POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA REDE EBSERH

Versão 2.0

® 2022, Ebserh. Todos os direitos reservados
Empresa Brasileira de Serviços Hospitalares – Ebserh
www.ebserh.gov.br

Material produzido pela Diretoria de Tecnologia da Informação e pelo Comitê de Segurança da Informação da Administração Central - Ebserh.
Permitida a reprodução parcial ou total, desde que indicada a fonte e sem fins comerciais.

Empresa Brasileira de Serviços Hospitalares – Ministério da Educação

Política de Segurança da Informação da Ebserh – Coordenado pelo Comitê de Segurança da Informação da Administração Central – Brasília: EBSERH – Empresa Brasileira de Serviços Hospitalares, 2022. 22p.

Palavras-chaves: 1 – Segurança da Informação; 2 – Tecnologia da Informação; 3 – Política

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES – EBSERH

Administração Central
Setor Comercial Sul - SCS, Quadra 09, Lote C, Ed. Parque Cidade Corporate,
Torre C, 1º ao 3º pavimento | CEP: 70308-200 | Brasília-DF |
Telefone: (61) 3255-8900 | Site: www.ebserh.gov.br

OSWALDO DE JESUS FERREIRA
Presidente

ANTONIO CESAR ALVES ROCHA
Vice-Presidente

SIMONE HENRIQUETA COSSETIN SCHOLZE
Diretora de Tecnologia da Informação

LEANDRO AMBRÓSIO COSTA
Gestor da Segurança da Informação da Administração Central

Comitê de Segurança da Informação da Administração Central – Composição 2021

Abilio da Cruz Ramos Neto; Adriana Martinelli Martins; Diego Leitao de Barros Falcao; Eduardo Ferreira de Sousa; Einstein da Silva Gomes de Lima; Eliane Cunha Marques; Fabiano Francisco Noetzold Saldanha; Fabio Campelo Santos da Fonseca Ribeiro; Francisco Italo Lopes França; Guilherme Campos Fonseca; Gustavo Tibau do Espirito Santo Alves; Joel de Sousa Ribeiro de Melo; Leonardo Fernandez Zago; Luiz Carlos Perluci Junior; Maria Rachel De Castro; Michele Cardoso da Silva; Paula Medeiros Rodolpho; Rafael Ribeiro Faim; Savana Karoline Farias Dantas e Wagner Santana.

HISTÓRICO DE REVISÕES

[redacted]			
07/02/2017	1.0	Elaboração do Documento	DTI
25/08/2021 a 15/09/2021	1.1	Consulta Pública	CSI
21/12/2021	1.2	Parecer do Jurídico	Priscila Correia Simões Michele Cardoso da Silva
16/05/2022	2.0	Atualização do documento	Abilio Da Cruz Ramos Neto; Adriana Martinelli Martins; Adriana Sales Silva de Oliveira; André Gomes Alay Esteves; Antônio Marcos Sousa Carvalho; Cláudia Brandão Gonçalves Silva; Eduardo Ferreira de Sousa; Einstein Da Silva Gomes De Lima; Eliane Cunha Marques; Fabiano Francisco Noetzold Saldanha; Fabio Campelo Santos Da Fonseca Ribeiro; Francisco Italo Lopes França; Guilherme Campos Fonseca; Gustavo Tibau Do Espirito Santo Alves; Joel De Sousa Ribeiro De Melo; José Arnon dos Santos Guerra; Juliana Pascualote Lemos De Almeida; Leandro Ambrosio Costa; Leonardo Fernandez Zago; Lucas Moreira dos Santos; Luciano Lovate Fardin; Luiz Carlos Perluci Junior; Maria Rachel de Castro; Michele Cardoso da Silva; Natalícia Batista Bueno; Paula Medeiros Rodolpho; Priscilla Correia Simões; Rafael Ribeiro Faim; Richelieu Ramos de Andrade Costa; Rodrigo Vaz dos Santos; Savana Karoline Farias Dantas; Tathiane Ribeiro da Silva; Telmo Nunes Costa; Victor Alex Begnini; Wagner Santana.

