MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE VIÇOSA
SECRETARIA DE ÓRGÃOS COLEGIADOS

Campus Universitário – Viçosa, MG – 36570-900 – Telefone: (31) 3612-1037 - E-mail: soc@ufv.br

RESOLUÇÃO Nº 16/2019

O **CONSELHO UNIVERSITÁRIO** da Universidade Federal de Viçosa, órgão superior de administração, no uso de suas atribuições legais, considerando decisão em sua 442ª reunião, realizada no dia 22.11.2019, e o que consta no Processo nº 007325/2019, resolve:

aprovar o Regimento Interno da Política de Segurança da Informação da Universidade Federal de Viçosa (POSIC).

Publique-se e cumpra-se.

Viçosa, 11 de dezembro de 2019.

Demetrius David da Silva
Presidente do CONSU

ANEXO DA RESOLUÇÃO Nº 16/2019 – CONSU

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIC) da UFV

CAPÍTULO I
DAS DIRETRIZES GERAIS

Art. 1º A Política de Segurança da Informação e Comunicações da Universidade Federal de Viçosa (UFV) visa estabelecer diretrizes e critérios para o manuseio da informação, de forma eletrônica ou não, observando os requisitos mínimos de confidencialidade, integridade, disponibilidade não-repúdio e autenticidade, além do atendimento à legislação pertinente, e normas definidas pelos órgãos reguladores.

§1º A POSIC é uma declaração formal da instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores no que diz respeito a seus direitos e responsabilidades com os recursos computacionais da instituição e as informações neles armazenados.

§2º As diretrizes estabelecidas nesta política devem estar alinhadas ao Estatuto da UFV, ao Regimento, ao Planejamento Estratégico Institucional, ao Plano Diretor de TI e em consonância com os valores institucionais.

§3º A POSIC se aplica a todas as unidades administrativas, servidores, estudantes, prestadores de serviço autorizados, e usuários de serviços de TIC e dos sistemas de informação mantidos na UFV.

§4ºA POSIC da UFV tem prazo de validade indeterminado, sendo que sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

CAPÍTULO II
DA FINALIDADE

Art. 2º A Política de Segurança da Informação e Comunicações tem por finalidade orientar a UFV no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações, em conformidade com as disposições constitucionais, legais e regimentais vigentes. Seu propósito é estabelecer as diretrizes a serem seguidas pela Instituição na adoção de procedimentos e mecanismos relacionados à segurança da informação.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos da Política de Segurança da Informação e Comunicações da UFV, considera-se:

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 Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

III. ALTA ADMINISTRAÇÃO[1]: pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível.

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

V. ANÁLISE/AVALIAÇÃO DE RISCOS: processo completo de uso sistemático de informações para identificar fontes de risco e estimar riscos e de uso de critérios para determinar sua importância/impacto.

VI. ARTEFATO MALICIOSO: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

VII. ATAQUE: tentativa de se destruir, expor, alterar, desabilitar, roubar, ganhar acesso não autorizado ou ainda realizar uso não autorizado de um ativo.

VIII. ATIVIDADES CRÍTICAS: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.

IX. 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.

X. AUDITORIA[2]: processo sistemático, independente e documentado utilizado para se obter evidências de conformidade ou uma avaliação objetiva que visa determinar em qual grau, ou extensão, os critérios normativos foram atendidos.

XI. AUTENTICAÇÃO: provisão de garantia de que uma característica declarada de uma dada entidade é correta.

XII. AUTENTICIDADE: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

XIII. BLOQUEIO DE ACESSO: processo que tem por finalidade suspender temporariamente o acesso.

---

1 A alta gerência tem o poder de delegar autoridade e fornecer recursos dentro da organização.
Se o escopo do sistema de gerenciamento abrange apenas parte de uma organização, a administração superior se refere àqueles que dirigem e controlam essa parte da organização.

2 Uma auditoria pode ser tanto interna (primeira parte) ou externa (de segunda parte ou terceira parte), podendo ainda ser uma auditoria combinada (agregando duas ou mais disciplinas).

