EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

Boletim de Serviço

Nº 79, 07 de agosto de 2017

Ministério da
Educação

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES - Ebserh

Complexo Hospitalar Universitário Professor Edgard Santos – Complexo HUPES

Rua Augusto Viana, s/n - Canela
CEP: 70.830-200 | Salvador (BA)
(71) 3283-8000 | http://www.complexohupes.ufba.br

JOSÉ MENDONÇA BEZERRA FILHO
Ministro de Estado da Educação

KLEBER DE MELO MORAIS
Presidente

ANTÔNIO CARLOS MOREIRA LEMOS
Superintendente do Complexo HUPES

PATRIZIA ALLEGRO RIBEIRO
Gerente de Atenção à Saúde do Complexo HUPES

LÚCIA BEISL NOBLAT
Gerente de Ensino e Pesquisa do Complexo HUPES

LÍLIA KÁTIA ANDRADE NUNES
Gerente Administrativa do Complexo HUPES

SUMÁRIO

SUPERINTENDÊNCIA 4
DESIGNAÇÃO 4
Portaria nº 151, de 01 de agosto de 2017 4
Portaria nº 152, de 01 de agosto de 2017 4
INSTITUIÇÃO 4
Portaria nº 150, de 02 de agosto de 2017 4
ANEXO ÚNICO 5

SUPERINTENDÊNCIA

DESIGNAÇÃO

Portaria nº 151, de 01 de agosto de 2017

O SUPERINTENDENTE DO COMPLEXO HOSPITALAR UNIVERSITÁRIO PROFESSOR EDGARD SANTOS, no uso de suas atribuições, que lhe foram conferidas conforme as Portarias 125/2012 e 961/2014 da EBSERH, resolve:

Art. 1º Designar a empregada pública FERNANDA DOS SANTOS LIMA GOIABEIRA, matrícula SIAPE nº 2232964, substituta do cargo de Chefe da Divisão de Gestão de Pessoas – DivGP, vinculada a Gerência Administrativa do Hospital Universitário da Universidade Federal Professor Edgar Santos da EBSERH, nas ausências e impedimentos do titular.

Art. 2° Revoga-se a Portaria nº 929, publicada no Boletim de Serviço n° 116 de 04 de setembro de 2015.

Art. 3º Esta Portaria entra em vigor na data de sua assinatura.

Antônio Carlos Moreira Lemos

Portaria nº 152, de 01 de agosto de 2017

O SUPERINTENDENTE DO COMPLEXO HOSPITALAR UNIVERSITÁRIO PROFESSOR EDGARD SANTOS, no uso de suas atribuições, que lhe foram conferidas conforme as Portarias 125/2012 e 961/2014 da EBSERH, resolve:

Art. 1º Tornar sem efeito as portarias nºs 146 e 147/2017, publicadas no Boletim de Serviço nº 78 de 31 de julho de 2017.

Art. 3º Esta Portaria entra em vigor na data de sua assinatura.

Antônio Carlos Moreira Lemos

INSTITUIÇÃO

Portaria nº 150, de 02 de agosto de 2017

O SUPERINTENDENTE DO COMPLEXO HOSPITALAR UNIVERSITÁRIO PROFESSOR EDGARD SANTOS, no uso de suas atribuições, que lhe foram

conferidas conforme as Portarias 125/2012 e 961/2014 da EBSERH que delega competência para a prática dos atos de gestão específica;

Considerando o 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.

Considerando a aprovação na integra pelo Superintendente em 26 de junho de 2017 da Política de Segurança da Informação e Comunicações no âmbito desse Complexo Hospitalar.

RESOLVE:

Art. 1º Instituir, na forma do Anexo Único desta portaria, a Política de Segurança da Informação e Comunicações do Complexo Hospitalar Universitário Professor Edgard Santos (POSIC/HUPES), em consonância com a Instrução Normativa nº 01, de 13 de junho de 2008 do Gabinete de Segurança Institucional da Presidência da República e dos itens 6 e 7 de sua Norma Complementar nº 03.

Parágrafo único: A presente Política tem como objetivo estabelecer as diretrizes da Política de Segurança da Informação do Complexo Hospitalar Universitário Professor Edgard Santos, e aplica-se a todos os usuários de recursos de tecnologia da informação disponibilizados pelo Complexo HUPES.

