UFOP

Universidade Federal
de Ouro Preto

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA UFOP

2019

Reitora
Profª. Cláudia Aparecida Marliéle de Lima

Vice-Reitor
Prof. Hermínio Arias Nalini Júnior

CHEFIA DE GABINETE
Chefe de Gabinete - Prof. Élido Bonomo
Assessora Técnica da Reitoria - Débora Walter dos Reis

Pró-Reitoria de Graduação - PROGRAD
Pró-Reitora de Graduação - Profª. Tânia Rossi Garbin
Pró-Reitor Adjunto de Graduação - Adilson Pereira dos Santos

Pró-Reitoria de Pesquisa e Pós-Graduação - PROPP
Pró-Reitor de Pesquisa e Pós-Graduação - Prof. Sérgio Francisco de Aquino
Pró-Reitora Adjunta de Pesquisa e Pós-Graduação - Profª. Renata Guerra de Sá Cota

Pró-Reitoria de Extensão - PROEX
Pró-Reitor de Extensão - Prof. Marcos Eduardo Carvalho G. Knupp
Pró-Reitora Adjunta de Extensão - Profª. Gabriela de Lima Gomes

Pró-Reitoria de Assuntos Comunitários e Estudantis - PRACE
Pró-Reitora - Natália de Souza Lisboa
Pró-Reitora Adjunta - Sabrina Magalhães Rocha

Pró-Reitoria de Planejamento e Desenvolvimento - PROPLAD
Pró-Reitor de Planejamento e Desenvolvimento - Prof. Eleonardo Lucas Pereira
Pró-Reitor Adjunto de Planejamento e Desenvolvimento - Prof. Máximo Eleotério Martins
Diretor de Orçamentos e Finanças - Eduardo Curtiss dos Santos
Prefeita do Campus Universitário - Profª. Sandra Maria Antunes Nogueira
Prefeito Adjunto do Campus Universitário - Edmundo Dantas Gonçalves

Pró-Reitoria de Administração - PROAD
Pró-Reitora de Administração - Profª. Rita de Cássia Oliveira
Coordenador de Gestão de Pessoas - Daniel Caldas
Coordenador de logística e segurança - Vicente Evangelista de Oliveira

Núcleo de Tecnologia da Informação - NTI
Diretor - Abelard Ramos Fernandes

Coordenadoria de Assuntos Internacionais - CAINT
Coordenadora - Jaqueline Pinheiro Schultz

Coordenadoria de Comunicação Institucional - CCI
Coordenador - Francisco José Daher Júnior
Sistema de Bibliotecas e Informação
Diretora - Gracilene Maria de Carvalho

Comitê de Tecnologia da Informação e Comunicação (PORTARIA REITORIA Nº 364, de 26 de junho de 2018)

Vice-Reitor - Prof. Hermínio Arias Nalini Júnior
Pró-Reitor de Planejamento e Desenvolvimento - Prof. Eleonardo Lucas Pereira
Pró-Reitora de Graduação - Profª. Tânia Rossi Garbin
Pró-Reitor de Pesquisa e Pós-Graduação - Prof. Sérgio Francisco de Aquino
Pró-Reitor de Extensão - Prof. Marcos Eduardo Carvalho G. Knupp
Pró-Reitora de Assuntos Comunitários e Estudantis - Natália de Souza Lisboa
Pró-Reitora de Administração - Profª. Rita de Cássia Oliveira
Diretor do Núcleo de Tecnologia da Informação (NTI) - Abelard Ramos Fernandes
Gerente de Projetos do NTI - Frederico Augusto de Cezar Almeida Gonçalves
Gerente de Serviços do NTI - Tiago Rodrigues Chaves
Coordenadora do Escritório de Governança do NTI - Daniele Cristine Silva

Constitui comissão para elaboração do Política de Segurança da Informação e Comunicação-POSIC (RESOLUÇÃO CTIC Nº 02, de 03 maio de 2019)