Sumário

CAPÍTULO I DO OBJETIVO E ÂMBITO DE APLICAÇÃO 6
CAPÍTULO II DAS DEFINIÇÕES 6
CAPÍTULO III DAS REFERÊNCIAS LEGAIS E NORMATIVAS 6
CAPÍTULO IV DOS PRINCÍPIOS 8
CAPÍTULO V DA ESTRUTURA NORMATIVA 8
CAPÍTULO VI DAS COMPETÊNCIAS E RESPONSABILIDADES 8
Seção I Da Presidência da Ebserh 8
Seção II Da Diretoria Executiva da Ebserh 9
Seção III Do Conselho de Administração da Ebserh 9
Seção IV Dos Colegiados Executivos dos Hospitais da Rede Ebserh 9
Seção V Das Superintendências dos Hospitais da Rede Ebserh 9
Seção VI Do Proprietário de Ativos de Informação em meios físico e digital 9
Seção VII Do Custodiante de Ativos de Informação em meio físico e digital 10
Seção VIII Dos Usuários de Informação 10
Seção IX Dos Terceiros e Fornecedores 10
CAPÍTULO VII DA DIVULGAÇÃO E CONSCIENTIZAÇÃO 11
CAPÍTULO VIII DA SEGURANÇA DA INFORMAÇÃO 11
Seção I Do Tratamento da Informação 11
Seção II Da Segurança Física e do Ambiente 11
Seção III Da Gestão de Tratamento de Incidentes de Segurança Cibernética – GETI11
Seção IV Da Gestão de Ativos de Informação 12
Seção V Da Gestão de Uso dos Recursos Computacionais 12
Subseção I Do Uso de Correio Eletrônico 12
Subseção II Do Acesso à Internet 12
Subseção III Do Uso das Redes Sociais e Ferramentas de Comunicação 12
Subseção IV Do Uso de Computação em Nuvem 12
Subseção V Do Uso de Painel de Análise de Dados Corporativos 13
Subseção VI Do Uso de Dispositivos Móveis e de Armazenamento Portáteis 13
Subseção VII Do Controle e Uso de Credenciais de Acesso 13
Seção VI Da Gestão de Riscos de Segurança da Informação – GRSI 13
Seção VII Da Gestão de Continuidade de Negócios – GECON 14
Seção VIII Do Monitoramento, Auditoria e Conformidade 14
Seção IX Da Gestão da Segurança da Informação – GESI 14
Seção X Da Proteção de Dados Pessoais 15
CAPÍTULO IX DA CLASSIFICAÇÃO DA INFORMAÇÃO 15
CAPÍTULO X DO TRABALHO REMOTO 15
CAPÍTULO XI 15

DA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO 15
CAPÍTULO XII DO PLANO DE INVESTIMENTOS 15
CAPÍTULO XIII DA PROPRIEDADE INTELECTUAL 15
CAPÍTULO XIV DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES 16
CAPÍTULO XV DAS PENALIDADES 16
CAPÍTULO XVI DA ATUALIZAÇÃO E VALIDADE 16
CAPÍTULO XVII DAS DISPOSIÇÕES FINAIS 16

CAPÍTULO I
DO OBJETIVO E ÂMBITO DE APLICAÇÃO

Art. 1º A Política de Segurança da Informação (PSI) tem por objetivo a instituição de diretrizes estratégicas contra ameaças e vulnerabilidades para garantir segurança na disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como para difundir atitudes adequadas para uso, manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer ativo de informação digital ou físico da Empresa Brasileira de Serviços Hospitalares (Ebserh), buscando a preservação das responsabilidades legais, proteção de dados pessoais de pacientes e empregados e da imagem institucional da Empresa.

Art. 2º A PSI trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito da rede Ebserh, em todo o seu ciclo de vida desde a criação, acesso, processamento, divulgação, armazenamento, transporte até descarte, visando à continuidade de seus processos críticos em conformidade com a legislação, os requisitos regulamentares e contratuais, os valores éticos e as melhores práticas de segurança da informação.

Art. 3º A PSI aplica-se à Administração Central e aos Hospitais Universitários Federais (HUFs) da Rede Ebserh, sendo de responsabilidade de todos os agentes públicos que, oficialmente, executem atividades vinculadas à atuação institucional, devendo ser dado amplo conhecimento de seu teor a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos da Ebserh.

Parágrafo único. As diretrizes da PSI constituem os principais pilares da Gestão de Segurança da Informação (GSI) da Ebserh, sendo norteadoras da elaboração das normas de Segurança da Informação (SI).

