EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

HOSPITAL DAS CLÍNICAS DA UFPE

Boletim de Serviço

Nº 76, 18 de maio de 2018

Ministério da
Educação

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES - EBSERH

Hospital das Clínicas- Universidade Federal de Pernambuco

Av. Prof. Moraes Rego S/N

Cep: 50740-900 Várzea- Recife/PE

Telefone: (081) 2126-3633

ROSSIELI SOARES DA SILVA

Ministro de Estado da Educação

KLEBER DE MELO MORAIS

Presidente

FREDERICO JORGE RIBEIRO

Superintendente

MARCOS ANTÔNIO VIEGAS FILHO

Gerente Administrativo e Financeiro

DÉLIA TEREZA DUARTE BORBA

Gerente de Atenção à Saúde

CÉLIA MARIA MACHADO BARBOSA DE CASTRO

Gerente de Ensino e Pesquisa

SUMÁRIO

SUPERINTENDÊNCIA

RETIFICAÇÃO

Portaria nº 090, de 11 de maio de 2018

O Superintendente do Hospital das Clínicas Da Universidade Federal de Pernambuco, filial Ebserh, no uso das atribuições que lhes são conferidas nos termos do artigo 16, alíneas "h", "i" e "j" do Regimento do Hospital das Clínicas, aprovado em 2 de fevereiro de 1979 e pela Portaria nº 125 de 11 de dezembro de 2012 da Empresa Brasileira de Serviços Hospitalares, resolve:

Retificar a Portaria nº 88, de 08 de maio de 2018. Onde se lê: "...JOSÉ ROBERTO ROCHA DA SILVA, matrícula/Siape: 1424932, representante da Gerência de Atenção à Saúde - Ambulatório de Cardiologia..." Leia-se: "...JOSÉ ROBERTO ROCHA DA SILVA, matrícula/Siape: 1424932, representante da Gerência de Atenção à Saúde - Ambulatório de Hematologia;..." E onde se lê: "...representantes da Superintendência do HC-UFPE – WAGNER DE LIMA CORDEIRO, matrícula/Siape: 1295815, Chefia dos Ambulatórios ..." Leia-se: "... representantes da Superintendência do HC-UFPE – WAGNER DE LIMA CORDEIRO, matrícula/Siape: 2295815, Enfermeiro da Estabilização;..."

Profª Célia Maria Machado Barbosa Castro
Superintendente em exercício

DIVULGAÇÃO

Portaria nº 091, de 17 de maio de 2018

O Superintendente do Hospital das Clínicas Da Universidade Federal de Pernambuco, filial Ebserh, no uso das atribuições que lhes são conferidas nos termos do artigo 16, alíneas "h", "i" e "j" do Regimento do Hospital das Clínicas, aprovado em 2 de fevereiro de 1979 e pela

Portaria nº 125 de 11 de dezembro de 2012 da Empresa Brasileira de Serviços Hospitalares, resolve:

Divulgar a Instrução Normativa Nº 001 DE 31 DE JULHO DE 2017, aonde o CHEFE DO SETOR DE GESTÃO DE PROCESSOS E TECNOLOGIA DA INFORMAÇÃO – SGPTI**,** no uso das atribuições que lhe são conferidas pela *Portaria No. 127 EBSERH/HC-UFPE de 20/07/2017*, que dispõe sobre o estabelecimento da Política de Governança de Tecnologia da Informação (PGTI) e a criação do Comitê de Governança de Tecnologia da Informação (CGTI), e alinhado às estratégias definidas pela Diretoria de Gestão de Processos e de Tecnologia da Informação (DGPTI) da EBSERH Sede;

CONSIDERANDO as informações geradas internamente, adquiridas ou absorvidas e os recursos computacionais, como patrimônio da **instituição**: HOSPITAL DAS CLÍNICAS DA UNIVERSIDADE FEDERAL DE PERNAMBUCO – HC-UFPE;

CONSIDERANDO a relevância da padronização do uso das informações e dos recursos computacionais;

CONSIDERANDO essas informações e recursos essenciais ao desempenho das atribuições do HC-UFPE;

CONSIDERANDO a importância de aprimorar e sistematizar em política as práticas institucionais de segurança, as quais contribuem para assegurar o suporte necessário ao pleno exercício das funções da instituição;

CONSIDERANDO a necessidade de estabelecer diretrizes gerais para orientar a elaboração de normas específicas de segurança e a definição de procedimentos que norteiem os processos de trabalho corporativos;

CONSIDERANDO a Instrução Normativa nº 01/2008, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta.

CONSIDERANDO a Portaria EBSERH nº 34, de 14 de março de 2016, que redefiniu o Comitê Gestor de Segurança da Informação e Comunicações da Ebserh-Sede (CGSIC) e instituiu diretrizes para a Gestão da Segurança da Informação e Comunicações na Empresa.

CONSIDERANDO a hierarquia de políticas indicada no Anexo D da NBR ISO/IEC 27003:2011, que prevê uma política geral de segurança de alto nível e políticas de alto nível sobre temas específicos;

CONSIDERANDO as boas práticas em segurança preconizadas pelas normas NBR ISO/IEC 22301:2012, 27001:2013, 27002:2013 e 27003:2011;

CONSIDERANDO o advento da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), que 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;

CONSIDERANDO o disposto nos incisos IV, X e XII do art. 5º da Constituição Federal;

RESOLVE:

Instituir a **POLÍTICA DE USO DOS RECURSOS COMPUTACIONAIS E SEGURANÇA DA INFORMAÇÃO**, no âmbito do HC-UFPE.

CAPÍTULO I - Do Objetivo

Art.1º. A **Política de Uso dos Recursos Computacionais e Segurança da Informação do HC-UFPE** procura regulamentar o *uso das Tecnologias da Informação e Comunicação (TIC)* no âmbito desta instituição, onde a *Segurança da Informação* é uma perspectiva-chave. Para efeito de simplificação, esta política será denominada de "**Política de Uso de TI**" e compreenderá todos os tópicos relacionados a este tema com a finalidade garantir a autenticidade, a integridade, a confidencialidade e a disponibilidade das informações armazenadas em meios eletrônicos, bem como disciplinar o uso dos recursos computacionais por parte todos os seus colaboradores no exercício de suas atribuições.

