PORTARIA Nº 265, DE 06 DE JUNHO DE 2024

Institui a nova Política de Segurança da Informação – PSI, do Crea-MG, define o fluxo do pedido de informações dentro do Conselho e dá outras providências.

O PRESIDENTE DO CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DE MINAS GERAIS - CREA-MG, no uso de suas atribuições legais e regimentais, e,

Considerando o disposto nas alíneas 'k' e 'm', do artigo 34, da Lei Federal nº 5.194, de 24 de dezembro de 1966, com suas alterações;

Considerando o disposto nos incisos V, XXVII e XLV, do artigo 96 do Regimento Interno do Crea-MG, homologado *ad referendum* pelo Plenário do Confea, através da Portaria AD nº 009, de 27 de janeiro de 2009;

Considerando a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018), que trata sobre a proteção de dados pessoais;

Considerando a Nota Técnica GTLGPD nº 1/2019, de 19 de novembro de 2019, do Confea, que orienta os Conselhos Regionais de Engenharia e Agronomia quanto a adequação à LGPD;

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Instituir a nova Política de Segurança da Informação – PSI, do Crea-MG.

Art. 2º A Política de Segurança da Informação do Conselho Regional de Engenharia e Agronomia de Minas Gerais (PSI – Crea-MG) é o documento que orienta e estabelece as diretrizes do Conselho para a proteção dos ativos de informação e, neste âmbito, regras de responsabilidade legal a colaboradores e prestadores de serviço.

Art. 3º A PSI – Crea-MG deve ser cumprida e aplicada em todos os setores da autarquia.

Art. 4º A presente PSI está baseada nas recomendações da ABNT NBR ISO/IEC 27.000:2018, reconhecida, mundialmente, como norma para gerir e conscientizar sobre a segurança da informação, com o objetivo de obter maior controle de ativos e informações sensíveis, bem como a conformidade de práticas com a lei e outras normas aplicáveis.

Art. 5º Para os fins desta Política, considera-se:

I - dado: o menor nível de abstração da informação, sendo o fato em sua forma primária. Os dados geram informação.

II - informação: reunião ou o conjunto de dados e conhecimentos organizados, que possam constituir referências sobre determinado acontecimento, fato ou fenômeno.

III - colaborador: toda e qualquer pessoa física contratada pelo Crea-MG, seja pelo regime da Consolidação das Leis do Trabalho (CLT), ou por meio de contrato de estágio, ou por contrato de menor aprendiz, bem como aqueles eleitos para exercerem funções de inspetor ou conselheiro em nome do Crea-MG.

IV - prestador de serviço: toda e qualquer pessoa, física ou jurídica, contratada e que exerça alguma atividade para o Crea-MG, dentro ou fora da autarquia;

V - usuário: colaborador ou prestador de serviço que tenha acesso autenticado

aos sistemas disponibilizados pelo Crea-MG para desempenhar determinada função, trabalho ou atividade;

VI - gestor: pessoa responsável por planejar e dirigir o trabalho de um grupo de colaborador, estagiários ou prestadores de serviço;

VII - proprietário da informação: pessoa ou organismo que tenha responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança de ativos, por exemplo, informações contidas em documentos eletrônicos e/ou físicos, sistemas de informação, bases de dados e/ou mídias de armazenamento.

VIII - custodiante da informação: aquele que tem a posse, temporária ou definitiva, da informação corporativa.

IX - acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

X - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

XI - incidente de segurança: indício de fraude, sabotagem, desvio, falha, ou perda ou evento indesejável/inesperado que tenha probabilidade de comprometer dados, informações, bem como sistemas de informação ou redes de computadores.

XII - tratamento: toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

CAPÍTULO II
DOS OBJETIVOS

Art. 6º A PSI - Crea-MG tem como objetivos:

I - estabelecer diretrizes e princípios gerais para implementar, manter e melhorar a gestão de segurança da informação no Crea-MG;

II - nortear a implementação de controles e processos para o cumprimento desta Política;

III - preservar as informações do Crea-MG quanto à:

a) integridade: garantir que a informação seja mantida no seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

b) confidencialidade: garantir que o acesso à informação ocorra somente por pessoas autorizadas;

c) disponibilidade: garantir que os colaboradores e prestadores de serviço autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 7º São princípios da Política de Segurança da Informação do Crea-MG (PSI – Crea-MG):

I - visão abrangente e sistêmica da segurança da informação;

II - treinamento e disseminação do conhecimento como alicerce fundamental para o fomento da cultura em segurança da informação;

III - orientação à gestão de riscos e à gestão da segurança da informação;

IV - prevenção e tratamento de incidentes de segurança da informação;

V - articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação.

CAPÍTULO IV
DA APLICABILILIDADE DA PSI – CREA-MG

Art. 8º Esta PSI é obrigatória a todos os colaboradores, independentemente do nível hierárquico ou da função exercida no Conselho, bem como, salvo disposição expressa em contrário, pelos prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Art. 9º A responsabilidade quanto à segurança da informação deve ser comunicada na fase de contratação ou posse dos colaboradores, bem como nos contratos de prestação de serviços.

§1º Todos os colaboradores e prestadores de serviços devem ser orientados pelo respectivo gestor sobre os procedimentos e normas relacionados à Segurança da Informação, bem como sobre o uso correto dos ativos a fim de reduzir possíveis riscos.