CAPÍTULO II
DAS DEFINIÇÕES

Art. 4º Para os efeitos da PSI, os conceitos e as definições dos termos técnicos utilizados encontram-se no Dicionário de Referência de TI, disponível na Intranet da Ebserh, no endereço http://intranet.ebserh.gov.br/tecnologia-da-informacao/dicionario e no Glossário de Segurança da Informação da Presidência da República - Gabinete de Segurança Institucional, disponível em https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1.

Art. 5º Adicionalmente aos conceitos e às definições referidos no art. 4º, para efeitos desta Política, considera-se:

I. **ativo de informação** - os ativos que suportam os meios de armazenamento, transmissão e processamento da informação, tais como os equipamentos necessários, os sistemas utilizados, os documentos impressos, os locais onde se encontram esses meios e os recursos humanos a eles associados;

II. **custodiante de ativos de informação** - qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal ou decorrente de suas atividades profissionais de proteger a informação que não lhe pertence e aplicar os níveis de controles de segurança em conformidade com as exigências de SI comunicadas pelo proprietário da informação;

III. **Etir** - Equipe de tratamento e resposta a incidentes cibernéticos;

IV. **proprietário de ativos de informação** - unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos em meio físico ou digital relacionados;

V. **sistema de informação** - conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos documentais, de tecnologia, informação ou comunicações de forma integrada; e

VI. **usuário de informação** - pessoa física, empregado, servidor ou prestador de serviços terceirizado, habilitada pela administração para acessar os ativos de informação de um órgão ou uma entidade da Administração Pública Federal, autorização formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º Além do disposto nesta PSI, deverá ser observado o disposto nos seguintes atos normativos:

I. **Lei nº 8.159, de 8 de janeiro de 1991:** dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

II. **Lei nº 9.983, de 14 de julho de 2000**: dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

III. **Lei nº 12.527, de 18 de novembro de 2011 -** Lei de Acesso à Informação (LAI): Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

IV. **Lei nº 12.550, de 15 de dezembro de 2011:** autoriza o Poder Executivo a criar a empresa pública denominada Empresa Brasileira de Serviços Hospitalares - Ebserh;

V. **Lei nº 13.709, de 14 de agosto de 2018 -** Lei Geral de Proteção de Dados Pessoais (LGPD): 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;

VI. **Lei 13.853, de 08 de julho de 2019:** altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados e dá outras providências;

VII. **Decreto nº 1.171, de 22 de junho de 1994**: aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VIII. **Decreto nº 3.505, de 13 de junho de 2000:** institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

IX. **Decreto nº 5.482, de 30 de junho de 2005:** dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores – Internet;

X. **Decreto nº 7.082, de 27 de janeiro de 2010:** institui o Programa Nacional de Reestruturação dos Hospitais Universitários Federais – REHUF;

XI. **Decreto nº 7.724, de 16 de maio de 2012**: regulamenta a Lei de Acesso à Informação (LAI);

XII. **Decreto nº 9.637, de 26 de dezembro de 2018**: institui a Política Nacional de Segurança da Informação;

XIII. **Decreto nº 9.832, de 12 de junho de 2019**: altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação da Presidência da República;

XIV. **Decreto nº 10.222, de 5 de fevereiro de 2020:** aprova a Estratégia Nacional de Segurança Cibernética;

XV. **Decreto nº 10.332 de 28 de abril de 2020:** institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

XVI. **Portaria GSI/PR nº 93, de 26 de setembro de 2019**: aprova o Glossário de Segurança da Informação;

XVII. **Portaria nº 1, de 08 de março de 2021:** estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados – ANP.

XVIII. **Resolução SE/GSI nº 1, de 11 de setembro de 2019**: aprova o Regimento Interno do Comitê Gestor de Segurança da Informação;

XIX. **Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020:** dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal; e

XX. **Normas Complementares nº 05 até 21 IN01/DSIC/GIS/PR**: disciplinam a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, disponíveis em https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao;

XXI. **Norma ABNT NBR ISO/IEC 27005:2011:** estabelece diretrizes para o processo de gestão de riscos de segurança da informação;

XXII. **Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013:** estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos entidades da Administração Pública Federal - APF, direta e indireta;

