Universidade Federal de Campina Grande

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

CAMPINA GRANDE - PB - 2021

Alta Direção

Antônio Fernandes Filho	Reitor
Mário Eduardo Rangel Moreira Cavalcanti Mata	Vice-Reitor
Giliara Carol Diniz de Luna Gurgel	Chefe de Gabinete
Caciana Cavalcanti Costa	Pró-Reitor de Ensino
Mário Eduardo Rangel Moreira Cavalcanti Mata	Pró-Reitor de Pós-Graduação
Onireves Monteiro de Castro	Pró-Reitora de Pesquisa e Extensão
Maria Angélica Sátyro Gomes Alves	Pró-Reitor de Assuntos Comunitários
José Ribamar Marques de Carvalho	Pró-Reitor de Gestão Administrativo-Financeira
Vilma Maria Sudério	Secretário de Recursos Humanos
Vinicius Farias Moreira	Secretário de Planejamento e Orçamento

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
01/07/2019	1.0	Política de Segurança da Informação e Comunicação	STI
19/07/2019	1.1	Política de Segurança da Informação e Comunicação	STI
04/06/2000	1.2	Formatação do documento	STI
07/11/2021	1.3	Alteração da minuta	CGD

Sumário

1 OBJETIVO

Fornecer diretrizes, responsabilidades, competências e apoio da alta direção na implementação da gestão de segurança da informação e comunicações da Universidade Federal de Campina Grande (UFCG), buscando assegurar a disponibilidade, integridade e confidencialidade das informações e com abrangência sobre toda a instituição estendendo-se, no que couber, para relação com outras instituições parceiras e/ou fornecedores

2 FUNDAMENTO LEGAL DA POLÍTICA DE SEGURANÇA

Essa Política de Segurança da Informação e Comunicação é definida conforme Decreto nº 9.637, de 26 de dezembro de 2018, que Institui a Política Nacional de Segurança da Informação, além do seguinte referencial:

- Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, de 14 de agosto de 2018;
- Decreto nº 7.579, de 11 de outubro de 2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal;
- Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Instrução Normativa ME nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC
- e-PING – Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.

3 CONCEITOS E DEFINIÇÕES

Comitê de Governança Digital (CGD): comitê responsável por apreciar e aprovar o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), a Política de Segurança da Informação e Comunicações (POSIC) e demais normas a esta última

relacionadas; analisar e aprovar os investimentos na área de Tecnologia da Informação e monitorar o estágio dos projetos e o nível dos serviços, recomendando ações para solução dos problemas de recursos e interesses da área;

Serviço de Tecnologia da Informação (STI): Unidade vinculada à Secretaria de Planejamento e Orçamento (SEPLAN), que planeja, dirige, avalia e executa as políticas de tecnologia da informação e comunicação (TIC) no âmbito da UFCG, em articulação com as Pró-Reitorias e as Direções Gerais dos Campi; Responsável pela manutenção local dos recursos de TIC (RTIC) e preservação da aplicação das políticas, diretrizes e regulamentações na área de informática e telecomunicações.

Recursos de Tecnologia da Informação e Comunicação (RTIC): os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados na UFCG, tais como:

a equipamentos de informática e de telecomunicações de qualquer espécie;

b infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;

c laboratórios de informática de qualquer espécie; e

d recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional da UFCG, redes ou outros sistemas de informação.

Sistemas de informação: os sistemas de controle, organização e planejamento acadêmicos e administrativos, bem como seus conteúdos hospedados e/ou armazenados em máquinas servidoras de responsabilidade do STI ou em máquinas locais com cópias de segurança em máquinas servidoras de responsabilidade do STI ou dos núcleos de tecnologia locais. São partes integrantes do sistema de informação os componentes clientes instalados nas máquinas locais;

Serviços de rede: todos os serviços oferecidos aos usuários por meio da infraestrutura de rede interna e externa, tais como: correio eletrônico, *websites* (páginas individuais e institucionais de conteúdos para a Internet), aplicações *web* (sistemas corporativos acessados via rede), repositórios de arquivos em rede, servidores de bancos de dados

individuais e corporativos, sistemas de autenticação de usuários de rede, serviços de segurança e monitoração, entre outros; bem como seus conteúdos (mensagens de correio eletrônico, dados corporativos, documentos, arquivos de configuração) que são hospedados e armazenados em máquinas servidoras de responsabilidade do STI ou dos núcleos de tecnologia locais;

Termo de Responsabilidade: termo assinado pelo usuário concordando e comprometendo-se com os termos, diretrizes, normas e procedimentos da Política de Segurança da Informação, assumindo proativamente a cultura de segurança institucional e contribuindo efetivamente para o alcance dos objetivos de controle e segurança: disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

