI aplica-se a todos os agentes públicos da Fundação Regional de Saúde, desde a Sede até seus equipamentos de saúde (diretores, gestores, funcionários públicos, terceirizados, estagiários, prestadores de serviços e consultores fixos ou temporários, bem como aos demais terceirizados, membros que necessitam usar a rede da Funsaúde).

8. DEVERES E RESPONSABILIDADES

8.1. Comitê Gestor de Segurança da Informação (CGSI)

8.1.1. Responsável pela publicação e atualizações da Política de Segurança da Informação – PSI;
8.1.2. Analisa e aprova tecnologias e processos inseridos no negócio;
8.1.3. Aprova as iniciativas para aumentar o nível de segurança no âmbito da Funsaúde;
8.1.4. Responsável pela orientação, supervisão e decisão referente a Política de Segurança da Informação e seus instrumentos;
8.1.5. Analisa e monitora os incidentes de Segurança da Informação;
8.1.6. Dissemina a cultura e a Política de Segurança da Informação;
8.1.7. Promove a elaboração e implantação de planos de contingência e recuperação de desastres;
8.1.8. Delibera sobre as questões que lhe tenham sido encaminhadas.

8.2. Coordenação de TI e Infraestrutura de Informática

8.2.1. Responsável pela gestão, coordenação e execução das ações relativas à segurança da informação e tratamento de incidentes de segurança da informação;
8.2.2. Cuida da integridade, confidencialidade e disponibilidade dos ativos de informação do órgão, devendo ser comunicadas quaisquer irregularidades, falhas ou desvios identificados à sua chefia imediata, assim como a área responsável pela segurança da informação;
8.2.3. Verifica periodicamente a conta *postmaster*, para detectar eventuais problemas que possam estar ocorrendo no servidor e na entrega de e-mail dos usuários;
8.2.4. Implementa o papel de moderador nas listas, com o objetivo de evitar *spams*.

8.3. Usuário

8.3.1. Zela pelo fiel cumprimento das normas e políticas estabelecidas neste documento;
8.3.2. Efetuar *logoff* ou bloqueio da tela ao afastar-se da estação de trabalho;
8.3.3. Utiliza adequadamente os equipamentos da Funsaúde, evitando acessos indevidos aos ambientes computacionais aos quais está habilitado, que possam comprometer a segurança das informações;
8.3.4. Busca orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
8.3.5. Notifica a gestão imediata, a Coordenação de TI e Infraestrutura ou o Comitê Gestor de Segurança da Informação (CGSI) de possível indício ou falha na Segurança da Informação;

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

8.3.6. Observa rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade da senha, realizando:
8.3.6.1. Substituição da senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível;
8.3.6.2. Não divulgar senha para outras pessoas e/ou reprodução em papéis ou em outros instrumentos passíveis de serem perdidos;
8.3.6.3. De maneira alguma ou sobre qualquer pretexto, procura descobrir as senhas de outras pessoas.
8.3.7. Não divulgar fotos do ambiente de trabalho nas redes sociais ou em qualquer outro meio que possa publicizar dados sensíveis da Funsaúde ou que de alguma maneira possa abalar a imagem das pessoas.
8.3.8. Proteger os dados da Funsaúde especialmente os de pacientes e de seus trabalhadores em conformidade com Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e a Constituição Federal (art. 5°, inciso LXXIX).
8.3.9. Os usuários agentes públicos que têm como atribuição o desenvolvimento de softwares para a Funsaúde deverão atentar aos requisitos previstos em seu contrato de trabalho, termos de cessão de propriedade ou documento similar.

8.4. Diretores e chefes de equipe
8.4.1. Os diretores e chefes de equipe devem cumprir e garantir que seus colaboradores cumpram as diretrizes nesta política estabelecidas;
8.4.2. Os diretores e chefes de equipe são responsáveis pelas definições dos direitos de acesso de seus colaboradores aos sistemas e informações da Fundação, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais. O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:
8.4.2.1. Que tipo de informação o usuário pode acessar;
8.4.2.2. Quem está autorizado a acessar determinada rotina e/ou informação;
8.4.2.3. Quem acessou determinada rotina e informação;
8.4.2.4. Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
8.4.2.5. Que informação ou rotina determinadas usuário acessou;
8.4.2.6. Quem tentou acessar qualquer rotina ou informação sem estar autorizado.
8.4.3. Dar causa a possível processo administrativo de apuração responsabilidade de usuário que infrinja os parâmetros estabelecidos nesta Política.