XXIII. **Norma ABNT NBR ISO/IEC 27001:2013:** estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

XXIV. **Norma ABNT NBR ISO/IEC 27002:2013:** institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 7º A PSI e suas ações serão norteadas pelos seguintes princípios:

I. **celeridade:** as ações de SI devem oferecer respostas rápidas a incidentes e falhas de segurança;

II. **ética**: os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SI;

III. **clareza**: as regras de segurança dos ativos de SI devem ser precisas, concisas e de fácil entendimento;

IV. **legalidade**: as ações de segurança devem respeitar as leis, normas, políticas organizacionais, administrativas, técnicas e operacionais da Ebserh e atribuições regimentais;

V. **publicidade**: transparência no trato da informação, observados os critérios legais;

VI. **responsabilidade**: os agentes públicos devem conhecer e respeitar a PSI da Ebserh e devem ser responsabilizados pelos atos que comprometem a segurança da informação; e

VII. **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Art. 8º Serão observados ainda outros princípios constitucionais que regem a Administração Pública Federal assim como os valores organizacionais da Rede Ebserh.

CAPÍTULO V
DA ESTRUTURA NORMATIVA

Art. 9º A Gestão de Segurança da Informação da PSI será norteada pela observância das regras dispostas neste normativo, bem como em normas operacionais e procedimentos operacionais.

§ 1ºA PSI define as regras e diretrizes de alto nível, que representam os princípios básicos incorporados pela Ebserh à gestão, de acordo com sua visão estratégica, servindo como base para que as normas operacionais e os procedimentos internos sejam criados e detalhados.

§ 2º As normas operacionais dispõem sobre obrigações a serem seguidas de acordo com as diretrizes específicas estabelecidas na PSI, apresentando os controles que deverão ser implementados para alcançar a estratégia estabelecida.

§ 3º Os procedimentos operacionais instrumentalizam o disposto na PSI e nas normas operacionais, viabilizando sua aplicação imediata nas tarefas operacionais da Empresa.

CAPÍTULO VI
DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I
Da Presidência da Ebserh

Art. 10 Para os fins de aplicação da PSI, compete à Presidência da Ebserh:

I. dar apoio à promoção da cultura de SI; e
II. nomear o Gestor de Segurança da Informação da Administração Central.

Seção II
Da Diretoria Executiva da Ebserh

Art. 11 Para os fins de aplicação da PSI, compete à Diretoria Executiva da Ebserh:

I. dar suporte à promoção da cultura de SI;
II. manifestar-se sobre a PSI previamente à aprovação pelo Conselho de Administração da Ebserh; e
III. aprovar programa orçamentário específico para as ações de SI, conforme proposto pelo Comitê de Segurança da Informação (CSI) da Administração Central, em conformidade com o art. 15, inciso V, do Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação - PNSI.

Seção III
Do Conselho de Administração da Ebserh

Art. 12 Para os fins de aplicação da PSI, compete ao Conselho de Administração da Ebserh aprovar a PSI.

Seção IV
Dos Colegiados Executivos dos Hospitais da Rede Ebserh

Art. 13 Para os fins de aplicação da PSI, compete aos Colegiados Executivos dos Hospitais da Rede Ebserh:

I. dar suporte à promoção da cultura de SI, em consonância com esta Política e com as normas complementares da Administração Central;
II. conduzir a implantação da PSI no âmbito da respectiva unidade hospitalar; e
III. aprovar programa orçamentário específico para as ações de SI, conforme proposto pelo CSI da respectiva unidade hospitalar.

Seção V
Das Superintendências dos Hospitais da Rede Ebserh

Art. 14 Para os fins de aplicação da PSI, compete às Superintendências dos Hospitais da Rede Ebserh:

I. dar suporte à promoção da cultura de SI, em consonância com esta Política e com as normas da Administração Central;
II. designar o Gestor de Segurança da Informação de sua unidade hospitalar; e
III. aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

Parágrafo único: O Gestor de Segurança da Informação designado deverá:

I - possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos aos temas de privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público; e

II - não se encontrar lotado no Setor de Tecnologia da Informação ou ser gestor responsável de sistemas de informação do órgão ou da entidade.