XIV. CLAREZA: As regras que se fundam nesta POSIC devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão.

XV. CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

XVI. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da Administração Pública Federal (APF).

XVII. COMUNIDADE OU PÚBLICO ALVO: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

XVIII. COMPROMETIMENTO: perda de segurança resultante do acesso não autorizado.

XIX. CONEXÃO À INTERNET: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP.

XX. CONFIABILIDADE: propriedade de prover resultados esperados e consistentes.

XXI. CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

XXII. CONFORMIDADE: atendimento (ou preenchimento) de um requisito.

XXIII. CONTAS DE SERVIÇO: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso.

XXIV. 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.

XXV. CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

XXVI. CREDENCIAIS OU CONTAS DE ACESSO: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

XXVII. DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

XXVIII. DISPOSITIVOS MÓVEIS: equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento.

XXIX. EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

XXX. EVENTO DE SEGURANÇA DA INFORMAÇÃO: ocorrência identificada de um sistema, serviço ou estado da rede indicando uma possível brecha na política de segurança da informação ou falha dos controles, ou ainda, uma situação previamente desconhecida que pode ser relevante para a segurança da informação.

XXXI. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: conjunto de processos que permite 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.

XXXII. GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.

XXXIII. GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: é responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da Administração Pública Federal (APF).

XXXIV. INCIDENTE DE SEGURANÇA: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

XXXV. INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

XXXVI. INFORMAÇÃO CLASSIFICADA: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada.

XXXVII. INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

XXXVIII. INTEGRIDADE: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

XXXIX. LEGALIDADE: As ações de segurança da informação e comunicações levarão em consideração as leis, as políticas, as normas e os procedimentos organizacionais, administrativos, técnicos e operacionais da UFV, formalmente estabelecidos.

XL. NÃO-REPUDIAÇÃO: habilidade de se provar a ocorrência de um evento requisitado (ou ação) e as entidades que o originaram.

XLI. PLANO DE CONTINUIDADE DE NEGÓCIOS: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração

Pública Federal (APF) mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.

XLII. 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.

XLIII. POLÍTICA: intenções e direção de uma organização formalmente expressa pela alta administração.

XLIV. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: 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.

XLV. PUBLICIDADE: Transparência no trato da informação, observados os critérios legais.

XLVI. QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

XLVII. REDUÇÃO DE RISCO: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.

XLVIII. RESPONSABILIDADE: Toda comunidade de usuários da UFV é responsável pelo cumprimento das normas de segurança da informação e comunicações.

XLIX. RISCO 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.

L. SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade das informações.

LI. SISTEMA DE INFORMAÇÃO: aplicações, serviços, ativos de tecnologia da informação, ou outros componentes de gerenciamento de informações.

LII. TERCEIRIZAÇÃO[3] (Outsourcing): arranjo no qual uma organização externa desempenha parte da função ou processo de uma organização.

LIII. TERMO DE RESPONSABILIDADE: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade, o não-repúdio e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

---

[3] Uma organização externa está fora do escopo do sistema de gerenciamento, embora a função ou processo terceirizado esteja dentro do escopo.

LIV. TRATAMENTO DA INFORMAÇÃO: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

LV. TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS: é o 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.

LVI. USUÁRIO: servidores, discentes, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Federal (APF), formalizada por meio da assinatura do Termo de Responsabilidade.

LVII. VULNERABILIDADE: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO IV
DOS PRINCÍPIOS E DIRETRIZES

Art. 4º As ações relacionadas à POSIC da UFV são norteadas pelos seguintes princípios:

I. Autenticidade
II. Confidencialidade
III. Clareza
IV. Disponibilidade
V. Integridade
VI. Legalidade
VII. Não-repudiação
VIII. Publicidade
IX. Responsabilidade

Art. 5º A Política de Segurança da Informação e Comunicações e suas normas complementares são regidas pelas seguintes diretrizes, que devem orientar a definição de normas e procedimentos específicos relacionados à segurança da informação e comunicação no âmbito da UFV:

I. Garantir a segurança das informações institucionais transportadas na rede acadêmica da UFV, inclusive no uso de dispositivos móveis.

II. Assegurar que todos os usuários estejam conscientes e cumpram as suas responsabilidades pela segurança da informação na UFV.

III. Identificar os ativos de informação da UFV e as responsabilidades apropriadas definidas para a proteção deles.

IV. Assegurar que a informação receba um nível adequado de proteção, de acordo com a legislação vigente.

V. Limitar o acesso (lógico e físico) à informação e aos recursos de processamento da informação da UFV, assegurando-se o acesso apenas às pessoas devidamente autorizadas.

VI. Garantir a operação segura e correta dos recursos de processamento da informação da UFV, visando, principalmente, a proteção contra perda de dados.

VII. Assegurar que os ativos de informação estejam protegidos contra códigos maliciosos.

VIII. Registrar eventos e gerar evidências nas operações envolvendo ativos de informação dentro da UFV.

IX. Garantir a integridade e atualizar periodicamente os sistemas computacionais utilizados dentro da rede acadêmica da UFV.

X. Garantir que a segurança da informação esteja projetada e implementada durante todas as fases do ciclo de vida dos sistemas de informação desenvolvidos dentro da UFV.

XI. Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

XII. Assegurar um enfoque consistente e efetivo para se gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

XIII. Assegurar a disponibilidade dos ativos de informação críticos através da implementação de mecanismos de redundância e de uma política de continuidade de negócios.

XIV. Evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação, e de quaisquer requisitos de segurança da informação, dentro da UFV.

CAPÍTULO VI
DAS PENALIDADES

Art. 6º Ações que violem a POSIC ou quaisquer de suas diretrizes e normas ou que quebrem os controles de segurança da informação serão apuradas por meio de sindicância e/ou processo disciplinar.

§1º Aos responsáveis pela violação desta POSIC serão aplicadas as sanções e penalidades previstas na legislação em vigor.

§2º Eventuais ações corretivas para mitigação de riscos à segurança da informação estarão enunciadas em normas específicas, decorrentes das diretrizes gerais de segurança da informação enumeradas nesta POSIC.

CAPÍTULO VII
COMPETÊNCIAS E RESPONSABILIDADES

Art. 7º A estrutura para a Gestão da Segurança da Informação e Comunicações na UFV é composta por:

I. Comitê de Segurança da Informação e Comunicações da UFV;
II. Gestor de Segurança da Informação da UFV;
III. Equipe de Tratamento e Resposta a Incidentes em Rede de Computadores da UFV (ETIR-UFV);
IV. Usuários das Soluções de Tecnologia da Informação.

Seção I
Do Comitê de Segurança da Informação e Comunicações da UFV (CSIC-UFV)

Art. 8º O Comitê de Segurança da Informação e Comunicações da UFV (CSIC-UFV) tem o objetivo de assessorar na implementação das ações de segurança, de constituir grupos de trabalho para tratar de temas e propor soluções específicas, e de aprovar normas e procedimentos internos de segurança da informação e comunicações em conformidade com diretrizes da presente POSIC e as legislações existentes sobre o tema.

Art. 9º Compete ao CSIC-UFV:
I. propor, avaliar e revisar, regularmente, a Política de Segurança da Informação e Comunicação e seus planos de ação;
II. propor, avaliar, revisar e aprovar normas complementares alinhadas à Política de Segurança da Informação e Comunicação em conformidade com as diretrizes da presente POSIC e as legislações vigentes;
III. apoiar as instâncias competentes nas ações de segurança da informação e comunicação; elaborar em conjunto com as instâncias competentes proposta anual de alocação de recursos orçamentários necessários às ações de segurança da informação e comunicação; e
IV. realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicação e propor programas destinados à conscientização e à capacitação de recursos humanos em segurança da informação e comunicação.

Parágrafo único. A composição e o funcionamento do Comitê de Segurança da Informação e Comunicações da UFV (CSIC-UFV) deverá ser regulamentado por regimento próprio.

