REPÚBLICA FEDERATIVA DO BRASIL
MINISTÉRIO DA EDUCAÇÃO

UFCSPA
UNIVERSIDADE FEDERAL DE CIÊNCIAS DA SAÚDE DE PORTO ALEGRE

Política de Segurança da Informação e Comunicação da Universidade Federal de Ciências da Saúde de Porto Alegre

2017-2020

***Pró-Reitora de Planejamento**: Alessandra Dahmer*
Grupo de Trabalho de Segurança da Informação:

- ***Evelise Fraga de Souza Santos** – Coordenadora de Desenvolvimento Institucional*
- ***Maurício Alves Gomes** – Coordenador da Divisão de Infraestrutura e Redes*
- ***Cristiano Bonato Both** – Coordenador do Núcleo de Inovação tecnológica e Empreeenderismo e Representante Docente da Área de Tecnologia da Informação*
- ***Juliana Herbert** – Coordenadora do Núcleo de Qualidade Interna*
- ***Márcia Giovenardi** – Coordenadora de Pós-Graduação Stricto sensu e Representante Docente*
- ***Graziella Cé** – Coordenadora da Divisão de Arquivo*

Porto Alegre, outubro de 2017

1. Sumário

2. Escopo

Fazem parte do escopo da Política da Segurança da Informação e Comunicação (PSI) da Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA):

a) apresentar de forma clara a visão da universidade, e de sua administração superior, relacionada à segurança da informação e comunicação;

b) definir diretrizes que orientarão a criação de normas e procedimentos relacionados à segurança da informação e comunicação no âmbito desta instituição; e

c) prover meios para atingir a excelência na qualidade dos serviços prestados por esta instituição, no que tange à confidencialidade, integridade, disponibilidade, autenticidade, confiabilidade e não-repúdio das informações.

3. Abrangência

Esta PSI, suas normas e procedimentos se aplicam a todos os usuários que utilizam de alguma forma os ativos de informação da UFCSPA, como discentes, docentes, técnicos-administrativos, estagiários, bolsistas, funcionários terceirizados e quaisquer outros usuários não mencionados anteriormente.

Os acordos de cooperação, contratos, convênios e demais instrumentos do mesmo gênero celebrados entre a UFCSPA e órgãos públicos ou privados devem estar de acordo com o conteúdo desta PSI.

4. Conceitos e Definições

Para efeito desta política serão adotadas as seguintes definições:

a) Ativo: qualquer bem, material ou não, que tenha valor para esta instituição;

b) Ativo Custodiado: Ativo de terceiro que é administrado e conservado por esta instituição;

c) Ativo de Informação: Ativo que guarda informação de valor para esta instituição;

d) Autenticidade: garantia da veracidade da identidade dos usuários e da origem das informações;

e) Classificação do Ativo: definição do nível de segurança adequado para um Ativo;

f) Confidencialidade: garantia de que uma informação estará disponível apenas para os usuários devidamente autorizados;

g) Cópia de Segurança: cópia reserva que deve ser utilizada no processo de restauração, caso a cópia original seja perdida ou danificada. Também conhecida como Backup;

h) Diretriz: conjunto de orientações que devem ser observadas para a produção de Normas e Procedimentos específicos;

i) Disponibilidade: garantia de que uma informação estará disponível sempre que os usuários autorizados necessitarem;

j) Gestor do Ativo: membro desta instituição responsável pela segurança de um determinado Ativo;

k) Incidente de Segurança: evento identificado em um Ativo que indica uma violação da Política de Segurança da Informação e Comunicação;

l) Integridade: garantia de que uma informação estará disponível de forma correta e completa, sem adulterações;

m) Não-repúdio: garantia de que os atos de um usuário são irretratáveis, ou seja, não poderão ser negados;

n) Norma: conjunto de regras que devem ser seguidas por um grupo;

o) Política de Segurança da Informação e Comunicação: conjunto de princípios que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gerencial da instituição, bem como por seus usuários internos e externos, a fim de garantir que os Ativos sejam assegurados; e

p) Procedimento: conjunto de ações que devem ser realizadas por um grupo para produzir algo.