Seção VI
Do Proprietário de Ativos de Informação em meios físico e digital

Art. 15 Para os fins de aplicação da PSI, compete ao proprietário de ativos de informação:

I. descrever o ativo de informação;
II. informar ao custodiante as informações cadastrais sobre o ativo, mantendo-as atualizadas;

III. indicar o valor do ativo para o negócio ou serviço que desempenha;
IV. definir as exigências de segurança da informação e comunicações do ativo de informação;
V. assegurar-se de que as exigências de segurança da informação e comunicações sejam cumpridas por meio de monitoramento contínuo;
VI. indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação;
VII. delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária dos ativos;
VIII. estabelecer critérios que assegurem a segregação de funções para evitar a detenção do controle de um processo ou sistema na sua totalidade por apenas um agente, de forma a reduzir o risco de mau uso acidental ou deliberado dos ativos de informação; e
IX. comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários.

Seção VII
Do Custodiante de Ativos de Informação em meio físico e digital

Art. 16 Para os fins de aplicação da PSI, compete ao custodiante de ativos de informação:
I. manter atualizado o cadastro dos ativos, sob sua custódia, no banco de dados de ativos de informação;
II. proteger o ativo de informação quanto ao armazenamento, acesso, transporte e processamento, de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação;
III. proteger os contêineres dos ativos de informação, aplicando os níveis de controles de segurança em conformidade com as exigências comunicadas pelo proprietário do ativo;
IV. implementar controles específicos, podendo, conforme a necessidade, delegar a um terceiro, sem prejuízo das responsabilidades pela proteção adequada dos ativos;
V. monitorar o ativo tecnológico diariamente e comunicar ao proprietário qualquer problema ou incidente de segurança envolvendo o ativo, devendo ainda registrar as ações que foram adotadas para sanar ou minimizar o problema;
VI. realizar as modificações necessárias nos ativos, de acordo com o planejamento;
VII. realizar cópias de segurança (*backup*) conforme Política de Backup e Recuperação de Dados da Rede Ebserh;
VIII. monitorar periodicamente os registros de auditoria (log), avisando imediatamente ao responsável qualquer problema encontrado; e
IX. zelar pelo adequado e seguro acesso e uso dos ativos de informação.

Seção VIII
Dos Usuários de Informação

Art. 17 Para os fins de aplicação da PSI, compete aos usuários de informação:
I. conhecer e cumprir todos os princípios, diretrizes e responsabilidades previstos nesta PSI, bem como os demais normativos e resoluções relacionados à SI;
II. evitar o acesso de pessoas não autorizadas a documentos físicos ou digitais, sob sua responsabilidade;
III. obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;
IV. utilizar, sempre que possível, ferramentas de comunicação institucionais, conforme normas internas específicas; e
V. comunicar os incidentes que afetam a segurança dos ativos de informação à ETIR.

Seção IX
Dos Terceiros e Fornecedores

Art. 18 Para os fins de aplicação desta Política, compete aos terceiros e fornecedores:
I. tomar conhecimento da PSI;

II. fornecer listas atualizadas de documentação dos ativos de informação, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

III. fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Art. 19 As responsabilidades e competências do CSI, do Gestor de Segurança da Informação e da ETIR estão descritas em normas específicas.

CAPÍTULO VII
DA DIVULGAÇÃO E CONSCIENTIZAÇÃO

Art. 20 A divulgação das regras e orientações de SI aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na intranet, seminários de conscientização e quaisquer outros meios, com vistas à criação de uma cultura de SI no âmbito da Ebserh.

Art. 21 Cabe ao Gestor de Segurança da Informação promover a divulgação interna da PSI e das normas dela decorrentes e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SI.

CAPÍTULO VIII
DA SEGURANÇA DA INFORMAÇÃO

Seção I
Do Tratamento da Informação

Art. 22 A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e aos serviços da Ebserh.

§ 1º A proteção deve ser realizada de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de classificação da informação.

§ 2º Os dados, as informações, os sistemas de informação, os documentos impressos e a infraestrutura da Ebserh devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir sua disponibilidade, integridade, confidencialidade e autenticidade.

Seção II
Da Segurança Física e do Ambiente

Art. 23 Os aspectos de segurança física e do ambiente (segurança orgânica, controles de acesso, etc.) e de recursos humanos (engenharia social) serão tratados em documentos independentes, a fim de complementar com maior especificidade e detalhamento as normas e recomendações de SI.

Parágrafo único. Todos os procedimentos relacionados à SI, definidos em instruções específicas, devem estar de acordo com esta Política, e uma vez divulgados, tornam-se parte integrante desta.