Diretor do Núcleo de Tecnologia da Informação - Abelard Ramos Fernandes
Gerente de Projetos do NTI - Frederico Augusto Cezar Almeida Gonçalves
Coordenador de Comunicação Institucional - Francisco José Daher Júnior
Chefe do Arquivo Central - Zenóbio dos Santos Junior
Representante da Coordenadoria de Assuntos Internacionais (CAINT) - Anderson Antonio Gamarano

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
29/11/2019	01	Versão inicial	**Comissão para elaboração Política De Segurança Da Informação E Comunicações Da Ufop - PoSIC**

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º É instituída a Política de Segurança da Informação e Comunicações (PoSIC) da Universidade Federal de Ouro Preto (UFOP), observados os princípios, objetivos e diretrizes estabelecidos nesta Resolução, bem como às disposições constitucionais, legais e regimentais vigentes.

§ 1º A PoSIC estabelece as orientações e diretrizes corporativas gerais de segurança e controle dos ativos de informação da UFOP, ou sob sua guarda, objetivando sua proteção e a prevenção de responsabilidade legal para todos os usuários.

§ 2º Integram também a PoSIC normas gerais e específicas de segurança da informação e comunicações, bem como procedimentos complementares, destinados à proteção dos ativos de informação e à disciplina de sua utilização, emanados no âmbito da UFOP.

Art. 2º. A estrutura da Segurança da Informação e Comunicações da UFOP é composta por três instrumentos normativos, de níveis hierárquicos distintos, relacionados a seguir:

I. Política de Segurança da Informação e Comunicações (PoSIC): define a estrutura,as diretrizes e as obrigações referentes à segurança da informação e comunicações;

II. Normas de Segurança da Informação e Comunicações (NSIC): identificam obrigações e procedimentos em conformidade com as diretrizes da PoSIC, a serem seguidas em todas as situações em que a informação é tratada;

III. Procedimentos de Segurança da Informação e Comunicações: instrumentalizam os dispositivos, permitindo a direta aplicação nas atividades da UFOP.

Art. 3º A PoSIC irá se alinhar às estratégias da UFOP e terá por objetivo garantir os princípios de segurança da informação e comunicações, das informações produzidas ou custodiadas pela universidade, abrangendo aspectos físicos, tecnológicos e humanos da organização.

Art. 4º A PoSIC e as normas de segurança da informação e comunicações devem ser disponibilizadas a todos os usuários da UFOP, de maneira que seu conteúdo possa ser acessado a qualquer momento.

Parágrafo único. Os procedimentos de segurança da informação e comunicações devem ser divulgados apenas às áreas relacionadas à sua execução.

CAPÍTULO II

DOS CONCEITOS E DAS DEFINIÇÕES

Art. 5º Para os efeitos da PoSIC e das normas por ela originadas, entende-se por:

I. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II. Agente Responsável: servidor incumbido de chefiar e gerenciar a Equipe de Tratamento de Incidentes em Segurança da Informação;

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

IV. Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

V. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI. Comitê de Tecnologia da Informação e Comunicação (CTIC): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações na UFOP;

VII. Controle, Proteção ou Contramedida: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

VIII. Custodiante do Ativo de Informação: servidor ou unidade da UFOP que tenha a responsabilidade formal de proteger um ou mais ativos de informação, aplicando os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações.

IX. Desastre: evento repentino e não planejado que causa perda para toda ou

parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

X. *Computer Security Incident Response Team* (CSIRT): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidente de segurança em computadores;

XI. Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso as ameaças se concretizem, que busca a oferta de uma estrutura que desenvolva a resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;

XII. 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;

XIII. Gestor da Informação: qualquer servidor ou unidade que, no exercício de suas competências, é responsável pela produção de informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues à UFOP;

XIV. Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da UFOP;

XV. Incidente de Segurança: ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança da informação, nos termos da Norma ISO/IEC TR no 18044:2004;

XVI. Plano de Continuidade de Negócios: plano constituído de um conjunto de medidas, regras, procedimentos e informações necessárias para que a UFOP mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

XVII. Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente

cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XVIII. Plano de Recuperação de Negócios: plano constituído de um conjunto de medidas, regras, procedimentos e informações necessárias para que a UFOP operacionalize o retorno das atividades críticas à normalidade;

