EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO – POSIC

2ª versão

HUPAA, fevereiro de 2017.

Ministério da Educação

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES - EBSERH
HOSPITAL UNIVERSITÁRIO PROFESSOR ALBERTO ANTUNES
Av. Lourival Melo Mota, s/n, Bairro: Cidade Universitária
Maceió - AL | CEP: 57072-900 | (82) 3202-3800
Site: www.hupaa.ebserh.gov.br

JOSÉ MENDONÇA BEZERRA FILHO
Ministro de Estado da Educação

KLEBER DE MELO MORAIS
Presidente

MARIA DE FÁTIMA SILIANSKY DE ANDREAZZI
Superintendente do Hospital Universitário Professor Alberto Antunes

HUAYNA VALENÇA PADILHA
Gerente Administrativo

KATHARINA VIDAL DE NEGREIROS MOURA
Gerente de Atenção à Saúde

REGINA MARIA DOS SANTOS
Gerente de Ensino e Pesquisa

Comitê Gestor de Segurança da Informação
BRUNO MORAIS SILVA
KLEBER JOSÉ DOS SANTOS
LUAN DE MASCARENHAS DOS SANTOS
MANOEL ÁLVARO LINS NETO
MARIA INEZ CARNEIRO
MARINA PEREIRA CORREIA DAS NEVES
THIAGO SOTERO FRAGOSO

Documento publicado no Boletim de Serviço do HUPAA, n. 121, de 10 de fev. de 2017.

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO HOSPITAL UNIVERSITÁRIO PROF. ALBERTO ANTUNES, DA UFAL

1. ESCOPO

1.1. A Política de Segurança da Informação e Comunicações - POSIC objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade e autenticidade das informações custodiadas e/ou de propriedade do Hospital Universitário Professor Alberto Antunes - HUPAA, de modo a preservar os seus ativos e sua imagem institucional.

1.2. A POSIC trata do uso e compartilhamento de dados, informações e documentos no âmbito do HUPAA, em todo o seu ciclo de vida – criação, manuseio, armazenamento, transporte e descarte, visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

2. CONCEITOS E DEFINIÇÕES

Para efeitos desta POSIC são estabelecidos os seguintes conceitos e definições:

2.1. **Agente público**: todo aquele que, por força de lei, contrato ou de qualquer ato jurídico, preste serviços de natureza permanente, temporária ou excepcional, ainda que sem retribuição financeira, desde que ligado direta ou indiretamente ao HUPAA;

2.2. **Ameaças**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

2.3. **Ativo**: qualquer bem, tangível ou intangível, que tenha valor para a organização (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional);

2.4. **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

2.5. **Ciclo de vida da informação**: compreende as fases de criação, manuseio, armazenamento, transporte e descarte de informação, considerando sua confidencialidade, integridade e disponibilidade;

2.6. **Classificação da informação**: atribuição, pela autoridade competente, de grau de sigilo, disponibilidade e integridade dado à informação, documento, material, área ou instalação;

Documento publicado no Boletim de Serviço do HUPAA, n. 121, de 10 de fev. de 2017.

2.7. **Comitê Gestor de Segurança da Informação - CGSI**: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do HUPAA;

2.8. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

2.9. **Conta de acesso**: conjunto do "nome de usuário" (conhecido também por login) e "senha" utilizado para acesso aos sistemas informatizados e recursos de TIC;

2.10. **Custodiante**: agente público responsável por zelar pelo armazenamento e pela preservação do ativo sob sua propriedade;

2.11. **Dado**: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

2.12. **Diretriz**: Conjunto de instruções ou indicações que orientam o que deve ser feito para se alcançar os objetivos estabelecidos na política;

2.13. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

2.14. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR**: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em recursos de TIC;

2.15. **Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

2.16. **Gestão de Riscos de Segurança da Informação e Comunicações**: conjunto de processos que permite identificar e implementar as medias de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

2.17. **Gestor de Segurança da Informação e Comunicações**: é responsável pelas ações de segurança da informação e comunicações no âmbito do HUPAA;

2.18. **Incidente de segurança**: qualquer evento ou ocorrência, confirmado ou sob

suspeita, que promova uma ou mais ações que comprometam ou que sejam uma ameaça à segurança da informação e comunicações;

2.19. **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

2.20. **Intranet**: rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

2.21. **Metodologia de Desenvolvimento de Sistemas**: conjunto de práticas que define o processo de desenvolvimento de sistemas de informação;