Parágrafo único. A Política de Uso dos Recursos Computacionais e Segurança da Informação observam os princípios, objetivos, diretrizes e processos previstos nesta Instrução Normativa e na Portaria No. 127 EBSERH/HC-UFPE de 20/07/2017 que institui a PGTI, bem como as disposições constitucionais, legais e regimentais vigentes.

Art. 2º. Para os efeitos desta Instrução Normativa, entende-se por:

segurança institucional: conjunto de ações integradas destinadas à proteção de pessoas, processos de negócio e ativos da instituição;

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;

incidente de segurança: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a incolumidade física de pessoas, a integridade patrimonial ou a segurança da informação;

colaborador ou usuário: servidor, funcionário, prestador de serviço terceirizado, estagiário ou qualquer pessoa com vínculo permanente ou transitório com a instituição que tenha acesso, de forma autorizada, às informações ou às dependências da instituição;

dignitário: autoridade da instituição, de outros órgãos públicos, entidades ou de organismos internacionais;

criticidade: grau de importância de um determinado ativo institucional para a continuidade do negócio da instituição;

interrupção: paralisação ou redução do desempenho de uma ou mais atividades por período de tempo considerado inaceitável para a organização;

atividade crítica: atividade cuja interrupção pode causar danos financeiros, operacionais, legais ou de imagem, considerados inaceitáveis pela instituição;

emergência: evento súbito que requer ação imediata devido à probabilidade de comprometer a incolumidade física das pessoas, interromper atividades críticas para o negócio ou causar riscos ao patrimônio da instituição;

resiliência institucional: poder de recuperação ou capacidade da organização para resistir aos efeitos de emergências ou interrupções;

Art. 3º A segurança institucional abrange aspectos humanos, físicos e tecnológicos da organização e orienta-se pelos seguintes princípios:

ativo: termo básico utilizado para expressar os bens, valores, créditos, direitos e assemelhados que, compõem o patrimônio da instituição e que são avaliados pelos respectivos custos.

precedência: a segurança das pessoas e da vida humana tem precedência sobre qualquer ativo da instituição;

invulnerabilidade: os ativos que compõem o patrimônio da instituição devem ter a integridade garantida, sendo protegidos de acessos não autorizados e de outros danos;

prevenção: os efeitos de eventos com manifesta probabilidade de ocorrência e com potencialidade de causar danos operacionais, legais, financeiros, à integridade física das pessoas

e à imagem da instituição devem ser evitados ou minimizados, adotando-se para isso um conjunto de medidas que busquem melhorar a resiliência institucional;

participação: autoridades da instituição, servidores, colaboradores e demais pessoas com acesso às dependências da organização devem atuar conjuntamente com vistas à proteção e à preservação dos ativos do hospital;

conscientização: construção de consciência institucional voltada à segurança, de modo a reduzir os riscos às pessoas e aos ativos da instituição, bem como permitir a efetivação dos princípios da prevenção e da participação; e

gerenciamento de segurança: o planejamento, execução e acompanhamento de medidas de segurança institucional devem ser realizados com base no potencial danoso de riscos e ameaças às pessoas, à instituição ou aos seus ativos mediante processo contínuo, dinâmico, flexível e permanente.

Art. 4º. Ficam estabelecidos os seguintes tópicos que deverão nortear os demais detalhamentos desta política:

Acesso e privacidade do ambiente e dos ativos de TIC;

Arquiteturas e equipamentos;

Interconexão e interoperabilidade;

Uso dos recursos;

Organização e formatação de informações;

Aquisição de bens e serviços;

Desenvolvimento e Aquisição de aplicações;

Gerenciamento e Governança de TIC;

Capacitação de Recursos Humanos.

CAPÍTULO II - Da Operacionalização

Art. 5º. As Políticas de Uso de TI serão publicadas no **Portal de Intranet do HC-UFPE**, compartilhado com todos os segmentos do HC-UFPE, e serão divulgadas por meio eletrônico para cada unidade organizacional do HC-UFPE.

Parágrafo único. Cada gestor de unidade organizacional ficará responsável pela divulgação e ações correspondentes.

Art. 6º. Com a expansão do processo de Governança de Tecnologia da Informação e Comunicação (TIC) serão implantadas outras ações como a gestão do Plano Diretor de Tecnologia da Informação (PDTI), dos indicadores e dos acordos de nível de serviço, que farão referência a esta política.

Art. 7º. Os Gestores cada unidade administrativa da instituição e seus respectivos colaboradores, deverão assinar solidariamente um **Termo de Responsabilidade** declarando ciência da Política Uso de TI, e responsabilizando-se garantir o seu cumprimento e evitar qualquer transgressão ao nela disposto.

CAPÍTULO III - Das Diretrizes

Art. 8º. As diretrizes da Política de Uso de TI estão relacionadas sob quatro enfoques:

I - **Desenvolvimento** da Ação, buscando a:
Padronização da infraestrutura;
Descentralização das responsabilidades, numa autonomia responsável;
Ampla participação da comunidade;
Atuação preventiva;
Potencialização das oportunidades;
Preservação das características culturais.
II - **Gerenciamento**, atuando de forma:
Competitiva;
Orientada por metas;
Avaliada por resultados.
III - **Orientação**, obedecendo aos princípios:
Orientado para o Público-Alvo;
Validado pela satisfação do Usuário/Cliente.
IV - **Alinhamento**, com:
A **Política de Segurança da Informação e Comunicações (PoSIC)**, definida pela *Diretoria de Gestão de Processos e de Tecnologia da Informação (DGPTI) da EBSERH Sede*; e,

Com a **Política de Segurança da Informação e Comunicações da Universidade Federal de Pernambuco** definida pela *Pró-Reitoria de Comunicação, Informação e Tecnologia da Informação (PROCIT-UFPE).*

A **Política de Governança de Tecnologia da Informação** do Hospital das Clínicas da Universidade Federal de Pernambuco (PGTI/HC-UFPE).

CAPÍTULO IV - Da Forma de Divulgação das Políticas

Art. 9º. As Políticas de Uso de TI e Segurança da Informação serão implantadas, regulamentadas e atualizadas através de Instruções Normativas e Normas Técnicas, emitidas pelo SGPTI.

Art. 10º. Todos os documentos de interesse ao âmbito do HC-UFPE serão disponibilizados na Intranet do HC-UFPE.