Autenticação: é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

Acesso Lógico: acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;

Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso a algum ativo de informação;

Incidente de Segurança: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados;

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

Risco: Probabilidade de que uma ameaça possa explorar uma ou mais vulnerabilidades, de um ou mais ativos, concretizando um ataque e causando impacto no negócio;

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

Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso podendo ser física (como, por exemplo, crachá, cartão e selo) ou lógica como identificação de usuário e senha;

Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) ou CSIRT (Computer Security Incident Response Team): Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

Usuário: qualquer colaborador, seja ele servidor, estagiário, cliente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza

recursos de Tecnologia da Informação disponibilizados pela Administração Pública Federal em local ou jornada de trabalho para este último. Os usuários poderão ser cadastrados ou não no domínio da UFCG e serão classificados, para fins de acesso aos recursos (RTIC), de acordo com os seguintes perfis:

servidores: qualquer servidor, ativo ou aposentado, com vínculo à UFCG;
alunos;
outros:

a responsável por entidade externa que utiliza o domínio da UFCG (procuradoria, grupos de pesquisa, e outros afins);

b entidade representativa de alunos;

c aluno bolsista;

d estagiário externo;

e servidores terceirizados;

f visitante;

g pensionista.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade com autorização para o acesso. [IN01/DSIC/GSIPR];

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado. [IN01/DSIC/GSIPR];

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. [IN01/DSIC/GSIPR];

Não-repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;

Segurança da informação: conjunto de políticas, normas e procedimentos que objetivam o controle de acesso, a preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade, integridade dos dados e responsabilidade das informações e dos recursos de TIC;

Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública

Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações. [IN01/DSIC/GSIPR];

4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A Política de Segurança da Informação e Comunicações da Universidade Federal de Campina Grande consiste na normatização e no disciplinamento de mecanismos que promovam a integridade da estrutura de rede e demais recursos de TIC nos quais trafegam informações e dados comuns ou restritos, neles incluídos os equipamentos que armazenam tais informações.

A Política de Segurança da Informação:

é constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pela UFCG.

é aplicável a todos os bens e serviços e a todo o pessoal que se utiliza dos recursos de Tecnologia da Informação e Comunicação (TIC), no âmbito da UFCG.

A Política de Segurança abrange os seguintes aspectos:

Requisitos de Segurança Lógica;

Requisitos de Segurança Física;

Requisitos de Segurança em Recursos Humanos; e

Requisitos de Segurança dos Recursos Criptográficos.

Os requisitos de segurança, dos itens citados em 4.2 serão regulamentados por meio de normas e procedimentos específicos elaborados pelo Comitê Gestor de Segurança da Informação e avaliados e aprovados pelo Comitê de Governança Digital ou Comitês equivalentes.

5 COMPETÊNCIAS, RESPONSABILIDADES E ESTRUTURA DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Ao Comitê de Governança Digital compete:

a) apreciar e aprovar a Política de Segurança da Informação e Comunicações.

Aos demais gestores compete: Zelar pelo cumprimento das diretrizes da POSIC.

A todos usuários compete:

a conhecer a POSIC e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares.

b adotar comportamento seguro, assumindo atitude proativa e engajada no que diz respeito à proteção das informações da UFCG.

À Secretaria de Recursos Humanos compete: Obter a assinatura do Termo de Responsabilidade e informar à equipe de Tecnologia da Informação sobre mudanças no quadro funcional da Instituição.

A todos os departamentos: Responsabilidade pela garantia da segurança da informação no âmbito da UFCG, ressalvadas as situações em que:

a informação for retirada do âmbito da rede da UFCG por usuários autorizados;

o usuário autorizado fornecer sua senha de acesso a qualquer outra pessoa;

o acesso à informação for limitado ou indisponibilizado por serviços e estruturas externas à UFCG ou de responsabilidade de outros órgãos ou empresas;

quando propositadamente ou inadvertidamente o usuário fizer uso inadequado dos recursos (RTIC), seja por inabilidade, conhecimento insuficiente ou intenção de causar dano à instituição ou a outrem.

Ao Comitê Gestor de Segurança da Informação compete:

elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (POSIC) e normas relacionadas, submetendo a aprovação do Comitê de Governança Digital ou órgão equivalente;

Assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF;

Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

propor, acompanhar e divulgar os planos de ação para aplicação da PSI, incluindo a conscientização de usuários;

propor a implantação de soluções para minimização dos riscos; e

elaborar propostas de normas complementares e políticas de uso dos recursos de informação.