2.22. **Política de Segurança da Informação e Comunicações**: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

2.23. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

2.24. **Recursos de TIC**: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, tablets, telefones, smartphones, servidores de rede, equipamentos de conectividade e infraestrutura;

2.25. **Segurança da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

2.26. **Severidade**: índice ou grau que se refere à medição do impacto de um evento ou incidente de segurança da informação;

2.27. **TI**: tecnologia da informação;

2.28. **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3. REFERÊNCIAS LEGAIS E NORMATIVAS

Decreto nº 1.171, de 22 de junho de 1994, que dispõe sobre o Código de Ética do Servidor Público Civil do Poder Executivo Federal.

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

Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados e informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Instrução Normativa nº 01/IN01/DSIC/GSIPR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal.

Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

NBR ISO/IEC 27001:2013 - Sistema de Gestão de Segurança da Informação.

NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação.

Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização.

Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que estabelece a metodologia de Gestão de Segurança da Informação e Comunicações.

Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

Norma Complementar nº 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal - APF, direta e indireta.

Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que regulamenta a criação de equipes de tratamento e resposta a incidentes em redes computacionais.

Norma Complementar nº 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009, que regulamenta a Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações;

Norma Complementar nº 07/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal – APF.

Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal - APF, direta e indireta.

Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

Norma Complementar nº 21/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal - APF, direta e indireta.

4. PRINCÍPIOS

As ações de Segurança da Informação e Comunicações no HUPAA são norteadas pelos seguintes princípios (sem prejuízo aos princípios da Administração Pública Federal, definidos no art. 37 da Constituição Federal):

4.1. **Alinhamento estratégico**: deve haver um alinhamento entre a POSIC com a missão institucional e seu planejamento estratégico.
4.2. **Diversidade organizacional**: a elaboração da POSIC deve levar em consideração a diversidade das atividades do HUPAA, respeitando a natureza e finalidade de cada setor da instituição.
4.3. **Propriedade da informação:** toda informação produzida ou armazenada no HUPAA é de sua propriedade e não de seu colaborador, exceto os casos onde a instituição atua como custodiante dessa informação.

5. DIRETRIZES GERAIS

Para fins desta política ficam estabelecidas as seguintes diretrizes gerais:

5.1. **Classificação da Informação**

5.1.1. As informações custodiadas ou de propriedade do HUPAA devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.
5.1.2. O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.
5.1.3. A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manuseio, armazenamento, transporte e descarte.
5.1.4. Todo agente público deve ser capaz de identificar a classificação atribuída a

uma informação custodiada ou de propriedade do HUPAA e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

5.2. **Tratamento das informações**

5.2.1. Toda informação criada, adquirida ou custodiada pelo agente público, no exercício de suas atividades para o HUPAA, é considerada um bem e deve ser protegida pela instituição de acordo com as regulamentações de segurança existentes.

5.2.2. As informações devem ser protegidas de acordo com as diretrizes descritas nesta POSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do HUPAA e preservar sua imagem.

5.2.3. As informações produzidas ou custodiadas pelo HUPAA devem ser descartadas conforme seu nível de classificação.

5.3. **Conscientização e Capacitação**

O HUPAA desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

5.4. **Tratamento de incidentes de redes**

5.4.1. Deve ser definida uma equipe para tratamento e resposta aos incidentes em redes computacionais, segundo critérios a serem definidos pelo setor de TI do HUPAA, a fim de receber, analisar e responder às notificações e atividades relacionadas aos incidentes de segurança em redes computacionais no órgão.

5.4.2. Os incidentes de segurança da informação devem ser registrados e gerenciados.

5.5. **Gestão de risco**

Deve ser adotada a gestão de riscos de segurança da informação, segundo critérios a serem definidos pelo setor de TI do HUPAA, para a identificação e implementação das medidas de proteção necessárias para a mitigação ou eliminação dos riscos.

5.6. **Gestão de continuidade**

Deve ser adotada a gestão de continuidade de negócios em segurança da informação, segundo critérios a serem definidos pelo setor de TI do HUPAA, visando minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, através de ações de prevenção, resposta e recuperação dos ativos que sustentam os processos críticos da instituição.