9. DIRETRIZES GERAIS

9.1. As diretrizes de Segurança da Informação estabelecidas nesta PSI aplicam-se às informações armazenadas, acessadas, produzidas, compartilhadas e transmitidas pela Funsaúde e devem ser seguidas pelos usuários em conformidade com os princípios neste documento estabelecidos.
9.2. As diretrizes desta PSI constituem os principais pilares da Segurança da Informação da Funsaúde, sendo norteadora da elaboração de normas relativas.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10. DIRETRIZES ESPECÍFICAS

10.1. Contratos, Convênios e Congêneres:

10.1.1. Todos os contratos celebrados pela Funsaúde com prestadores de serviços devem conter cláusulas que determinem a observância da PSI e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência. Os prestadores de serviços sob contrato com a Funsaúde serão obrigados a assinar Termo de Aceitação, em obediência ao estabelecido na PSI e LGPD.

10.1.2. Nos contratos de serviços relacionados ao provimento, gerenciamento e suporte da infraestrutura computacional de TI, deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de Segurança da Informação por parte do prestador.

10.1.3. Em relação aos contratos mencionados, cabe à Coordenação de TI e Infraestrutura de Informática supervisionar o tratamento de incidentes de Segurança da Informação para o fiel cumprimento das suas atribuições.

10.2. Abertura de Chamados de TI:

10.2.1. As aberturas de chamado para a área de Tecnologia da Informação deverão estar registradas no sistema de abertura de chamados no endereço: http://servicedesk.funsaude.ce.gov.br

10.2.2. Exclusivamente, em caso de indisponibilidade do sistema, a solicitação deverá ser feita através de e-mail institucional para o endereço servicedesk@funsaude.ce.gov.br

10.2.2.1. Caso o sistema esteja disponível e a solicitação ocorra via e-mail, a área de Tecnologia da Informação não se obriga a atendê-la.

10.2.3. A solicitação deve conter informações detalhadas do problema detectado inclusive, telas de erro e número de tombo do equipamento (dependendo da situação);

10.2.4. O técnico ao qual o atendimento for atribuído, ficará responsável pelo andamento e resolução do problema. A comunicação entre técnico e usuário será via sistema e notificações por e-mail, ficando assim registrado o histórico da comunicação.

10.3. Empréstimo de Notebook, Projetor e Webcam:

10.3.1. Todas as solicitações de empréstimo de *notebook*, projetor e *webcam* devem seguir os procedimentos abaixo relacionados:

10.3.2. Registro em sistema de abertura de chamados da Funsaúde;

10.3.3. Os equipamentos devem ser solicitados com no mínimo 24 (vinte e quatro) horas úteis de antecedência, para que seja possível verificar a disponibilidade/agenda, bem como proceder com as configurações necessárias para o equipamento;

10.3.4. Todas as solicitações precisam conter: justificativa, data inicial, data final, horário e local;

10.3.5. O solicitante ficará responsável pelo (s) equipamento (s).

[1] Os e-mails criados para acesso aos Drives deverão estar vinculados ao seguinte endereço de e-mail ti@funsaude.ce.gov.br para resgate de senha.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10.3.6. Após a utilização do equipamento, o responsável deverá entrar em contato com a Coordenação de TI e Infraestrutura de Informática, para que seja feita a conferência e o recolhimento de todos os equipamentos e a solicitação seja finalizada no sistema de chamados com a emissão da OS pelo sistema de chamados, que deve conter a assinatura do técnico designado para o recolhimento do (s) equipamento (s), bem como a assinatura do solicitante pelo empréstimo.

10.4. Solicitações de Novos Computadores:

10.4.1. Todas as solicitações de novos computadores devem seguir os procedimentos relacionados abaixo:

10.4.2. As solicitações devem ser realizadas por meio de sistema de abertura de chamados contendo: justificativa, setor para instalação e usuário que utilizará a máquina;

10.4.3. A solicitação será registrada no sistema de chamados para análise e possível aprovação mediante disponibilidade de equipamento;

10.4.4. Os computadores só serão liberados para uso, após a realização das configurações e instalação padrão de programas e softwares necessários para o adequado funcionamento.

