UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG
CONSELHO UNIVERSITÁRIO
RESOLUÇÃO Nº 8, DE 26 DE MARÇO DE 2018

Aprova a Política de Segurança da Informação e Comunicação da UNIFAL-MG e dá outras providências

O Conselho Universitário da UNIFAL-MG, no uso de suas atribuições estatutárias e regimentais, tendo em vista o que consta do Processo nº 23087.001894/2016-13 e o que ficou decidido em sua 208ª reunião, realizada em 26-03-2018, resolve **aprovar** a Política de Segurança da Informação e Comunicação da Universidade Federal de Alfenas – UNIFAL-MG, nos seguintes termos:

CAPÍTULO I
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 1º Fica estabelecida a Política de Segurança da Informação e Comunicação (PSIC) da Universidade Federal de Alfenas (UNIFAL-MG), que contém as diretrizes de segurança da informação e comunicação a serem observadas no âmbito da Universidade.

Parágrafo Único. As diretrizes estabelecidas na PSIC dizem respeito à segurança dos recursos de Tecnologia da Informação e Comunicação (TIC) e das informações geradas e/ou gerenciadas pela UNIFAL-MG, independente da sua forma de armazenamento.

Art. 2º A PSIC alinha-se às estratégias da Universidade e tem por objetivo garantir a autenticidade, confidencialidade, disponibilidade e integridade das informações produzidas ou custodiadas pela instituição.

Art. 3º Integram a PSIC as normas gerais e específicas de utilização, procedimentos e resoluções.

Art. 4º Para fins dessa Política, entende-se por:

I - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto independente da sua forma de armazenamento;

II - comunicação: transferência de informação, independente do meio pela qual seja veiculada;

III - segurança da Informação e comunicação: proteção da informação, da comunicação e dos ativos institucionais contra quaisquer tipos de ameaças, visando garantir a continuidade das atividades, a minimização dos riscos e a maximização da eficiência e da efetividade das ações;

IV - ameaça: Possibilidade de qualquer evento que explore vulnerabilidades, causando potenciais incidentes indesejados, que possam resultar em danos para a Universidade;

V - vulnerabilidade: qualquer fraqueza que possa ser explorada e comprometer a segurança da informação e comunicação.

VI - risco: combinação da probabilidade (chance da ameaça se concretizar) de um evento ocorrer e de suas consequências para a Universidade.

VII - incidente de segurança da informação: evento adverso que tenha a probabilidade de comprometer as operações da Universidade ou ameaçar a segurança da informação;

VIII - análise de riscos: identificação de possíveis riscos, potenciais danos causados e planos de contingência.

IX - gerenciamento de riscos: processo que visa a proteção dos serviços por meio da aceitação, redução, eliminação ou transferência de riscos, conforme seja técnica, econômica e estrategicamente viável.

X - Plano de Continuidade de Negócio: conjunto de normas que têm como objetivo estabelecer procedimentos capazes de manter em funcionamento os serviços e processos críticos relacionados na eventualidade de ocorrência de incidentes de qualquer natureza.

XI - ativo: tudo que tenha valor para a Universidade e para as atividades institucionais, como informações, softwares, hardwares, pessoas, processos e serviços.

XII - gestor da informação: reitor em exercício e ocupantes de funções de direção, comando ou chefia do Grupo - Direção e Assessoramento Superiores - DAS, nível DAS 101.5 ou superior, e seus equivalentes que, no exercício de suas competências, produz, utiliza e/ou obtém informações, sendo responsável por sua gestão, observada a legislação vigente;

XIII - custodiante: entidade ou pessoa detentora da posse, mesmo que transitória, de informação produzida e/ou recebida pela Universidade;

XIV - rótulo: identificação física ou eletrônica da classificação de confidencialidade atribuída à informação.

XV - documento de domínio público: documento ou obra (artística, invenção, desenho industrial, etc.) que pode ser livremente reproduzido, apresentado ou explorado sem necessidade de autorização ou de pagamento de direitos autorais, por esgotamento do prazo previsto em lei ou por outro motivo que tenha feito expirar a propriedade intelectual.

XVI - documento de natureza pública: documento relativo ou pertencente à coletividade, de uso comum a todos, universalmente conhecido ou sem restrição de acesso a qualquer pessoa;

XVII - usuário: toda e qualquer pessoa ou entidade que faça uso da informação gerada e/ou gerenciada pela UNIFAL-MG, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em órgão ou entidades da administração pública direta ou indireta do Governo Federal, discentes de qualquer nível ou modalidades de curso, incluindo, ainda, visitantes, voluntários e público externo;

XVIII - integridade da informação - tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental; e

XIX - confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do seu conteúdo; e

XX - disponibilidade da informação garante que usuários autorizados acessem a informação sempre que necessário.

CAPÍTULO II
OBJETIVOS E ESCOPO

Art. 5º A PSIC tem os seguintes objetivos:

I - definir o escopo da segurança da informação da UNIFAL-MG;

II - orientar as ações de segurança, para reduzir riscos e garantir a integridade, autenticidade, confidencialidade e disponibilidade dos ativos da UNIFAL-MG;

III - permitir a adoção de soluções de segurança integradas; e

IV - servir de referência para auditoria, apuração e avaliação de responsabilidades.

Art. 6º A Política de Segurança da Informação da UNIFAL-MG abrange os seguintes requisitos de segurança:

I - criptográficos;

II - na gestão, manuseio e tratamento da informação;

III - na comunicação da informação;

IV - de rede;

V - de operações de sistemas da informação;

VI - contratual e acordo de níveis de serviço;

VII - de recursos humanos;

VIII - de gestão de software;

IX - de aquisição e gestão de ativos de TI; e

X - de serviços de TI.

Parágrafo único: A responsabilidade sobre os ativos de TI e os requisitos de segurança dos itens supracitados serão regulamentados por meio de normas específicas.

CAPÍTULO III
CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 7º Para fins de segurança da informação, os usuários que tenham acesso, de forma autorizada, às informações produzidas ou custodiadas pela Universidade classificam-se em:

I - usuário interno: qualquer servidor em atividade na Universidade;

II - usuário colaborador: prestador de serviço terceirizado, estagiário, bolsista ou qualquer outro colaborador da Universidade;

III - usuário discente: qualquer pessoa física que tenha vínculo em algum curso oferecido pela Universidade; e

IV - usuário externo: qualquer pessoa física ou jurídica que não seja caracterizada como usuário interno, colaborador ou discente.

Art. 8º O acesso dos usuários às informações produzidas ou custodiadas no âmbito da Universidade, que não sejam de natureza pública, deve ser limitado às atribuições necessárias ao desempenho das suas respectivas atividades.

§ 1º Qualquer outra forma de uso que extrapole as atribuições necessárias ao desempenho das atividades dos usuários internos, usuários externos, discentes ou colaboradores necessitará de prévia autorização formal, pelo gestor da informação.

§ 2º O acesso, quando autorizado, dos usuários discentes, usuários internos, colaboradores ou externos a informações produzidas ou custodiadas pela Universidade que não sejam de natureza pública é condicionado ao aceite de termo de sigilo e responsabilidade a ser definido pelo gestor da informação.

Art. 9º Quanto à confidencialidade, as informações produzidas ou custodiadas pela Universidade classificam-se nos seguintes graus:

I - públicas: informações que podem ser divulgadas a qualquer pessoa;

II - restritas: informações que, por sua natureza ou por interesse da Universidade, só podem ser divulgadas a um grupo restrito de pessoas;

III - secretas: informações que, em razão de lei, interesse público ou para a preservação de direitos individuais, devam ser de conhecimento reservado; e

IV - pessoais: informações relativas à intimidade privada, vida privada, honra e imagem das pessoas.

§ 1º Para a classificação da informação em determinado grau de sigilo deverá ser utilizado o critério menos restritivo possível.

§ 2º Ao conjunto de informações que não possa sofrer fracionamento para fins de acesso deverá ser atribuído o grau de confidencialidade da sua parte cuja classificação seja a mais restritiva.

§ 3º Toda informação não pública deve ter seu grau de confidencialidade identificado por meio de rótulos padronizados ou classificação padrão de acordo com sua categoria, ressalvados os limites de fracionamento indicados no parágrafo anterior.

§ 4º Toda informação não pública terá os prazos de restrição de acesso definidos de acordo com a legislação vigente.

Art. 10. Cabe ao gestor da informação classificá-la quanto à confidencialidade no momento em que a informação for produzida ou obtida.

§ 1º No ato da classificação da informação, o gestor deve considerar a legislação em vigor, em especial a que regula o acesso à informação, os controles administrativos e tecnológicos necessários ao tratamento da confidencialidade da informação, as necessidades de compartilhamento ou restrição de acesso e os custos de proteção.

§ 2º O gestor da informação, ao classificá-la como não pública, deve indicar, necessariamente, o grupo de pessoas, unidades ou entes da Universidade com permissão para acessá-la.

§ 3º As informações produzidas no âmbito da Universidade podem ser reclassificadas pelo gestor da informação ou pela autoridade competente, por iniciativa própria ou por solicitação de qualquer usuário, cabendo comunicação imediata da alteração aos custodiantes da informação para correta rotulação.

Art. 11. É vedado o tratamento não público às informações contidas em documentos que, por força de lei, sejam de natureza pública ou de domínio público.

Art. 12. São responsabilidades do gestor da informação, no que concerne às informações sob sua gestão, produzidas ou custodiadas pela Universidade:

I - classificar as informações, observada esta política, os dispositivos legais e regimentais relativos ao sigilo e a outros requisitos de classificação pertinentes;

II - propor regras, procedimentos e critérios específicos ao acesso, uso e ao trânsito das informações sob sua gestão; e

III - adotar as medidas e procedimentos adequados para garantir a segurança das informações.

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

§ 2º As informações a serem fornecidas a pessoa física ou jurídica externa à Universidade serão submetidas, adicionalmente, a medidas de segurança da informação compatíveis com os requisitos pactuados com quem as receberá.

§ 3º Nos processos e documentos de sua competência, o Gestor da informação pode indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação.

Art. 13. São responsabilidades do custodiante da informação:

I - garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação;

II - comunicar tempestivamente ao gestor sobre situações que comprometam a segurança das informações sob custódia; e

III - comunicar eventuais limitações para cumprimento dos critérios definidos pelo gestor para segurança da informação, para que este decida quanto à cessão ou não da informação.

CAPÍTULO IV
GERENCIAMENTO DE RISCOS, INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE

Art. 14. O processo de gerenciamento de riscos da informação, não armazenada em meio digital, será instituído e revisto periodicamente pelo gestor da informação correspondente.

Art. 15. O processo de gerenciamento de riscos de ativos de TI institucionais será instituído e revisto periodicamente pela Gerência de Segurança da Informação do NTI.

Parágrafo único. Todos os ativos de TI da UNIFAL-MG deverão ser inventariados pelas áreas competentes do NTI e classificados em relação à segurança da informação pela Gerência de Segurança da Informação do NTI.

Art. 16. A Gerência de Segurança da Informação apresentará planos de gerenciamento e ação de resposta a incidentes de TI a serem avaliados e aprovados pelo Comitê Gestor de Tecnologia da Informação (CGTI).

Art. 17. O Plano de Continuidade de Negócio, no que diz respeito a ativos de TI da UNIFAL-MG, será elaborado pelo NTI com base na análise de riscos para aprovação pelo CGTI conforme definido na ABNT NBR 15999.

CAPÍTULO V
DEVERES E RESPONSABILIDADES

Art. 18. A PSIC deve ser observada e respeitada por todos que possuírem interação com os ativos institucionais.

Art. 19. É dever de todo usuário da UNIFAL-MG:

I - preservar a integridade e guardar sigilo das informações classificadas de que fazem uso, bem como zelar e proteger os ativos institucionais;

II - cumprir a PSIC sob pena das sanções disciplinares e legais cabíveis;

III - utilizar os sistemas de informação da UNIFAL-MG e os recursos a eles relacionados apenas para os fins previstos por essa universidade;

IV - respeitar a legislação de propriedade intelectual vigente, quando da instalação, utilização, inspeção, cópia, armazenamento ou fornecimento de ativos da instituição ou de terceiros, incluindo, enfaticamente, programas de computador / software;

V - responder por todo acesso realizado aos ativos de TI da UNIFAL-MG por meio de sua credencial de acesso (usuário / senha);

VI - reportar qualquer incidente de segurança da informação à Gerência de Segurança da Informação do NTI;

VII - respeitar restrições de acesso definidas de acordo com a natureza da informação.

Art. 20. É dever de todo ocupante de cargo de chefia na UNIFAL-MG:

I - adotar medidas administrativas cabíveis em caso de violação das regras estabelecidas de acordo com as normas e procedimentos de segurança da informação;

II - atualizar-se, periodicamente quanto às políticas, normas e procedimentos de segurança da informação vigentes na UNIFAL-MG; e

III - manter o devido registro e controle ao autorizar e fornecer acesso aos ativos sob sua responsabilidade a servidores, discentes ou terceiros.

Art. 21. Compete ao Núcleo de Tecnologia da Informação (NTI), através da Gerência de Segurança da Informação, no contexto de ativos de TI:

I - coordenar e acompanhar e implementação da PSIC e das normas complementares;

II - monitorar, auditar e avaliar periodicamente as práticas de segurança da informação adotadas pela Universidade;

III - constituir e coordenar a Equipe de Tratamento a Incidentes de Segurança da Informação;

IV - responder as diligências relativas à segurança da informação, promovidas por meio de auditoria interna ou externa, bem como demais questionamentos dos órgãos competentes; e

V - coordenar a divulgação e conscientização dessa política à comunidade;

CAPÍTULO VI
SANÇÕES E PENALIDADES

Art. 22. Em caso de descumprimento dos termos estabelecidos pela PSIC, serão aplicadas, isolada ou cumulativamente, sanções administrativas, civis e penais, assegurados

aos envolvidos o contraditório e a ampla defesa, nos termos da legislação aplicável, especialmente o Regimento Geral da Universidade Federal de Alfenas, o Código de Ética do Servidor Público Civil do Poder Executivo Federal (Decreto nº 1.117/2004) e o Regime Jurídico dos Servidores Públicos Civis da União (Lei nº 8.112/1990).

CAPÍTULO VII
COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO (CGTI)

Art. 23. Ficam atribuídas ao CGTI, enquanto órgão normativo, consultivo e deliberativo na área de tecnologia da informação da Universidade as seguintes responsabilidades:

I - assessorar na implementação das ações de segurança da informação e comunicação da UNIFAL-MG;

II - constituir grupos de trabalho presidido por um membro do CGTI com participação obrigatória do Gerente de Segurança da Informação, ou de um representante por ele indicado, para tratar de todo e qualquer tema e/ou proposição de soluções relacionadas à segurança da informação e comunicação para posterior deliberação;

III - deliberar sobre assuntos relacionados à segurança da informação; e

IV - atualizar esta política sempre que necessário, objetivando atender a requisitos técnicos, legais e institucionais;

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 24. Essa política deverá ser amplamente divulgada e comunicada, a fim de que todos tenham ciência da mesma para usufruírem dos benefícios e assumirem as responsabilidades inerentes à segurança da informação.

Art. 25. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pela Universidade devem observar os dispositivos integrantes desta política.

Art. 26. Os casos omissos nessa Resolução serão resolvidos pelo CGTI.

Art. 27 Esta Resolução entra em vigor na data de sua publicação no Quadro de Avisos da Secretaria Geral.

Prof. Sandro Amadeu Cerveira
Presidente do Conselho Universitário

DATA DA PUBLICAÇÃO
UNIFAL-MG
02-04-2018