5. Referências normativas

- ABNT NBR ISO/IEC 27002:2007 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.
- ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- Decreto nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Decreto nº 7.845, de 14 de novembro de 2012 - 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.
- Código de Ética do Servidor Público Civil do Poder Executivo Federal.
- Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
- Instrução Normativa nº 04 da SLTI/MPOG, de 12 de novembro de 2010.
- Lei Nº 12.527, de 18 de novembro de 2011.
- Regimento Interno da UFCSPA.
- DECRETO Nº 8.638 DE 15, DE JANEIRO DE 2016 - Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional

5.1 Normas Complementares

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

• Norma Complementar nº 02/IN01/DSIC/GSIPR - Metodologia de Gestão de Segurança da Informação e Comunicações.

• 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 05/IN01/DSIC/GSIPR **-** Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

• Norma Complementar nº 06/IN01/DSIC/GSIPR **-** Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

• Norma Complementar nº 07/IN01/DSIC/GSIPR **-** Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

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

• Norma Complementar nº 11/IN01/DSIC/GSIPR **-** Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

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

6. Princípios

A PSI/UFCSPA alinha-se às estratégias da Universidade e abrange aspectos de segurança de usuários, física e lógica que sustentam os procedimentos, os processos de negócio e dos ativos da informação utilizados nos serviços oferecidos pela UFCSPA, com base nos seguintes princípios:

I - confidencialidade: garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

II - disponibilidade: garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido;

III - integridade: garante a não violação das informações, com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital;

IV - autenticidade: assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

7. Diretrizes Gerais

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

Independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida e preservada, de acordo com esta Política.

Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pela UFCSPA serão utilizados estritamente para propósito institucional.

As diretrizes da Política de Segurança da Informação e Comunicação da UFCSPA constituem os principais pilares da Gestão de Segurança da Informação e Comunicação da UFCSPA e visam garantir a disponibilidade, integridade,

confidencialidade e autenticidade das informações. Para cada uma das diretrizes devem ser elaboradas normas e procedimentos específicos.

8. Diretrizes Específicas

8.1 Tratamento da Informação

a) A UFCSPA, representada pelo Comitê Gestor de Segurança da Informação e Comunicação, providenciará para que as normas sejam amplamente divulgadas e que os procedimentos sejam observados por todos os usuários de ativos da informação da universidade.

b) O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a confidencialidade, integridade, disponibilidade e autenticidade da informação, observada a legislação em vigor no que diz respeito ao estabelecimento de graus de sigilo.

c) A utilização da informação e dos recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelos usuários.

d) O acesso, divulgação e tratamento da informação classificada ficarão restritos às pessoas com necessidade de conhecê-la.

e) O acesso à informação classificada (dependendo do grau de sigilo) poderá ser acessada por qualquer pessoa mediante autorização da autoridade competente, no qual o agente público se compromete a manter o sigilo da informação, sob pena de responsabilidade penal, cível e administrativa, na forma da lei.

f) As informações classificadas como sigilosas/pessoais requerem controle e proteção especiais contra acessos não autorizados, assim como as informações que necessitem sigilo em virtude de lei ou contrato.

g) As informações institucionais não deverão ser eliminadas indevidamente de sistemas informacionais sem a devida autorização, conforme legislação pertinente.

h) Os sistemas informatizados deverão garantir que as informações armazenadas sejam acessíveis a longo prazo, oportunizando, dessa forma, o seu acesso e a preservação.

8.2 Confidencialidade da Informação

Quanto à confidencialidade, as informações produzidas ou custodiadas pela Universidade classificam-se nos seguintes graus de confidencialidade: ultrassecretas, secretas, reservadas ou pessoais.

a) ultrassecretas: informações cuja competência de classificação são do Presidente da República, Vice-Presidente da República, Ministros de Estado e autoridades com as mesmas prerrogativas, Comandantes da Marinha, do Exército, da Aeronáutica, e Chefes de Missões Diplomáticas e Consulares permanentes no exterior;
b) secretas: informações que, em razão de lei, interesse público ou para preservação de direitos individuais, devam ser de conhecimento reservado;
c) reservadas: informações que, por sua natureza ou por interesse da Universidade, só podem ser divulgadas a um grupo restrito de pessoas;
d) pessoais: informações relativas à intimidade privada, vida privada, honra e imagem das pessoas.
e) públicas: informações que podem ser divulgadas a qualquer pessoa.

Para a classificação da informação em determinado grau de sigilo deverá ser utilizado o critério menos restritivo possível.

Ao conjunto de informações que não possa sofrer fracionamento para fins de acesso deverá ser atribuído o grau de confidencialidade da sua parte cuja classificação seja a mais restritiva.

Informações classificadas como sigilosas terão os prazos de restrição de acesso definidos de acordo com a legislação vigente, a saber: 5 (cinco) anos para informações reservadas, 15 (quinze) anos para informações secretas e 25 (vinte e cinco) anos para informações ultrassecretas.

As informações produzidas ou custodiadas pela Universidade são classificadas quanto à disponibilidade em função do impacto que a indisponibilidade da informação acarretaria à imagem ou às operações vitais das atividades finalísticas da Universidade.

8.3 Gestão de Riscos

a) As normas e procedimentos para implantação e gerenciamento de riscos serão definidos em documento específico elaborado pelo Comitê Gestor de Segurança da Informação e Comunicação e em conformidade com a Política de Gestão de Riscos da UFCSPA, aprovada pelo Conselho Universitário da UFCSPA em 10 de agosto de 2017 (Resolução nº 39/2017).
b) O processo de Gestão de Riscos tem por objetivo identificar os riscos às atividades da universidade e, a partir de critérios de priorização, gerar ações que minimizem seus efeitos.
c) Cabe ao Comitê Gestor de Segurança da Informação e Comunicação determinar as formas de tratamento de riscos.
d) As necessidades de melhorias identificadas deverão ser comunicadas ao Comitê Gestor de Segurança da Informação e Comunicação e ao Comitê de Governança Digital da UFCSPA para que sejam apreciadas e aprovadas.

8.4 Gestão de Contingência e Continuidade

a) O plano de Contingência e Continuidade da UFCSPA será definido pelo Comitê Gestor de Segurança da Informação e Comunicação com base na análise de riscos.
b) O plano de Contingência e Continuidade deverá ser mantido de forma a permitir que os sistemas e recursos de infraestrutura possam atingir um nível mínimo de operação. Da mesma forma, minimizar os impactos decorrentes de falhas, desastres ou indisponibilidade significativas dos serviços, processos e atividades operacionais.

c) O plano deverá ter revisões periódicas, uma vez por ano, em função de resultados de testes realizados, ou após alguma mudança significativa nos ativos de informação.
d) O processo de gestão do plano de Contingência e Continuidade deverá ter a capacidade de identificar potenciais ameaças e possíveis impactos nas operações da instituição, caso essas ameaças se tornem concretas.
e) O Comitê Gestor de Segurança da Informação e Comunicação deve analisar e propor os recursos necessários e melhorias para que o a continuidade das operações seja possível.

O Comitê Gestor de Segurança da Informação e Comunicação deverá desenvolver a cultura de Gestão de Continuidade da UFCSPA.

8.5 Auditoria e Conformidade

Com relação à Auditoria e Conformidade devem ser considerados os seguintes aspectos:

a) As atividades da UFCSPA estão associadas ao conceito de confiança e, como tal, representam instrumentos que facilitam a percepção e transmissão da mesma à comunidade de usuários.
b) A auditoria servirá para manter a rastreabilidade das ações e o não-repúdio das transações efetuadas nos sistemas da universidade.
c) Cabe ao Comitê Gestor de Segurança da Informação e Comunicação da universidade responder as diligências relativas à Segurança da Informação, promovidas por meio de auditoria interna ou externa, bem como responder aos questionários enviados anualmente pelo Tribunal de Contas da União e Controladoria Geral da União.
d) A conformidade da política de segurança deve cumprir as legislações, normas e procedimentos relacionados à Segurança da Informação da Administração Federal e regimento interno da universidade.

e) A avaliação da conformidade deve ser contínua, através de análise de riscos e auditorias internas.

f) As não conformidades relativas às legislações, normas e procedimentos devem ser tratadas conforme Norma Complementar específica.

g) Os responsáveis pela avaliação de conformidade devem ser capacitados nas legislações relacionadas à Segurança da Informação.

8.6 Controle de Acessos

Com relação ao Controle de Acesso, que envolve o Acesso Lógico e Físico aos Ativos, devem ser considerados os seguintes aspectos:

a) todo uso dos Ativos deve ser autorizado pelo respectivo Gestor do Ativo e ocorrer mediante identificação única e intransferível do usuário;

b) todo uso dos Ativos deve ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de uso deve ser previamente autorizada formalmente pelo respectivo Gestor do Ativo;

c) sempre que houver a admissão, mudança das atribuições ou desligamento de membros desta instituição, será responsabilidade da chefia imediata notificar aos Gestores dos Ativos utilizados por esse membro. Os Gestores dos Ativos deverão providenciar os ajustes necessários dos privilégios de acesso dos respectivos Ativos; e

d) todo ambiente deve ser classificado e protegido com mecanismos adequados de segurança de acordo com a criticidade e o sigilo dos Ativos que são mantidos naquele local.

8.7 Tratamento de Incidentes

A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes em segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas.

O processo de Gestão de Incidentes de Segurança da Informação será composto pelas seguintes etapas:

8.7.1 Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação.

8.7.2. Investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação ações de contenção, quando necessárias.

8.7.3. Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

8.7.4. Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê Gestor de Segurança da Informação e Comunicação (CGSI) e a Alta Administração da UFCSPA deverão ser comunicados, para avaliação das providências cabíveis.

9. Competências e Responsabilidades

É responsabilidade de todos que possuem acesso aos ativos da UFCSPA o aceite e o cumprimento desta política, conforme suas normas e procedimentos.

9.1 Da Alta Administração

A Alta Administração deve prover a orientação e o apoio necessários às ações de segurança da informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes, tendo como responsabilidades:

a) instituir o Comitê Gestor de Segurança da Informação e Comunicação;
b) avaliar a Política de Segurança da Informação e Comunicação e encaminhar ao Conselho Universitário para aprovação;
c) designar o Gestor de Segurança da Informação;
d) garantir os recursos necessários para implementação desta Política.

9.2 Das Chefias

São responsabilidades das Chefias as seguintes atividades:

a) gerenciar o cumprimento da PSI/UFCSPA, por parte dos servidores sob sua supervisão;
b) identificar os desvios praticados e adotar as medidas corretivas apropriadas;
c) proteger, em nível físico e lógico, os ativos de informação e de processamento da UFCSPA relacionados com sua área de atuação;
d) tratar e organizar a informação relacionada com sua área de atuação;
e) definir os requisitos de segurança para os ativos sob sua responsabilidade;
f) garantir que o pessoal sob sua supervisão compreenda e colabore para a proteção dos ativos de informação da UFCSPA;
g) se necessário definir a custódia de um ativo sob sua responsabilidade;
h) solicitar ao NTI a concessão de acesso privilegiado a usuários sob sua supervisão para acessar as informações da unidade administrativa sob sua responsabilidade;
i) solicitar ao NTI a retirada de acesso privilegiado a usuários sob sua supervisão que podem acessar as informações da unidade administrativa sob sua responsabilidade.

9.3 Dos Usuários

É dever de todo usuário dos ativos de informação:

b) preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de tecnologia da informação (TI) e ativos da informação;

c) cumprir a PSI/UFCSPA, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

d) utilizar os Sistemas de Informações da UFCSPA e os recursos a ela relacionados somente para os fins previstos pela universidade;

e) cumprir as regras, normas e procedimentos de proteção estabelecidos aos ativos de informação;

f) responder por todo e qualquer acesso aos recursos de TI da UFCSPA, bem como pelos efeitos desses acessos efetivados através do seu usuário de rede ou outro atributo empregado para esse fim (login, crachá, carimbo, e-mail, assinatura digital, etc.);

g) abster-se de utilizar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação à legislação de propriedade intelectual pertinente;

h) comunicar ao seu superior imediato qualquer irregularidade ou desvio.

9.4 Do Comitê Gestor de Segurança da Informação e Comunicação (CGSI)

O Comitê Gestor de Segurança da Informação e Comunicação (CGSI) será composto por representantes das áreas abaixo discriminadas, indicados pelo Gestor de Segurança da Informação e Comunicação:

I. Pró-reitoria de Planejamento

II. Divisão de Suporte Técnico do NTI

III. Divisão de Segurança da Informação e Infraestrutura do NTI

IV. Divisão de Análise e Desenvolvimento do NTI

V. Divisão de Arquivo

VI. Núcleo de Inovação Tecnológica e Empreendedorismo (NITE-Saúde)

VII. Assessoria de Comunicação Social

VIII. Representante Docente da Área de Tecnologia da Informação

São responsabilidades do CGSI:

a) propor a revisão da PSI/UFCSPA, de modo a atualizar a política frente a novos requisitos corporativos, segundo a legislação vigente;

b) propor, analisar e aprovar propostas de normas e políticas de uso dos recursos de informação, tais como: classificação das informações; gerenciamento de identidade e controle de acesso lógico; controle de acesso físico; controle de acesso à internet; utilização do correio eletrônico; utilização de equipamentos de tecnologia da informação; desenvolvimento e obtenção de softwares; utilização de programas e aplicativos; utilização de armazenamento lógico, entre outros;

c) elaborar proposta e promover um Plano de Gestão de Riscos que inclua um Plano de Gestão de Incidentes de Segurança da Informação e um Plano de Contingência e Continuidade, com medidas que garantam a continuidade das atividades da Universidade em caso de desastre ou falhas nos recursos que suportam os processos vitais da UFCSPA;

d) apoiar a implementação das ações de segurança da informação e comunicação; e

e) analisar os casos relacionados à segurança da informação e comunicação omissos nesta política.

9.5 Do Gestor de Segurança da Informação e Comunicação

O Gestor de Segurança da Informação e Comunicação, designado pelo Reitor, é o responsável pelas ações de segurança da informação e comunicações da UFCSPA.

São responsabilidades do Gestor de Segurança da Informação e Comunicação:

a) promover e disseminar a cultura de segurança da informação e comunicações;

b) coordenar a elaboração da Política de Segurança da Informação e Comunicações;

c) instituir e coordenar o Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

d) coordenar as ações de segurança da informação e comunicações;

e) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

f) propor recursos necessários às ações de segurança da informação;

g) coordenar o Comitê Gestor de Segurança da Informação e Comunicação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

h) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

i) manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação;

j) propor normas e procedimentos relativos à segurança da informação na UFCSPA.

9.6 Da Equipe de Tratamento e Resposta a Incidente em Redes Computacionais (ETIR)

A UFCSPA deverá criar e manter uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

O Gestor de Segurança da Informação e Comunicação será responsável por instituir a ETIR e designar um Agente Responsável, o qual ficará encarregado da coordenação, nos termos das Normas Complementares 03/IN01/DSIC/GSIPR e 05/IN01/DSIC/GSIPR.

A ETIR tem como missão a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais, além de atividades de resposta e tratamento a incidentes em redes, tais como: recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais.

9.7 De Terceiros e Fornecedores

É responsabilidade dos terceiros e fornecedores:

I - proteger os ativos da UFCSPA, incluindo informação, evitando perda ou modificação de dados, software e hardware;

II - assegurar o retorno ou a destruição da informação e dos ativos no final do contrato, ou em um dado momento definido no acordo;

III - observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;

IV - observar restrições em relação à manutenção e instalação de software e hardware;

V - atender à política de controle de acesso da UFCSPA;

VI - relatar incidentes de segurança da informação e violação da segurança à equipe de segurança e à equipe de tratamento e respostas a incidentes;

VII - atender aos princípios e diretrizes contidos nesta PSI, incluindo normas e procedimentos complementares destinados à SIC.

10. Penalidades

Ações que violem esta PSI, diretrizes, normas e procedimentos, ou que quebrem os controles de segurança da informação serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas previstas na legislação em vigor, em especial no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo decreto nº 1.117/2004, na Lei nº 8.112/1990 e no disposto no Regimento Interno da UFCSPA

referente ao regime disciplinar, sem prejuízo das demais medidas cíveis e penais cabíveis.

Processo disciplinar específico deverá ser elaborado para apurar as ações que constituem em quebra das diretrizes impostas por esta PSI.

11. Atualização

Esta política e os instrumentos normativos gerados a partir dela devem ser revisados sempre que necessário, contanto que não exceda o período máximo de 4 (quatro) anos.