Ao Presidente do Comitê Gestor de Segurança da Informação, no âmbito de suas atribuições, incumbe:

promover cultura e segurança da informação e comunicações;

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

propor recursos necessários às ações de segurança da informação e comunicações;

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

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

manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR) para o trato de assuntos relativos à segurança da informação e comunicações; e

propor normas relativas à segurança da informação e comunicações.

6 DIRETRIZES

TRATAMENTO DA INFORMAÇÃO

Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da instituição de tal forma a garantir a integridade, facilidade de localização e evitar o uso dessas informações por pessoas não autorizadas.

O descarte de informações sensíveis deverá ser realizado através de trituração, incineração ou remoção dos dados de forma segurança.

Deverão ser realizadas cópias de segurança das informações tomando como base norma de gerenciamento de cópias de segurança da informação da UFCG a ser elaborada e revisada periodicamente pela STI.

GESTÃO DE RISCOS E TRATAMENTO DE INCIDENTES

Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços da UFCG, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:

a o que deve ser protegido;

b análise de riscos (contra quem ou contra o que deve ser protegido);

c avaliação de riscos (análise da relação custo/benefício).

A STI apresentará planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê de Governança Digital e executados pela STI e seus núcleos de tecnologia locais.

As normas e procedimentos para implantação e gerenciamento de riscos de Informação serão definidos em documento específico elaborado pelo Comitê Gestor de Segurança da Informação.

A UFCG deverá realizar treinamentos específicos de conscientização para todos os servidores em noções de segurança da informação visando à implantação e gerenciamento de todos os componentes do Sistema de Gestão de Segurança da Informação (SGSI) e a agilidade da notificação de qualquer evento relacionado a segurança da informação que venha a ocorrer.

GESTÃO DE CONTINUIDADE

O Plano de Continuidade de Negócio (PCN) tem como objetivo manter em funcionamento os serviços e processos críticos da UFCG na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, sinistros, falhas humanas e qualquer outro tipo de eventualidade que venha a ocorrer.

O PCN da UFCG será definido pelo Comitê Gestor de Segurança da Informação com base na análise de riscos e terá a aprovação do Comitê de Governança Digital ou órgão equivalente.

AUDITORIA E CONFORMIDADE

Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos (RTIC).

Os procedimentos de auditoria e de monitoramento de uso dos recursos (RTIC) serão realizados periodicamente pela STI, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a POSIC e normas complementares, será permitido à STI auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário, à direção geral do campus e/ou a Reitoria da UFCG dependendo da gravidade. Sendo considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços.

Será mantido pela Ouvidoria da UFCG canal de comunicação para receber denúncias de infração a qualquer parte desta política de segurança.

CONTROLE DE ACESSO E UTILIZAÇÃO DOS RECURSOS

Todos os usuários da UFCG têm o direito ao uso dos recursos (RTIC) da UFCG de acordo com as diretrizes de seu perfil, definidas por meio de requisitos técnicos ou por determinação específica da Reitoria ou dos órgãos da administração superior dos campus.

6.5.2. É vedado o uso de recursos de TICs que não tenham sido oficialmente liberados e homologados pela STI, o que inclui computadores e outros equipamentos particulares como roteadores, hubs, switches, sistemas e aplicativos que não pertençam ao patrimônio da UFCG;

O acesso aos serviços de rede da UFCG que necessitam autenticação só será permitido a usuários cadastrados.

O acesso aos recursos (RTIC) será feito por controles físicos ou lógicos, com objetivo de proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. Quando da utilização de nome de usuário e senha, estes serão definidos no momento de ingresso na UFCG.

Todos os usuários deverão por meio de um termo de responsabilidade específico assumir o compromisso de:

a declarar o conhecimento e aceitação dos termos desta política de segurança e de suas diretrizes, normas e procedimentos, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

b declarar estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria; e

c manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos, a critério da STI.

Todos os usuários e qualquer outra pessoa que entre nos setores administrativos da instituição deverão possuir algum tipo de identificação visível e ter seu acesso registrado, onde possa ser visualizada a data e hora de sua entrada e saída.

Qualquer tipo de informação referente a conteúdos que dizem respeito à instituição deverá ser guardado em lugar seguro como, por exemplo, cofres, armários e mobílias que possuam algum tipo de fechadura quando não estiverem em uso.

Qualquer tipo de equipamento de armazenagem e processamento de informação com tombamento (Ex.: estações de trabalho, notebooks, celulares) só poderão ser utilizados fora das dependências da UFCG ou do departamento de sua responsabilidade com

autorização prévia e protegido de forma adequada contra furto, roubo ou perda da informação.