XIX. Plano de Tratamento dos Riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

XX. Programa de Gestão da Continuidade de Negócios: processo contínuo de gestão e governança suportado pela alta direção que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial; e manter estratégias e planos de recuperação, e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção;

XXI. Recurso: é um meio de qualquer natureza (humano, físico, tecnológico, financeiro, de imagem de mercado, de credibilidade, entre outros) que permite alcançar aquilo a que se propõe;

XXII. Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

XXIII. Riscos de Segurança da Informação e Comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXIV. Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXV. Tratamento da Informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XXVI. Trilhas de Auditoria: arquivos de Logs do sistema, que contêm as gravações das ações realizadas no sistema, de modo a identificar quem ou o que causou algo;

XXVII. Usuário Externo: qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativa ou academicamente à

UFOP;

XXVIII. Usuário Interno: qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativa ou academicamente à UFOP;

XXIX. Usuários: usuários internos e externos; servidores, terceirizados, colaboradores, consultores, auditores e estagiários/bolsistas que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão.

CAPÍTULO III

DOS ATRIBUTOS E DOS PRINCÍPIOS

Art. 6º A segurança da informação e comunicações, coberta pela presente PoSIC, terá, dentre outros inerentes à Administração Pública Federal, os seguintes atributos:

I. Confidencialidade: define que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

II. Disponibilidade: define que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

III. Integridade: define que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

IV. Autenticidade: define que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Art. 7º A presente PoSIC terá, dentre outros inerentes à Administração Pública Federal, os seguintes princípios:

I. Responsabilidade: preservação da integridade e tratamento de maneira adequada, de acordo com sua classificação, da informação, bem como preservar e zelar pelos ativos de informação;

II. Clareza: as regras que se fundam nesta PoSIC devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão;

III. Publicidade: transparência às informações, respeitando a privacidade do cidadão.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 8º A Segurança da Informação e Comunicações deve ser responsabilidade de todos, baseada em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso dos ativos de informação.

Art. 9º Os dirigentes das unidades e demais chefias da UFOP atuarão junto à CSIRT naquilo que forem solicitados, assim como no desenvolvimento de suas atividades, de forma colaborativa, em estrita observância às orientações determinadas pela CSIRT, naquilo que tange a Segurança da Informação e Comunicações, objetivando minimizar as vulnerabilidades e ameaças que possam comprometer o negócio da instituição.

Art. 10. A utilização dos ativos de informação deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

SEÇÃO I

DO TRATAMENTO DA INFORMAÇÃO

Art. 11. Todo ativo de informação sob a responsabilidade da UFOP é considerado um bem e deve ser protegido pela instituição, de acordo com as diretrizes descritas nesta PoSIC e demais regulamentações em vigor, com o objetivo de minimizar os riscos aos serviços e atividades, bem como preservar a imagem institucional.

Art. 12. A classificação da informação obedecerá às diretrizes estabelecidas pela Lei de Acesso à Informação – LAI – regulamentada pelo Decreto no 7.724/2012, do Governo Federal, e do Serviço de Informação ao Cidadão – SIC no âmbito da UFOP.

SEÇÃO II

DO TRATAMENTO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Art. 13. A fim de evitar ou minimizar os impactos de situações de interrupção dos sistemas de informação e comunicações causados por incidentes de segurança, a CSIRT deverá manter um Plano de Gerenciamento de Incidentes, elaborado e alinhado ao Programa de Gestão de Continuidade de Negócios, conforme a Norma Complementar no 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009.

Art. 14. Todo incidente de segurança, bem como suas providências, deverá ser comunicado ao Gestor de Segurança da Informação e Comunicações da UFOP.

SEÇÃO III

DA GESTÃO DE RISCOS

Art. 15. A UFOP deve adotar processo contínuo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, conforme estabelecido na Norma Complementar no 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, ou documento correspondente que venha a substituí-lo.