Seção II
Do Gestor de Segurança da Informação da UFV (GSIC-UFV)

Art. 10 O Diretor de Tecnologia da Informação atua como Gestor de Segurança da Informação e Comunicações da UFV (GSIC-UFV)

Art. 11 O Gestor de Segurança da Informação e Comunicações da UFV tem as seguintes competências:

I. Promover a cultura de segurança da informação e comunicações;

II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor recursos necessários às ações de segurança da informação e comunicações; Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

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

V. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) para o trato de assuntos relativos à segurança da informação e comunicações; e

VI. Propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito da UFV.

Seção III
Da Equipe de Tratamento e Resposta a Incidentes em Rede de Computadores da UFV (ETIR-UFV)

Art. 12 A ETIR-UFV terá como missão coordenar as atividades de tratamento e resposta a incidentes, tais como recuperação de sistemas, análise de ataques e intrusões, análise e tratamento de interrupção do funcionamento de aplicações e serviços suportados por tecnologias de informação e comunicação (TIC).

Art. 13 A ETIR-UFV será nomeada por ato específico e regulamentada por normas da CSIC-UFV.

Seção IV
Dos Usuários das Soluções de Tecnologia da Informação

Art. 14 Compete aos usuários das das soluções de tecnologia da informação oferecidas pela UFV: conhecer e cumprir os princípios, diretrizes e responsabilidades desta Política de Segurança da Informação e Comunicação, bem como suas demais normas e resoluções complementares; zelar pela segurança da informação e comunicação; comunicar os incidentes de segurança, por eles conhecidos e propor melhorias à segurança da informação e comunicação no âmbito da UFV.

CAPÍTULO VIII
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 15 A POSIC da UFV está em consonância, entre outros, com os seguintes atos normativos:

I. Lei n° 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

II. Lei n° 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação – LAI;

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

IV. Lei nº 13.709, de 14 de agosto de 2018, que Lei Geral de Proteção de Dados Pessoais (LGPD).

V. Decreto n° 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

VI. Decreto n° 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores – Internet;

VII. Decreto n° 8.135 de 4 de novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

VIII. Portaria Interministerial n° 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores – internet e dá outras providências;

IX. Norma Complementar n° 02/IN01/DSIC/GSI/PR, de 5 de fevereiro de 2013, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

X. Norma Complementar n° 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;

XI. Norma Complementar n° 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 e Comunicações (GRSIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

XII. Norma Complementar n° 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 e indireta;

XIII. Norma Complementar n° 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009, que disciplina as Diretrizes para Gestão de Continuidade de Negócios nos aspectos

relacionados à Segurança da Informação e Comunicações (GCN) nos órgãos e entidades da Administração Pública Federal, direta e indireta;

XIV. Norma Complementar n° 07/IN01/DSIC/GSI/PR, de 15 de julho de 2014, que estabelece 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; e dá outras providências;

XV. Norma Complementar n° 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 de Segurança em Redes Computacionais dos órgãos e entidades da Administração Pública Federal, direta e indireta;

XVI. Norma ABNT NBR ISO/IEC 27001:2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

XVII. Norma ABNT NBR ISO/IEC 27002:2013, que institui o código de melhores práticas para Gestão de Segurança da Informação e Comunicação;

XVIII. Norma ABNT NBR ISO/IEC 27005:2011, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação;

XIX. Instrução Normativa GSI/PR N° 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;

XX. Plano de Desenvolvimento Institucional da UFV 2012-2017 (PDI/UFV);

XXI. Plano Diretor de Tecnologia da Informação da UFV 2016-2019 (PDTI/UFV).

CAPÍTULO IX
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 16 A POSIC será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 17 As propostas de alteração ou criação de normas internas sobre Segurança da Informação e Comunicações deverão ser encaminhadas ao CSIC-UFV.

Art. 18 Após sua publicação, o CSIC-UFV deverá dar ampla divulgação da POSIC a todos os agentes públicos.

Art. 19 Os casos omissos e as dúvidas surgidas na aplicação desta Resolução serão dirimidos pelo CSIC-UFV.

Art. 20 A Política de Segurança da Informação e Comunicações da Universidade Federal de Viçosa entrará em vigor na data de sua publicação.