§2º Todos os colaboradores e prestadores de serviços devem, também, assinar o Termo de Responsabilidade sobre a utilização da rede interna (intranet), internet, computadores e *e-mail* corporativo do Crea-MG.

§3º Todos os colaboradores e prestadores de serviços devem conhecer a Política de Privacidade de Dados do Crea-MG, a qual está disponível no site do Conselho.

Art. 10. A partir desta PSI, cada colaborador e prestador de serviço compreendem que os ambientes, sistemas, computadores, *e-mails* corporativos, internet e redes do Crea-MG poderão ser monitorados e, quando pertinente e necessário, os dados serão gravados e registrados conforme previsto nas leis brasileiras.

CAPÍTULO V
DAS OBRIGAÇÕES GERAIS

Art. 11. São obrigações gerais de todos os colaboradores, prestadores de serviço e usuários de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do Crea-MG:

I - promover a segurança dos respectivos dados e credenciais de acesso, assumindo responsabilidades como custodiante de informações;

II - seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao manuseio de documentos físicos e ao uso dos recursos computacionais e informacionais do Conselho;

III - utilizar, de forma ética, legal e consciente, os recursos computacionais e informacionais do Crea-MG;

IV - manter-se atualizado quanto a esta PSI e aos procedimentos e normas a ela relacionados, buscando orientações do seu gestor ou da Divisão de Tecnologia da Informação do Crea-MG, neste caso quando se tratar de procedimento de Tecnologia da Informação, ou da Divisão de Gestão da Informação, quando se tratar de procedimento envolvendo documentos físicos e/ou eletrônicos, sempre quando não estiver absolutamente seguro nos processos de aquisição, uso e/ou descarte de informações, sempre quando não estiver absolutamente seguro nos processos de aquisição, uso e/ou descarte de informações.

Art. 12. Todo incidente que afete a segurança da informação deverá ser comunicado inicial e imediatamente ao respectivo gestor e ao Encarregado pelo Tratamento de Dados Pessoais (DPO) do Crea-MG.

Parágrafo único: o Encarregado pelo Tratamento de Dados Pessoais (DPO) do Crea-MG deverá comunicar o incidente ao Presidente do Conselho e à CRI, assim como tomar as demais medidas previstas no Plano de Resposta a Incidentes com Dados.

Art. 13. É proibido o uso de computadores, equipamentos eletrônicos e demais recursos tecnológicos do Crea-MG para:

I - tentar ou obter acesso não autorizado a outro computador, servidor ou rede, para, inclusive, acessar informações confidenciais sem explícita autorização do proprietário;

II - burlar quaisquer sistemas de segurança;

III - vigiar secretamente outrem, por dispositivos eletrônicos ou *softwares*, como, por exemplo, analisadores de pacotes (*sniffers*);

IV - interromper serviços, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

V - praticar ou ser cúmplice de atos de violência moral, assédio sexual, perturbação, manipulação ou violação de direitos autorais ou de propriedades intelectuais sem a devida anuência do titular;

VI - acessar, distribuir ou armazenar material pornográfico, racista ou qualquer outro com conteúdo discriminatório referente a religião, orientação sexual e procedência nacional em clara desrespeito ao ordenamento jurídico pátrio;

VII - violar ou tentar violar a ordem pública;

VIII - utilizar *software* sem licença de uso;

IX - transmitir e/ou instalar vírus ou outro tipo de *malware* de forma proposital.

CAPÍTULO VI
DAS RESPONSABILIDADES ESPECÍFICAS

Seção I
Do gestor

Art. 14. Cabe a cada gestor, inclusive relativamente aos colaboradores e prestadores de serviço sob a sua gestão:

I - ter postura exemplar no que tange à segurança da informação, servindo como parâmetro e modelo de conduta;

II - conhecer, assinar, bem como fazer conhecer e assinar o Termo de Responsabilidade sobre a utilização da rede interna (intranet), internet, computadores e *e-mail* corporativo do Crea-MG, de tal forma a assumir o dever de observância às normas nele estabelecidas, bem como comprometer-se a manter sigilo e confidencialidade sobre todos os ativos de informações do Crea-MG;

III - preliminarmente à concessão de acesso às informações do Conselho, dar conhecimento à esta PSI aos colaboradores e prestadores de serviço;

IV - adaptar ou, quando não for competente, requerer a adaptação de normas, procedimentos e sistemas para atender à PSI – Crea-MG.

Seção II
Do Departamento de Planejamento, Gestão e Tecnologia do Crea-MG

Art. 15. O Departamento de Planejamento, Gestão e Tecnologia do Crea-MG, através da Divisão de Tecnologia da Informação e da Divisão de Gestão da Informação, como custodiantes de informações, têm os seguintes deveres específicos:

I - testar a eficácia dos controles utilizados e informar os gestores sobre riscos residuais eventualmente existentes;

II - implementar e testar, no mínimo anualmente, plano de contingência e continuidade dos principais sistemas e serviços, para reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação;

III - registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas;

IV - acessar, enquanto administradora e operadora dos sistemas computacionais, arquivos e dados de outros usuários apenas quando necessário à execução de atividades operacionais sob sua responsabilidade, tais como manutenção de computadores, realização de cópias de segurança, auditoria e testes nos ambientes;

V - administrar, proteger e testar cópias de segurança dos programas e dados relacionados a processos críticos e relevantes para o Crea-MG que estejam armazenados no *Data Center* do Conselho;