Art. 16. O processo de GRSIC deverá ser revisto periodicamente pelo Núcleo de Tecnologia da Informação NTI, com a participação da CSIRT, a fim de aperfeiçoar e agir proativamente contra riscos advindos de novas tecnologias e ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção dos seus ativos de informação.

Art. 17. Caberá ao Núcleo de Tecnologia da Informação - NTI a criação e atualização do Plano de Tratamento de Riscos, com a participação da CSIRT e de grupos de trabalho específicos.

SEÇÃO IV

DA GESTÃO DE CONTINUIDADE

Art. 18. Com o objetivo de evitar situações de interrupção e manter em funcionamento os sistemas de informação e comunicações da UFOP, o Núcleo de Tecnologia da Informação - NTI deverá manter um Programa de Gestão da Continuidade de Negócios, conforme a Norma Complementar no

06/IN01/DSIC/GSI/PR de 11 de novembro de 2009.

SEÇÃO V

DA AUDITORIA E CONFORMIDADE

Art. 19. O Núcleo de Tecnologia da Informação - NTI deverá propor normas complementares ao CTIC, a fim de manter registros, como mecanismo de auditoria que possibilite o rastreamento, acompanhamento, controle e verificação de acesso aos serviços, sistemas de informação e rede interna, em conformidade com a Norma Complementar no 21/IN01/DSIC/GSI/PR, de 8 de outubro de 2014.

SEÇÃO VI

DOS CONTROLES DE ACESSO

Art. 20. A concessão de acesso aos ativos de informação da UFOP tem por objetivo garantir aos usuários a realização de suas atividades.

Art. 21. O uso dos ativos de informação na UFOP, pelos seus usuários, deve ser direcionado prioritariamente para a realização das atividades de ensino, pesquisa, extensão e de administração desempenhadas nos limites da ética, razoabilidade e legalidade.

Art. 22. A conta de acesso e a senha de cada usuário são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representam nível de delegação concedida para o desempenho de suas funções.

Art. 23. O CTIC deverá normatizar o acesso físico e lógico aos ativos de tecnologia da informação da UFOP, como forma de garantir a sua proteção.

SEÇÃO VII

DO USO DE E-MAIL

Art. 24. Os usuários da UFOP terão direito a uma conta de correio eletrônico no serviço de correio eletrônico da instituição, que terá uma única titularidade, determinando a responsabilidade sobre sua utilização.

Art. 25. O usuário deve utilizar a sua conta de correio eletrônico em conformidade

com a lei, a moral, os bons costumes e a ordem pública.

Parágrafo único. O e-mail não deverá ser usado para a prática de atos ilícitos – proibidos pela lei ou pela presente diretriz ou normas complementares que venham a ser editadas – lesivos aos direitos e interesses da UFOP ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os ativos de informação, bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

SEÇÃO VIII

DO ACESSO A INTERNET

Art. 26. O Núcleo de Tecnologia da Informação - NTI deve propor normas ao CTIC, de forma que os órgãos de TIC possam definir procedimentos e implementar mecanismos de autenticação que determinem a titularidade de todos os acessos à Internet feita pelos usuários que estejam sob sua responsabilidade.

Art. 27. Aplica-se ao usuário da Internet o disposto no art. 25 e seu parágrafo único.

SEÇÃO IX

DOS SÍTIOS

Art. 28. Os serviços e servidores da instituição, tais como os de páginas de Internet, correio eletrônico, sistemas administrativos e sistemas acadêmicos, deverão ser configurados para usar tecnologias de autenticação e criptografia visando a garantir a integridade, o sigilo e a autenticidade das informações.

Art. 29. Caberá ao Núcleo de Tecnologia da Informação - NTI definir e pôr em prática as medidas necessárias para preservar a segurança dos serviços e servidores institucionais que estiverem sob sua responsabilidade, de forma a não comprometer a segurança das redes internas e externas à instituição.

Parágrafo único. A unidade que adotar domínio próprio deverá pôr em prática as medidas necessárias para preservar a segurança dos seus serviços e servidores, definidas pelo Núcleo de Tecnologia da Informação - NTI, de forma a não comprometer a segurança das redes internas e externas à instituição.