Art. 2º Esta portaria entra em vigor na data de sua publicação

Antônio Carlos Moreira Lemos

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC) DO COMPLEXO HUPES

Sumário

PRINCIPAIS SIGLAS 0
1. ESCOPO 1
1.1. Objetivo 1
1.2. Abrangência 1
2. CONCEITOS E DEFINIÇÕES 1
3. REFERÊNCIAS LEGAIS E NORMATIVAS 4
4. PRINCÍPIOS 5
5. DIRETRIZES GERAIS 5
6. DIRETRIZES ESPECÍFICAS 8
6.1. Subcomitê Gestor de Segurança da Informação e Comunicação (SGSIC) 8
6.2. Gerenciamento de Segurança da Informação e Comunicações (GESIC) 8
6.3. Gerenciamento de Riscos de Segurança da Informação e Comunicações (GRSIC) 10
6.3.1. Plano de Gerenciamento de Riscos (PGR) 10
6.3.2. Plano de Gerenciamento de Incidentes (PGI) 11
6.4. Gerenciamento de Ativos de Informação 11
6.5. Tratamento da Informação 12
6.6. Classificação da Informação 12
6.7. Monitoramento, Auditoria e Conformidade 12
6.8. Controle de Acesso 13
6.9. Uso de e-mail 13
6.10. Acesso à internet 13
6.11. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação 13
6.12. Propriedade Intelectual 14
6.13. Uso de Computação em Nuvem 14
6.14. Uso de Dispositivos Móveis 14
7. PENALIDADES 14
8. COMPETÊNCIAS E RESPONSABILIDADES 15
8.1. Cabe à Superintendência do Complexo HUPES: 15
8.2. Cabe ao Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC): 16
8.3. Cabe ao SGPTI: 16
8.4. Proprietário de Ativos de Informação: 16
8.5. Cabe ao Custodiante dos Ativos de Informação: 17

8.6. Terceiros e Fornecedores: 17
8.7. Cabe Aos Usuários: 17
9. DIVULGAÇÃO E CONSCIENTIZAÇÃO 17
10. ATUALIZAÇÃO 18
11. ASSINATURA 19
12. CONTROLE DE VERSÃO 19

PRINCIPAIS SIGLAS

EBSERH	Empresa Brasileira de Serviços Hospitalares
GESIC	Gerenciamento de Segurança da Informação e Comunicações
GRSIC	Gerenciamento de Riscos de Segurança da Informação e Comunicações
HUF	Hospitais Universitários Federais
Complexo HUPES	Complexo Hospitalar Universitário Professor Edgard Santos
PGI	Plano de Gerenciamento de Incidentes
PGR	Plano de Gerenciamento de Riscos
POSIC	Política de Segurança da Informação e Comunicações
SGPTI	Setor de Gestão de Processos e Tecnologia da Informação
SGSIC	Subcomitê Gestor de Segurança da Informação e Comunicações Local
SIC	Segurança da Informação e Comunicações
TIC	Tecnologia da Informação e Comunicação
UFBA	Universidade Federal da Bahia

1. ESCOPO

1.1. Objetivo

Instituir diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e a autenticidade dos dados, informações, documentos e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio dos sistemas de informação do Complexo Hospitalar Universitário Professor Edgard Santos (Complexo HUPES) contra ameaças e vulnerabilidades, de modo a preservar os seus ativos de informação, inclusive a sua imagem institucional, direcionado as ações do Complexo HUPES à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações (SIC), alinhadas e em conformidade com a Política de Segurança da Informação e Comunicações (POSIC) da Empresa Brasileira de Serviços Hospitalares (EBSERH).

1.2. Abrangência

O conhecimento desta POSIC aplica-se ao Complexo HUPES, sendo de responsabilidade de todos os servidores, empregados, colaboradores internos ou externos, bem como a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do Complexo HUPES. Todos esses atores são responsáveis por garantir a segurança das informações a que tenham acesso.