5.7. **Uso de Recursos de TIC**

O uso de recursos de tecnologia da informação e comunicação do HUPAA pelos agentes públicos deve ser direcionado prioritariamente para realização das necessidades profissionais e atividades do HUPAA nos limites dos princípios da ética, razoabilidade e legalidade.

5.8. **Sistemas de Telecomunicações**

5.8.1. O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos digitais, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de TI.

5.8.2. Ao final de cada mês, para controle, serão enviados relatórios informando a cada chefia quanto foi gasto por cada ramal digital.

5.9. **Auditoria e Conformidade**

5.9.1. O HUPAA deve criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e intranet da instituição.

5.9.2. Deve-se manter a conformidade com as regulamentações de segurança e legislações vigentes.

5.10. **Controles de acesso**

5.10.1. O HUPAA deve sistematizar a concessão de acesso como forma de evitar a quebra de segurança, bem como prover mecanismos de controle de acesso como consequência do processo de gestão de riscos de segurança da informação e comunicações.

5.10.2. O acesso às informações custodiadas ou de propriedade do HUPAA pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.

5.10.3. O acesso físico às instalações do HUPAA deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos ativos da instituição.

5.10.4. Todo acesso à informação sigilosa se dará através de mecanismos de identificação e controle de acesso.

5.10.5. Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação.

5.11. **Segurança de recursos humanos**

Todo agente público deve ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de TIC, inclusive por ocasião da mudança

de atividades.

5.12. Segurança física e do ambiente

Todo ambiente que contenha ativos deve ser protegido de acordo com sua severidade.

5.13. Gerenciamento de operações e comunicações

Deve-se garantir a operação segura e correta dos recursos de processamento da informação através das ações de segurança.

5.14. Aquisição, desenvolvimento e manutenção de sistemas

5.14.1. Todos os sistemas de informação adquiridos ou desenvolvidos para uso da instituição devem ter sua continuidade garantida, independentemente de eventuais mudanças na relação HUPAA – fornecedor.

5.14.2. Todo desenvolvimento de sistemas de informação para o HUPAA deve ser realizado com base em uma Metodologia de Desenvolvimento de Sistemas publicada.

6. PENALIDADES

A violação de um ou mais itens da POSIC e normas correlatas estará sujeita a sanções da esfera administrativa, civil ou penal.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. É dever de todo agente público do HUPAA conhecer e zelar pelo cumprimento da POSIC.

7.2. Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como: crachá, conta de acesso, certificado digital e endereço de correio eletrônico.

7.3. A identificação do agente público deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.

7.4. Independente da adoção de outras medidas, o agente público deverá, de imediato, comunicar todo incidente de segurança que ocorra no âmbito de suas atividades à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - EITR do HUPAA.

7.5. No âmbito do HUPAA, será instituída a seguinte estrutura para Gestão da Segurança

da Informação e Comunicações:

7.5.1. O Gestor de Segurança da Informação e Comunicações, que será exercido pela chefia do setor de TI;

7.5.2. O Comitê Gestor de Segurança da Informação e Comunicações - CGSI, cuja composição será definida em norma específica;

7.5.3. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, que funcionará em conformidade com norma específica.

7.5.4. São competências do Gestor de Segurança da Informação e Comunicações:

a) Promover cultura de segurança da informação e comunicações;
b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
c) Propor recursos necessários às ações de segurança da informação e comunicações;
d) Coordenar o Comitê Gestor de Segurança da Informação e Comunicações - CGSI;
e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
f) Manter contato permanente e estreito com a Superintendência do HUPAA para o trato de assuntos relativos à segurança da informação e comunicações;
g) Propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do HUPAA.

7.5.5. São competências do Comitê Gestor de Segurança da Informação e Comunicações - CGSI:

a) Assessorar na implementação das ações de segurança da informação e comunicações;
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
c) Propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

8. DIVULGAÇÃO

Após a publicação desta POSIC, deverá ser dada ampla divulgação a todos os agentes públicos do HUPAA, inclusive com publicação permanente na página da intranet da instituição.

9. ATUALIZAÇÃO

A POSIC, bem como o conjunto de instrumentos normativos gerados a partir dela, deverá ser revisada e atualizada quando identificada necessidade ou a cada 12 meses a contar da data de sua publicação.

Documento publicado no Boletim de Serviço do HUPAA, n. 121, de 10 de fev. de 2017.

10. VIGÊNCIA

Este documento entra em vigor na data de sua publicação.