Seção III
Da Gestão de Tratamento de Incidentes de Segurança Cibernética – GETI

Art. 24 Compete à Etir, instituída pelo CSI e integrada pela Diretoria de Tecnologia da Informação e pelos Setores de Tecnologia da Informação e Saúde Digital dos HUFs, monitorar, receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança cibernética.

Art. 25 Os eventos e incidentes de SI devem ser comunicados, registrados e tratados de acordo com o Plano de Gestão de Incidentes de Segurança Cibernética.

Seção IV
Da Gestão de Ativos de Informação

Art. 26 A gestão de ativos de informação em meio físico ou digital da Ebserh deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua.

Art. 27 Os ativos de informação da Ebserh deverão ser inventariados, com a classificação em termos de valor, requisitos legais, sensibilidade e criticidade da informação para a Ebserh, e serão atribuídos aos respectivos responsáveis.

Parágrafo único. O uso dos ativos de informação deve estar em conformidade com os princípios e as normas operacionais de SI e ser destinado exclusivamente ao uso institucional, vedada a utilização para fins em desconformidade com os interesses da Ebserh.

Art. 28 O usuário deve ter acesso apenas aos ativos de informação necessários e indispensáveis à finalidade de seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação.

Art. 29 É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, acessadas, processadas, armazenadas, transportadas, descartadas ou custodiadas pela Ebserh.

Seção V
Da Gestão de Uso dos Recursos Computacionais

Subseção I
Do Uso de Correio Eletrônico

Art. 30 O correio eletrônico da Ebserh é um recurso de comunicação institucional cujas regras de acesso e utilização devem atender a todas as orientações da PSI, da Política de Comunicação Institucional e das normas específicas, além das demais diretrizes da Administração Pública Federal.

Subseção II
Do Acesso à Internet

Art. 31 O acesso à rede mundial de computadores, Internet, no ambiente de trabalho deve ser regido por normas e procedimentos específicos, atendendo às determinações da PSI, às demais orientações governamentais e à legislação.

Subseção III
Do Uso das Redes Sociais e Ferramentas de Comunicação

Art. 32 A utilização de perfis institucionais mantidos em redes sociais e de ferramentas de comunicação deve ser regida pela Política de Comunicação Social da Rede Ebserh, pelo Manual de Conduta em Mídias Sociais, por normas internas específicas e deve estar em consonância com a PSI e com os objetivos estratégicos da instituição.

Subseção IV
Do Uso de Computação em Nuvem

Art. 33 O uso de recursos de computação em nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo a determinações da PSI, e demais orientações governamentais e legislação , com vistas a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas na nuvem, privada ou pública, em especial aquelas sob custódia e gerenciamento de prestador de serviço.

Subseção V
Do Uso de Painel de Análise de Dados Corporativos

Art. 34 O acesso e uso de paineis de análise de dados corporativos deve ser feito de maneira controlada, mediante cadastramento dos usuários.

Art. 35 A estratégia de segurança de construção e uso dos paineis de análise de dados corporativos deve ser constantemente monitorada e observar normas específicas, de modo a garantir que os acessos sejam concedidos apenas aos usuários autorizados.

Art. 36 Incumbe à Diretoria de Tecnologia da Informação (DTI) elaborar e manter atualizada Norma de Uso de Painel de Análise de Dados Corporativos, com objetivo de fornecer orientações e restrições quanto ao seu uso internamente na Rede Ebserh.

Subseção VI
Do Uso de Dispositivos Móveis e de Armazenamento Portáteis

Art. 37 As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e correio eletrônico da Ebserh devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo à PSI, e devem ser regidas por normas específicas, as quais contemplarão recomendações sobre o uso desses dispositivos.

Art. 38 Incumbe à DTI elaborar e manter atualizada Norma de Uso Responsável de Unidades Portáteis de Armazenamento de Dados Corporativos e Dispositivos Móveis, com objetivo de fornecer orientações e restrições quanto ao uso desses dispositivos internamente na Rede Ebserh.

Subseção VII
Do Controle e Uso de Credenciais de Acesso

Art. 39 As credenciais de acesso aos recursos tecnológicos institucionais, inclusive senha, são pessoais e intransferíveis.