É de total responsabilidade do usuário a proteção das informações institucionais que estejam sob sua responsabilidade, utilizadas no âmbito da UFCG ou fora de suas dependências.

O gerenciamento de informações, documentos e materiais sigilosos da UFCG deverão estar em conformidade com a Lei nº 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências, com o Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento e com a Lei nº 13.709/2018 que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais.

CORREIO ELETRÔNICO

Os serviços de correio eletrônico mantidos pela UFCG são oferecidos como um recurso profissional (no apoio aos seus) para apoiar os usuários cadastrados da UFCG no cumprimento dos objetivos institucionais e são passíveis de auditoria.

Os serviços de correio eletrônico citados em 6.6, deverão garantir o sigilo, a confidencialidade, o não-repúdio, a autenticidade, a disponibilidade geral do serviço e, os usuários que o utilizarem, deverão assegurar que o endereçamento da mensagem esteja correto.

PUBLICAÇÃO E ACESSO À INTERNET

Todos os servidores têm o direito de acesso à internet, conforme as permissões de acesso estipuladas nas normas de segurança da instituição. Esse acesso deverá ser feito exclusivamente para fins diretos e complementares às atividades da instituição, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

Toda informação publicada no portal da UFCG é de responsabilidade da Assessoria de Comunicação – Ascom.

7 PENALIDADES

São considerados inaceitáveis e passíveis de punição os seguintes usos de TIC no âmbito do UFCG: qualquer uso das TICs que não atenda à legislação em vigor; compartilhamento de senhas e contas de usuários de computadores e sistemas, bem como, outras permissões de acesso individual; acesso ou uso desautorizado pela STI a redes, sistemas ou informações informatizadas; interferência na capacidade de outras pessoas acessarem ou usarem sistemas, redes ou informações; divulgação de informações destinadas para uso interno da UFCG, ou que comprometam a privacidade e segurança servidores, inclusive imagens; fraudar ou alterar as configurações de segurança dos sistemas; utilização de equipamentos ou sistemas para interesse pessoal ou que não sejam de uso e interesse da UFCG; uso de arquivos ou softwares que não estejam licenciados ou que estejam licenciados de forma inadequada; visualização, armazenamento ou transmissão de conteúdo pornográfico; uso de sistemas para objetivos que não sejam compatíveis com os valores do UFCG, por exemplo, ameaças, intimidação, bullying, discriminação, assédio moral ou disseminação de ódio.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários, quando na utilização dos recursos de processamento da informação da UFCG, ficando os transgressores sujeitos às sanções previstas neste documento e na lei vigente, quando cabível.

A quem descumprir esta política de segurança, as normas e procedimentos estabelecidos pela UFCG serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

a na Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

b no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;

c no Código Penal, através do Decreto-Lei nº 2848/1940;

d da Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

e no Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança.

f Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

8 DISPOSIÇÕES GERAIS

Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicações da UFCG, devem ser direcionados ao Comitê Gestor de Segurança da Informação, com a interveniência do Comitê de Governança Digital ou Órgão equivalente.

O Serviço de Tecnologia da Informação - STI/SEPLAN é responsável por emitir normas complementares e operacionais no tocante a essa Política de Segurança da Informação e Comunicação;

As Normas e procedimentos devem ser publicizadas em boletim interno da UFCG e disponíveis na Internet e Intranet para todos os usuários dos recursos de tecnologia da informação da UFCG;

9 ATUALIZAÇÃO

Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 01 (um) ano.

10 VIGÊNCIA

A presente política passa a vigorar a partir da data de sua publicação.

REFERÊNCIAS

Constituição da República Federativa do Brasil de 1988.

Lei Geral de Proteção de Dados Pessoais (LGPD) -- LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

Lei nº 8.112 de 11 de dezembro de 1990 - Regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

Decreto nº 9.637, de 26 de dezembro de 2018, que Institui a Política Nacional de Segurança da Informação.

Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Decreto Nº 7.579, de 11 de outubro de 2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal.

Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Instrução Normativa GSI Nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e demais normas complementares.

Decreto 1.171, de 24 de junho de 1994 - Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências.

Instrução Normativa ME Nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

e-PING – Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.

Resolução CUNI Nº 054, de 5 de julho DE 2011, que dispõe sobre a Política de Segurança da Informação e Comunicações da Universidade Federal de Lavras.

Resolução Nº 18, de 31 de maio de 2010, que normatiza o uso dos recursos de tecnologia da informação e comunicação do IFRO

Política de Segurança da Informação e Comunicação – IFPB, de 19 de junho de 2017.