10.5. Solicitações de Mudança de Computadores e Impressoras:

10.5.1. Todas as solicitações de mudança de computadores e impressoras devem seguir os procedimentos relacionados abaixo:

10.5.2. As solicitações devem ser registradas em sistema de abertura de chamado, informando: justificativa, tombamento da máquina, setor de origem e destino;

10.5.3. Mudanças e transferências só serão realizadas após a análise do ambiente, onde serão verificadas as instalações elétricas, cabeamento de rede e outros pontos essenciais para a instalação do equipamento;

10.5.4. Não será permitida a transferência de computadores de um setor para outro, mesmo quando da transferência de um colaborador para outro setor visto que, cada departamento tem seus equipamentos, no entanto, caso não haja uma alternativa, a transferência só será realizada mediante solicitação do Gestor imediato do setor de origem à Coordenação de TI e Infraestrutura.

10.6. Acesso à Rede / E-Mail / Internet / Intranet/ Compartilhamentos / Sistemas:

10.6.1. As solicitações de acesso à rede / e-mail / internet/ intranet / compartilhamentos / sistemas visam permitir, aos usuários autorizados, a concessão de uso de um serviço e bloquear/excluir acesso a usuários não autorizados.

10.6.2. As permissões de acesso devem ser concedidas de acordo com as atribuições dos usuários, sempre por necessidade de trabalho;

10.6.3. O usuário deverá ser somente de pessoa física, sendo vetado outros tipos como: setoriais, sistemas, numéricas, entre outras;

10.6.4. O gestor do funcionário deverá solicitar o acesso à Coordenadoria de Tecnologia da Informação e Infraestrutura por meio do sistema de abertura de chamados;

10.6.5. A Coordenadoria concederá o (s) acesso (s) e informará ao interessado e/ou gestor imediato, via sistema de suporte: o login, senha provisória e a Política de Segurança da Informação da Funsaúde;

10.6.6. A senha padrão fornecida, deverá ser alterada obrigatoriamente no primeiro acesso, por uma senha de escolha do usuário, seguindo as políticas de troca de senha.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

A nova senha será confidencial, pessoal e intransferível, não podendo ser compartilhada com qualquer pessoa, mesmo que seja do próprio departamento.

10.6.7. Os usuários são responsáveis pelos seus acessos, devendo zelar pela gestão de guarda de seu usuário e senha.

10.6.8. Quando da AUSÊNCIA (férias ou licença) (se aplicável), MUDANÇA DE SETOR ou DESLIGAMENTO do colaborador, o DP (responsável pelo contrato do colaborador) deverá comunicar formalmente à Coordenação de TI e Infraestrutura de Informática, via sistema de suporte, para que seja adotado o procedimento de bloqueio/ remanejamento ou exclusão dos acessos do colaborador.

10.6.9. As redefinições de senha de colaborador, deverão ser realizadas pelos próprios usuários, sendo solicitadas algumas informações pessoais, ou pelo gestor imediato via chamado sempre que necessário.

10.7. O Uso de Senhas:

10.7.1. Toda conta de usuário precisa possuir senha e deve seguir os padrões estabelecidos nesta Política;

10.7.1.1. Não utilizar para criação de senhas: o mesmo nome do usuário (ex: usuário: maria, senha: maria), o nome ou combinações destes nomes de familiares, datas de aniversário, número de telefone, informações pessoais ou fáceis de serem obtidas;

10.7.1.2. Utilizar para criação de senhas: Tamanho mínimo de senha de 8 ou mais caracteres, número mínimo de caracteres maiúsculos: 1, número mínimo de caracteres especiais: 1 (Tipo: ", ', !, @, #, $, %, &, *, (,),-, _, <, >, :, ;, {, }, [,], /, ?, +, =, §), número mínimo de caracteres numéricos: 2