CAPÍTULO V - Das Responsabilidades

Art. 11º. As informações e os recursos computacionais do HC-UFPE têm por finalidade servir às suas atividades bem como possibilitar a prestação de serviços à sociedade.

Art. 12º. Cabe ao Chefe do SGPTI designar os responsáveis de cada Serviço de TI e disponibilizar oportunamente na Intranet as informações dos Serviços de TI e seus respectivos responsáveis, bem como divulgar outras informações úteis aos usuários sobre os serviços em questão.

Seção I - Dos Direitos dos Usuários Internos

Art. 13º. São direitos dos usuários internos:

Utilizar os recursos computacionais;

Ter conta para acesso à rede corporativa;

Ter acesso aos registros de suas ações na rede corporativa;

Ter acesso às informações que lhe são franqueadas;

Ter privacidade das informações na sua área privativa;

Solicitar suporte técnico ao SGPTI.

Seção II - Das Obrigações dos Usuários Internos

Art. 14º. São obrigações dos usuários internos:

Adotar as regras definidas nesta Instrução Normativa e nos demais instrumentos oficiais derivados da presente política;

Responder pelo uso exclusivo de sua conta;

Manter em caráter confidencial e intransferível a senha de acesso aos recursos computacionais;

Fazer uso dos recursos computacionais com segurança para trabalhos de interesse exclusivo da instituição;

Identificar, classificar e enquadrar as informações da rede corporativa, relacionadas às suas atividades;

Zelar por toda e qualquer informação armazenada na rede corporativa contra alteração, destruição, divulgação, cópia e acesso não autorizados;

Informar à sua gerência os descumprimentos das regras estabelecidas nesta Instrução Normativa;

Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail corporativo, exclusivamente por meio de suas credenciais eletrônicas (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância às disposições contidas neste documento;

Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;

Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar conhecimento pessoas não autorizadas;

Não me ausentar da estação de trabalho sem efetuar o “Bloqueio da sessão” no equipamento em uso, em caso de curto tempo de ausência. Ou fazer o *Logoff* (desconexão de sua credencial

eletrônica: usuário/senha) para os demais casos, evitando assim o uso indevido de meu *Login* (credencial eletrônica) por terceiros;

Alterar a senha, sempre que requisitado ou que tenha suspeição de seu conhecimento por terceiros. Na elaboração ou alteração de sua senha, o usuário não deverá utilizar combinações simples, ou dados pessoais de fácil reconhecimento que possam ser facilmente descobertas, como por exemplo: número de matrícula, nomes de familiares ou datas;

Assumir total responsabilidade com os arquivos presentes na pasta COMPARTILHADA do seu setor;

Gerenciar sua pasta PESSOAL, observando a limitação do espaço de quota[1] disponível, para garantir que sejam armazenados arquivos de conteúdo meramente institucionais, sendo VEDADA o armazenamento de arquivos de extensões descritas no Item XII do **Art. 15º**;

Salvaguardar em caráter confidencial e intransferível o uso de seu Correio Eletrônico (E-mail) corporativo, não permitindo o seu uso por terceiros, por se tratar de canal onde trafegam informações de propriedade da instituição;

Relatar imediatamente ao SGPTI qualquer problema ou incidente referente ao uso dos equipamentos do parque tecnológico do HC-UFPE, da Rede de Computadores da instituição, assim como referente ao uso das suas credenciais eletrônicas (usuário/senha), bem como de sua conta de Correio Eletrônico (E-mail) corporativo;

Assumir a responsabilidade por dano causado por algum procedimento de iniciativa própria de tentativa de modificação da configuração, física ou lógica, do computador e/ou rede sem a autorização expressa da SGPT;

Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

Responsabilizar-se pelos danos causados em decorrência da não observância às regras de proteção da informação e dos recursos computacionais, nos termos previstos nesta Instrução Normativa;

Estar ciente de que constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos Sistemas ou Banco de Dados da Administração Pública, com fim de obter vantagem indevida para si ou para outrem, ou mesmo

[1] Este parâmetro operacional deverá ser regulamentado por Norma Técnica específica.

para causar dano; bem como modificar ou alterar o Sistema de Informações ou Programa de informática sem autorização ou sem a solicitação de autoridade competente;

Responder, em todas as instâncias, pelas consequências das ações ou omissões que possam pôr em risco e/ou comprometer o uso exclusivo de duas credenciais eletrônicas (usuário/senha), ou ainda das transações e informações a que tenha acesso.

Seção III - Das Vedações aos Usuários Internos

Art. 15º. É expressamente vedado aos usuários internos:

Usar, copiar ou armazenar software ou qualquer informação, utilizando recursos computacionais, em violação à lei de direitos autorais;

Utilizar os recursos computacionais para constranger, assediar, prejudicar ou ameaçar qualquer pessoa;

Fazer-se passar por outra pessoa ou esconder sua identidade quando utilizar os recursos computacionais;

Instalar ou retirar componentes dos recursos computacionais, sem a expressa autorização do SGPTI;

Instalar, alterar ou remover software em qualquer dos recursos computacionais, sem a expressa autorização do SGPTI;

Retirar qualquer recurso computacional do HC-UFPE, sem a expressa autorização do SGPTI;

Divulgar informações confidenciais ou de uso interno;

Acessar ou alterar, sem autorização, dados armazenados nos recursos computacionais;

Violar os sistemas de segurança dos recursos computacionais;

A navegação nos sites pertencentes às categorias abaixo:

Pornográfico e/ou de caráter sexual;

De Pornografia infantil (pedofilia);

De compartilhamento de arquivos (ex.: peer to peer, Bit Torrent, Emule, etc.);

Que faça apologia ao terrorismo;

Que faça apologia às drogas;

Que façam apologia a ações ou conhecimentos relacionados a pessoas aficionadas por informática que utilizam seu conhecimento para fins criminosos (Crackers);

De relacionamento (Badoo, Tinder, Ashley Madison, etc.);

Que façam apologia à violência e agressividade de qualquer natureza (racismo, preconceito, etc.);

Que realizem violação de direito autoral (pirataria, etc.);

De entretenimento (áudio ou vídeo), salvo com conteúdo relacionados diretamente às atribuições profissionais do colaborador;

Conteúdo impróprio, ofensivo, ilegal, discriminatório, e similares.

