CAMPUS OFICIAL
Atos administrativos publicados no informativo eletrônico UFV em Rede da Univerdidade Federal de Viçosa

PORTARIA NORMATIVA Nº 0005/2020/RTR

PORTARIA NORMATIVA Nº 0005/2020/RTR, de 31 de julho de 2020 - A Vice-Reitora da Universidade Federal de Viçosa, no uso de suas atribuições, conferidas pela Portaria nº 0641/2019, de 07/06/2019, publicada no Diário Oficial da União de 10/06/2019, considerando o que consta do Processo SEI 23114.905674/2020-72, resolve:

CAPÍTULO I

PREÂMBULO

Art. 1º Fica normatizado o controle de acesso (lógico e físico) aos ativos de informação da Universidade Federal de Viçosa (UFV), visando preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações.

Art. 2º As diretrizes estabelecidas nesta Portaria Normativa devem ser aplicadas a toda a UFV, em todos os seus *campi* e unidades.

Art. 3º Para os fins desta Portaria Normativa, adotam-se as seguintes definições:

I - ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II - ADMINISTRADOR DE REDE - pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade;

III - ADMINISTRADOR DE SISTEMA - pessoa física que administra um ou mais sistemas computacionais; IV - APF - Administração Pública Federal;

V - ATIVIDADE CRÍTICA - 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;

VI - ATIVO - qualquer coisa que tenha valor para a organização;

VII - ATIVOS DE INFORMAÇÃO - os meios de processamento, armazenamento e transmissão da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e também os recursos humanos que a eles têm acesso;

VIII - AUDITORIA - processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

IX - AUTENTICAÇÃO - processo que busca verificar a identidade digital de uma entidade de um sistema no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já predefinidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

X - AUTENTICAÇÃO DE MULTIFATORES (MFA) - utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema;

XI - AUTENTICIDADE - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

XII - AUTORIZAÇÃO - processo que ocorre após a autenticação e tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado;

XIII - AVALIAÇÃO DE RISCOS - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

XIV - BACKUP ou CÓPIA DE SEGURANÇA - conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

XV - BLOQUEIO DE ACESSO - processo que tem por finalidade suspender temporariamente o acesso;

XVI - CONFIDENCIALIDADE - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade, não autorizados nem credenciados;

XVII - CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - cumprimento das legislações, normas e procedimentos relacionados à SI da organização;

XVIII - CONSCIENTIZAÇÃO - atividade que tem por finalidade orientar sobre o que é SI, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade;

XIX - CONTA DE SERVIÇO - conta de acesso à rede corporativa de computadores necessária a um procedimento automático (aplicação, script, etc) sem qualquer intervenção humana no seu uso;

XX - CONTÊINER DOS ATIVOS DE INFORMAÇÃO - local onde é armazenado o ativo de informação;

XXI - 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;

XXII - CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XXIII - CONTROLE DE ACESSO LÓGICO - conjunto de procedimentos associados a mecanismos de tecnologia da informação (hardware e software) que visam controlar os processos de identificação, autenticação e autorização de usuários a ativos de informação;

XXIV - CONTROLE DE ACESSO FÍSICO - conjunto de procedimentos e tecnologias que buscam proteger ambientes, equipamentos ou informações cujo acesso deve ser restringido. Pode envolver o uso de chaves, trancas, vigilantes, crachás, cercas, biometria, etc;

XXV - CONTROLES DE SEGURANÇA - medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros;

XXVI - CONSU - Conselho Universitário da UFV;

XXVII - CREDENCIAL (OU CONTA DE ACESSO) - permissão, concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá) ou lógica (como a identificação de usuário e senha);

XXVIII - CREDENCIAMENTO - processo pelo qual o usuário recebe credenciais de segurança que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

XXIX - CRIPTOGRAFIA - técnica de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno);

XXX - CSIC-UFV - Comitê de Segurança da Informação e Comunicações da UFV;

XXXI - DIREITO DE ACESSO - privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

XXXII - DISPONIBILIDADE - propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado

sistema, órgão ou entidade devidamente autorizados;

XXXIII - DOCUMENTOS CLASSIFICADOS - documentos que contenham informação classificada em qualquer grau de sigilo;

XXXIV - DTI - Diretoria de Tecnologia da Informação da UFV;