10.7.1.3. Não registrar a senha em papel, em local visível, no computador ou na Internet;

10.7.1.4. Não revelar senhas em questionários ou formulários;

10.7.1.5. Não revelar senhas para colegas de trabalho enquanto estiver de férias ou licença.

10.8. O Uso/Gestão de Ativos Físicos e da Informação:

10.8.1. O uso/gestão de ativos físicos e da informação seguirão as seguintes regras:

10.8.2. Todos os ativos físicos devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos;

10.8.3. O acesso ao ativo da informação não gera direito real sobre o mesmo e nem sobre os frutos de sua utilização;

10.8.4. Todos os setores possuem estações de trabalho para uso individual e/ou coletivo, tendo cada funcionário acesso por meio de *login* com usuário e senha individuais, portanto tudo o que for manipulado/executado na estação de trabalho fica sob a responsabilidade do usuário que autenticou o acesso;

10.8.5. Não é permitido realizar *login* em mais de uma máquina, ou seja, não é permitido login simultâneo em diferentes máquinas salvo, para os técnicos da TI quando estiverem prestando suporte remoto ou por outras pessoas;

10.8.6. Os ativos de informação da Fundação devem ser protegidos contra ações indevidas intencionais ou acidentais que impliquem perda, destruição, inserção, cópia, extração, alteração, uso e exposição indevidos, em conformidade com os princípios da confidencialidade, integridade e disponibilidade;

10.8.7. Não é permitida a instalação de nenhum tipo de *software/hardware* sem autorização/supervisão da Coordenação de TI e Infraestrutura de Informática da Funsaúde;

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10.8.8. No ambiente informatizado, devem ser utilizados e instalados somente *softwares* homologados, originais e devidamente licenciados;

10.8.9. Os computadores, *notebooks* e servidores são equipamentos fornecidos pela Funsaúde e devem ser utilizados para assuntos relativos ao trabalho da instituição, portanto, não é permitida gravação/armazenamento de quaisquer arquivos de ordem pessoal, exemplos: áudio, vídeo, imagem, documento;

10.8.10. Todos os dados/arquivos relativos à Fundação devem ser mantidos no servidor de arquivos, que conta com *backup* diário e confiável;

10.8.11. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Fundação é considerada de sua propriedade, não podendo ser compartilhada nem divulgada sem autorização de acordo com as diretrizes de que trata este documento;

10.8.12. Arquivos não corporativos (pessoais), ou que não estejam salvos no servidor de arquivos da Fundação, são de responsabilidade do usuário e não serão realizados *backups* ou qualquer tipo de recuperação em caso de defeito na máquina utilizada ou problema na unidade de armazenamento;

10.8.13. Nos casos de realização de manutenção preventiva dos computadores e notebooks, o backup realizado será apenas dos arquivos de trabalho, os arquivos pessoais não são de responsabilidade da Coordenação de TI e Infraestrutura de Informática da Funsaúde;

10.8.14. Não será permitido ingresso/conexão de nenhum equipamento particular (seja este de colaboradores da Fundação ou qualquer outra pessoa) no domínio da Fundação para uso dos recursos computacionais, salvo para acesso ao *Wi-fi*, mediante login com usuário e senha de rede (para funcionários) ou emissão de *voucher* (para visitantes) que pode ser solicitado na Coordenação de TI e Infraestrutura de Informática da Funsaúde;

10.8.15. Os usuários temporários ou visitantes poderão acessar a rede móvel da Funsaúde específica para esta finalidade, qual seja a rede de visitantes.

10.8.16. Em nenhuma hipótese será liberada conexão de rede a cabo para visitantes.

10.8.17. É vedado aos agentes públicos a utilização de recursos de TICs da Funsaúde para acessar, transmitir, armazenar ou divulgar qualquer material relacionado à pornografia, racismo e xenofobia, pedofilia, assédio moral ou sexual, códigos maliciosos, misoginia, machismo ou androcentrismo, *spams,* programas de entretenimento, jogos ou qualquer outro que viole a legislação em vigor no país, o direito autoral, a propriedade intelectual, a ordem pública, bem como material de conteúdo político ou religioso; conforme o disposto no art. 15, inciso II, do Código de Conduta, Ética e Integridade da Funsaúde;**10.8.18. Inventário**

a) todos os ativos devem possuir um responsável (proprietário), formalmente designado, que fará a correta classificação e acompanhamento periódico dos ativos;

b) o inventário dos ativos deve conter as informações que ajudem a assegurar a sua proteção efetiva: nome do ativo, proprietário, custodiante, localização, cópia de segurança, criticidade dentre outras especificações.