A troca de arquivos de vídeo ou música, bem como de quaisquer informações que estejam incluídas nas categorias no Item X;

A transferência/instalação de qualquer tipo de programa para a rede interna da instituição sem a expressa autorização do SGPTI;

A realização de downloads de arquivos de extensões tipo: .EXE, .MP3, .WAV, .BAT, .COM, .SYS, .SCR, .MPEG, .AVI, .RMVB, .DLL, e de programas de entretenimento ou jogos, salvo os estritamente relacionados ao exercício de suas atribuições;

O acesso a programas de TV na internet ou qualquer conteúdo sob demanda (streaming), quando não relacionado diretamente às atribuições profissionais do colaborador;

O uso de jogos, incluindo os da internet (onlines);

Demais restrições regulamentadas por Normas Técnicas específicas.

Seção IV - Dos Gerentes e Chefes de Divisão, Setor, Unidade ou Serviço

Art. 16º. Compete aos gerentes e chefes de unidades administrativas:

Solicitar ao SGPTI novos serviços, sistemas de informação e recursos computacionais;

Monitorar a observância desta Instrução Normativa pelos seus subordinados, devendo informar à gerência superior os casos de descumprimento;

Autorizar a criação, o bloqueio e o cancelamento de credenciais eletrônicas, bem como a modificação dos perfis de acesso aos Sistemas de Informação em Saúde, para seus subordinados, desde que as permissões não sejam reguladas pelo Setor de Regulação e Avaliação em Saúde - SRAS;

Ser solidariamente responsável pela permissão atribuída ao seu colaborador, assim como pelos atos destas decorrentes;

Informar ao SGPTI o afastamento (permanente ou definitivo) de colaboradores do quadro de pessoal, assim como a eventual transferência de colaboradores entre setores da instituição: buscando evitar o acesso indevido de ex-colaboradores, ou de colaboradores cujas atribuições foram modificadas, que venham a colocar em risco a segurança do ambiente tecnológico corporativo, incluindo o uso Sistemas de Informação em Saúde.

Seção V - Da Competência do SGPTI

Art. 17º. Compete ao SGPTI:

Monitorar a observância desta Instrução Normativa, devendo, em caso de descumprimento, informar ao Superintendente e tomar ações imediatas de restrições de uso dos serviços, de acordo com o disposto nas normas, a fim de garantir a segurança do ambiente tecnológico corporativo;

Implantar a autorização/restrição de acesso às informações do ambiente tecnológico corporativo;

Instalar, configurar, manter e auditar os serviços de TI, tais como uso de pastas compartilhadas, correio eletrônico e internet;

Instalar, configurar, manter e auditar os recursos computacionais;

Fornecer o suporte, manter e auditar os sistemas de informação;

Estabelecer requisitos para acesso externo ao ambiente tecnológico corporativo;

Registrar as ações dos usuários no ambiente tecnológico corporativo;

Fornecer aos usuários internos consulta aos registros de suas ações no ambiente tecnológico corporativo;

Realizar inventário periódico no parque tecnológico da instituição, visando a racionalização do uso dos recursos computacionais, inclusive estando autorizada a recolher e/ou realocar equipamentos sem uso ou subutilizados, mediante comunicação prévia à chefia imediata dos setores/serviços;

Efetuar revisão periódica das Políticas instituídas por esta Instrução Normativa e/ou derivadas desta, visando seu aprimoramento constante;

Elaborar e manter os documentos vinculados às Políticas instituídas por esta Instrução Normativa e/ou derivadas desta;

Garantir o maior grau possível de adesão aos princípios de segurança definidos no CAPÍTULO I desta Instrução Normativa;

Garantir que as políticas de licenciamento de software sejam estritamente obedecidas;

Divulgar a presente política no âmbito do HC-UFPE.

Seção VI - Das Proibições do SGPTI

Art. 18º. É vedado ao SGPTI (e seus agentes) atender a solicitações de serviços de informática em softwares ou equipamentos não pertencentes ao HC-UFPE ou que não estejam a serviço desta instituição.

Parágrafo único. A fim de garantir o acesso a serviços da rede corporativa, caberá ao SGPTI fornecer orientações sobre a configuração necessária em softwares ou equipamentos não pertencentes à instituição, considerando que este acesso pode ocorrer com restrições, visando a garantia da segurança do ambiente tecnológico corporativo.

Art. 19º. É vedado ao SGPTI (e seus agentes) acessar informações de usuários que não sejam para o exclusivo cumprimento das atribuições de sua competência, conforme estabelecido pelo **Art. 17º.**

CAPÍTULO VI - Das Disposições Finais

Art. 20º. As ações de cada usuário no ambiente tecnológico corporativo serão registradas para consultas, monitoramento ou auditorias futuras.

Art. 21º. As infrações ao disposto nesta Instrução Normativa serão tratadas, no que couber, conforme o Estatuto dos Funcionários Públicos Civis da União, Decreto-Lei No 1.713, de 28 de outubro de 1939.

Art. 22º. As infrações ao disposto nesta Instrução Normativa poderão ainda ser enquadradas no Código Penal Brasileiro, conforme responsabilização por crime contra a administração pública tipificado no art. 313-A e 313-B.

Art. 23º. Nos contratos e convênios que impliquem acesso, cessão ou manuseio de informações do HC-UFPE por parte de terceiros, deverá constar cláusula com menção expressa ao dever de observância e cumprimento das Políticas instituídas por esta Instrução Normativa.

Art. 24º. As normas referentes ao ambiente tecnológico corporativo, devido à sua natureza técnica, serão elaboradas e mantidas pelo SGPTI.

Art. 25º. As informações, softwares, processos, procedimentos e métodos, criados pelos colaboradores do HC-UFPE no exercício de suas funções, são patrimônio intelectual desta instituição, não cabendo a seus criadores qualquer forma de direito autoral, a não ser que formalizado expressamente por instrumento reconhecido pela Superintendência.

Art. 26º. Esta Instrução Normativa entra em vigor em 01 de agosto de 2017.

Art. 27º. Revogam-se as disposições em contrário.