XXXV - ENDEREÇO IP (Internet Protocol) - endereço utilizado na rede internet para identificar unicamente um dispositivo a ela conectado;

XXXVI - EXCLUSÃO DE ACESSO - processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e de perfil de acesso;

XXXVII - GESTÃO DE RISCOS - processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

XXXVIII - GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO - aplicação sistemática de políticas, procedimentos e práticas de gestão às atividades de comunicar, consultar, estabelecer o contexto, identificar, analisar, avaliar, tratar, monitorar e revisar os riscos de segurança da informação;

XXXIX - IDENTIFICAÇÃO - durante a identificação o usuário diz ao sistema quem ele é (normalmente através de um nome de usuário ou endereço de e-mail);

XL - IDENTIFICAÇÃO DE RISCOS - processo de localizar, listar e caracterizar elementos de risco;

XLI - IDENTIFICADOR DE USUÁRIO (ID DE USUÁRIO) - identificador que permite determinar, inequivocamente, a identidade de um determinado usuário, associando-o com suas responsabilidades e ações;

XLII - INFORMAÇÃO - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XLIII - 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, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

XLIV - INFORMAÇÃO SIGILOSA - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo;

XLV - INFRAESTRUTURA CRÍTICA DA UFV - instalações, serviços, bens e sistemas, virtuais ou físicos, que, se forem incapacitados, destruídos ou tiverem desempenho

extremamente degradado, são capazes de provocar sérios impactos sobre as atividades institucionais da UFV;

XLVI - INFRAESTRUTURA CRÍTICA DE INFORMAÇÃO DA UFV - sistemas de tecnologia da informação e comunicação que suportam ativos e serviços chaves da infraestrutura acadêmica da UFV;

XLVII - INTEGRIDADE - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XLVIII - IP (Internet Procotol) - protocolo de roteamento utilizado na internet;

XLIX - LOG OU REGISTRO DE AUDITORIA - registro de eventos relevantes em um dispositivo ou sistema computacional;

L - NECESSIDADE DE CONHECER - condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

LI - NECESSIDADE DE USO - o usuário somente deve ter permissão para acessar os recursos de processamento da informação (equipamentos de TI, aplicações, procedimentos, salas) de que necessita para desempenhar a sua tarefa/função/papel;

LII - NORMA ABNT NBR 14565 - norma que estabelece os requisitos para um sistema de cabeamento estruturado para uso nas dependências de um único edifício ou de um conjunto de edifícios comerciais em um campus;

LIII - PERÍMETRO DE SEGURANÇA FÍSICA - delimitador, ou barreira física, que tem como objetivo controlar, restringir, ou mesmo impedir, o acesso a determinado ativo da UFV;

LIV - PRINCÍPIO DO MENOR PRIVILÉGIO - estratégia de segurança da informação baseada na concessão de autorizações de acesso lógico aos ativos de informação apenas quando realmente sejam necessárias ao desempenho de uma atividade específica;

LV - PROGRAMAS UTILITÁRIOS DE SISTEMA - são aplicações com credencial para acessar recursos do sistema operacional;

LVI - QUEBRA DE SEGURANÇA - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

LVII - RISCO (conceito geral) - possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade;

LVIII - RISCO (de SI) - 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;

LIX - SI - Segurança da Informação;

LX - SIC - Segurança da Informação e Comunicações;

LXI - SISTEMA BIOMÉTRICO - conjunto de ferramentas que se utiliza das características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca;

LXII - SISTEMA DE ACESSO - conjunto de ferramentas que se destina a controlar e a dar permissão de acesso a uma pessoa a um recurso;

LXIII - SSH (Secure Shell) - protocolo de rede que permite acesso remoto e seguro a um servidor;

LXIV - TERMO DE RESPONSABILIDADE - termo assinado pelo usuário concordando em contribuir com a disponibilidade, integridade, confidencialidade e autenticidade das informações a que tiver acesso, bem como em assumir responsabilidades decorrentes de tal acesso;

LXV - TI - Tecnologia da Informação;

LXVI - TIC - Tecnologia da Informação e Comunicações;

LXVII - TRATAMENTO DA INFORMAÇÃO - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

LXVIII - TRATAMENTO DA INFORMAÇÃO CLASSIFICADA - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo;

LXIX - TRILHA DE AUDITORIA - registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento;

LXX - UFVNet - rede acadêmica e administrativa da UFV, constituída pela infraestrutura de rede de dados e telefonia da Instituição;

LXXI - USUÁRIO - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade;

LXXII - USUÁRIO (OU PERFIL) ADMINISTRADOR GENÉRICO - conta institucional de acesso privilegiado a serviços, sistemas e ativos da UFV não associada a um usuário em específico;

LXXIII - VPN (Virtual Private Network) - Rede Privada Virtual.