Art. 30. Deverá haver pelo menos um responsável para atuar como contato no que se refere à segurança dos serviços e servidores na unidade responsável pelo

mesmo.

SEÇÃO X

DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 31. O processo de Gestão da Segurança da Informação e Comunicações deverá ser proposto por uma comissão interdisciplinar, a qual será coordenada pelo Núcleo de Tecnologia da Informação - NTI e aprovado pelo CTIC em norma complementar.

SEÇÃO XI

DA SEGURANÇA FÍSICA DO AMBIENTE DE TI

Art. 32. Para os sistemas de missão crítica, deverão ser contratados serviços ou utilizados equipamentos que disponham de recursos de redundância de processamento, de armazenamento de dados, de sistemas elétricos, etc., bem como controle de corrente elétrica (rede estabilizada), temperatura, umidade e acesso físico restrito.

Parágrafo único. Cabe ao CTIC classificar os sistemas de missão crítica e a sua definição de proteção, considerando a criticidade das informações e os ativos de informação envolvidos nesses sistemas.

Art. 33. Os servidores computacionais, onde se encontram os sistemas de missão crítica, devem estar em sala segura contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios, acesso indevido, etc.).

Parágrafo único. Cabe ao Núcleo de Tecnologia da Informação - NTI a definição de dispositivos ou serviços de proteção, considerando a criticidade das informações e dos ativos de informação envolvidos, e que estejam sob sua responsabilidade.

Art. 34. No caso de hospedagem de serviços dentro das instalações da UFOP, a subestação de energia e refrigeração do ambiente onde se encontram estes sistemas deve garantir o seu pleno funcionamento, devendo ser enviado relatório anual ao Núcleo de Tecnologia da Informação - NTI, com o quadro da situação destes.

Parágrafo único. Cabe ao Agente Responsável pela CSIRT o envio anual deste relatório ao gestor de segurança da informação.

SEÇÃO XII

DA SEGURANÇA LÓGICA DO AMBIENTE DE TI

Art. 35. A UFOP deverá manter soluções de proteção contra problemas de segurança lógica (vírus, acesso não autorizado, invasões, etc.), cabendo ao Núcleo de Tecnologia da Informação - NTI à definição de tais soluções de proteção, considerando a criticidade dos ativos de informação envolvidos e que estejam sob sua responsabilidade.

Art. 36. Caberá ao Núcleo de Tecnologia da Informação - NTI a definição dos procedimentos de segurança para a implantação, manutenção, atualização, desinstalações e recuperação de softwares, sistemas operacionais, SGDBs, de forma a garantir que estes ambientes lógicos da UFOP não tragam vulnerabilidades que comprometam a segurança da informação, cabendo ao CTIC a normatização.

Art. 37. Cabe aos órgãos da UFOP providenciar para que os ambientes lógicos, sob sua responsabilidade, tenham o seu acesso restrito por senhas seguras, ou outros mecanismos de segurança apropriados, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela Núcleo de Tecnologia da Informação - NTI.

SEÇÃO XIII

DA SEGREGAÇÃO DE AMBIENTES

Art. 38. O CSIRT deve assegurar que todos os sistemas de informação sob a responsabilidade do Núcleo de Tecnologia da Informação - NTI da UFOP sejam aderentes às diretrizes a seguir:

I. Segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais;

II. Os ambientes de produção somente poderão ser acessados por usuários internos responsáveis pela implantação dos sistemas de informação;

III. O acesso às bases de dados dos ambientes de produção será feito, sempre que possível, por meio dos sistemas de informação, ou, não sendo possível, o acesso deverá ser feito por um membro da equipe responsável pela base de dados com autorização de um usuário interno com nível gerencial da área solicitante. O acesso direto deverá ser registrado em meio que permita a

identificação do que foi modificado e quem foi responsável pela modificação;

IV. Os sistemas de informação que forem transferidos para o ambiente de produção deverão ter seu código-fonte original mantido por um sistema de gerenciamento de repositórios de código-fonte interno;