Alexandre Luna, PhD

Chefe do Setor de Gestão de Processos e Tecnologia da Informação – SGPTI**.**

Frederico Jorge Ribeiro

Superintendente

Portaria nº 092, de 17 de maio de 2018

O Superintendente do Hospital das Clínicas Da Universidade Federal de Pernambuco, filial Ebserh, no uso das atribuições que lhes são conferidas nos termos do artigo 16, alíneas "h", "i" e "j" do Regimento do Hospital das Clínicas, aprovado em 2 de fevereiro de 1979 e pela Portaria nº 125 de 11 de dezembro de 2012 da Empresa Brasileira de Serviços Hospitalares, resolve:

Divulgar a seguinte Norma Técnica:

Controle do Documento

Produtos Relacionados ao Portfólio SGPTI: SGPTI - Unidade de Infraestrutura – Segurança da Informação – 03-Políticas de Acesso	
Versão: v1 31/07/2017	**Sumário**: Controle da Norma

Autores: Alexandre Luna Manoel Batista Valadão Filho Bartolomeu Alves Bezerra II	Objetivo Fundamentos e Definições Processo Aplicação Penalidades Unidades Envolvidas Distribuição Vigência
Documentos Relacionados: Instrução Normativa SGPTI 001/2017 – Definição de Responsabilidades	
Alterações em relação à versão anterior: N/A	

Objetivo

Estabelecer requisitos mínimos de criação, uso e guarda de senha, a fim de reduzir o risco de acesso não autorizado aos recursos computacionais.

Fundamentos e Definições

Negócio da organização (*core-business*)

É a razão de ser da organização. O motivo pelo qual ela existe. Aquilo no qual está concentrada a sua missão. No caso do HC-UFPE : "*Prestar um serviço de excelência à sociedade nos âmbitos da assistência, do ensino, da pesquisa e da extensão, com o intuito de avançar nos conhecimentos científicos relacionados à saúde, promoção e preservação da vida*"[2].

Ambiente tecnológico corporativo

É o ambiente formado pelo conjunto de *capacidades* e *recursos tecnológicos* utilizados pela organização para apoiar as operações de seu negócio. Ou seja, para apoiar as ações que vão possibilitar à organização o alcance da sua missão institucional. São exemplos dos componentes que fazem parte deste ambiente: rede de computadores, ativos de rede que permitem o funcionamento desta rede e seu acesso a outras redes (como é o caso da internet), equipamentos de segurança da informação, Sistemas de Informação, equipamentos onde estão instalados os

Sistemas de Informação, data center, e mesmo a estação de trabalho sobre a sua mesa, dentre outros.

Credencial eletrônica

É a identidade digital requerida para acessar o ambiente tecnológico corporativo da instituição. É composto pelo *binômio* das informações de: [1] identificação do usuário (login) e [2] sua respectiva senha. Esta credencial é fornecida pelo SGPTI a cada colaborador da instituição que precise acessar o ambiente tecnológico corporativo sob sua gestão.

Nível de acesso

Em função do tipo de atividade de cada usuário e do uso que ele precisar realizar do ambiente tecnológico corporativo no exercício de suas atribuições, o SGPTI deverá configurar um nível de acesso (ou permissão) a este ambiente, mediante solicitação explícita do seu superior, que se torna solidariamente responsável pela permissão atribuída ao seu colaborador, assim como pelos atos destas decorrentes.

Administrador de Serviço

Usuário interno do SGPTI responsável por criar e manter as contas de acesso ao ambiente tecnológico corporativo.

Senha temporária

Nova senha informada por um técnico do SGPTI ao usuário, que deverá ser modificada na primeira oportunidade pelo usuário. Esta senha poderá ser fornecida nas seguintes situações:

Após a criação da conta do usuário;

Devido a esquecimento da senha anterior.

Processo

Premissas

Todo usuário deve ter uma credencial eletrônica pessoal e intransferível.

Qualquer recurso computacional somente poderá ser acessado após a autenticação da credencial eletrônica do usuário, garantida pelo preenchimento correto de sua identidade digital (login) e sua senha.

Critérios para criação da senha

Deve conter 8 (oito) caracteres no mínimo.

Deve ser definida com pelo menos 3 (três) das seguintes características:

Letra maiúscula;

Letra minúscula;

Número;

Caractere especial.

Evitar incluir:

Número da matrícula, CPF ou SIAPE;

Espaço entre os caracteres;

Parte do nome do usuário;

Palavra de dicionário em qualquer idioma, mesmo que utilizando caracteres especiais ou números em substituição a algumas letras, tais como: sport e $p0rt, JESUS e J3SUS;

Palavra baseada em informações pessoais, tais como, placa do carro, nome de familiares e telefone;

Seqüência de letras ou números, tais como, aaabbb, qwerty, zyxwvuts, 123321.

Validade

A senha tem validade de no máximo 3 (três) meses, após o que o usuário será requisitado a modificá-la.

Vigência mínima

A senha não pode ser modificada 2 (duas) vezes no mesmo dia.

Bloqueio da conta

A conta será bloqueada após 5 tentativas consecutivas em que a senha for digitada incorretamente, e somente poderá ser desbloqueada por um técnico do SGPTI.

Aplicação da Norma

Usuário

Direitos

Alterar a senha sempre que achar conveniente, respeitando o exposto nos itens 4.b. (critérios para criação da senha), 4.c (validade) e 4.d (duração mínima).

Abrir um chamado técnico para solicitar uma senha temporária em caso de esquecimento da senha.

Responsabilidades

Manter a confidencialidade da senha. Ou seja, não compartilhar, ceder ou “emprestar” a senha a outra pessoa.

Não solicitar a senha de outro usuário.

Não informar a senha, mesmo que solicitado pelo superior ou pelo SGPTI.

Alterar a senha temporária assim que for informado pelo SGPTI da criação da conta ou da mudança da senha.

Alterar a senha imediatamente após suspeitar que seu sigilo tenha sido violado.

Comunicar ao SGPTI qualquer suspeita de violação, ou de tentativa de violação, do sigilo da senha.

Alterar a senha imediatamente quando solicitado pelo SGPTI.

Não salvar a senha em arquivo, exceto se criptografada.

Não tornar público o método utilizado para criar a senha.

Não reutilizar qualquer senha anterior.

Não relacionar uma nova senha à senha anterior de tal modo que crie uma seqüência. Por exemplo, se a antiga senha fosse XptoA2006, a nova não deveria ser XptoB2007.

Não utilizar a senha em cadastros de terceiros, tais como, sites da Internet, bancos e provedores.

Não utilizar a mesma senha para contas diferentes, no caso do usuário ter mais de uma conta.