c) a classificação quanto à criticidade obedecerá aos seguintes critérios:

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

●Muito alta **-** quando a interrupção do ativo provocar parada total das atividades.
●Alta - quando a interrupção do ativo provocar perda de mais de 70% das atividades.
●Média - quando a interrupção do ativo provocar perda entre 40 e 70% das atividades.
●Baixa **-** quando a interrupção do ativo provocar perdas abaixo de 40% das atividades.

d) Para todo ativo da Informação do Governo do Estado do Ceará deverá ser designado um proprietário;

10.8.17. Toda informação produzida e armazenada pela Funsaúde, conforme a Política de Segurança da Informação do Governo do Estado do Ceará, deverá receber um nível adequado de proteção, considerando a sua confidencialidade, integridade e disponibilidade, bem como qualquer outro requisito que seja considerado;

10.8.18. Toda informação deverá ser classificada para indicar a sua criticidade, requisitos legais e sensibilidade;

10.8.19. A classificação quanto ao sigilo obedecerá aos seguintes critérios:

● Confidenciais **-** informação restrita aos limites da empresa, cuja divulgação ou perda pode levar ao desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante os usuários externos;

● Internas **-** informações de caráter setorial pertencentes a um órgão. O acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;

● Secretas **-** informação crítica para as atividades da Funsaúde, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital;

● Públicas - informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da Funsaúde, e cuja integridade não é vital.

10.8.20. A classificação quanto à criticidade obedecerá aos seguintes critérios:

● Muito alta - quando a interrupção do ativo provocar parada total das atividades;
● Alta - quando a interrupção do ativo provocar perda de mais de 70% das atividades;
● Média - quando a interrupção do ativo provocar perdas entre 40 e 70% das atividades;
● Baixa - quando a interrupção do ativo provocar perdas abaixo de 40% das atividades.

10.8.21. A troca de informações, *softwares* e sistemas entre órgãos do Governo do Estado do Ceará e entidades externas deverão ser realizadas de maneira formal.

10.8.22. Se algum usuário souber sobre qualquer violação a esta norma deverá comunicar ao Setor competente de TIC, a sua chefia imediata ou ao Comitê Gestor de Segurança da Informação (CGSI).

10.9. Uso de e-mail Institucional:

10.9.1. Os usuários que se utilizarem de e-mail institucional deverão fazê-lo no estrito interesse da instituição, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público;

10.9.2. O correio eletrônico é um instrumento de comunicação institucional, devendo ser usado exclusivamente para envio/recebimento de mensagens relativas à atividade da Fundação, seja para usuários internos ou para pessoas/organizações em endereços externos;

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10.9.3. Não é permitido o uso da correspondência eletrônica institucional para a administração de contas pessoais em mídias sociais;
10.9.4. As mensagens do correio eletrônico devem ser escritas em linguagem profissional e que não comprometa a imagem, nem os princípios éticos da Fundação;
10.9.5. O usuário da conta de e-mail é o responsável pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico, cabendo a ele todas as responsabilidades;
10.9.6. O conteúdo do correio eletrônico de cada usuário, pode ser acessado pela Coordenação de TI e Infraestrutura da Informação quando em situações que ponham em risco à imagem, o seu negócio e/ou a segurança da Fundação.
10.9.7. Este acesso será feito a critério da Coordenação, mediante comunicação ao superior imediato do usuário, devendo ser registrado formalmente permitindo auditoria desse procedimento. Procedimentos desse tipo são para evitar ataques de *phishing, spam's, DDOS*, ataques em massa e similares;
10.9.8. Os usuários deverão adotar o hábito de leitura diária dos e-mails;
10.9.9. Não acessar, quando não autorizado, a caixa postal de outro usuário e ao Banco de Dados do Correio Eletrônico de outro Órgão;
10.9.10. Contas com inatividade por um período igual ou superior a 60 (noventa) dias serão bloqueadas, pois caracterizam assim contas "inativas";
10.9.11. Os usuários não deverão enviar, armazenar ou manusear material que caracterize: corrente, promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas, assuntos de caráter obsceno ou pornográfico, preconceito a determinadas classes, como: sexo, raça, orientação sexual, idade, religião, política, nacionalidade ou deficiência física;
10.9.12. Os usuários não deverão abrir anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela Coordenação de TI e Infraestrutura de Informática, se não tiver certeza de que solicitou esse e-mail;
10.9.13. O (s) usuário(s) que estiver(em) utilizando conta de e-mail de forma inadequada (conforme política de e-mail) terá (ão) sua conta inicialmente bloqueada e será comunicado ao seu gestor imediato para tomada de medidas cabíveis;
10.9.14. Constatado o uso irregular dos recursos do E-mail institucional será realizado o cancelamento da caixa de correio eletrônico e serão aplicadas as penalidades, de acordo com a legislação vigente;
10.9.15. O usuário infrator deverá ser notificado e a ocorrência de transgressão comunicada ao seu chefe imediato e à diretoria correspondente;
10.9.16. As mensagens de correio eletrônico sempre deverão incluir assinatura com formato padrão da Funsaúde.
10.9.17. Os casos de afastamento do trabalho em virtude de férias, licenças e desligamentos deverão ser comunicados via e-mail à TI por meio do endereço eletrônico: ti@funsaude.ce.gov.br para que os devidos acessos sejam suspensos, nos dois primeiros casos, temporariamente. Os colaboradores deverão ser removidos dos grupos de WhatsApp institucionais durante seus períodos de afastamento.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10.10. Listas de Distribuição (e-mail)

10.10.1. Uma lista de distribuição se caracteriza pelo agrupamento de várias contas de e-mail em um único grupo, para que seja possível o envio em massa.

10.10.2. Para que seja criada uma lista de distribuição, esta deve conter no mínimo 05 (cinco) assinantes (contas de e-mail institucionais);

10.10.3. A criação do grupo de e-mail seguirá os padrões de utilização e solicitação de acesso das contas individuais de e-mail.

10.11. Uso de Internet

10.11.1. O acesso à Internet é uma concessão e não um direito. Portanto, a sua utilização deve ser para atividades inerentes aos trabalhos desenvolvidos. O acesso à Internet é feito unicamente pela conexão fornecida pela instituição, ficando proibida a utilização diferente.

10.11.2. O usuário é o responsável pelos acessos à Internet realizados pela sua conta;

10.11.3. O mau uso de uma conta de acesso à Internet por terceiros será responsabilidade de seu titular, sujeitando-o às penalidades cabíveis;

10.11.4. O ambiente de Internet disponibilizado para os usuários (independentemente de sua relação contratual) deve ser utilizado prioritariamente para o desempenho das atividades profissionais em benefício da Funsaúde. Sites que não contenham informações que agreguem conhecimento profissional devem ter seus acessos minimizados;

10.11.5. É vedado ao agente público prejudicar o rendimento no trabalho em razão do uso não apropriado de internet e mídias sociais;

10.11.6. Todas as contas de acesso à Internet terão uma titularidade, determinando a responsabilidade sobre a sua utilização;

10.11.7. É de interesse desta instituição que seus colaboradores estejam bem-informados, por isso, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos, nem implique em conflitos de interesse com os seus objetivos de negócio, portanto:

10.11.8. A utilização dos recursos com finalidade pessoal é permitida, desde que seja em um nível mínimo e que não viole as normas/políticas adotadas;

10.11.9. Todos os registros de acessos à Internet são passíveis de auditoria e serão monitorados por meio de ferramentas próprias quando necessário;

10.11.10. O usuário deve desconectar-se imediatamente de um site que contenha acesso restrito ou que contrarie a Política de Segurança da Informação, mesmo que tenha sido aceito pelos sistemas de bloqueio;

10.11.11. Não é permitido:

i) O uso de aplicativos e/ou ferramentas com a finalidade de burlar os mecanismos de segurança da Internet, tais como *firewall e proxy*

ii) Acesso à Internet para violar leis e regras brasileiras ou de qualquer outro país;

iii) Acessar sites de qualquer tipo de jogos, inclusive jogar pela Internet;

iv) Usar programas que implementem P2P, onde o computador do usuário atua como servidor;

v) Acesso *Web* rádio e *Web* TV (sessões de transmissão contínua de vídeo e áudio);

vi) Distribuir *software* ou conteúdo não autorizado (pirataria);

vii) Fazer *download* de programas não relacionados às atividades fins.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10.11.12. No caso de evidências de uso irregular dos recursos de acesso à Internet, o usuário terá seu acesso bloqueado para averiguação. Ao se constatar a irregularidade será realizado o cancelamento do acesso à Internet e serão aplicadas as penalidades, de acordo com a legislação vigente.

10.12. Tratamento de Dados Pessoais e Dados Pessoais Sensíveis

10.12.1. Os agentes públicos da Funsaúde, em conformidade com a Lei Geral de Proteção de Dados (LGPD), devem adotar as práticas necessárias para o tratamento adequado dos dados pessoais, sensíveis e sigilosos utilizados na condução das atividades da instituição.

10.12.2. Os agentes públicos deverão efetuar o tratamento dos dados pessoais com boa-fé, sendo acessados ou tratados somente para a realização de tarefas da Funsaúde, devendo ser observada a finalidade a qual se destina o uso de tais informações.

10.12.3. Os agentes públicos somente poderão compartilhar dados pessoais ou sensíveis com terceiros quando houver previsão legal, cabendo-lhes certificar-se de que foram adotados todos os parâmetros definidos na LGPD.

10.13. Acesso Remoto

10.13.1. Esta política define requisitos e regras de segurança para acesso remoto (ANEXO II) às estações de trabalho e servidores que compõem o ambiente tecnológico da Funsaúde e se aplica a todos os agentes públicos ou indivíduos que direta ou indiretamente utilizam ou dão suporte aos sistemas, portanto:

10.13.2. As solicitações de acesso remoto de uma rede externa às estações de trabalho e servidores da Funsaúde devem ser realizadas através do sistema de abertura de chamados contendo justificativa, período de trabalho e autorizado pelo gestor da área;

10.13.3. Os usuários autorizados ao acesso remoto, devem proteger suas credenciais e em nenhum momento devem disponibilizar seu login ou qualquer informação de acesso, para terceiros, garantindo a não utilização do seu perfil de acesso remoto por outras pessoas.

10.14. Serviço de Backup

10.14.1. Define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução. Todos os trabalhos e documentos em geral do órgão, devem ser salvos no servidor de arquivos e nunca no disco local do equipamento, para que as cópias de backup possam ser realizadas;

10.14.2. Evitar nomes extensos para arquivos e pastas (abreviar palavras quando possível). Evitar também acentuação, caracteres especiais e se possível, substituir os espaços em branco por "_" (underline). Usando essas regras, o backup e a restauração dos arquivos são mais rápidos. Exemplo de nome de arquivo: rotina_backup_arq.doc;

10.14.3. O tempo mínimo para restauração de um arquivo do backup é de 8 (oito) horas, contados a partir da atribuição do chamado. O chamado deve conter o caminho completo do arquivo, o nome do arquivo com extensão e a data da última vez que ele foi acessado;

10.14.4. Todos os backups devem ser automatizados por sistemas de agendamento, para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática;

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

10.14.5. Procedimentos de backup diários e semanais íntegros de forma que a recuperação dos dados possa ser realizada de forma segura e em qualquer momento;
10.14.6. O período de retenção das cópias de segurança deve ser acordado com a Coordenadoria de TI e Infraestrutura respeitados os preceitos legais para o tipo de dado envolvido.

11. SANÇÕES

11.1. Ações que violem a Política de Segurança da Informação – PSI ou que quebrem os controles de segurança da informação serão devidamente apuradas e notificadas. O Comitê Gestor de Segurança da Informação poderá atuar na apuração juntamente com as demais áreas envolvidas.
11.2. A ocorrência de transgressão será comunicada ao gestor imediato e/ou à coordenadoria correspondente, e aos responsáveis serão aplicadas as sanções administrativas, civis e penais em vigor, já que o usuário é responsável por qualquer atividade a partir de sua conta. O mesmo responderá por qualquer ação legal apresentada à Funsaúde.

12. CONSIDERAÇÕES FINAIS

12.1. Os colaboradores da Funsaúde devem declarar o seu conhecimento e comprometimento com a Política de Segurança da Informação, através da assinatura de um **TERMO DE COMPROMISSO** (ANEXO III).
12.2. O descumprimento das disposições constantes neste documento e demais diretrizes de segurança da informação caracteriza infração funcional em conformidade com as normas de Gestão de Pessoal da Funsaúde violando o Código de Conduta, Ética e Integridade da Funsaúde.
12.3. A PSI será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.
12.4. Os casos omissos e as dúvidas decorrentes da aplicação desta PSI devem ser geridos pelo Comitê Gestor de Segurança da Informação – CGSI.

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

13. REFERÊNCIAS

13.1. Código de Conduta, Ética e Integridade da Funsaúde;
13.2. [ISO/IEC 13335-1:2004];
13.3. Lei Geral de Proteção de Dados Lei n° 13.709/2018;
13.4. Planejamento Estratégico da Funsaúde;
13.5. Política de Segurança da Informação dos Ambientes de TIC do Governo do Estado do Ceará

14. HISTÓRICO DE REVISÃO

VERSÃO	DATA	DESCRIÇÃO DA ALTERAÇÃO	REVISADO POR:
02	05/08/2022	Inserção de cláusula de desativamento de email e whatsapp institucional durante afastamento temporário	Manoela Fleck de Paula Pessoa

ELABORAÇÃO		
Dieison Roberto Vieira Rabelo Manoela Fleck de Paula Pessoa Rochelle Gonçalves de Souza	**Data:** 01/03/2022	**Assinaturas:**
REVISÃO		
Unidade de Planejamento e Gestão da Informação Unidade de Conformidade e Gestão de Riscos Coordenação de Inovação Tecnológica	**Data:** 19/05/2022	**Assinaturas:**
APROVAÇÃO		
Diretoria Executiva	**Data: 05/09/2022**	**Assinaturas:**

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

ANEXO I

Internet (*Wi-fi* ou Cabeada)

Todos os usuários da Fundação Regional de Saúde já possuem por padrão acesso à Internet, tanto na rede *Wi-fi* como na rede cabeada (GR_FW_RESTRITO), que deve ser autenticada no dispositivo/ equipamento com seu *login* e senha de rede.

Caso haja necessidade de um acesso mais amplo, é necessário que o gestor imediato formalize a solicitação seguindo as orientações da Política de Segurança da Informação (PSI).

Grupos de Internet:

GR_FW_RESTRITO – Acesso Restrito (sites governamentais);

GG_FW_PADRAO – Acesso Default (sites governamentais, bancários, sites de buscas,jornais);

GG_FW_INTERMEDIARIO – Acesso Intermediário (GR01 + web chat (whatsapp/Telegram) e

GG_FW_FULL – Acesso Full (GR02 + Redes Sociais e Stream de Vídeo).

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

ANEXO II

ACESSO REMOTO (Interno e Externo)

Os programas utilizados para acesso remoto:

- Internamente: VNC SERVER, SSH ou RDP

- Externamente: SSL_VPN (via cliente vpn)

ANEXO III

FUNDAÇÃO REGIONAL DE SAÚDE – SEDE			
Tipo de Documento:	**POLÍTICA**	PO.DIGER-SEDE.001 Páginas: 1/20	
Origem do documento:	**DIRETORIA GERAL**	Classificação: Público	Emissão: 19/05 /2022
Título do Documento:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**	Versão: 02	Próxima revisão: 19/ 05/2023

TERMO DE COMPROMISSO

NOME:	
DATA: / /	**SETOR:**
TELEFONE:	**CPF:**

Comprometo-me a:

- Conhecer e cumprir fielmente à Política de Segurança da Informação;
- Responder por toda atividade executada por meio de minha identificação;
- Utilizar adequadamente os equipamentos, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações desta instituição;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados;
- Notificar a gestão imediata ou a Coordenadoria de TI e Infraestrutura indício ou falha na Segurança da Informação;

1. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade da minha senha de acordo com os itens abaixo:

    - Substituir a senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível;Não divulgar a minha senha para terceiros e nunca escrever a minha senha, sempre memorizá-la;

    - De maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outras pessoas.

Assinatura: _____