V. O código-fonte dos sistemas de informação sob domínio do Núcleo de Tecnologia da Informação - NTI deverão ser gerenciados por ferramenta específica de controle de versão. O acesso à ferramenta deverá ser restrito através de perfis de acesso específicos e registrados em trilhas de auditoria. O controle de versão deve permitir a identificação do responsável pela inclusão/exclusão/alteração do código-fonte, assim como a recuperação de versões recentes;

VI. O ambiente do sistema computacional destinado à execução dos sistemas e o ambiente de produção não deverão ser utilizado para testes. Os testes deverão ser feitos em ambiente apropriado e gerenciado;

VII. A passagem de programas e dados para o ambiente de produção deverão ser controlada de maneira a garantir a integridade e disponibilidade desse ambiente para sua execução;

CAPÍTULO V
DAS SANÇÕES E PENALIDADES

Art. 39. Atos ou ações que violem o disposto nesta Resolução ou em quaisquer de suas normas e/ou procedimentos complementares, ou que prejudiquem os controles de segurança da informação, no âmbito da UFOP, serão apuradas mediante instauração de processo administrativo disciplinar.

Parágrafo único. Os responsáveis por prejuízos ou irregularidades mencionados no *caput* deste artigo responderão administrativa, civil e/ou penalmente pelos seus atos.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 40. A estrutura para a Gestão de Segurança da Informação e Comunicações na UFOP é composta pelo (a):

I. Comitê de Tecnologia da Informação e Comunicação (CTIC);

II. Gestor de Segurança da Informação e Comunicações;

III. Equipe de Tratamento de Incidentes em Segurança da Informação (CSIRT).

SEÇÃO I

COMITÊ DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 41. O CTIC é o responsável pela edição de Políticas, Normas e Procedimentos Institucionais que se façam necessárias para a garantia da segurança e mitigação de riscos ao ambiente de Tecnologia da Informação e Comunicações da UFOP.

Art. 42. São atribuições do CTIC:

I. Definir o escopo e os limites da Segurança da Informação e Comunicações na UFOP;

II. Assessorar na implementação das ações de Segurança da Informação e Comunicações;

III. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação e Comunicações;

IV. Propor a Política de Segurança da Informação e Comunicações (PoSIC) e suas alterações;

V. Propor normas relativas à Segurança da Informação e Comunicações;

VI. Propor investimentos e definir a ordem de prioridade de execução dos projetos e aplicação dos recursos necessários ao cumprimento da PoSIC;

VII. Monitorar a aplicação dos recursos para a Segurança da Informação e Comunicações;

VIII. Propor alteração no regimento interno, quando necessário;

IX. Propor prioridade em assuntos relacionados à Segurança da Informação e Comunicações;

X. Acolher e analisar as demandas quanto à Segurança da Informação e Comunicações;

XI. Propor estudos e projetos relativos à competência do CTIC.

SEÇÃO II

DA PRESIDÊNCIA E DA SECRETARIA DO COMITÊ

Art. 43. A presidência do CTIC será exercida pelo Vice-Reitor, em conformidade com a Resolução CUNI Nº 2156 de 14 de dezembro de 2018.

Art. 44. São atribuições do Presidente do CTIC:

I. Coordenar ações relacionadas à política de segurança da informação e comunicação da UFOP;

II. Convocar e presidir as reuniões ordinárias e extraordinárias;

III. Aprovar a pauta das reuniões;

IV. Resolver as questões de ordem;

V. Decidir em caso de empate, utilizando o voto de qualidade;

VI. Baixar atos necessários à organização interna do CTIC;

VII. Autorizar a presença nas reuniões de pessoas que possam contribuir para os trabalhos do CTIC;

VIII. Indicar membros para a realização de estudos, levantamentos, investigações e emissão de pareceres necessários à consecução da finalidade do CTIC, bem como relatores das matérias a serem apreciadas;

IX. Requisitar informações e diligências necessárias à execução das atividades do CTIC;

X. Assinar documentos, atas das reuniões, bem como proposições referentes ao CTIC;

XI. Expedir, ad referendum do CTIC, em vista de circunstâncias de urgência, normas complementares relativas ao seu funcionamento e à ordem dos trabalhos, bem como atos administrativos, ficando o tema obrigatoriamente inscrito na pauta da próxima reunião;

XII. Designar servidores responsáveis pelos trabalhos de apoio operacional e administrativo às reuniões.

Art. 45. A Secretaria do CTIC será exercida por servidor designado pelo Vice-reitor.