Art. 40 As regras de controle de acesso a todos os sistemas institucionais, à intranet, à Internet, às informações, aos dados e às instalações físicas da Ebserh deverão ser definidas e regulamentadas por meio de normas específicas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos digitais de informação da Empresa.

Art. 41 Incumbe à DTI elaborar e manter atualizada Norma de Controle de Acesso aos sistemas institucionais, à intranet, à Internet, às informações e aos dados.

Seção VI
Da Gestão de Riscos de Segurança da Informação – GRSI

Art. 42 A GRSI é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos físicos e digitais de informação da Ebserh, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Art. 43 As áreas responsáveis por ativos de informação deverão implementar processo contínuo de gestão de riscos, que será aplicado na implementação e operação da GRSI.

Art. 44 A GRSI deve ser implementada no âmbito da Ebserh, visando identificar os ativos de informação relevantes e determinar ações de gestão apropriadas, devendo ser atualizada periodicamente, no mínimo uma vez por ano ou sempre que necessário, em função de inventários de ativos de informação, mudanças, ameaças ou vulnerabilidades.

Parágrafo único. A GRSI deve incluir um Plano de Continuidade de Negócios - PCN e um Plano de Gestão de Incidentes - PGI.

Art. 45 O PCN deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

Art. 46 O PGI definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas perante incidentes de SI.

Seção VII
Da Gestão de Continuidade de Negócios – GECON

Art. 47 A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da Ebserh, em meio físico ou digital, assim como possíveis impactos nas operações de negócio, caso essas ameaças se concretizem.

Parágrafo único. A GECON prevê a definição de uma estrutura para aprimorar a resiliência organizacional, com vistas a responder com efetividade aos incidentes de SI e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da Ebserh, além de recuperar perdas de ativos de informação.

Art. 48 As áreas da Ebserh deverão manter seus processos de GECON, de modo a evitar que os respectivos negócios sejam interrompidos, e assegurar a sua retomada em tempo hábil, bem como, deverão estabelecer um conjunto de estratégias e procedimentos a serem adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

Art. 49 A resiliência contra possíveis interrupções na capacidade de cumprir objetivos institucionais deve ser prática proativa dos titulares das unidades administrativas e técnicas, buscando a preservação das responsabilidades legais, proteção de dados pessoais de pacientes e empregados e da imagem institucional da Empresa.

Art. 50 As medidas constantes do PGI deverão assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto de situações inesperadas, os desastres, as falhas de segurança, entre outras, até que se retorne à normalidade.

Art. 51 Incumbe à DTI elaborar e manter atualizadas as políticas e normas necessárias à continuidade dos serviços de TI, com objetivo de garantir a disponibilidade dos recursos tecnológicos, para que, em caso de incidentes, estes sejam restabelecidos no menor tempo possível, evitando a perda de dados e os impactos às atividades das áreas de negócio da Ebserh.

Seção VIII
Do Monitoramento, Auditoria e Conformidade

Art. 52 O monitoramento, a auditoria e a conformidade de ativos de informações em meio físico ou digital observarão o seguinte:

I. o uso dos ativos de informação é passível de monitoramento e auditoria, devendo ser implementados e mantidos mecanismos que permitam a sua rastreabilidade;
II. a entrada e saída de ativos de informação da Ebserh deverá ser registrada e autorizada por autoridade competente mediante procedimento formal;
III. as áreas responsáveis manterão registros e procedimentos específicos, tais como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos respectivos ativos de informação; e
IV. a Ouvidoria da Ebserh será responsável por manter canal de comunicação para recebimento de denúncias de infração a qualquer artigo da PSI.

Seção IX
Da Gestão da Segurança da Informação – GESI

Art. 53 Todos os mecanismos de proteção utilizados para a SI devem ser planejados e mantidos com o objetivo de garantir a continuidade dos negócios da Ebserh.

Art. 54 Os requisitos de SI da Ebserh devem ser explicitamente citados em todos os termos de compromisso celebrados entre a Empresa e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, devendo também ser exigido Termo de Compromisso de Manutenção de Sigilo.

Seção X
Da Proteção de Dados Pessoais

Art. 55 Os dados pessoais, a privacidade e o acesso do titular à própria informação deverão ser protegidos em consonância com o que estabelece a Política de Proteção de Dados Pessoais da Ebserh e a Lei Geral de Proteção de Dados.