2. CONCEITOS E DEFINIÇÕES

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

- **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;
- **Ameaça:** conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco;
- **Atividade**: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
- **Ativo**: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;
- **Ativos de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **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;

- **Avaliação de riscos:** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;
- **Celeridade**: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;
- **Classificação da informação**: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identifica-las, além de determinar os controles de proteção necessários a cada uma delas;
- **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
- **Continuidade do Negócio**: Garantir que os serviços essenciais sejam devidamente identificados e preservados, em situação normal de funcionamento da empresa dentro do contexto do negócio do qual ela faz parte;
- **Controle de acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
- **Desastre:** evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;
- **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- **Ética**: os direitos dos agentes públicos devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;
- **Evento de segurança da informação**: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação, ou falta de controle, ou situação previamente desconhecida que possa ser relevante para a segurança da informação;
- **Gerenciamento de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- **Gestão de continuidade dos negócios**: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse 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;
- **Gerenciamento de riscos de segurança da informação e comunicações:** conjunto de processos que permitem identificar e implementar as medidas 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;
- **Gestão de segurança da informação e comunicações**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

- **Identificação de Riscos** – processo para localizar, listar e caracterizar elementos do risco;
- **Incidente de SIC**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Política de Segurança da Informação e Comunicações**: documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
- **Proprietário de ativos de informação**: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;
- **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- **Resiliência**: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;
- **Responsabilidade**: os agentes públicos devem conhecer e respeitar todas as normas de segurança da informação e comunicações da instituição;
- **Risco de SIC**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- **Segurança física e do ambiente**: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;
- **Sistema estruturante**: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;
- **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à EBSERH;
- **Transferir risco:** uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;
- **Tratamento da informação**: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;
- **Tratamento de incidentes**: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas; e realizar as prováveis correções dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- **Tratamento dos riscos**: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;
- **Usuário**: qualquer pessoa que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação;

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

3. REFERÊNCIAS LEGAIS E NORMATIVAS

- Lei nº 12.550, de 15 de dezembro de 2011, que autoriza o Poder Executivo a criar a empresa pública denominada Empresa Brasileira de Serviços Hospitalares - EBSERH;
- Decreto nº 7.082, de 27 de janeiro de 2010, que institui o Programa Nacional de Reestruturação dos Hospitais Universitários Federais – REHUF;
- 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;
- Lei nº 9.983, de 14 de julho de 2000, que 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;
- Lei 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;
- Lei nº 12.527, de 18 de novembro de 2011, que regulamenta o acesso às informações públicas;
- Decreto Nº 8.638, de 15 de janeiro de 2016, que institui a Política de Governança Digital.
- Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores – Internet;
- Decreto Lei nº 5.452, de 1º de maio de 1943, que aprova a Consolidação das Leis do Trabalho;
- Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;
- Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, e dá outras providências, e respectivas normas complementares;
- Instrução Normativa GSI/PR nº 02, de 5 de fevereiro de 2013, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;
- Norma ABNT NBR ISO/IEC 27001:2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

- Norma ABNT NBR ISO/IEC 27002:2013, que institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;

- Norma ABNT NBR ISO/IEC 27005:2011, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação;

4. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações e suas ações serão norteadas pelos seguintes princípios, assim definidos:

- **Celeridade:** As ações de SIC devem oferecer respostas rápidas a incidentes e falhas de segurança;
- **Ética:** Os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIC;
- **Clareza:** As regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
- **Legalidade:** As ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do Complexo HUPES e EBSERH;
- **Publicidade:** Transparência no trato da informação, observados os critérios legais.

5. DIRETRIZES GERAIS

As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo Complexo HUPES, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, deverá sempre ser protegida adequadamente, de acordo com esta política.

Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo Complexo HUPES serão utilizados estritamente para seu propósito.