Art. 46. São atribuições do (a) Secretário (a):

I. Auxiliar o Presidente na coordenação, orientação e supervisão das atividades do CTIC;

II. Fazer as convocações determinadas pelo Presidente;

III. Secretariar as reuniões;

IV. Propor o calendário de reuniões;
V. Elaborar e distribuir previamente a pauta das reuniões, com cópias dos respectivos temas a serem tratados;
VI. Redigir, providenciar as devidas assinaturas e divulgar as atas das reuniões;
VII. Organizar e distribuir documentos correlatos à pauta das reuniões;
VIII. Encaminhar minutas de resoluções do CTIC à Procuradoria Federal da UFOP (PGF), quando necessário;
IX. Lavrar as resoluções e atas da reunião e encaminhá-las ao Presidente e demais representantes;
X. Organizar, manter e disponibilizar os documentos correlatos ao CTIC;
XI. Comunicar as ações e melhorias definidas e propostas pelo CTIC a todas as partes interessadas;
XII. Assistir aos membros do CTIC no exercício da sua função.

SEÇÃO III

DO GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 47. O Gestor de Segurança da Informação e Comunicações será indicado pelo Vice-reitor e será designado pelo Reitor.

Art. 48. Compete ao Gestor de Segurança da Informação:
I. Promover a cultura de Segurança da Informação e Comunicações;
II. Monitorar, em conjunto com o Agente Responsável, as operações da equipe de resposta a incidentes de Segurança da Informação e Comunicações;
III. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de Segurança da Informação e Comunicações;
IV. Propor recursos necessários às ações de Segurança da Informação e Comunicações;
V. Propor e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação e Comunicações;
VI. Manter, sistematicamente, contato direto com o Presidente do CTIC e com o diretor da Núcleo de Tecnologia da Informação - NTI para o trato de assuntos relativos à Segurança da Informação e Comunicações;
VII. Propor alterações na PoSIC;
VIII. Propor normas relativas à Segurança da Informação e Comunicações.

SEÇÃO IV

DA EQUIPE DE TRATAMENTO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Art. 49. A UFOP constituirá uma Equipe de Tratamento de Incidentes em Segurança da Informação – CSIRT – e, no seu Documento de Constituição adotará as recomendações do Anexo A da Norma Complementar no 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, ou documento correspondente que venha a substituí-lo.

Parágrafo único. A CSIRT será instituída por portaria normativa expedida pelo Reitor.

SEÇÃO V

DOS GESTORES DE INFORMAÇÃO

Art. 50. São responsabilidades dos gestores da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pela Universidade:

I. Adotar as medidas e procedimentos necessários para garantir a segurança das informações;

II. Definir procedimentos, critérios de acesso e classificar as informações, observados os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes, considerando a Portaria Normativa de que dispões sobre os procedimentos da Lei de Acesso à informação e do Serviço de Informação ao Cidadão – SIC, no âmbito da UFOP;

III. Propor regras específicas ao uso das informações;

IV. Manter o devido registro e controle ao autorizar e fornecer acesso aos ativos de TI sob sua responsabilidade aos usuários.

§ 1o As informações recebidas de pessoa física ou jurídica externa à Universidade serão submetidas, adicionalmente, às medidas de segurança da informação compatíveis com os requisitos pactuados com quem as forneceu.

§ 2o O Reitor, os Pró-Reitores e os Diretores de Unidade poderão indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem a garantir a segurança da

informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes.