CAPÍTULO II

DISPOSIÇÕES PRELIMINARES

Art. 4º A identificação, autorização, autenticação, o interesse do serviço, a necessidade de uso e a necessidade de conhecer são condicionantes prévios para a concessão de acesso (físico e lógico) aos ativos de informação da UFV.

Art. 5º A identificação dos controles de acesso lógico e físico aos ativos de informação da UFV relacionados à segurança da informação e comunicações (SIC) deverá ser decorrência do processo de gestão de riscos de segurança da informação e comunicações da Instituição.

§1º Os ativos de informação deverão ser classificados em níveis de criticidade, considerando-se o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base, além do processo de gestão de riscos em segurança da informação, o processo de gestão de continuidade de negócios em segurança da informação.

§2º A implementação dos controles de acesso identificados através do processo de gestão de riscos de segurança da informação e comunicações da UFV estará condicionada à prévia aprovação do CSIC-UFV.

§3º Além de normas e procedimentos relativos ao controle de acesso (lógico e físico) aos ativos de informação, para a implementação dos controles de segurança aprovados, a UFV, através do CSIC-UFV, deverá elaborar e divulgar, quando pertinente, programas periódicos de sensibilização e conscientização, em conformidade com a Política de Segurança da Informação e Comunicações da UFV (POSIC-UFV).

Art. 6º A UFV estabelecerá, através do CSIC-UFV, regras específicas para o credenciamento de usuários aos ativos de informação em áreas e infraestruturas consideradas críticas, em conformidade com a legislação vigente.

CAPÍTULO III

REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 7º Esta Portaria Normativa baseia-se nas seguintes referências legais e normativas:

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

II - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política de

Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III - Norma Complementar nº 07/IN01/DSIC/GSIPR, que estabelece as diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;

IV - Portaria nº 93, de 26 de setembro de 2019, que institui o glossário de segurança da informação;

V - Plano de Desenvolvimento Institucional da UFV 2018-2023 (PDI/UFV);

VI - Plano Diretor de Tecnologia da Informação da UFV 2020-2023 (PDTI/UFV);

VII - Política de Segurança da Informação da UFV (POSIC/UFV).

CAPÍTULO IV

CONTROLE DE ACESSO LÓGICO

Art. 8º Quanto à Criação e Administração de Contas Institucionais de Acesso Lógico:

§1º A criação de contas institucionais de acesso lógico aos ATIVOS DE INFORMAÇÃO UFV requererá procedimentos prévios de credenciamento para qualquer usuário;

§2º Deverá ser disponibilizado ao usuário, que não exerça funções de administração, somente uma única conta institucional de acesso lógico aos ATIVOS DE INFORMAÇÃO DA UFV, que seja pessoal e intransferível, com identificador de usuário (ID de usuário) único, de modo a permitir relacionar o usuário com suas responsabilidades e ações;

§3º A concessão de senhas aos usuários, para acesso aos ATIVOS DE INFORMAÇÃO DA UFV, deverá ser controlada por meio de um processo de gerenciamento formal, capaz de permitir a análise crítica dos direitos de acesso em intervalos regulares, além do estabelecimento de regras para credenciamento, bloqueio e exclusão de contas institucionais de acesso lógico, inclusive para ambientes de desenvolvimento de software;

I- O usuário que incorrer na quebra de segurança da informação, ocorrida com a utilização de sua respectiva senha de acesso lógico, será devidamente responsabilizado de acordo com o Termo de Responsabilidade (Acesso aos Ativos de Informação da UFV). (Em Anexo)

§4º A utilização de contas institucionais de acesso lógico com perfil de administrador de sistema, para execução de tarefas específicas na administração de ATIVOS DE INFORMAÇÃO DA UFV, somente será concedida a usuários previamente cadastrados e expressamente autorizados;

I - Quando for inevitável a necessidade de utilização de perfis de administrador de sistema genéricos, procedimentos específicos deverão ser estabelecidos a fim de se inibir sua utilização indevida (inclusive em relação à manutenção da confidencialidade das senhas de acesso lógico compartilhadas);

II - Programas utilitários de sistema capazes de sobrepor os controles dos sistemas e aplicações, quando imprescindíveis, devem ter sua utilização controlada e restrita a um número mínimo de usuários confiáveis e autorizados.

§5º A criação de contas institucionais de acesso lógico, para utilização em serviços vinculados a um processo automatizado (conta de serviço), exigirá regras específicas;

§6º Sempre que possível, deverá ser implementada autenticação de multifatores para a concessão de acesso lógico aos ATIVOS DE INFORMAÇÃO DA UFV;

Art. 9º Quanto ao Acesso Lógico à UFVNet, Sistemas e Ativos de Informação da UFV:

§1º As credenciais de acesso lógico aos ATIVOS DE INFORMAÇÃO DA UFV somente serão concedidas após a data de contratação, entrada em exercício do servidor, ou efetivação de matrícula do aluno;

I - Os usuários apenas receberão permissão de acesso às redes, serviços e ativos de informação associados, dos quais tenham sido expressamente autorizados a utilizar;

§2º As credenciais de acesso lógico aos ATIVOS DE INFORMAÇÃO DA UFV deverão ser restringidas, removidas, ou suspensas, quando do desligamento do usuário;

I - Caso o servidor, funcionário, fornecedor ou terceiro, que esteja se desvinculando da UFV, tenha conhecimento de senhas de contas institucionais de acesso lógico que permanecem ativas, estas deverão ser alteradas, após encerramento das atividades e/ou contrato.

§3º Deverão ser mantidos, para fins de auditoria na UFVNet, sistemas e ativos de informação associados, mecanismos que permitam registrar, identificar e rastrear endereços IPs, logs de acesso remoto, bem como de acesso a serviços utilizados, por um período mínimo de cinco (5) anos;

§4º Deverão ser utilizados mecanismos automáticos que inibam a conexão não autorizada de equipamentos externos à UFVNet, seus sistemas e ativos associados;

§5º Para a concessão de acesso lógico às informações sigilosas contidas nos sistemas e ativos associados à UFVNet, bem como para acesso remoto através de canal seguro (ex: VPN, SSH), deverão ser observadas as normas e diretrizes específicas;

§6º As regras de acesso lógico à Internet e à rede sem fio institucional da UFV estarão detalhadas na Norma de Uso dos Serviços da UFVNet;

§7º A UFVNet, seus serviços e ativos associados, deverão conter ferramentas de proteção contra acesso lógico não autorizado, que favoreçam, preferencialmente, a administração de forma centralizada;

I - Os projetos, aquisições e instalações de cabeamentos, equipamentos e demais dispositivos de rede de dados e telefonia, que venham necessitar acesso à UFVNet, devem ser previamente comunicados à DTI, a fim de verificar a compatibilidade e conformidade com esta norma, com a norma ABNT NBR 14565 vigente, e com os

equipamentos homologados pela DTI;

II - É vedada a instalação de cabeamentos, equipamentos, e demais dispositivos não homologados e não autorizados pela DTI, para fins de acesso à UFVNet.

§8º Para se configurar credenciais ou contas de acesso lógico dos usuários aos ATIVOS DE INFORMAÇÃO DA UFV, deverá ser respeitado o princípio do menor privilégio, concedendo-se autorização de acesso apenas quando realmente for necessário ao desempenho de alguma atividade específica;

§9º Os ATIVOS DE INFORMAÇÃO DA UFV considerados críticos ou relevantes, ou que contenham informações sigilosas, deverão possuir registros de eventos (LOGs) para fins de segurança e rastreamento de acesso lógico previamente definidos;

I - Deverá haver mecanismos capazes de garantir a integridade desses registros de auditoria.

§10. O uso de ATIVO DE INFORMAÇÃO UFV que não guarde relação com o exercício do cargo, função, atividades acadêmicas ou administrativas, será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil;

§11. As regras relacionadas ao uso do Correio Eletrônico estarão detalhadas na Norma de uso do Correio Eletrônico da UFV.

CAPÍTULO V

CONTROLE DE ACESSO FÍSICO

Art. 10. Quanto ao Controle de Acesso Físico aos ativos de informação, a UFV, em suas diversas instâncias organizacionais, deverá:

§1º Estabelecer regras para o uso de credenciais de acesso físico, as quais se destinam ao controle de acesso dos usuários às áreas e instalações sob responsabilidade da UFV;

§2º Definir e orientar a instalação de sistemas de detecção física de intrusos nas áreas e instalações sob sua responsabilidade;

§3º Orientar a utilização de barreiras físicas de segurança, bem como a instalação de equipamentos ou mecanismos de controle de entrada e saída;

I - Os ativos de informação deverão estar protegidos contra ações de vandalismo, sabotagem, ataques, etc, especialmente em relação àqueles ativos considerados críticos;

II - As áreas e instalações com ativos de informação deverão ser classificadas de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando-se aquelas áreas consideradas críticas;

a. Os ativos de informação classificados como sigilosos exigirão procedimentos especiais de controles de acesso físico, em conformidade com a legislação vigente;

b. Os controles para as áreas e instalações consideradas críticas deverão ser intensificados, em conformidade com a legislação vigente;

c. A UFV deverá definir perímetros de segurança física, suas dimensões, equipamentos, e tipos especiais de controles de acesso físico aos ativos de informação;

c.1. Deverão ser ilustrados em documentação própria, e permitido que sejam identificados, os perímetros de segurança física de cada ativo de informação por todos os que transitarem ou tiverem acesso a tais espaços, em especial às áreas e instalações consideradas críticas;

c.1.1. Todas as mídias contendo cópias de segurança (backups) de ativos da informação da UFV deverão, sempre que possível, estar armazenadas em perímetros de segurança.

c.2. O armazenamento e/ou veiculação de imagens, de vídeo e de áudio, registrados em perímetros de segurança física serão regulamentados por norma específica.

IV. Nas respectivas unidades e departamentos, deverão ser implementadas áreas de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 11. Para fins de conscientização dos usuários em relação à importância das regras de acesso aos ativos de informação, a UFV deverá:

I - Difundir e exigir o cumprimento desta Portaria Normativa, da Política de Segurança da Informação e Comunicações da UFV (POSIC-UFV), das demais normas e procedimentos de segurança decorrentes da política e da legislação vigente sobre o tema;

II - Conscientizar os usuários, a fim de que adotem comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações;

III - Identificar e avaliar sistematicamente os riscos à segurança da informação e comunicações dos ativos de informação e quais controles devem ser aplicados quanto aos acessos dos usuários;

IV - Definir regras específicas para autorização de acesso e credenciamento dos usuários em conformidade com a Política de Segurança da Informação e Comunicações da UFV (POSIC-UFV) e a política de classificação dos ativos de informação.

Art. 12. Os casos omissos serão dirimidos pelo Comitê de Segurança da Informação e

Comunicações da UFV (CSIC-UFV).

Art. 13. Esta Portaria Normativa entrará em vigor na data de publicação no Campus Oficial.

Publique-se e cumpra-se. (a) Rejane Nascentes – Reitora em Exercício.

ANEXO

TERMO DE RESPONSABILIDADE - ACESSO AOS ATIVOS DE INFORMAÇÃO DA UFV

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ da Universidade Federal de Viçosa (UFV), DECLARO, sob pena das sanções cabíveis nos termos da legislação vigente, que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio da UFV;

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da UFV;

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV) utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da UFV;

V) responder, perante a UFV, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Local, UF, _____de _____de _____

_____

Assinatura (Nome do usuário e seu setor organizacional)

CAMPUS OFICIAL

BOLETIM DE INFORMAÇÃO INTERNA DA UNIVERSIDADE FEDERAL DE VIÇOSA

Editado pela Diretoria de Comunicação Institucional (DCI). Edifício Fábio Ribeiro Gomes – Campus Universitário – CEP: 36.570-000 – Viçosa – Minas Gerais • Telefone: (31) 3612-1095 • comunicar@ufv.br

Reitor: Demetrius David da Silva • Vice-Reitora: Rejane Nascentes • Diretor de Comunicação Institucional: Ricardo Duarte Gomes da Silva • Elaboração: Dayse Amâncio