VI - Fiscalizar e exigir a administração, a proteção e os testes de cópias de segurança dos programas e dados relacionados a processos críticos e relevantes para o Crea-MG que estejam armazenados em *Data Centers* de terceiros;

VII - atribuir cada conta ou dispositivo de acesso (a computadores, sistemas, bases de dados e qualquer outro ativo de informação) a determinado responsável identificável como pessoa física, sendo que:

a) as permissões dadas aos usuários (*logins*) individuais de colaboradores são definidas pelo seu gestor. Tais pemissões são aplicadas pela Divisão de Tecnologia da Informação em conjunto com a Divisão de Recursos Humanos, a quem compete o controle da matriz de acesso.

b) as permissões dadas aos usuários (*logins*) de prestadores de serviço são de responsabilidade do gestor da área contratante. Tais pemissões são aplicadas pela Divisão de Tecnologia da Informação em conjunto com a Divisão de Recursos Humanos, a quem compete o controle da matriz de acesso.

VIII - proteger continuamente todos os ativos de informação do Conselho contra códigos maliciosos, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de códigos maliciosos e/ou indesejados;

IX - diligenciar para que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção do Conselho;

X - definir regras formais para instalação de *software* e *hardware* em ambiente de produção corporativo, exigindo o seu cumprimento dentro do Conselho;

XI - garantir, conforme instrução de serviços específica da Divisão de Recursos Humanos, o bloqueio do acesso de colaborador ou de prestador de serviço, quando houver rescisão do contrato ou alteração de suas funções, e de Conselheiros quando houver o encerramento do mandato eletivo. Tal bloqueio deverá ocorrer mediante solicitação do Gestor responsável ou por requisição direta da Divisão de Recursos Humanos;

XII - monitorar o ambiente de TI, gerando indicadores e históricos de:

a) uso da capacidade instalada da rede e dos equipamentos;

b) incidentes de segurança (vírus, *trojans*, furtos, acessos indevidos);

c) atividade de todos os colaboradores e prestadores de serviço durante os acessos às redes externas, inclusive internet (por exemplo: *sites* visitados, *e-mails* recebidos/enviados, *upload /download* de arquivos, entre outros).

Art. 16. No âmbito da segurança da informação, a Divisão de Gestão da Informação, a Divisão de Tecnologia da Informação e o Encarregado pelo Tratamento de Dados Pessoais (DPO) devem, em conjunto:

I - propor metodologias e processos específicos para a segurança da informação,

como avaliação de risco e sistema de classificação da informação;

II - propor e apoiar iniciativas que visem à segurança dos ativos de informação do Crea-MG;

III - publicar, divulgar e promover a PSI – Crea-MG e demais normas de segurança da informação;

IV - promover a conscientização dos colaboradores e prestadores de serviço quanto a relevância da segurança da informação para o Crea-MG, mediante campanhas, palestras, treinamentos e outras formas de *endomarketing*;

V - apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

VI - analisar, criticamente, incidentes de segurança da informação, em conjunto com o Comitê de Resposta a Incidentes – CRI, do Crea-MG.

CAPÍTULO VII
DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 17. Para garantir as regras mencionadas nesta PSI, o Crea-MG poderá:

I - utilizar sistemas de monitoramento nas estações de trabalho*, notebooks* corporativos, tablets corporativos, equipamentos de servidores, correio eletrônico, conexões com a internet, dispositivos móveis como *pendrives* e HDs externos ou *wireless*, e outros componentes da rede. A informação gerada por tais sistemas poderá, ainda, ser usada para identificar usuários e respectivos acessos efetuados, bem como o material manipulado;

II - compartilhar quaisquer informações obtidas pelos sistemas de monitoramento e auditoria, nas hipóteses de exigência judicial, solicitação de gerentes (ou superiores hierárquicos) ou por determinação da Divisão de Recursos Humanos do Crea-MG;

III - realizar, a qualquer tempo, inspeções físicas nos equipamentos do Crea-MG; instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CAPÍTULO VIII
DA PRIVACIDADE DA INFORMAÇÃO

Art. 18. Toda informação produzida ou recebida por colaboradores e prestadores de serviço, como resultado da atividade exercida em nome ou para o Crea-MG, pertence ao referido Conselho.

Art. 19. Considera-se necessária a proteção da privacidade das informações pertencentes aos respectivos titulares e que são manipuladas ou armazenadas nos meios sobre os quais o Crea-MG detém controle administrativo.

Art. 20. As diretivas abaixo refletem os valores institucionais do Crea-MG e reafirmam o compromisso da autarquia com a melhoria contínua dos processos:

I - as informações são acessadas apenas por pessoas autorizadas e capacitadas para o uso adequado;

II - as informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, exigindo-se de tais organizações o cumprimento das políticas e das diretivas de segurança e privacidade de dados do Conselho, devendo tal prestação de serviço ser auditada, a qualquer tempo, pelo Conselho, para verificar o cumprimento das exigências;

III - as informações e os dados constantes dos cadastros do Crea-MG, bem como outras solicitações que venham a garantir direitos legais, somente serão compartilhadas aos próprios interessados ou a terceiros para cumprimento de decisões judiciais e obrigações legais;

IV - os dados pessoais são coletados, de forma ética e legal, para propósitos específicos e devidamente informados, ao teor da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

CAPÍTULO IX
MESA LIMPA

Art. 21. Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);

Art. 22. Informações restritas ou confidenciais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente fica vazio;

Art. 23. Documentos, quando impressos, devem ser retirados da impressora imediatamente;

Art. 24. Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;

Art. 25. Documentos contendo informação restrita ou confidencial não devem ser deixados na mesa;

Art. 26. Informações restritas ou confidenciais devem ser mantidas em local apropriado;

Art. 27. Todos os documentos e meios eletrônicos no final do dia de trabalho devem ser devidamente guardados/organizados, com proteção adequada;

Art. 28. Documentos contendo informações pessoais devem ser mantidos trancados.

CAPÍTULO X
DO TRATAMENTO DAS INFORMAÇÕES

Art. 29. Todos os colaboradores e prestadores de serviço devem observar exigências e requisitos para tratar informações, haja vista o tipo de conteúdo considerado.

§1º As exigências previstas no *caput* serão definidas pelo proprietário ou responsável pela informação, seguindo orientações disponíveis nesta PSI.

§2º Os proprietários podem atribuir controles adicionais para maior restrição de acesso ou para ampliar a proteção de informações confidenciais ou restritas.

§3º Todos os colaboradores e prestadores de serviço devem ser signatários do termo de confidencialidade e do termo de responsabilidade de uso da informação que trata do acesso às informações, devendo ser arquivado em sua pasta funcional.

Art. 30. O atendimento aos pedidos de informação deverá seguir o fluxo estruturado no Anexo I desta PSI, denominado "PIN-001/Pedido de Informações".

Art. 31. A divulgação e o compartilhamento de informações confidenciais ou restritas, tais como processos de infração ao código de ética, processos de sindicância e processos administrativos disciplinares, é estritamente proibida, salvo quando previamente autorizada pelo proprietário da informação.

Art. 32. O transporte físico das informações confidenciais e/ou restritas requer a observação ao disposto em normas correlatas.

Art. 33. Quando as informações não forem mais necessárias e quando exigências legais ou regulatórias para a retenção não mais se aplicarem, deverão ser eliminadas de acordo com as normas previstas neste Capítulo, respeitando-se a legislação vigente e a regulamentação do CONARQ, mediante avaliação e autorização da Comissão Permanente de Avaliação de Documentos - CPAD.

Art. 34. É proibida a eliminação de documentos contendo dados pessoais e/ou informações sigilosas em latas de lixo ou em depósitos de papel encaminhados para reciclagem sem a devida descaracterização/anonimização das informações.

Parágrafo único. Os documentos mencionados no *caput* devem, quando não houver disposição contrária ou norma específica, ser destruídos com picotador/fragmentador, sempre observando o disposto no Art. 36.

Art. 35. A informação confidencial e/ou restrita armazenada em fitas magnéticas ou outras mídias de armazenamento digital deve ser eliminada via reformatação ou exclusão dos dados, caso o suprimento seja reutilizado no Conselho.

Parágrafo único. A depender da avaliação do gestor, o suprimento informático poderá ser definitivamente destruído para proteger as informações confidenciais ou restritas nele existentes.

CAPÍTULO XI
DOS DISPOSITIVOS, DOS EQUIPAMENTOS E DOS RECURSOS ELETRÔNICOS, DE COMUNICAÇÃO E DE INFORMÁTICA

Art. 36. Os dispositivos, os equipamentos e os recursos eletrônicos, de comunicação e de informática disponibilizados pelo Crea-MG a colaboradores e, se for o caso a prestadores de serviços, são de propriedade do Conselho.

§1º Os usuários devem utilizar e manusear corretamente os itens mencionados no *caput* para a realização de atividades profissionais em nome ou para o Crea-MG.

§2º O uso pessoal dos itens mencionados no *caput* é permitido desde que não prejudique o desempenho dos sistemas e serviços do Crea-MG, devendo sempre observar as orientações desta política para garantir a segurança das informações do Crea-MG que estejam sob sua responsabilidade.

Art. 37. É proibido todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de dispositivos, equipamentos e recursos eletrônicos, de comunicação e de informática, de propriedade do Crea-MG sem prévio conhecimento e acompanhamento de técnico(s) da Divisão de Tecnologia da Informação do Conselho, ou de quem essa determinar.

Art. 38. Os colaboradores e os prestadores de serviço deverão manter a configuração dos dispositivos, dos equipamentos e dos recursos eletrônicos, de comunicação e de informática, disponibilizados pela Divisão de Tecnologia da Informação do Crea-MG, seguindo os devidos controles de segurança exigidos por esta Política de Segurança da Informação e por normas específicas do Conselho.

Art. 39. Todas as atualizações e correções de segurança – sejam dos sistemas operacionais, sejam dos aplicativos – somente poderão ser realizadas após validadas no respectivo ambiente de homologação, e uma vez disponibilizadas pelo fabricante ou fornecedor.

Art. 40. Os sistemas e dispositivos, equipamentos e recursos eletrônicos, de comunicação e de informática, de propriedade do Crea-MG ou que operem na rede corporativa do Conselho (CORP-Conselho), devem contar com antivírus instalado, ativado e permanentemente atualizado (versões de *software* mais recentes).

Parágrafo único. O usuário, em caso de suspeita de vírus ou problemas de funcionalidade, deverá contatar o setor técnico responsável mediante chamado no sistema de solicitações do Crea-MG.

Art. 41. Arquivos imprescindíveis para as atividades dos colaboradores e, se for o caso, de prestadores de serviço deverão ser salvos em diretórios de rede, definidos e indicados pela Divisão de Tecnologia da informação e pela Divisão de Gestão da Informação, por exemplo, como: grupos novos, *tmp* e público, observando-se as regras de acesso à

informação em conformidade com as definições de segurança definidas pela Divisão de Tecnologia da Informação, pela Divisão de Gestão da Informação e pela área de Proteção de Dados.

Parágrafo único. Os arquivos mencionados no *caput*, se gravados apenas localmente nos dispositivos eletrônicos (por exemplo, no *drive* C: de computadores), não terão garantia de *backup* e poderão ser perdidos caso ocorram falhas no equipamento.

Art. 42. Colaboradores e prestadores de serviço com acesso à internet do Conselho não poderão efetuar *upload* de documentos, informações e/ou de qualquer dado que seja de propriedade ou de responsabilidade do Conselho, sem expressa autorização do gestor responsável.

Art. 43. Colaboradores e prestadores de serviço devem informar, ao setor técnico responsável, a existência de eventual dispositivo desconhecido e suspeito conectado a equipamento eletrônico de propriedade do Crea-MG, tais como: *pendrives*, hds externos, *notebooks*, *desktops, tablets*, celulares, etc.

Art. 44. Todos os *modems/switches/hubs,* internos e externos, não fornecidos pela Divisão de Tecnologia da Informação do Crea-MG devem ser removidos ou desativados para impedir a invasão/evasão de informações e programas.

Parágrafo único. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso dos equipamentos mencionados no *caput* para planos de contingência, mediante a autorização dos gestores das áreas e após aprovação da Divisão de Tecnologia da Informação do Crea-MG.

Art. 45. É expressamente proibido o consumo de alimentos, bebidas e/ou fumo na mesa de trabalho e próximo aos equipamentos e documentos do Conselho.

Art. 46. Os setores que necessitarem de instalar e/ou testar equipamentos de informática e/ou *softwares* deverão solicitar, previamente, apoio técnico à Divisão de Tecnologia da Informação do Crea-MG por meio de chamado interno.

Art. 47. Todos os computadores, *tablets* e impressoras deverão ser protegidos com senha (bloqueados) quando não forem utilizados, sempre que o responsável não estiver próximo aos equipamentos (tela limpa).

Art. 48. Todos os dispositivos, os equipamentos e os recursos eletrônicos, de comunicação e de informática, adquiridos pelo Crea-MG, devem ter, imediatamente, as respectivas senhas padrão (*default*) alteradas pela Divisão de Tecnologia da Informação do Conselho.

Art. 49. É vedada a utilização de computadores, *notebooks*, *tablets* e *smartphones* pessoais de colaboradores e prestadores de serviço na rede interna do Crea-MG, na rede de dados e na rede corporativa *wi-fi* (CORP-Conselho), salvo mediante prévia autorização do Gestor responsável e posterior configuração do equipamento a ser realizada pela Divisão de Tecnologia da Informação.

§1º O uso de computadores, *notebooks, tablets e smartphones* pessoais é permitido no acesso à rede *wi-fi* "PROFISSIONAL-Conselho" ou à rede *wi-fi* "Crea-Eventos", quando houver necessidade.

§2º Demais equipamentos portáteis como *pendrives, HDs* externos e *players* de qualquer espécie, somente terão seu uso e conexão autorizados na rede corporativa para usuários autorizados pelo respectivo gestor imediato, conforme procedimento definido por meio de Instrução de Serviço específica elaborada pela Divisão de Tecnologia da Informação.

§3º Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas ao Crea-MG.

CAPÍTULO XII
DO CORREIO ELETRÔNICO (E-MAIL CORPORATIVO)

Art. 50. O uso do correio eletrônico do Crea-MG é permitido somente para fins corporativos e relacionados às atividades do colaborador e, se for o caso, do prestador de serviço dentro da instituição.

Art. 51. É proibido o uso do correio eletrônico do Crea-MG, pelos usuários, para:

I - fins pessoais;

II - enviar mensagens não solicitadas para múltiplos destinatários, exceto quando relacionadas a legítimo interesse do Conselho;

III - enviar mensagem por correio eletrônico com o nome de usuário de outro colaborador/prestador de serviço ou através de endereço de correio eletrônico que não esteja autorizado a utilizar;

IV - divulgar informações não autorizadas contidas em documentos e/ou imagens de tela *(print screen)* – incluindo de sistemas – e afins sem autorização expressa e formal concedida pelo proprietário do ativo de informação;

V - falsificar informações de endereçamento, adulterar cabeçalhos para ocultar a identidade de remetentes e/ou destinatários, com o objetivo de evitar punições previstas;

VI - deletar mensagens de correio eletrônico quando qualquer uma das unidades do Crea-MG estiver sujeita a investigações e auditorias;

VII - produzir, transmitir ou divulgar mensagem que:

a) contenha documento ou forneça orientação que conflite ou contrarie os interesses do Crea-MG;

b) contenha ameaças eletrônicas, como *spam*, *mail bombing*, vírus de computador;

c) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src,.cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente risco à segurança dos sistemas de dados;

d) objetive obter acesso não autorizado a outro computador, servidor ou rede;

e) objetive interromper serviços, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

f) objetive burlar sistema de segurança;

g) objetive vigiar ou assediar pessoas;

h) objetive acessar informações confidenciais sem explícita autorização do proprietário;

i) objetive acessar, indevidamente, informações que possam causar prejuízos a outrem;

j) inclua imagens criptografadas ou de qualquer forma mascaradas;

k) contenha anexo(s) superior(es) à 15MB para envio interno ou externo e de 15MB para recebimento externo, sendo autorizado o compartilhamento via drive licenciado para o Conselho;

l) contenha conteúdo impróprio, obsceno ou ilegal;

m) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

n) contenha discriminação ou preconceito de raça, cor, etnia, religião ou procedência;

o) contenha fins políticos (propaganda política);

p) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Art. 52. As mensagens de correio eletrônico sempre deverão incluir assinatura com os seguintes dados:

I - nome do colaborador ou do prestador de serviço;

II - cargo e/ou função;

III - Departamento, Divisão ou Seção a que estiver vinculado;

IV - endereço;

V - telefone(s);

VI - correio eletrônico;

VII - aviso de confidencialidade, nos termos definidos pela Divisão de Gestão da Informação.

CAPÍTULO XIII
INTERNET

Art. 53. As regras contidas neste capítulo da Política de Segurança da Informação (PSI – Crea-MG), bem como no Termo de Responsabilidade sobre a utilização da rede interna (intranet), internet, computadores e *e-mail* corporativo do Crea-MG e no Termo de Uso do Serviço de Acesso à internet via rede *wi-fi*, visam boas práticas e comportamentos profissionais éticos no uso da internet.

Art. 54. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a auditorias.

Parágrafo único. O Crea-MG, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos ocorridos através da rede mundial de computadores.

Art. 55. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet, os quais são de propriedade do Conselho, poderão analisar e, se necessário, bloquear qualquer arquivo (armazenado em diretório da rede e/ou disco local), site, correio eletrônico, domínio ou aplicação, com o intuito de assegurar o cumprimento desta Política de Segurança da Informação e da legislação vigente.

Art. 56. Toda alteração ou tentativa de alteração dos parâmetros de segurança da internet, por qualquer colaborador ou prestador de serviço, sem o devido credenciamento e autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

Parágrafo único. Caso a alteração ou tentativa de alteração mencionada no *caput* ocorra para a prática de atividades ilícitas, serão aplicáveis as sanções previstas no Capítulo XVI desta Política sem prejuízo da cooperação do Crea-MG com as autoridades competentes para a repressão de ilícitos criminais e civis.

Art. 57. A internet disponibilizada pela instituição aos colaboradores e prestadores de serviço, poderá ser utilizada para fins pessoais, desde que:

I - não prejudique o andamento dos trabalhos nos setores;

II - não comprometa a banda da rede, principalmente durante o expediente do Conselho;

III - não implique conflitos de interesse com as finalidades institucionais do Conselho.

Art. 58. É proibida a divulgação e/ou o compartilhamento indevido de informações administrativas e gerenciais em listas de discussão, aplicativos de comunicação, sites, comunidades de relacionamento, salas de bate-papo e comunicadores instantâneos, salvo quando estes recursos forem adotados institucionalmente como ferramenta de trabalho a critério do(s) gestor(es).

Art. 59. O acesso a *softwares peer-to-peer* e *storage backup* não é permitido.

Art. 60. O acesso a serviços de armazenamento na nuvem tais como *Google Drive*, *Dropbox* e *One Drive*, somente será liberado ao usuário quando autorizados pelo respectivo gestor imediato, por meio de registro de chamado junto à Divisão de Tecnologia da Informação por meio da GLPI.

Parágrafo único. Serviços de *streaming* (rádios on-line, canais de *broadcast* e afins) são permitidos quando sua utilização for para acessar e/ou divulgar material produzido pelo Sistema CONFEA/Crea ou para fins de treinamento.

Art. 61. Não é permitido acesso a sites e/ou *softwares* de *proxy*, bem como o uso de VPN na rede do Crea-MG, inclusive por meio de dispositivos móveis, para infringir as regras de bloqueio do *firewall*.

CAPÍTULO XIV
DOS SISTEMAS, DRIVERS E DA REDE INTERNA

Art. 62. Os sistemas, *drivers* e a rede interna são de domínio do Conselho, que poderá analisar e, se necessário, bloquear qualquer arquivo ou aplicação neles armazenados, com o intuito de assegurar o cumprimento desta Política de Segurança da Informação e da legislação.

Parágrafo único. O Crea-MG, ao monitorar os sistemas, *drivers* e a rede interna, busca garantir a integridade dos dados, programas e aplicações.

Art. 63. Os sistemas e os servidores são utilizados por colaboradores e, se for o caso, por prestadores de serviço para a realização de atividades em nome ou para o Crea-MG.

Art. 64. Arquivos pessoais e/ou não pertinentes ao Crea-MG (fotos, músicas, vídeos, dentre outros) não deverão ser copiados/movidos para os *drivers* de rede do Conselho, pois sobrecarregam o armazenamento nos servidores.

Parágrafo único. Caso identificada a existência dos arquivos mencionados no *caput*, estes poderão ser permanentemente excluídos sem prévia comunicação ao titular.

Art. 65. Os colaboradores e prestadores de serviço não devem executar nenhum tipo de comando ou programa, os quais possam sobrecarregar a rede corporativa, sem prévia solicitação e autorização da Divisão de Tecnologia da Informação do Conselho.

Art. 66. Toda alteração ou tentativa de alteração dos parâmetros de segurança da rede, por qualquer colaborador ou prestador de serviço, sem o devido credenciamento e autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

Parágrafo único. Caso a alteração ou tentativa de alteração mencionada no *caput* ocorra para a prática de atividades ilícitas, serão aplicáveis as sanções previstas no "Capítulo XVII das violações e sanções administrativas" desta Política, sem prejuízo da cooperação do Crea-MG com as autoridades competentes para a repressão de ilícitos criminais e civis.

Art. 67. Apenas os colaboradores e prestadores de serviço autorizados pelo Crea-MG poderão enviar documentos e/ou imagens de tela *(print screen*) – incluindo de sistemas – a terceiros, com a devida observância a normas internas de privacidade e segurança da informação, bem como à legislação federal referente a uso de imagens, direitos autorais, proteção da imagem e de dados pessoais.

CAPÍTULO XV
DA IDENTIFICAÇÃO DO COLABORADOR E DO PRESTADOR DE SERVIÇO

Art. 68. Os dispositivos de identificação protegem a identidade do colaborador e do prestador de serviço, de forma a prevenir que pessoas não autorizadas desempenhem atividades de funcionários, estagiários, inspetores, conselheiros e/ou contratados do Crea-MG perante o próprio Conselho e/ou perante terceiros (art. 307 do Código Penal – crime de falsa identidade).

Art. 69. Todos os dispositivos de identificação utilizados para o exercício de atividades administrativas no Crea-MG – número de registro; crachá; identificações de acesso a equipamentos eletrônicos, ambiente de rede e sistemas, com login e senha; certificados e assinaturas digitais e dados biométricos – devem encontrar-se associados a determinada pessoa física e atrelados inequivocamente aos documentos oficiais por ela apresentados e reconhecidos pela legislação brasileira.

§1º Caberá à Divisão de Tecnologia da Informação instituir *login* e senha aos colaboradores e, se for o caso, aos prestadores de serviço do Conselho.

§2º Ao realizar o primeiro acesso no equipamento eletrônico, ambiente de rede local ou sistema, o usuário deverá trocar imediatamente a senha padrão conforme as orientações recebidas.

§3º A senha deverá conter caracteres em número e tipologia suficientes à proteção das informações e à garantia do sigilo dos dados;

§4º Cada usuário deverá memorizar a própria senha e/ou armazená-la em local seguro;

§5º Caso o colaborador ou o prestador de serviço não se lembre do *login* e/ou senha, deverá requisitar, formalmente, a troca ou comparecer, pessoalmente, à área técnica responsável para cadastrar uma nova sequência.

§6º Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

§7º Os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

§8º As senhas não devem ser anotadas e não devem ser armazenadas em arquivos eletrônicos (*Word, Excel* etc.) compreensíveis por linguagem humana, isto é, arquivos não criptografados; não devem ser baseadas em informações pessoais, como o próprio nome, nomes de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do setor; e não devem ser constituídas de combinações e sequências óbvias, tais como “abcdefgh”, “87654321”, entre outras.

§9º Os meios de identificação pessoal (crachás, *logins*, identificação biométrica, etc.) não poderão ser utilizados para liberação de acesso a terceiros.

§10º É proibido, em qualquer caso, o compartilhamento de senhas para funções relacionadas à administração de sistemas.

Art. 70. O usuário vinculado aos dispositivos identificadores mencionados no Art. 71 é responsável pelo seu uso correto, perante o Conselho e em nome do Conselho, e deverá dar ciência imediatamente à área responsável em caso de perda, furto, roubo ou violação.

Art. 71. A Divisão de Tecnologia da Informação deverá instituir campanhas e processos regulares para a renovação de senhas dos respectivos colaboradores e prestadores de serviço.

Parágrafo único. Os usuários podem alterar a própria senha a qualquer tempo, mediante requerimento à Divisão responsável pelo dispositivo de identificação, e devem fazê-lo imediatamente caso suspeitem que terceiros obtiveram acesso indevido ao respectivo *login* e senha.

Art. 72. Todos os acessos a equipamentos eletrônicos, ambiente de rede e sistemas, bem como às dependências físicas do Crea-MG devem ser bloqueados:

I - quando houver o término do vínculo do colaborador com o Crea-MG decorrente do encerramento do mandato eletivo de conselheiro ou inspetor, da extinção do contrato de trabalho de funcionário ou da extinção de contrato de estágio;

II - quando houver o término do vínculo do prestador de serviço com o Crea-MG decorrente da extinção do contrato de prestação de serviços.

§1º Para fins de bloqueio de identificações de acesso a equipamentos eletrônicos, ambiente de rede e sistemas, certificados, assinaturas digitais e dados biométricos, o término do vínculo do colaborador ou do prestador de serviço com o Conselho deve ser comunicado imediatamente à Divisão de Tecnologia da Informação do Crea-MG:

a) pela Divisão de Recursos Humanos do Crea-MG, se se tratar de funcionários e estagiários;

b) pela Secretaria de Apoio ao Plenário do Crea-MG, se se tratar de conselheiros;

c) pela Divisão de Gestão de Colégios do Crea-MG, se se tratar de inspetores;

d) pelo respectivo fiscal de contrato, quando se tratar de prestador de serviço.