SEÇÃO VI

DO CUSTODIANTE DA INFORMAÇÃO

Art. 51. São responsabilidades do custodiante da informação:

I. Garantir a segurança da informação sob sua custódia;

II. Comunicar oportunamente ao CTIC sobre situações que comprometam a segurança das informações sob sua custódia;

III. Comunicar ao CTIC eventuais limitações para cumprimento dos critérios definidos para segurança da informação;

IV. Observar procedimentos, critérios de acesso e classificação das informações definidos pelos Gestores da Informação.

SEÇÃO VII
DOS DIRIGENTES DAS UNIDADES E DEMAIS CHEFIAS

Art. 52. São responsabilidades dos dirigentes e demais chefias das unidades da UFOP no que se refere à segurança da informação:

I. Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

II. Incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

III. Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão;

IV. Avaliar os danos, para sua área, decorrentes de quebra de segurança;

V. Tomar as providências cabíveis quando da comunicação conclusiva do incidente encaminhada pelo CTIC.

SEÇÃO VIII
DOS USUÁRIOS DE ATIVOS DE INFORMAÇÃO

Art. 53. É dever de todos os usuários de ativos de informação:

I. Conhecer e cumprir as diretrizes e normas desta PoSIC;

II. Responsabilizar-se por todo e qualquer acesso aos ativos de informação da UFOP, bem como pelos efeitos desse acesso, realizado por meio de seu código de identificação;

III. Comunicar o mais breve possível os incidentes de segurança da informação, por ele conhecido, ao setor responsável;

IV. Colaborar com as investigações de incidentes, envolvendo direta ou indiretamente sua área.

SEÇÃO IX

DO RELACIONAMENTO COM TERCEIROS

Art. 54. Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para UFOP, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta PoSIC.

CAPÍTULO VII

DAS DISPOSIÇÕES TRANSITÓRIAS, GERAIS E FINAIS

Art. 55. Esta Resolução deverá ser revisada e atualizada a cada dois (2) anos, a contar da sua vigência, ou quando identificada a necessidade pelo CTIC.

Art. 56. Os casos omissos nesta Resolução serão decididos pelo Presidente do CTIC, ouvidos, quando for o caso, os membros do referido comitê.

Art. 57. As diretrizes da PoSIC serão implementadas de forma incremental, conforme projeto de implantação aprovado pelo CTIC.

Art. 58. O projeto de implantação da PoSIC será desenvolvido pela CSIRT em conjunto com o CTIC e o Núcleo de Tecnologia da Informação - NTI da UFOP.

Art. 59. A presente Resolução entra em vigor na data de sua publicação no Boletim Administrativo da Universidade, revogadas as disposições em contrário.

ANEXO I

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

I. Instrução Normativa do Gabinete de Segurança Institucional da presidência da Republica (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;
II. Norma Complementar no 03/IN01/DSIC/GSI/PR, de 30 de Junho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta;
III. Norma Complementar no 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta;
IV. Norma Complementar no 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal, direta ou indireta;
V. Norma Complementar no 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009, que disciplina as Diretrizes para a Gestão de Continuidade de Negócios nos aspectos relacionados à Segurança da Informação e Comunicações (GCN) nos órgãos e entidades da Administração Pública Federal, direta ou indireta;
VI. Norma Complementar no 07/IN01/DSIC/GSI/PR, de 15 de julho de 2014, que disciplina as diretrizes para a implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta ou indireta;
VII. Norma Complementar no 08/IN01/DSIC/GSI/PR, de 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) dos órgãos e entidades da Administração Pública Federal, direta ou indireta;
VIII. Norma Complementar no 21/IN01/DSIC/GSI/PR, de 08 de outubro de 2014, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes em Redes

Computacionais (ETIR) dos órgãos e entidades da Administração Pública Federal, direta ou indireta;
IX. Norma ABNT NBR ISSO/IEC 27001:2006 – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;
X. Norma ABNT NBR ISSO/IEC 27002:2005 – Técnicas de Segurança – Código de Práticas para a Segurança da Informação;
XI. Norma ABNT NBR ISSO/IEC 27005:2008 – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação;
XII. Lei 9.609 de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências.