EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

Boletim de Serviço

Nº 83, 06 de setembro de 2018

EXTRAORDINÁRIO

Hospital Universitário de Sergipe

EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES – EBSERH
HOSPITAL UNIVERSITÁRIO DE SERGIPE

Rua Cláudio Batista, 505 –Palestina | CEP: 49060025

Aracaju-SE| Telefone: (79) 2105-1700

ROSSIELI SOARES DA SILVA

Ministro de Estado da Educação

KLEBER DE MELO MORAIS

Presidente

ARNALDO CORREIA DE MEDEIROS

Diretor Vice-Presidente Executivo – Substituto Diretor de Atenção à Saúde

ANGELA MARIA DA SILVA

Superintendente

MARCOS ANTÔNIO COSTA DE ALBUQUERQUE

Gerente de Atenção à Saúde / HU-UFS

ROQUE PACHECO DE ALMEIDA

Gerente de Ensino e Pesquisa

EDÉLZIO ALVESCOSTA JÚNIOR

Gerente Administrativo /HU-UFS

SUMÁRIO

SUPERINTENDÊNCIA

Instrução Normativa n° 003/2018

Institui a Política de Segurança – Diretrizes e Normas relativa ao uso legal de recursos computacionais disponibilizados pelo Hospital Universitário da Universidade Federal de Sergipe – HU-UFS/EBSERH, a todos os usuários e estabelece providências correlatas.

A SUPERINTENDENTE DO HOSPITAL UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DE SERGIPE, FILIADA A EMPRESA BRASILEIRA DE SERVIÇOS HOSPITALARES-EBSERH, no uso das suas atribuições legais e considerando a delegação de competência prevista pela Portaria n° 125, de 11 de dezembro de 2012, firmada pelo Presidente da Empresa Brasileira de Serviços Hospitalares, publicada no DOU de 13/12/2012, nos termos do art. 4°, parágrafo único e,

Considerando a Política de Segurança da Informação e Comunicação da Empresa Brasileira de Serviços Hospitalares (EBSERH)/Sede, publicada por meio da Portaria n.º 35, de 6 de março de 2017, para aplicação em toda a Rede Ebserh;

Considerando os destaques do Livro Verde – Segurança Cibernética no Brasil (GSI/PR, 2010, p.14) relacionados a fenômenos da nova conformação da Sociedade da Informação: elevada convergência tecnológica; aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos; aumento crescente e bastante substantivo de acesso à Internet e das redes sociais; avanços das Tecnologias de Informação e Comunicação (TIC); aumento das ameaças e das vulnerabilidades de segurança cibernética; e, ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças;

Considerando a necessidade de proteger todos os usuários dos sistemas de TIC, sejam eles, funcionários, contratados, pacientes ou parceiros, além do próprio HU-UFS de ações ilegais realizadas por indivíduos clientes ou não;

Considerando a necessidade e importância de garantir o correto uso dos recursos informáticos do HU-UFS, bem como garantir a autenticidade, confiabilidade e integridade das informações gerenciadas pelo HU-UFS;

Considerando as seguintes Referências Legais e Normativas:

- Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores

públicos civis da União, das autarquias e das fundações públicas federais;

- Lei nº 12.527, de 18 de novembro de 2011, que regulamenta o acesso às informações públicas;

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

- Decreto-lei nº 2.848, de 7 de dezembro de 1940;

- Decreto-Lei nº 5.452, de 1º de maio de 1943, que aprova a Consolidação das Leis do Trabalho (CLT);

- 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;

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

- Decreto nº 7.724, 16 de maio de 2012, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição;

- Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

- Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

- Norma Complementar nº 04/IN01/DSIC/GSIPR, Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;

- Norma Complementar nº 06/IN01/DSIC/GSIPR, Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações;

- Norma Complementar nº 07/IN01/DSIC/GSIPR, Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

- Norma Complementar nº 08/IN01/DSIC/GSIPR, gestão de ETIR: diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal;

- Norma Complementar nº 10/IN01/DSIC/GSIPR, Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

- Norma Complementar nº 12/IN01/DSIC/GSIPR, Uso de Dispositivos Móveis nos Aspectos

relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

- Norma Complementar nº 15/IN01/DSIC/GSIPR, diretrizes para o uso seguro das redes sociais na Administração Pública Federal;

- Norma Complementar nº 17/IN01/DSIC/GSIPR, atuação e adequações para profissionais da área de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;

- Norma Complementar nº 18/IN01/DSIC/GSIPR, diretrizes para as atividades de ensino em segurança da informação e comunicações nos órgãos e entidades da administração pública federal;

- Norma Complementar nº 19/IN01/DSIC/GSIPR, padrões mínimos de segurança da informação e comunicações para os sistemas estruturantes da Administração Pública Federal;

- Norma Complementar nº 20/IN01/DSIC/GSIPR, diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal;

- Norma Complementar nº 21/IN01/DSIC/GSIPR, diretrizes para o registro de eventos, coleta, e preservação de evidências de incidentes de segurança em redes;

- NBR ISO/IEC 23301:2013;

- NBR ISO/IEC 27001:2013;

- NBR ISO/IEC 27002:2013;

- NBR ISO/IEC 27005:2011.

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança dos recursos computacionais disponibilizados pelo HU-UFS, com o objetivo de proteger todos os usuários do sistema de tecnologia da informação e o próprio HU-UFS de ações ilegais realizadas por indivíduos, clientes ou não.