É vedado, a qualquer usuário do Complexo HUPES, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo,

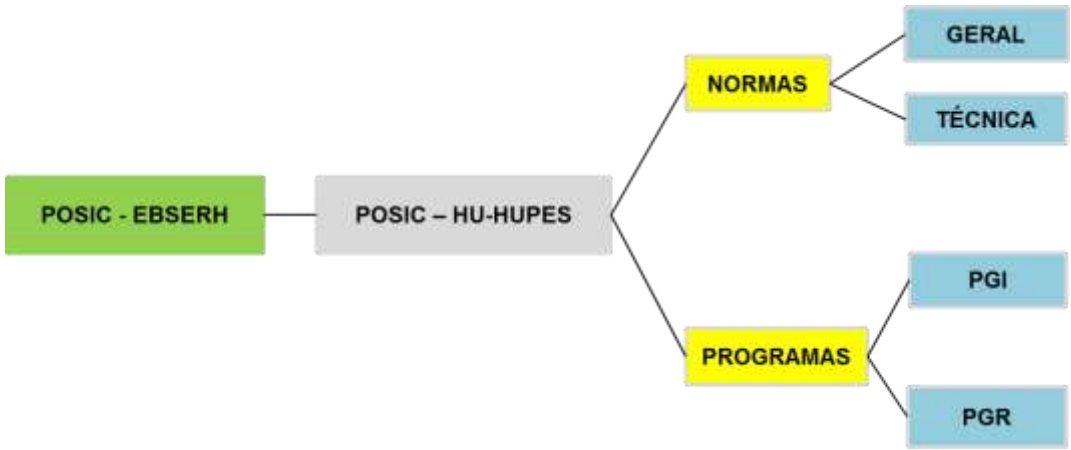
possam constranger assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

As diretrizes desta POSIC constituem os principais pilares da Gestão de Segurança da Informação e Comunicação, norteando a elaboração dos seguintes documentos relacionados abaixo:

- Normas de Gestão da Segurança da Informação
  - Norma Geral de POSIC do Complexo HUPES: destinado aos usuários.
  - Norma Técnica de POSIC do Complexo HUPES: destinado ao SGPTI.
- Programas de Gestão de Riscos de Segurança da Informação e Comunicação
  - Plano de Gerenciamento de Riscos de Segurança da Informação e Comunicação (PGR).
  - Plano de Gerenciamento de Incidentes de Segurança da Informação e Comunicação (PGI).

Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta POSIC, devem ser direcionados ao Subcomitê Gestor de Segurança da Informação e Comunicações local (SGSIC).

Figura 01 – Conjunto de Documentos que representam a Gestão de SIC e de Riscos no Complexo HUPES



6. DIRETRIZES ESPECÍFICAS

6.1. Subcomitê Gestor de Segurança da Informação e Comunicação (SGSIC)

Deve ser formalmente constituído por colaboradores nomeados pela Superintendência do COMPLEXO HUPES. Sendo a sua composição formada por:

- **Um representante e suplente da Gerência de Atenção à Saúde;**
- **Um representante e suplente da Gerência de Administração;**
- **Um representante e suplente da Gerência de Ensino e Pesquisa;**
- **Um representante e suplente do Setor de Gestão de Processos e Tecnologia da Informação;**
- **Um representante e suplente do Setor Jurídico;**
- **Um representante e suplente da Unidade de Planejamento;**
- **Um representante e suplente do Serviço de Comunicação Social;**
- **Um representante e suplente da Ouvidoria.**

O SGSIC deverá reunir-se semestralmente, ou a qualquer tempo sempre que for necessário, para deliberar sobre algum incidente grave ou definição relevante para o Complexo HUPES.

O SGSIC poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico.

6.2. Gerenciamento de Segurança da Informação e Comunicações (GESIC)

Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade do negócio. As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Os requisitos de SIC do Complexo HUPES devem ser explicitamente citados em todos os termos celebrados entre a instituição e terceiros, através de cláusula específica

sobre a obrigatoriedade de atendimento às diretrizes desta política, bem como deverá ser exigido o **"Termo de compromisso de uso dos ativos de tecnologia da informação do Complexo HUPES"**.

6.3. Gerenciamento de Riscos de Segurança da Informação e Comunicações (GRSIC)

O GRSIC 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 seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

Qualquer instância administrativa, assistencial ou de ensino do Complexo HUPES torna-se uma área responsável por ativos de informação.

O GRSIC deve ser realizado no âmbito do Complexo HUPES, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizado periodicamente, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades. Trata-se de um instrumento do programa de Gerenciamento de Riscos que deve incluir um Plano de Gerenciamento de Riscos (PGR) e um Plano de Gerenciamento de Incidentes (PGI).

O PGR consiste no processo de identificar, avaliar e administrar eventos diante de incertezas críticas.

O PGI definirá responsabilidade e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

6.3.1. Plano de Gerenciamento de Riscos (PGR)

A gestão de riscos é um processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos positivos ou negativos capazes de afetar os objetivos, programas, projetos ou processos de trabalho do Complexo HUPES nos níveis estratégico, tático e operacional.

Seu objetivo é aumentar a probabilidade e o impacto dos riscos positivos (oportunidades) e reduzir a probabilidade e o impacto dos riscos negativos (ameaças).

6.3.2. Plano de Gerenciamento de Incidentes (PGI)

As medidas constantes deste plano deverão assegurar disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até o retorno à normalidade.

As áreas do Complexo HUPES que dependam de recursos de TIC serão cobertas pelo PGI, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do Complexo HUPES.

6.4. Gerenciamento de Ativos de Informação

O gerenciamento de ativos de informação deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua.

Os ativos de informação do Complexo HUPES deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de SIC e são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação.

É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Complexo HUPES.

6.5. Tratamento da Informação

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do Complexo HUPES.

Os dados, as informações e os sistemas de informação do Complexo HUPES devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

A informação deve ser protegida de acordo com sua classificação, o seu valor, sensibilidade e criticidade.

6.6. Classificação da Informação

Toda informação criada, manuseada, armazenada, transportada ou descartada do Complexo HUPES será classificada de acordo com a Lei nº 12.527, de 18 de novembro 2011.

O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo Complexo HUPES e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas. As informações sob gestão do Complexo HUPES terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento com o objetivo de limitar a exploração às informações exclusivas da instituição.

6.7. Monitoramento, Auditoria e Conformidade

O monitoramento, auditoria e conformidade observarão o seguinte:

- O uso dos recursos de TIC disponibilizados pelo Complexo HUPES é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;
- A entrada e saída de ativos de informação do Complexo HUPES serão registradas e autorizadas por autoridade competente mediante procedimento formal;
- Qualquer instância do Complexo HUPES poderá ser um canal de comunicação para receber denúncias de infração a qualquer parte desta POSIC.

6.8. Controle de Acesso

As regras de controle aos meios de identificação dos usuários nos sistemas corporativos, intranet, internet, informações, dados do Complexo HUPES deverão ser definidas e regulamentadas, por meio da "Norma Geral de SIC", com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição, sem prejuízo de eventuais normas de controle de acesso institucionais.

6.9. Uso do Correio Eletrônico

O correio eletrônico é um recurso de comunicação corporativa do Complexo HUPES e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta POSIC e da "Norma Geral de SIC", além das demais diretrizes do governo.

6.10. Acesso à internet

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por meio da "Norma Geral de SIC", atendendo as determinações dessa POSIC, e demais orientações governamentais e legislação em vigor.

6.11. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação são restritas ao SGPTI e devem observar critérios e controles de segurança para garantir o respeito aos atributos básicos de segurança da informação.

6.12. Propriedade Intelectual

As informações produzidas por usuários internos ou externos, no exercício de suas funções, são patrimônio intelectual do COMPLEXO HUPES e não cabe a seus criadores qualquer forma de direito autoral, ressalvando o direito de autoria, se for o caso.

É vedada a utilização de patrimônio intelectual do COMPLEXO HUPES em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

6.13. Uso de Computação em Nuvem

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 à determinações desta POSIC e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

6.14. Uso de Dispositivos Móveis

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações, internet e e-mail do COMPLEXO HUPES, devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a essa POSIC e regida por meio da “Norma Geral de SIC”.

7. PENALIDADES

Ações que violem essa política ou quaisquer de suas diretrizes, normas ou procedimentos ou que quebrem os controles de Segurança da Informação e

Comunicações serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à instituição, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

8. COMPETÊNCIAS E RESPONSABILIDADES

8.1. Cabe à Superintendência do COMPLEXO HUPES:

- Promover a cultura de segurança da informação e comunicações;
- Aprovar a Política de Segurança da Informação e Comunicações (POSIC);
- Nomear o Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC).