§2º Para fins de bloqueio de crachá e demais autorizações de acesso às dependências do Crea-MG, o término do vínculo do usuário com o Conselho deve ser comunicado imediatamente à Divisão Administrativa e Financeira do Crea-MG pela:

a) pela Divisão de Recursos Humanos do Crea-MG, se se tratar de funcionários e estagiários;

b) pela Secretaria de Apoio ao Plenário do Crea-MG, se se tratar de conselheiros;

c) pela Divisão de Gestão de Colégios do Crea-MG, se se tratar de inspetores;

d) pelo respectivo fiscal de contrato, quando se tratar de prestador de serviço.

CAPÍTULO XVI
DO SERVIÇO DE BACKUP

Art. 73. Os procedimentos próprios relacionados ao serviço de *backup* (cópia de segurança) estão previstos na Política de *Backup* e Recuperação de Dados Digitais do Crea-MG, consideradas as seguintes diretrizes gerais:

I - o serviço de *backup* deve ser automatizado por sistemas informacionais próprios, com execuções agendadas – fora do horário normal de expediente do Conselho ("janelas de *backup*", isto é, períodos em que há pouco ou nenhum acesso de usuários, bem como reduzidos processos automatizados);

II - a administração das mídias de *backup* deve ser contemplada em normas complementares sobre o serviço, para garantir a segurança e a integridade do processo;

III - a execução de rotinas de *backup* e *restore* deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

CAPÍTULO XVII
DAS VIOLAÇÕES E SANÇÕES ADMINISTRATIVAS

Seção I
Das violações

Art. 74. São consideradas violações a esta Política, a normas ou a procedimentos de segurança da informação, sem prejuízo de atos e omissões outras:

I - inobservância das obrigações constantes no "Capítulo V das obrigações gerais" e no "Capítulo VI das responsabilidades específicas", desta política;

II - quaisquer ações que exponham ou possam expor o Crea-MG ou os titulares dos dados em poder dessa autarquia a perdas e danos, direta ou indiretamente, em claro comprometimento aos ativos de informação;

III - o uso indevido de dados do Conselho e divulgação não autorizada de informações, sem expressa e prévia permissão do gestor;

IV - o uso de dados, informações, equipamentos, *software*, sistemas e outros recursos tecnológicos para propósitos ilícitos, com violação de leis, regulamentos, preceitos éticos e/ou exigências das entidades reguladoras do Crea-MG;

V - a não comunicação ao gestor imediato de quaisquer descumprimentos a esta Política, a normas ou a procedimentos de segurança da informação que, porventura, o colaborador e/ou o prestador de serviços tome conhecimento direta ou indiretamente no exercício da função.

Seção II
Das sanções

Art. 75. O Crea-MG exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, doloso, negligente ou imprudente, dos recursos e serviços concedidos a colaboradores e prestadores de serviço, reservando-se o direito de, quando necessário, adotar todas as medidas legais cabíveis, dentre elas, o direito de regresso e a representação criminal.

Art. 76. As sanções administrativas aplicáveis nas hipóteses de descumprimento da Política de Segurança da Informação do Crea-MG (PSI – Crea-MG) são:

I - advertência;

II - suspensão;

III - rescisão do contrato de trabalho, se se tratar de funcionário;

IV - rescisão do contrato de prestação de serviços, se se tratar de prestador de serviços.

Art. 77. As sanções serão aplicadas preferencialmente de forma gradativa, de acordo com as peculiaridades do caso concreto e em decorrência de sindicância e/ou procedimento administrativo disciplinar, conforme o caso, com direito ao contraditório e à ampla defesa, considerados os seguintes parâmetros:

I - a natureza da infração, a gravidade e a extensão do dano;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a reincidência,

V - a cooperação do infrator com a apuração dos fatos.

VI - A proporcionalidade entre a gravidade da falta, a extensão do dano e o prejuízo causado e a intensidade da penalidade.

Art. 78. O rito processual a ser seguido para Sindicâncias e Procedimentos Administrativos Disciplinares é normatizado por instrução de serviço específica, cuja publicação e atualização é de responsabilidade da Divisão de Recursos Humanos.

Parágrafo único. Quando a infração for cometida por prestador de serviços, aplicar-se-á o estabelecido pela Lei 8.666/93, Estatuto de Licitações, e Lei nº. 14.133, nova lei de licitações.

Art. 79. A imposição das penalidades supracitadas não substitui sanções administrativas, civis e penais definidas em lei especificas.

CAPÍTULO XVIII
DAS DISPOSIÇÕES FINAIS

Art. 80. Esta Política de Segurança da Informação do Crea-MG entra em vigor a partir de sua publicação.

Art. 81. Esta Política não exclui as demais normas de segurança da informação aprovadas pelo Comitê de Segurança da Informação do Crea-MG e demais normas do Conselho referentes a privacidade e proteção de dados pessoais.

Art. 82. O uso inadequado do disposto nesta Portaria fica sujeito à apuração de responsabilidade penal, civil e administrativa, na forma da legislação em vigor.

Art. 83. Esta Portaria entra em vigor na data de sua assinatura.

Art. 84. Revogam-se as disposições em contrário, em especial a Portaria nº 50, de 27 de janeiro de 2022.

Art. 85. Dê-se ciência e cumpra-se.

Belo Horizonte, 06 de junho de 2024.

MARCOS VENICIUS GERVASIO:51986353672

Assinado de forma digital por MARCOS VENICIUS GERVASIO:51986353672
Dados: 2024.06.19 17:10:16 -03'00'

Eng. Civil e de Seg. do Trabalho Marcos Venícius Gervásio
Presidente do Crea-MG

PSI – ANEXO I
Pedido de Informações