Não incluir a senha em sistemas automatizados de autenticação. Por exemplo, não se deve marcar “Lembrar minha senha” na janela de acesso ao Webmail da EBSERH.

SGPTI

Responsabilidades

Informar a senha temporária ao usuário assim que criar a conta ou alterar a senha da conta.

Executar varredura automatizada de busca de senhas fracas a cada 3 meses e tomar as medidas apropriadas em caso de detecção.

Garantir que aplicações adquiridas ou desenvolvidas pelo HC-UFPE ou EBSERH não violem o sigilo das senhas.

Proibições

Solicitar a senha do usuário sob qualquer pretexto.

Alterar a senha de qualquer usuário, exceto quando por ele solicitado.

Penalidades

A não observância dos termos desta Norma Técnica, devidamente apurada e comprovada, implica bloqueio de sua credencial eletrônica. Como consequência o usuário não poderá durante o bloqueio utilizar serviços como: acesso à internet e acesso à rede, por exemplo.

O caso será informado ao usuário interno infrator e seu superior imediato para ciência, e ao Chefe do SGPTI para deliberação.

Unidades Envolvidas

SGPTI: criação e manutenção desta Norma Técnica.

Demais setores HC-UFPE: aplicação das políticas.

Distribuição

Intranet da instituição: Conteúdo completo.

Imprensa da instituição: Comunicado da inclusão ou alteração de novas políticas.

Vigência

Esta Política entrará em vigor a partir da data de sua publicação, revogando-se as disposições em contrário.

Hospital das Clínicas da Universidade Federal de Pernambuco, em, 31 de julho de 2017

Alexandre Luna, PhD

Chefe do Setor de Gestão de Processos e Tecnologia da Informação – SGPTI.

Frederico Jorge Ribeiro

Superintendente

Portaria nº 093, de 17 de maio de 2018

O Superintendente do Hospital das Clínicas Da Universidade Federal de Pernambuco, filial Ebserh, no uso das atribuições que lhes são conferidas nos termos do artigo 16, alíneas "h", "i" e "j" do Regimento do Hospital das Clínicas, aprovado em 2 de fevereiro de 1979 e pela Portaria nº 125 de 11 de dezembro de 2012 da Empresa Brasileira de Serviços Hospitalares, resolve:

Divulgar a seguinte Norma Técnica:

Controle do Documento

Produtos Relacionados ao Portfólio SGPTI: SGPTI - Políticas de Uso do Recursos de Tecnologia e Segurança da Informação - PUSI	
Versão: v1 26/03/2018 **Autores:** Alexandre Luna Felipe Fernandes Filipe Aguiar Luisa Sette	**Sumário**: Controle da Norma Objetivo Fundamentos e Definições Processo Aplicação Penalidades Unidades Envolvidas Distribuição Vigência
Documentos Relacionados: Norma NBR ISO/IEC 27000 - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos - Requisito 6.0; Norma NBR ISO/IEC 17799 - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para a Gestão da Segurança da Informação; 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, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências; Política de Segurança da Informação da EBSERH. Política de Segurança da Informação da UFPE. Política de Segurança da Informação do HC-UFPE. Instrução Normativa SGPTI 001/2017 – Definição de Responsabilidades.	
Alterações em relação à versão anterior: N/A	

Objetivo

Estabelecer o fluxo principal para cadastro de usuários e alteração de perfil de acesso nos Sistemas de Informação em Saúde (SIS) do Hospital das Clínicas da UFPE.

Fundamentos e Definições

Sistemas de Informações em Saúde (SIS)

São instrumentos padronizados de monitoramento e coleta de dados, que tem como objetivo o fornecimento de informações para análise e melhor compreensão de importantes problemas de saúde da população, subsidiando a tomada de decisões nos níveis municipal, estadual e federal. A Organização Mundial da Saúde define Sistema de Informação em Saúde - SIS, como *um mecanismo de coleta, processamento, análise e transmissão da informação necessária para se planejar, organizar, operar e avaliar os serviços de saúde. Considera-se que a transformação de um dado em informação exige, além da análise, a divulgação, e inclusive recomendações para a ação*[3]. São exemplos de SIS em uso na instituição: AGHU, Mastertools, dentre outros.

Ambiente tecnológico corporativo (ATC)

É o ambiente formado pelo conjunto de *capacidades* e *recursos tecnológicos* utilizados pela organização para apoiar as operações de seu negócio. Ou seja, para apoiar as ações que vão possibilitar à organização o alcance da sua missão institucional. São exemplos dos componentes que fazem parte deste ambiente: os próprios *Sistemas de Informação em Saúde*, a rede de computadores, ativos de rede que permitem o funcionamento desta rede e seu acesso a outras redes (como é o caso da internet), equipamentos de segurança da informação, equipamentos onde estão instalados os Sistemas de Informação, data center, e mesmo a estação de trabalho sobre a sua mesa, dentre outros. A Figura 1, ilustra a relação de pertinência entre o(s) SIS(s) e o ATC.

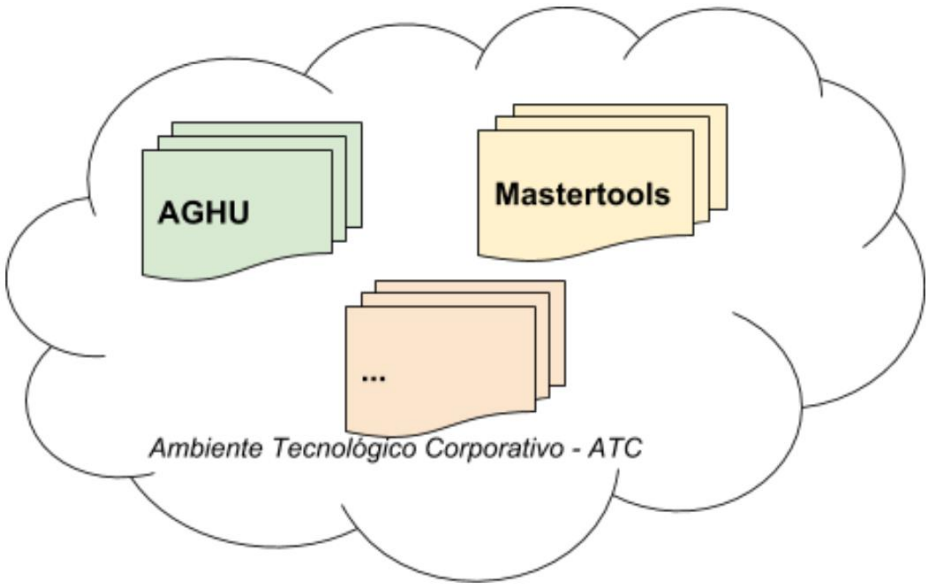

Figura 1 - Relação entre Ambiente Tecnológico Corporativo e o(s) SIS(s).

Usuário

Os *usuários* ou *utilizadores* são pessoas que utilizam um determinado tipo de serviço e podem ser classificados segundo a área de interesse. Os usuários em sistemas de informação são agentes externos ao sistema que usufruem da tecnologia para realizar determinado trabalho. Descritos de forma genérica como "colaboradores", os usuários podem ser: funcionários da instituição (RJU ou EBSERH), alunos, professores, residentes ou prestadores de serviço (terceirizados).

Credencial eletrônica (para uso do ambiente tecnológico corporativo)

É a identidade digital requerida para acessar o ambiente tecnológico corporativo da instituição. É composto pelo *binômio* das informações de: [1] identificação do usuário (login) e [2] sua respectiva senha. Esta credencial é fornecida pelo SGPTI a cada colaborador da instituição que precise acessar o ambiente tecnológico corporativo sob sua gestão, conforme descrito na Norma Técnica Nº001/SGPTI/HC-UFPE/EBSERH: Uso de Credencial Eletrônica (login e senha), atrelada à Instrução Normativa SGPTI Nº 001/2017 – Políticas de Uso da Tecnologia da Informação e Comunicação.

Login (para uso do SIS)

É a identidade digital requerida para acessar qualquer SIS na instituição. É composto pelo *binômio* das informações de: [1] identificação do usuário (login) e [2] sua respectiva senha. Esta

credencial é fornecida pelo SGPTI a cada colaborador da instituição que precise acessar os SIS sob sua gestão, mediante solicitação explícita, conforme detalhado no item a seguir.

Perfil de acesso

Em função do tipo de atividade de cada usuário, e do uso que ele precisar fazer do SIS, no exercício de suas atribuições, o SGPTI poderá configurar um (ou mais) perfil(s) de acesso (ou permissão) para cada sistema. Para fornecimento do login (vide item anterior: *login*), o cadastro de usuários e as alterações de perfil de acesso deverão ocorrer mediante solicitação explícita do superior de cada colaborador, que se torna solidariamente responsável pela permissão atribuída ao seu colaborador, assim como pelos atos destas decorrentes. Os perfis podem ser classificados, em *perfis regulados* ou não. Dentre os perfis sob regulação, àqueles relacionados à marcação de exames e/ou consultas são regulados pelo Setor de Regulação e Avaliação em Saúde (SRAS). Da mesma forma àqueles perfis relacionados à execução orçamentária e financeira são regulados pela Gerência Administrativo-Financeira (GAF).

Administrador de SIS

Usuário interno do SGPTI (ou representante de empresa contratada para tal fim) responsável por criar e manter os logins de acesso aos SIS, mediante registro formal, rastreável e auditável desta operação, seguindo os procedimentos descritos por esta Norma Técnica.

Senha temporária

Nova senha informada por um representante do SGPTI ao usuário, que deverá ser modificada na primeira oportunidade pelo usuário. Esta senha poderá ser fornecida nas seguintes situações: (i) após a criação da conta do usuário; (ii) devido a esquecimento da senha anterior.

Processo

Premissas

Todo usuário deve ter um credencial eletrônica pessoal e intransferível.

Qualquer recurso computacional somente poderá ser acessado após a autenticação da credencial eletrônica do usuário, garantida pelo preenchimento correto de sua identidade digital (login) e sua senha.

Todo usuário deve ter login de acesso pessoal e intransferível à SIS.

Qualquer SIS somente poderá ser acessado após a autenticação do login de acesso do usuário, garantida pelo preenchimento correto de sua identidade digital (login) e sua senha.

Critérios para criação da senha do Login do SIS

Deve conter 8 (oito) caracteres no mínimo.

Deve ser definida com pelo menos 3 (três) das seguintes características:

Letra maiúscula;

Letra minúscula;

Número;

Caractere especial.

Evitar incluir:

Número da matrícula, CPF ou SIAPE;

Espaço entre os caracteres;

Parte do nome do usuário;

Palavra de dicionário em qualquer idioma, mesmo que utilizando caracteres especiais ou números em substituição a algumas letras, tais como: sport e $p0rt, JESUS e J3SUS;

Palavra baseada em informações pessoais, tais como, placa do carro, nome de familiares e telefone;

Seqüência de letras ou números, tais como, aaabbb, qwerty, zyxwvuts, 123321.

Validade

A validade da senha depende da política de uso de cada SIS.

Vigência mínima

A vigência mínima da senha depende da política de uso de cada SIS.

Bloqueio da conta

O login de qualquer SIS será bloqueado após 3 tentativas consecutivas em que a senha for digitada incorretamente.

Após sua ocorrência, este bloqueio somente poderá ser removido por um representante do SGPTI, mediante verificação da identidade do usuário.

Procedimentos de Cadastro de Usuários (criação de login) e alteração de Perfil

O procedimento de cadastro e/ou de alteração de perfil de acesso ao SIS deverá ocorrer mediante preenchimento de formulário fornecido pelo SGPTI, conforme os passos descritos na Figura 2.

No caso de uso de formulário(s) em papel, onde lê-se *assinatura* ou *anuência*, deve-se considerar: assinatura e carimbo do responsável pelo setor.

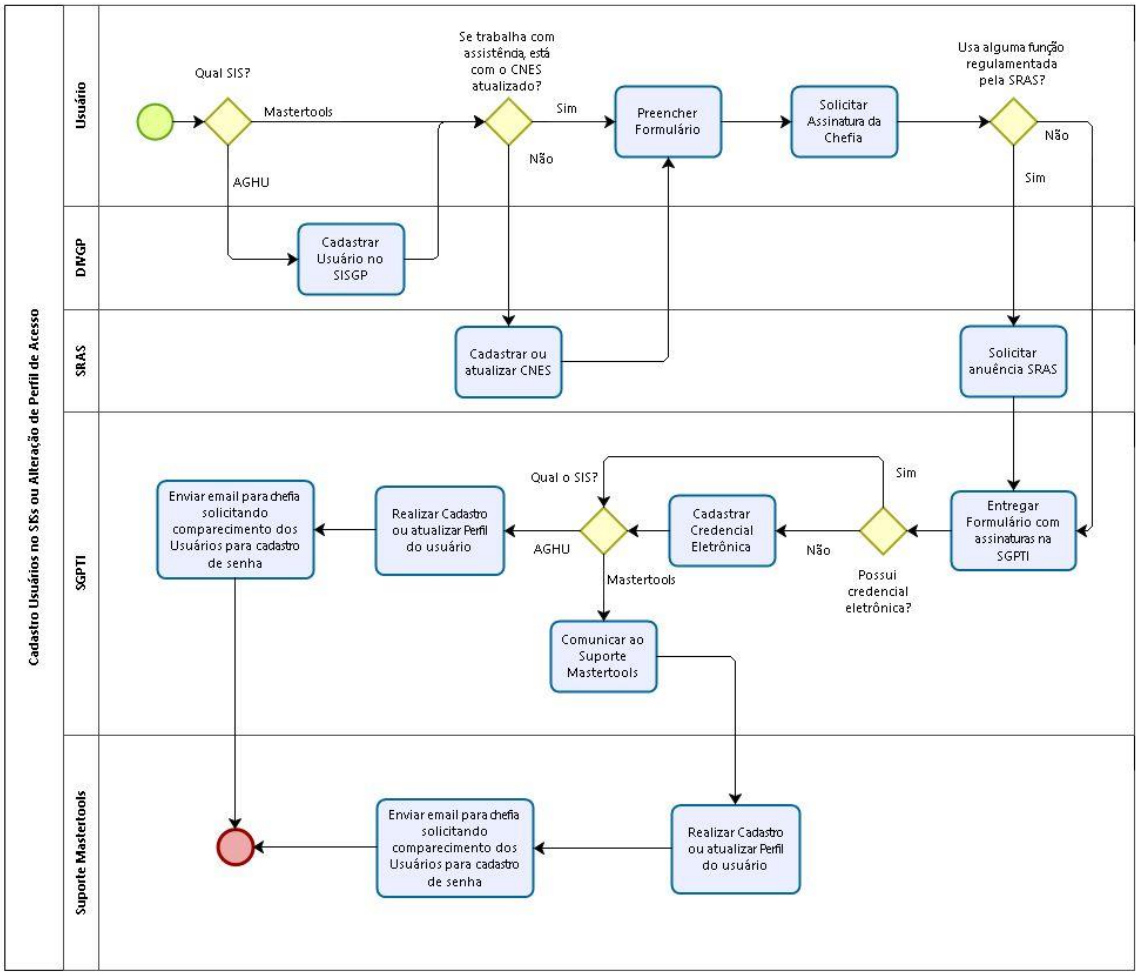

Figura 2 - Fluxograma de Criação de Usuários e/ou alteração de perfil de acesso aos SIS.

Aplicação da Norma

Usuário

Direitos

Alterar a senha sempre que achar conveniente, respeitando o exposto nos itens 4.b. (critérios para criação da senha), 4.c (validade) e 4.d (duração mínima).

Abrir um chamado técnico para alteração de senha em caso de esquecimento da senha. Será necessária a verificação da identidade do usuário pelo SGPTI antes da realização do procedimento.

Responsabilidades

Manter a confidencialidade da senha. Ou seja, não compartilhar, ceder ou “emprestar” a senha a outra pessoa.

Não solicitar a senha de outro usuário.

Não informar a senha, mesmo que solicitado pelo superior ou pelo SGPTI.

Alterar a senha temporária assim que for informado pelo SGPTI da criação da conta ou da mudança da senha.

Alterar a senha imediatamente após suspeitar que seu sigilo tenha sido violado.

Comunicar ao SGPTI qualquer suspeita de violação, ou de tentativa de violação, do sigilo da senha.

Alterar a senha imediatamente quando solicitado pelo SGPTI.

Não salvar a senha em arquivo, exceto se criptografada.

Não tornar público o método utilizado para criar a senha.

Não reutilizar qualquer senha anterior.

Não relacionar uma nova senha à senha anterior de tal modo que crie uma seqüência. Por exemplo, se a antiga senha fosse XptoA2006, a nova não deveria ser XptoB2007.

Não utilizar a senha em cadastros de terceiros, tais como, sites da Internet, bancos e provedores.

Não utilizar a mesma senha para contas diferentes, no caso do usuário ter mais de uma conta.

Não incluir a senha em sistemas automatizados de autenticação. Por exemplo, não se deve marcar a opção “Lembrar minha senha” no navegador de internet ou janelas de acesso ao SIS.

SGPTI

Responsabilidades

Informar a senha temporária ao usuário assim que criar a conta ou alterar a senha da conta, mediante a verificação da identidade do usuário.

Executar varredura automatizada de busca de senhas fracas a cada 3 meses e tomar as medidas apropriadas em caso de detecção.

Garantir que aplicações adquiridas ou desenvolvidas pelo HC-UFPE ou EBSERH não violem o sigilo das senhas.

Proibições

Solicitar a senha do usuário sob qualquer pretexto.

Alterar a senha de qualquer usuário, exceto quando por ele solicitado, e após verificar a autenticidade de tal solicitação.

Penalidades

A não observância dos termos desta Norma Técnica, devidamente apurada e comprovada, implica bloqueio de seu login. Como consequência o usuário não poderá durante o bloqueio utilizar o SIS em questão.

O caso será informado ao usuário interno infrator e seu superior imediato para ciência, e ao Chefe do SGPTI para deliberação.

Unidades Envolvidas

SGPTI: criação e manutenção desta Norma Técnica.

Demais setores HC-UFPE: aplicação das políticas.

Distribuição

Intranet da instituição: Conteúdo completo.

Imprensa da instituição: Comunicado da inclusão ou alteração de novas políticas.

Vigência

Esta Política entrará em vigor a partir da data de sua publicação, revogando-se as disposições em contrário.

Hospital das Clínicas da Universidade Federal de Pernambuco, em, 26 de março de 2018.

Alexandre Luna, PhD

Chefe do Setor de Gestão de Processos e Tecnologia da Informação – SGPTI.

Frederico Jorge Ribeiro

Superintendente