8.2. Cabe ao Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC):

- Promover a cultura e divulgação da SIC;
- Elaborar, avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do COMPLEXO HUPES e às legislações vigentes;
- Coordenar as ações de segurança da informação e comunicações;
- Aprovar a abertura de processo administrativo mediante constatação de quebra de segurança da informação;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Superintendência do COMPLEXO HUPES os resultados consolidados de tais investigações e avaliações;
- Propor recursos necessários às ações de Segurança da Informação e Comunicações;
- Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;
- Propor e atualizar normas relativas à Segurança da Informação e Comunicações;
- Prover os meios necessários para capacitação, o aperfeiçoamento técnico dos usuários, bem como prover a infraestrutura necessária para o seu funcionamento;

8.3. Cabe ao SGPTI:

O SGPTI, como mantenedor dos ativos de TIC, será regido por norma própria descrita na “Norma Técnica de SIC”

8.4. Proprietário de Ativos de Informação:

- Proteger e manter os ativos de informação;
- Seguir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com essa POSIC;

- Garantir a segurança dos ativos de informação sob sua responsabilidade através de monitoramento contínuo;
- Comunicar as exigências de SIC a todos os usuários sob sua responsabilidade;
- Conceder e revogar acessos aos ativos de informação;
- Comunicar ao SGPTI e/ou SGSIC a ocorrência de incidentes de SIC; e
- Designar custodiante dos ativos de informação, quando aplicável.

8.5. Cabe ao Custodiante dos Ativos de Informação:

- Proteger e manter os ativos de informação;
- Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com essa POSIC.
- Seguir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com essa POSIC.

8.6. Terceiros e Fornecedores:

- Tomar conhecimento dessa POSIC;
- Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
- Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

8.7. Cabe Aos Usuários:

- Proteger e manter os ativos de informação sob sua responsabilidade;
- Conhecer e cumprir essa POSIC;
- Assinar o "Termo de compromisso de uso dos ativos de TIC do COMPLEXO HUPES";
- Comunicar os incidentes que afetam à segurança dos ativos de informação e comunicações à chefia imediata.

9. DIVULGAÇÃO E CONSCIENTIZAÇÃO

A divulgação das regras e orientações de segurança aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na

Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança dentro do COMPLEXO HUPES.

Cabe ao SGSIC providenciar a divulgação interna desta POSIC e das normas, inclusive com publicação permanente na página da intranet do COMPLEXO HUPES, para que seu conteúdo possa ser consultado a qualquer momento e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIC.

10. ATUALIZAÇÃO

A segurança da informação e comunicações, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Os instrumentos normativos gerados a partir dessa POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas da EBSERH Sede conforme os seguintes critérios:

1) Política de Segurança da Informação e Comunicações (POSIC):

- Nível de Aprovação: Superintendência do Complexo HUPES
- Periodicidade de Revisão: A cada dois anos

2) Normas e Planos de SIC:

- Nível de Aprovação: SGSIC
- Periodicidade de Revisão: Anual

3) Procedimentos Operacionais:

- Nível de Aprovação: SGPTI
- Periodicidade de Revisão: Anual

Essa POSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

11. ASSINATURA

	Titular/Suplente	Data	Assinatura
CRIAÇÃO/VALIDAÇÃO	Monalisa Viana Sant'Anna/ Lindemberg Assunção Costa		
	Licia Pereira Lima Bastos/ Erica Marques Jorge		
	Regina de Jesus Santos/ Renata Lopes Britto		
	Givaldo Barbosa Macedo Junior/Verena Nunes Martins		
	Wilker Invenção Azevedo de Oliveira/ Anilton de Oliveira Antunes		
	Suzy Ribeiro dos Santos Moreno/ Luciana Batista Sacramento dos Santos		
	Maralba Oliveira Santos Jordão/ Danilo da silva Soares		
	Ederaldo Muniz Barreto Junior/Alexandre Jesus de Souza		
APROVAÇÃO	Dr. Antônio Carlos Lemos		

12. CONTROLE DE VERSÃO

VERSÃO	DATA	DESCRIÇÃO DAS ATUALIZAÇÕES
1.0	Janeiro/2010	Versão Original
2.0	Novembro/2012	Formatação e numeração
3.0	Agosto/2014	Atualização de conteúdo
4.0	Abril/2017	Atualização conforme a Norma Complementar 03, da Instrução Normativa 01, do GSIPR e Política de Segurança da EBSERH.