Parágrafo único. Para os fins desta Portaria, entende-se por:

I - Acesso Remoto: Qualquer tipo de acesso à rede corporativa do HU-UFS, através de uma rede não controlada pelo HU-UFS, independentemente do meio de comunicação que esteja sendo utilizado.

II - Administrador: Usuário com privilégios e/ou poderes de administração sobre determinados recursos computacionais do HU-UFS, diferentes do usuário comum, tais como: administradores de rede, administradores de sistemas, administradores do correio eletrônico, administradores de segurança, administradores de banco de dados;

III - Chefe de Setor: Pessoa responsável pelo setor ou unidade de trabalho;

IV - Datacenter: Consiste numa estrutura modular própria para hospedagem de equipamentos de TIC, composta por sistemas de climatização, energia ininterrupta, sensores de ambiente, bem como dispositivos de detecção e combate a incêndio, trata-se de uma área crítica e de alta complexidade, já que sustenta todos os serviços e processos de uma instituição;

V - Equipe de Segurança de TI: Equipe formada por funcionários do SGPTI, composta pelo administrador de rede, pelo gestor de segurança e por uma analista de sistemas com a finalidade de garantir a confidencialidade, integridade e disponibilidade das informações contidas na rede do HU-UFS;

VI - Extranet: Rede criada pela interseção da rede corporativa do HU-UFS com a rede de terceiros para a facilitação de negócios entre o HU-UFS e seus parceiros;

VII - Gestor de Segurança: Funcionário do SGPTI com a atribuição de implementar a política de segurança definida pelo HU-UFS, gerenciar a Equipe de Segurança de TI, pesquisar soluções de segurança, homologar as soluções a serem adotadas e acompanhar a sua implementação, e estabelecer a comunicação entre a equipe técnica e os usuários na solução dos incidentes de segurança;

VIII - HU-UFS: Hospital Universitário da Universidade Federal de Sergipe;

IX - Incidente de Segurança: Qualquer evento, confirmado ou sob suspeita, que viole os aspectos de confidencialidade, integridade e disponibilidade das informações contidas na rede do HU-UFS;

X – Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XI - Internet: Rede mundial de computadores, acessada através da rede corporativa do HU-UFS, mas que não está sob a responsabilidade e controle dos administradores de rede do HU-UFS;

XII - Intranet: Ambiente "web" interno de uso exclusivo do HU-UFS;

XIII - Política de mesa limpa: práticas de segurança da informação recomendadas para o local de trabalho a fim de evitar a exposição desnecessária de informações consideradas sensíveis, com objetivo de se evitar o comprometimento da informação.

XIV - Recursos computacionais: Todos os recursos de hardware e software do HU-UFS, tais como: computadores, impressoras, periféricos, cabos de rede, sistemas aplicativos, equipamentos de rede, no-breaks ou tomadas, informações geradas e/ou disponibilizadas, Internet, Intranet e Extranet, sistemas corporativos, sistemas operacionais, meios de armazenamento, contas de correio eletrônico, serviços web, serviços ftp e outros meios de comunicação;

XV – Rede corporativa: Rede de computadores do HU-UFS, independentemente desta ser remota ou local;

XVI - SGPTI: Setor de Gestão de Processos e Tecnologia da Informação;

XVII - Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XVIII – TI: Tecnologia da Informação;

XIX – Usuário: Qualquer pessoa que faça uso dos recursos computacionais ou se utilize de informações geradas e disponibilizadas pelo HU-UFS, tais como: funcionários do HU-UFS, empregados terceirizados, consultores, fornecedores, contratados, estagiários, acadêmicos ou empregados temporários.

Art. 2º É um dever considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para HU-UFS devendo sempre ser tratada profissionalmente.

Art. 3º Todos os recursos computacionais disponibilizados pelo HU-UFS só poderão ser utilizados por pessoas autorizadas pelo HU-UFS.

Parágrafo único. Nos casos de Internet cedida a usuários do sistema SUS, o acesso deve ser realizado através de recursos computacionais do próprio usuário particular, sendo tecnicamente segregada da rede de dados utilizadas pelos colaboradores do HU-UFS.

Art. 4º Todos os recursos computacionais devem ser especificados, padronizados, instalados, mantidos, monitorados, disponibilizados, realocados e retirados pelo SGPTI e somente podem ter

suas configurações modificadas com o seu conhecimento e autorização.

Art. 5º Sempre que possível toda informação de caráter sigiloso ou vulnerável será criptografada antes de seu armazenamento.

Art. 6º Por razões de segurança, os administradores de rede e o gestor de segurança do HU-UFS podem monitorar a qualquer momento todos os recursos computacionais.

Art. 7º É reservado ao SGPTI o direito de auditar redes e sistemas periodicamente como forma de garantir e verificar se a utilização dos recursos está em concordância com a Política de Segurança estabelecida nesta Portaria.

CAPÍTULO II

DAS RESPONSABILIDADES

Seção I

Dos Colaboradores em Geral

Art. 8º Todo e qualquer usuário de recursos tecnológicos da instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de TI, bem como, levar ao conhecimento do Comitê de Segurança da Informação qualquer incidente ou evento relacionado à falha de segurança.

Art. 9º Todo equipamento de TI, disponibilizado pelo HU-UFS, deverá ter um usuário individualmente responsável por ele, indicado através de Termo de Responsabilidade, em três vias, cuja 1ª via deverá ser assinada pelo usuário e devolvida ao SGPTI para que seja arquivada. A 2ª via deste documento será encaminhada à Unidade de Patrimônio. A 3ª via ficará em poder do usuário.

Parágrafo único. O responsável pelo equipamento de TI deverá cuidar para que o equipamento sob sua responsabilidade seja usado apenas para o exercício das atividades relacionadas aos negócios do HU-UFS.

Art. 10. É de inteira responsabilidade de cada usuário dos recursos de informática disponibilizados pelo HU-UFS o conhecimento e aceitação das regras de segurança estabelecidas nesta Portaria e do seu fiel cumprimento.

§1º Todos os recursos computacionais são de propriedade do HU-UFS, devendo o usuário responder pelo uso ilegal desses recursos;

§2º É de responsabilidade de cada usuário observar os procedimentos definidos pelo SGPTI para o uso de recursos diretamente ligados às suas atividades diárias, sejam eles computadores, periféricos, informações ou meios de comunicação.

§3º Todo usuário deve manter absoluto sigilo relativo às informações de senhas de contas de acesso aos recursos computacionais e correio eletrônico.

§4º Todo usuário deve estar atento à política de 'mesa limpa' mantendo seguras as informações.

Seção II

Dos Colaboradores em Regime de Exceção (Temporários), Estudantes e Residentes

Art. 11. Esse documento deve ser seguido por qualquer pessoa que utilize os recursos de Tecnologia da Informação disponibilizados pelo HU-UFS, valendo as mesmas normas, diretrizes e responsabilidades seguidas pelos Colaboradores.

Seção III

Dos Gestores de Pessoas

Art. 12. Os gestores devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão.

Art. 13. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação do HU-UFS, tomando as ações necessárias para cumprir tal responsabilidade. Adicionalmente, difundir a Política de Segurança da Informação e viabilizar, no âmbito de sua gestão, a educação, treinamento e conscientização sobre segurança da informação.

Art. 14. É de responsabilidade de cada gerência, divisão, setor ou unidade, a criação de manuais de procedimentos informando a conduta correta de utilização dos recursos relacionados à sua área de atuação, caso estes não estejam previstos nesta Portaria.

Parágrafo único. Os manuais de utilização de sistemas corporativos deverão ser elaborados pelo SGPTI em conjunto com as respectivas áreas.

Art. 15. Cabe à Divisão de Gestão de Pessoas (DivGP) entregar, junto com os contratos de trabalho, uma cópia desta Política de Segurança da Informação, juntamente com o Termo de Responsabilidade e Confidencialidade, como parte das responsabilidades de trabalho dos funcionários/colaboradores.

Art. 16. Cabe à Gerência de Ensino e Pesquisa (GEP) entregar uma cópia desta Política de Segurança da Informação aos estudantes/residentes/alunos, juntamente com o Termo de Responsabilidade e Confidencialidade, integrando parte das responsabilidades dos mesmos enquanto usuários dos recursos de Tecnologia da Informação.

Seção IV

Da Alta Administração

Art. 17. Manter, apoiar e aprovar a Política de Segurança da Informação.

Art. 18. Promover a cultura de segurança da informação.

Art. 19. Aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

Art. 20. Prover os meios necessários para capacitação, o aperfeiçoamento técnico dos membros da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), bem como, prover a infraestrutura necessária para o seu funcionamento.

Seção V

Do Setor de Gestão de Processos e Tecnologia da Informação (SGPTI)

Art. 21. Coordenar a elaboração da Política de Segurança da Informação e Comunicações.

Art. 22. Promover a cultura de segurança da informação e comunicações.

Art. 23. Receber da Alta Administração a responsabilidade pelo projeto, implementação, gerenciamento das normas, procedimentos, padrões e guias de Segurança da Informação.

Art. 24. Coordenar as ações de segurança da informação.

Art. 25. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Superintendência do HU-UFS os resultados consolidados de tais investigações e avaliações;

Art. 26. Compete aos administradores de rede, de segurança e de sistemas a criação de um nível aceitável de segurança dos recursos relacionados a suas atividades, como forma de garantir a privacidade e integridade desses recursos para os usuários.

Parágrafo único. Não é de responsabilidade dos administradores a garantia de qualquer nível de

segurança relacionado a recursos localizados em redes e parques computacionais de terceiros.

CAPÍTULO III

DAS PROIBIÇÕES

Art. 27. É terminantemente proibido a todo usuário:

I - realizar atividades que não estejam em conformidade com a legislação vigente, nacional ou internacional, enquanto estiver utilizando os recursos computacionais do HU-UFS;

II - violar direitos de qualquer pessoa ou empresa protegidos por direitos autorais, segredos de negócios, patentes ou outras modalidades de propriedade intelectual, inclusive a pirataria e distribuição de software de propriedade do HU-UFS;

III - utilizar, copiar e distribuir nas instalações do HU-UFS, materiais protegidos por direitos autorais, tais como: digitalização de imagens e textos de revistas, livros, músicas ou outras fontes, através da Internet ou discos ou outras mídias;

IV - exportar softwares, aplicações, informações técnicas, algoritmos de criptografia e tecnologias, em violação a leis nacionais ou internacionais;

V - introduzir programas maliciosos na rede corporativa do HU-UFS, tais como: vírus, correio eletrônico bombas, cavalos-de-troia ou outros programas nocivos análogos;

VI - armazenar, exibir ou transmitir materiais impróprios ou de conteúdo erótico e textos obscenos pela rede corporativa do HU-UFS;

VII - negociar informações, sigilosas ou não, e recursos de propriedade do HU-UFS;

VIII - utilizar equipamentos do HU-UFS para elaboração de trabalhos pessoais;

IX - adulterar ou omitir qualquer tipo de informação, como forma de obter vantagens ilícitas;

X - provocar falhas intencionais na rede corporativa do HU-UFS, por intermédio de programas como *port scanning, network sniffing, pinged floods, packet spoofing, denial of service* ou outros análogos, como forma de se obter acesso a recursos indevidos ou de explorar possíveis vulnerabilidades no ambiente de segurança;

XI - executar qualquer tipo de monitoramento na rede, como forma de interceptar informações não

autorizadas;

XII - criar ou divulgar formas de acessar equipamentos burlando a segurança do sistema de informática;

XIII - compartilhar senhas;

XIV - permitir o acesso aos recursos computacionais do HU-UFS a qualquer visitante, tais como filhos, cônjuges, amigos e outros parentes.

CAPITULO IV

DAS PENALIDADES

Art. 28. A violação desta política de segurança é qualquer ato que, além de transgredir as normas e diretrizes descritas neste documento, também:

I - Exponha a instituição a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.

II - Envolva a revelação de dados confidenciais, direitos autorais, negociações ou uso não autorizado de dados corporativos.

III - Envolva o uso de dados e recursos de rede e tecnológicos para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Art. 29. As violações das regras estabelecidas nesta Portaria sujeitarão os infratores, dependendo da natureza e gravidade da infração, as seguintes medidas:

I - Processo administrativo disciplinar;

II - Processo criminal;

III - Processo civil.

CAPITULO V

DAS NORMATIVAS

Seção I

Controle de Acesso Físico ao HU-UFS

Art. 30. O acesso físico ao HU-UFS deverá ser feito através de controle de acesso capaz de identificar e distinguir um funcionário de um visitante, ou de um estudante ou residente.

Parágrafo único. O acesso físico deve ser controlado e orientado, de maneira a disciplinar a movimentação e circulação de pessoas, materiais, equipamentos e veículos.

Art. 31. O controle de acesso físico deve ter a capacidade de distinguir entre o pessoal autorizado e o não autorizado mediante sua identificação, que deve respeitar pelo menos duas entre três premissas básicas:

I - O que a pessoa é: sua identificação ou características biométricas;

II - O que a pessoa possui: uso de cartões ou chaves;

III - O que a pessoa sabe: uso de senhas ou códigos.

Art. 32. Deverão ser adotadas formas de controlar a entrada e a saída de equipamentos, registrando data, horário e responsável.

Art. 33. Deverão ser adotadas formas de controlar a entrada e saída de visitantes, registrando data, horários e local da visita e, dependendo do nível de segurança necessário, acompanhá-los até o local de destino.

Art. 34. Deverá ser instituída vigilância no prédio do HU-UFS, 24 horas por dia, 7 (sete) dias da semana.

Art. 35. A equipe de limpeza e manutenção deverá ser supervisionada, pessoalmente, sempre que for realizar trabalhos fora do horário normal de expediente.

Parágrafo único. No caso do *caput* deste artigo, caberá ao responsável pelo setor indicar o funcionário que irá supervisionar a equipe de limpeza e de manutenção.

Art. 36. As dependências do HU-UFS deverão ser monitoradas por alarmes e sistema de captura de imagem.

Seção II

Controle de Acesso Físico ao SGPTI

Art. 37. O acesso físico ao Datacenter do HU-UFS deve ser feito através de um sistema

automatizado de controle de acesso, interligado à base de dados de usuários, por meio de tecnologias de identificação (cartão, senha, biometria, etc.).

Art. 38. O cadastramento de usuários no sistema de controle de acesso físico, bem como mudanças de perfil ou local de trabalho, obedecerão aos procedimentos definidos pela Equipe de Segurança de TI.

Art. 39. O acesso físico de usuários não cadastrados e prestadores de serviço às dependências do SGPTI, requer autorização prévia da chefia do setor.

Art. 40. O acesso rotineiro ao Datacenter deve ser restrito à Equipe de Suporte de Rede, mediante sistema eletrônico de controle de acesso (cartões magnéticos, biometria, chaves, etc.).

Art. 41. O Datacenter deve possuir controle sobre as variáveis ambientais que possam afetar o desempenho dos equipamentos críticos ali instalados, segundo as recomendações dos fabricantes. Assim como dispositivos de combate ao fogo e de proteção contra a instabilidade da rede de energia.

Art. 42. Todo e qualquer acesso ao Datacenter deverá ser supervisionado pela Equipe de Segurança de TI.

Seção III

Controle de acesso lógico a sistemas de informação

Art. 43. O SGPTI deverá implementar um rigoroso controle de acesso a todos os ambientes e servidores que são: produção, desenvolvimento, homologação e treinamento.

Art. 44. O SGPTI deverá implementar procedimentos específicos para disciplinar as seguintes hipóteses:

I - Criação de nova conta de acesso a sistemas computacionais;

II - Fornecimento de senhas temporárias em caso de esquecimento;

III - Disponibilização de acesso aos sistemas em produção;

IV - Ocorrência de “log on" com e sem sucesso.

Art. 45. O usuário somente deve utilizar os recursos computacionais quando autorizado pelo chefe imediato em que este irá exercer suas atividades.

Art. 46. As contas de acesso dos usuários, reservam-se apenas ao uso dos recursos computacionais definidos pelo gerente da área.

Art. 47. Quando possível, as contas de acesso devem possuir requisitos de expiração baseados no tempo de duração do contrato de serviço.

Seção IV

Acesso remoto

Art. 48. Estão compreendidas nas modalidades de acesso remoto consideradas por esta Portaria, as seguintes conexões:

I - *frame-relay*;

II - ISDN (*integrated services digital network*);

III - DSL (*digital subscriber line*);

IV - VPN (*virtual private network*);

V - PPP (ponto a ponto).

Art. 49. A modalidade de acesso remoto preferencial será através de VPN (Rede Privada Virtual), em casos onde isso não seja tecnicamente possível ou viável, caberá ao SGPTI definir um modelo de acesso que disponibilize níveis de segurança compatíveis com os requeridos pelo serviço disponibilizado remotamente.

Art. 50. É de responsabilidade dos usuários, com privilégio de acesso remoto à rede corporativa do HU-UFS, a observância das regras de segurança adotadas para a rede local, independentemente do tipo de conexão.

Art. 51. Não é permitido o acesso remoto à rede corporativa do HU-UFS com intuito recreativo, pessoal ou para desenvolver atividades ilegais ou não relacionadas aos negócios do HU-UFS.

Art. 52. É proibido ao usuário fornecer os dados da conta e senha de acesso remoto a qualquer pessoa.

Art. 53. É de inteira responsabilidade do usuário remoto o controle para que membros de sua família ou outras pessoas não violem as normas de segurança adotadas pelo HU-UFS.

Art. 54. O usuário, com privilégio de acesso remoto, deverá garantir que o computador usado para o acesso não deverá estar conectado ao mesmo tempo com qualquer outra rede local ou remota.

Art. 55. Os usuários com privilégios de acesso remoto não deverão usar contas de correio eletrônico

pessoais ou outros recursos externos e pessoais para conduzir negócios relacionados ao HU-UFS.

Art. 56. Os roteadores utilizados para conexões dedicadas deverão ser configurados com um nível de autenticação seguro, dentro dos padrões estabelecidos pelo SGPTI. Na hipótese de equipamentos instalados por empresa prestadora de serviço, o SGPTI deverá ser solicitada para auxiliar na configuração adequada dos equipamentos envolvidos.

Art. 57. Todos os computadores que possam se conectar à rede corporativa do HU-UFS deverão estar com o ambiente atualizado de proteção antivírus adotado pelo HU-UFS.

Art. 58. Para que os equipamentos pessoais se conectem remotamente à rede corporativa do HU-UFS, deverão estar em conformidade com a política de segurança estabelecida nesta Portaria.

Art. 59. O acesso remoto à rede corporativa do HU-UFS somente será realizado após aprovação e liberação pela área de segurança do SGPTI.

Art. 60. Todo acesso será auditado.

Seção V

Senhas

Art. 61. Todas as senhas de sistema tais como *root*, *enable*, NT *admin*, contas de *schedules*, contas de aplicações, dentre outras, deverão ser trocadas periodicamente por seus responsáveis diretos, cabendo ao SGPTI estabelecer os intervalos de tempo máximo para a troca.

Art. 62. Todas as senhas deverão ser administradas e armazenadas no banco de dados global de contas da rede corporativa do HU-UFS.

Art. 63. Todas as senhas de usuários relativas a correio, *web*, computadores pessoais, rede, deverão ser trocadas periodicamente por seus responsáveis diretos, cabendo ao SGPTI estabelecer os intervalos de tempo máximo para a troca.

Art. 64. Os usuários que necessitam de contas com privilégios de administradores deverão possuir duas contas, com e sem privilégio, e as mesmas deverão obrigatoriamente possuir senhas distintas.

Art. 65. As senhas não devem ser inseridas dentro de mensagens de correio ou qualquer outra forma de comunicação, eletrônica ou não.

Art. 66. Todas as contas "padrões" de acesso a recursos da rede, como contas de roteadores, contas do protocolo SNMP (*simple network management protocol*), contas de sistemas operacionais e contas de acesso a banco de dados deverão ser trocadas imediatamente após a instalação do recurso

e deverão ter senhas condizentes com o nível de proteção exigido pelo recurso.

Art. 67. Todos os computadores deverão estar configurados com a opção de bloqueio automático (ctrl+alt+delete) que deverá ser ativada após 10 (dez) minutos de inatividade.

Art. 68. É de inteira responsabilidade do usuário o bloqueio de sua máquina ou "*log off"*, quando o mesmo se ausentar por qualquer período.

Parágrafo único. Para efeito de auditoria, o usuário registrado "*log on"* no computador é o responsável por todas as atividades, ilícitas ou não, realizadas em seu computador.

Art. 69. Todas as senhas de usuários ou sistemas deverão observar as diretrizes de criação de senhas estabelecidas no artigo seguinte e as diretrizes de proteção do art. 33 desta Portaria.

Art. 70. Todas as contas deverão possuir senhas fortes, seguras e confiáveis independentemente de seu uso ou finalidade, sejam elas, contas de sistema, contas de acesso à rede, contas de correio, contas de proteção de tela de computadores, contas de roteadores ou outros dispositivos de rede.

§1º São consideradas fortes as senhas com 8 ou mais caracteres contendo letras maiúsculas e minúsculas (a-z e A-Z), números (0-9) e caracteres especiais (@ # $ % &, etc).

§2º As características das senhas fortes devem ser exigidas por software sempre que for possível.

Art. 71. Deverão ser observadas as seguintes diretrizes para proteção de senhas:

I - não armazenar senhas em arquivos, agendas, blocos de anotações, debaixo do teclado, escritas na mesa de trabalho, etc.;

II - não usar no HU-UFS a mesma senha de outros serviços como cartões de banco, acesso a provedores de Internet, acesso a outras instituições, etc.;

III - sempre que possível, não usar a mesma senha para acesso a recursos diferentes dentro do HU-UFS, como senhas de correio eletrônico, senhas de rede, senhas de sistemas operacionais (Unix, Linux, Windows, IOS, entre outros), senhas de proteção de telas, etc.;

IV - não compartilhar senha com ninguém, familiares, administradores, secretárias, colegas, etc;

V - não enviar senha por qualquer meio de comunicação não confiável (correio, telefone, fax, etc.) mesmo que para cadastramento inicial;

VI - não falar sobre senha na presença de outras pessoas;

VII - não revelar sua senha para seu chefe ou superior imediato;

VIII - não revelar sua senha no caso de ausências;

IX - não usar opções de "relembrar senhas" encontradas em muitos aplicativos como Internet Explorer, Chrome, Mozilla Firefox, Outlook, entre outros;

X - não incluir senha em processos automáticos de acesso a sistema, por exemplo, armazenadas em macros ou em teclas de função;

Parágrafo único. A senha é pessoal e reservada e, será tratada como uma informação confidencial do HU-UFS.

Art. 72. A política de senhas do HU-UFS não permitirá a reutilização de senhas durante um período de 4 ciclos de troca.

Art. 73. Na hipótese de suspeita de que a senha foi descoberta, o usuário deverá trocá-la imediatamente e comunicar sua suspeita ao grupo de segurança do SGPTI.

Art. 74. A área de segurança do SGPTI poderá executar programas de quebras de senhas periodicamente, como forma de identificar possíveis senhas fracas no sistema. Caso estas senhas sejam identificadas, o usuário será comunicado para sua troca imediata.

Art. 75. A área de desenvolvimento de aplicações do SGPTI deverá se certificar que seus programas possuem as seguintes precauções de segurança:

I - suportar autenticação individual e nunca de grupos;

II - não armazenar senhas no formato de texto livre ou através de algoritmos que possam ser quebrados facilmente;

III - permitir que usuários de nível de acesso superior tenham acesso aos recursos de nível de acesso inferior;

IV - sempre que possível, utilizar padrões de autenticação e criptografia adotados pelo HU-UFS.

Art. 76. As senhas de autenticação remota desses usuários serão diferenciadas de suas senhas de acesso local, devendo estas senhas serem mais fortemente geradas e criptografadas pela solução de VPN adotada.

Art. 77. As ausências temporárias de colaboradores em decorrência de férias, licença, suspensão, etc., levarão ao bloqueio de suas contas de acesso durante o respectivo período, devendo ser

comunicadas previamente pela DivGP.

Art. 78. Nos casos em que um colaborador for desligado definitivamente do HU-UFS, seus direitos de acesso devem ser imediatamente revogados e seus computadores e informações retornados ao HU-UFS.

Art. 79. É de responsabilidade da DivGP informar aos administradores de rede sobre o desligamento de funcionários para que sejam efetuadas a exclusões das suas contas de acesso.

Art. 80. Os desbloqueios de contas de acesso de usuários serão efetuados mediante a confirmação de algumas informações pessoais, tais como: CPF, RG e data de nascimento.

Art. 81. As senhas de servidores, elementos ativos e serviços de usuários deverão ser armazenadas em local seguro, como mídias eletrônicas ou envelopes lacrados, sob a responsabilidade do HU-UFS.

Seção VI

Internet

Art. 82. São de responsabilidade do SGPTI a criação e manutenção de um ambiente de proteção bem definido, com o propósito de garantir a confiabilidade e integridade do site Internet e Intranet do HU-UFS, bem como, controlar e monitorar a utilização da Internet pelos usuários da rede corporativa do HU-UFS.

Art. 83. É de responsabilidade do SGPTI a liberação ou não do acesso a serviços http, ftp, correio, *news* e outras informações existentes na Internet.

Parágrafo único. Em benefício do serviço do setor, as Chefias podem solicitar eventuais liberações e bloqueios ao SGPTI, e este avaliará os impactos causados pela solicitação.

Art. 84. É de responsabilidade dos usuários a correta utilização dos serviços e informações liberados como ferramenta facilitadora de suas atividades pertinentes aos negócios do SGPTI.

Art. 85. É terminantemente proibida aos usuários a utilização da Internet:

I - como ferramenta de entretenimento e pesquisa não relacionada aos negócios do HU-UFS;

II - para acessar sites com conteúdo erótico, de natureza discriminatória, de diversão, chats e bate-papos, pedofilia, hackerismo, bem como outros sites ligados a atividades criminosas;

III - para copiar ou utilizar ilegalmente quaisquer recursos, tais como: textos, programas, fotos,

músicas, dentre outros que estejam protegidos por leis de direitos autorais ou similares;

IV - para estabelecer comunicação com terceiros, correio eletrônico, bate-papos, videoconferências, etc., quando o assunto envolvido não for pertinente aos negócios do HU-UFS ou de seu interesse;

V - para distribuir informações restritas do HU-UFS para terceiros;

VI - para praticar atividades ilícitas, agindo como *hackers* ou *crackers*.

Art. 86. É de responsabilidade do SGPTI o monitoramento contínuo e permanente da utilização da Internet pelos usuários, como forma de identificar possíveis maus usos dos serviços liberados.

Art. 87. É de total responsabilidade dos usuários quaisquer prejuízos que os mesmos venham a sofrer pelo acesso a *sites* Internet não confiáveis e de origem e propriedades obscuras.

Art. 88. Os "*downloads*" de arquivos somente poderão ser efetuados pelos usuários em conformidade com a cota estabelecida pela Equipe de Segurança de TI, a qual deverá também administrar os casos de exceção.

Seção VII

Correio Eletrônico

Art. 89. Correio eletrônico é a transferência eletrônica de informações, mensagens, memorandos e documentos anexados, de uma parte remetente para uma ou mais partes destinatárias através do uso de um sistema de comunicação informatizado.

Art. 90. O correio eletrônico somente deverá ser usado para as comunicações internas e externas que sirvam aos propósitos do HU-UFS. Será tolerada a utilização do correio eletrônico para interesses particulares, com moderação, desde que não possuam conteúdos indevidos ou impróprios e não venham a trazer prejuízos à rotina de trabalho, nem impactem a utilização dos recursos de informática.

Art. 91. O uso do correio eletrônico não é geral, cabendo a cada gerência identificar as suas reais necessidades de uso e solicitar formalmente ao SGPTI uma ou mais caixas de correio eletrônico.

Art. 92. O acesso ao correio eletrônico é identificado individualmente, sendo, portanto, necessária a criação de conta para cada usuário que necessite de acesso.

Art. 93. Serão criadas Caixas Postais Coletivas (Contas Conjuntas) por setor ou unidade operacional do HU-UFS, tais como gerencia.huufs@ebserh.gov.br ou sgpti.huufs@ebserh.gov.br, onde serão alocados todos os usuários, pertencentes aos respectivos setores ou unidades operacionais, que

possuem acesso ao correio eletrônico, devendo constar qual usuário integrante da caixa postal terá permissão de exclusão de mensagem.

Parágrafo único. Para os casos em que seja necessária uma conta de caráter específico tal como recadastro.huufs@ebserh.gov.br", se fará necessária a solicitação formal da criação de uma Caixa Postal Coletiva, onde deverá ser informado quais usuários do sistema terão acesso e a quem será dado permissão de exclusão de mensagens.

Art. 94. As mensagens do correio eletrônico do HU-UFS não são pessoais.

Art. 95. Os usuários devem tomar precauções, relativas a guarda e troca de suas senhas de acesso, para prevenir o uso por usuários não autorizados.

Art. 96. O correio eletrônico não deverá ser usado para reter informações, mensagens e anexos por um longo período de tempo, sendo obrigação do usuário a limpeza periódica de sua caixa postal como forma de minimizar custos de armazenamento desnecessários.

Parágrafo único. Caso se faça necessário o armazenamento por um período longo, o usuário deverá salvar a sua informação em outro sistema de armazenamento, como seu próprio disco ou áreas de armazenamento compartilhado.

Art. 97. É obrigação do usuário:

I - seguir os padrões de etiqueta no envio de mensagens;

II - proteger e garantir a confiabilidade e privacidade no uso do sistema;

III - avaliar a importância das informações para o HU-UFS, antes de remover as mensagens;

IV - proteger suas senhas;

V - remover e administrar suas caixas postais de maneira adequada;

VI - não enviar correio eletrônico sem a concordância de seus destinatários (spam), como correio eletrônico de publicidades, piadas, vendas, “correntes”, “pirâmides”, filmes, musicas, desenhos, fotos e imagens cujo conteúdo não guarde relação com os negócios do HU-UFS;

VII - identificar no título do correio eletrônico o principal objetivo do mesmo;

VIII - não cadastrar seu correio eletrônico em listas de discussão ou *newsgroups*, salvo em casos relacionados às suas atividades diárias.

Seção VIII

Rede do HU-UFS

Art. 98. Os endereços internos, configurações, e outras informações relacionadas às redes de computadores do HU-UFS devem ser restritos, de modo que sistemas e usuários externos não tenham acesso sem a devida aprovação do Gestor de Segurança.

Art. 99. Todas as redes que estão conectadas à rede do HU-UFS devem estar consistentes com os requisitos de segurança, sendo que o HU-UFS se reserva o direito de suspender imediatamente a conexão com as redes que não sigam estes requisitos.

Art. 100. Informações de acesso relativas a computadores ou sistemas de comunicação, como número telefônico de sistemas de acesso remoto, são consideradas confidenciais, sendo que, este tipo de informação não deve ser colocado em sistemas de acesso público, catálogos telefônicos, cartões de visita ou ficar disponível para terceiros, sem a respectiva aprovação do Gestor da Segurança.

Art. 101. Microcomputadores de mesa ligados a rede do HU-UFS não podem ter modem instalado, exceto quando previamente autorizado pelo Gestor da Segurança.

Art. 102. Microcomputadores de mesa e portáteis, quando ligados na rede do HU-UFS através de placas de rede, não podem fazer uso do modem.

Art. 103. Usuários não podem disponibilizar materiais do HU-UFS (software, memorandos internos, notícias, banco de dados) em qualquer computador publicamente acessível, a não ser mediante autorização da Gerencia SGPTI.

Art. 104. Compras para o HU-UFS, ou qualquer procedimento que gere operação financeira, através da Internet, só poderão ser efetuadas se o site em questão tiver certificação digital.

Art. 105. Cada usuário, ao armazenar informações na rede, deve considerar os acessos permitidos ao diretório que esteja utilizando.

Seção IX

Software

Art. 106. Todo “software” adquirido pelo HU-UFS, desenvolvido por seus funcionários ou desenvolvido por empresas contratadas, é de propriedade exclusiva do HU-UFS.

Art. 107. Todo “software” deverá ser usado em conformidade com suas licenças, contratos e regras

de utilização e distribuição.

Art. 108. Toda a aquisição de software ou licença deverá ser conduzida pelo SGPTI, como forma de garantir a sua compatibilidade com o ambiente de software atual e possibilitar a aquisição com melhores preços e garantias de suporte adequadas.

Parágrafo único. Qualquer sugestão de padrões diferenciados e/ou necessidade de aquisição de software específico para determinada área também deverá ser submetida ao SGPTI que avaliará a solicitação.

Art. 109. Cada usuário é individualmente responsável pela leitura e entendimento do regulamento aplicável ao software utilizado nos computadores da rede corporativa do HU-UFS.

Parágrafo único. Qualquer duplicação de software licenciado para o HU-UFS, exceto para backup, será considerada uma violação de leis nacionais sobre direitos autorais de software.

Art. 110. Os padrões de "softwares" suportados e mantidos pelo quadro técnico do SGPTI, instalados nos computadores da rede corporativa do HU-UFS serão definidos em documento denominado de "RELAÇÃO DE SOFTWARES PADRÃO".

Parágrafo único. A relação de "software" mencionada no caput deste artigo, deverá ser publicada no site do SGPTI.

Art. 111. Qualquer "software" não mencionado na "Relação de Softwares Padrão" deverá ser solicitado ao SGPTI. Cada solicitação será avaliada na conformidade da política de compra estabelecida nesta Portaria.

Parágrafo único. Para a instalação e utilização de "software" fora do padrão definido pelo SGPTI, nos computadores do SGPTI, o usuário deverá obter uma autorização formal do SGPTI.

Art. 112. Todo e qualquer software somente poderá ser instalado pelo quadro técnico do SGPTI, que deve efetuar testes de compatibilidade dos mesmos com outros aplicativos utilizados, evitando assim que ocorram problemas em consequência da instalação do novo aplicativo.

Art. 113. É de responsabilidade do usuário comunicar ao SGPTI sempre que for informado de que seu ambiente de proteção de vírus esteja desatualizado.

Art. 114. O SGPTI está autorizado a remover dos recursos computacionais do HU-UFS qualquer "software" instalado sem sua autorização formal.

Seção X

Hardware

Art. 115. Todos os computadores, impressoras, periféricos ou qualquer "hardware", adquiridos e disponibilizados pelo HU-UFS, só podem ser utilizados para a criação, pesquisa e processamento de materiais relacionados ao HU-UFS.

Parágrafo único. A utilização desses recursos pressupõe que o usuário assume total responsabilidade pelo uso correto dos mesmos e concorda em obedecer às regras estabelecidas nesta Portaria.

Art. 116. Todo o hardware adquirido pelo HU-UFS é de propriedade exclusiva do HU-UFS.

Art. 117. Todo "hardware" deverá ser usado em conformidade com suas licenças, contratos e regras de utilização e distribuição.

Art. 118. Toda aquisição de hardware deverá ser conduzida pela SGPTI, como forma de garantir a sua compatibilidade com o ambiente de hardware atual, e possibilitar a aquisição com melhores preços e garantias de suporte.

Parágrafo único. Qualquer sugestão de padrões diferenciados e/ou necessidade de compra de hardware específico para determinada área deverá ser submetida ao SGPTI, que avaliará a solicitação.

Art. 119. Nenhum equipamento de terceiro poderá ser utilizado e/ou conectado na rede corporativa do HU-UFS, salvo com a autorização expressa do SGPTI.

Seção XI

Incidentes de Segurança

Art. 120. Toda suspeita de incidente de segurança deve ser imediatamente comunicada ao Gestor de Segurança.

Art. 121. Todo usuário da rede do HU-UFS é obrigado a relatar violação e problemas de segurança tão logo os perceba, a fim de que medidas corretivas possam ser tomadas imediatamente, devendo essas comunicações serem feitas de modo confidencial ao Gestor de Segurança.

Art. 122. É proibido o relato de problemas de violação de segurança ou vulnerabilidade de dados para fora do HU-UFS, exceto para auditorias externas, e nas hipóteses de autorização formal do Gestor de Segurança.

Art. 123. Todas as infestações por vírus devem ser comunicadas o mais rápido possível ao Gestor de

Segurança do HU-UFS, de modo que este possa tomar as devidas providências.

CAPITULO VI

ATUALIZAÇÃO E VIGÊNCIA

Art. 124. Esta Política de Segurança da Informação deve ser avaliada e atualizada periodicamente.

Art. 125. Esta Portaria entrará em vigor na data da sua publicação.

Art. 126. Revogam-se as disposições em contrário.

Gabinete da Superintendência,

Aracaju, em 06 de setembro de 2018

Angela Maria da Silva

Superintendente