CAPÍTULO IX
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 56 Toda informação criada, acessada, processada, armazenada, transportada, descartada ou custodiada pela Ebserh deverá estar em consonância com o que estabelece a Política de Classificação de Informação, Sigilo e Temporalidade da Rede Ebserh.

Art. 57 O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 58 A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.

Art. 59 O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pela Ebserh e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Parágrafo único. Para o tratamento das informações consideradas de alta criticidade e dos dados sensíveis serão necessárias medidas especiais, com o objetivo de limitar a exploração de informações exclusivas da Empresa.

CAPÍTULO X
DO TRABALHO REMOTO

Art. 60 O acesso e uso de ativos de informação em meio físico ou digital objeto de trabalho remoto deve ser regido por normas e procedimentos específicos, observadas as disposições da PSI, demais orientações da Administração Pública Federal e a legislação em vigor.

CAPÍTULO XI
DA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Art. 61 As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança estabelecidos pela DTI, seguindo a legislação e boas práticas de mercado, com vistas a garantir o respeito aos atributos básicos de segurança da informação.

CAPÍTULO XII
DO PLANO DE INVESTIMENTOS

Art. 62 Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um Plano de Investimentos em SI e, no que couber, no Plano Diretor de Tecnologia da Informação (PDTI), em consonância com o que estabelece a PNSI.

CAPÍTULO XIII
DA PROPRIEDADE INTELECTUAL

Art. 63 As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual da Ebserh e não cabe a seus criadores qualquer forma de direito de propriedade intelectual, ressalvado o direito moral de reconhecimento de autoria.

Art. 64 É vedada a utilização de patrimônio intelectual da Ebserh em quaisquer projetos ou atividades de uso diverso do estabelecido pela Empresa, exceto quando houver autorização específica por parte da Diretoria Executiva da Empresa.

CAPÍTULO XIV
DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 65 Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância da PSI.

Art. 66 O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas complementares, aos empregados, prepostos e todos os envolvidos em atividades vinculadas à Ebserh.

CAPÍTULO XV
DAS PENALIDADES

Art. 67 Ações que infrinjam a PSI ou quaisquer de seus princípios, normas ou procedimentos serão devidamente apuradas no âmbito de processo administrativo específico, sendo aplicadas aos responsáveis as sanções penais, administrativas e cíveis cabíveis.

Art. 68 O usuário responderá disciplinarmente ou civilmente pelo prejuízo que vier a ocasionar à Empresa, podendo resultar em seu desligamento e, se aplicáveis, eventuais processos criminais.

CAPÍTULO XVI
DA ATUALIZAÇÃO E VALIDADE

Art. 69 A SI relativa a ativos de informação em meio digital ou físico é tema de permanente acompanhamento e aperfeiçoamento no âmbito da Ebserh, devendo ser revista e atualizada sempre que necessário.

Art. 70 Os instrumentos normativos gerados a partir da PSI deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação federal pertinente ou de diretrizes políticas da Administração Pública Federal, e deverão observar os seguintes critérios:

I. Política de Segurança da Informação:
   a. nível de aprovação: Conselho de Administração; e
   b. periodicidade de revisão: no máximo a cada três anos;
II. Normas de Segurança da Informação:
   a. nível de Aprovação: Diretoria Executiva; e
   b. periodicidade de Revisão: no máximo a cada dois anos;
III. Procedimentos Operacionais:
   a. nível de aprovação: Área Técnica; e
   b. periodicidade de revisão: a qualquer tempo.

Art. 71 A PSI tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

CAPÍTULO XVII
DAS DISPOSIÇÕES FINAIS

Art. 72 Independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida adequadamente, de acordo com a PSI.

Art. 73 Quaisquer recursos e ativos de informação da Ebserh devem ser usados pelos agentes públicos exclusivamente para a realização de suas atividades profissionais.

Art. 74 Os HUFs deverão criar Comitês de Segurança da Informação nas respectivas unidades hospitalares e poderão estabelecer procedimentos específicos em conformidade com a PSI.

Art. 75 Os casos omissos e as dúvidas decorrentes da aplicação do disposto na PSI, devem ser direcionados ao CSI da Administração Central e no âmbito dos HUFs para o CSI respectivo.

Art. 76 A PSI entra em vigor na data de sua publicação.