Boletim de Serviço Eletrônico em 21/05/2019

Ministério da Justiça e Segurança Pública- MJSP
Conselho Administrativo de Defesa Econômica - CADE
SEPN 515 Conjunto D, Lote 4 Ed. Carlos Taurisano, 1º andar - Bairro Asa Norte, Brasília/DF, CEP 70770-504
Telefone: (61) 3221-8552 - www.cade.gov.br

PORTARIA CADE Nº 408, DE 20 DE MAIO DE 2019.

Regulamenta o uso de computadores no âmbito do Conselho Administrativo de Defesa Econômica – Cade.

O **PRESIDENTE DO CADE**, no uso da atribuição que lhe é conferida pelo disposto no artigo 10, inciso IX, da Lei nº 12.529/2011, no artigo 21, inciso IX, do Decreto nº 9.011/2017, e no artigo 60, inciso IX, do Regimento Interno do Cade, aprovado pela Resolução nº 20, de 7 de junho de 2017,

RESOLVE:

Art. 1º Regulamentar o uso de computadores no âmbito do Conselho Administrativo de Defesa Econômica – Cade, em consonância com o inciso VII do artigo 5º da Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, e com a Portaria Cade nº 403, de 20 de maio de 2019, que institui a Política de Segurança da Informação e Comunicações – Posic.

Seção I

Dos Papéis e Responsabilidades

Art. 2º Compete para os assuntos de segurança da informação:

I - à Coordenação-Geral de Tecnologia da Informação – CGTI:

a) adquirir, instalar, gerenciar os computadores e *notebooks* do Cade;

b) prover os sistemas e recursos necessários para monitorar o uso de computadores e *notebooks* institucionais;

c) avaliar e homologar os *softwares* requeridos pelas unidades administrativas do Cade;

d) prover e instalar *softwares* necessários para a execução das atividades do Cade;

e) elaborar procedimentos e diretrizes para o uso de computadores e *notebooks*;

f) estabelecer procedimentos para manutenção preventiva e corretiva de computadores e *notebooks*; e

g) agir de forma proativa e reativa quando identificados eventos de segurança envolvendo o uso de computadores e *notebooks*.

II - às unidades administrativas do Cade:

a) divulgar os normativos de segurança da informação para todos os seus servidores e colaboradores.

b) a Coordenação-Geral de Gestão de Pessoal - CGESP e a Assessoria de Comunicação – Ascom – devem apoiar o processo de divulgação, avaliação e sensibilização dos assuntos referentes à segurança da informação e comunicação.

c) solicitar computadores e *notebooks* para novos usuários, conforme Norma de contratação, permanência e desligamento de pessoas do Cade.

III - aos chefes ocupantes de cargo ou função igual ou superior a DAS/FCPE 4:

a) divulgar e fomentar as diretrizes do uso de computadores entre seus servidores, colaboradores e estagiários; e

IV - aos servidores, colaboradores e estagiários do Cade:

a) zelar pelo bom funcionamento dos computadores e *notebooks*;

b) comunicar à CGTI sobre eventos e incidentes envolvendo computadores e *notebooks*;

c) comunicar à CGTI, CGOFL e CGESP sobre perda, furto ou roubo de *notebooks*; e

d) cumprir com as diretrizes e orientações das normas de segurança da informação do Cade, assim como apoiar o desenvolvimento e identificação de novas necessidades.

Seção II

Das Disposições Gerais

Art. 3º Para efeito no referido normativo, todos os termos e definições estão descritos no Glossário da Posic, instituído pela Portaria Cade nº 404, de 20 de maio de 2019.

Art. 4º O uso de computadores e notebooks patrimoniados pelo Cade está restrito às atividades exercidas por servidores, colaboradores e estagiários em seu cotidiano institucional.

§ 1º É vedado o uso de computadores e *notebooks* patrimoniados pelo Cade para atividades que tragam ganhos e benefícios monetários e pessoais.

§ 2º Toda informação institucional do Cade deve ser tratada visando as suas funções administrativas, informativas, probatórias e comunicativas, sendo vedada a apropriação dessas informações em caso de desligamento de servidores, colaboradores e estagiários.

§ 3º O uso de computadores, *notebooks* e *softwares* para as atividades finalísticas do Cade está condicionado aos recursos disponíveis conforme Mapa de Recursos Mínimos e catálogo de serviços de TI.

Art. 5º A administração de computadores e *notebooks* é restrita à CGTI por meio de seus servidores ou colaboradores de empresa contratada.

§ 1º Servidores, colaboradores e estagiários das demais unidades administrativas não possuirão direitos de administrador de notebooks e computadores.

§ 2º Caso haja necessidade de acesso de administrador para fim de apoiar as atividades no Cade, a concessão será dada por meio de solicitação formal do chefe ocupante de cargo ou função igual ou superior a DAS/FCPE 4 e os computadores e *notebooks* serão auditados periodicamente.

Art. 6º Computadores e *notebooks* corporativos devem ser classificados de acordo com o local de instalação, atribuição do usuário ou a informação neles contida.

Art. 7º Todos os computadores e *notebooks* corporativos devem ter seus discos protegidos por sistemas criptográficos.

§ 1º A gestão de senhas e chaves criptográficas deverá ser feita pela equipe da CGTI.

§ 2º Discos de recuperação para casos de esquecimento de senhas ou chaves criptográficas deverão ser armazenadas em local adequado e salvaguardadas pela CGTI.

§ 3º Arquivos sensíveis armazenados na infraestrutura do Cade devem ser criptografados.

Art. 8º Serão estabelecidos mecanismos de bloqueio de tela em caso de ociosidade de computadores e *notebooks*.

Art. 9º Auditorias periódicas devem ser executadas para identificação do uso de *softwares* não homologados pela CGTI, assim como garantir que os controles de segurança implementados estão vigentes e em conformidade com as definições institucionais.

Art. 10. *Backups* dos computadores e *notebooks* devem ser feitos periodicamente.

§ 1º Em caso de desligamento do órgão, os dados produzidos pelo usuário durante seu tempo em exercício no Cade pertencem ao órgão, não sendo permitido ao usuário a remoção, cópia ou alteração maliciosa dos dados ao longo do processo de desligamento.

§ 2º Quando possível, a área de trabalho do usuário deve ser configurada para acesso, criando cópia automática de todos os arquivos definidos como necessários para atividade do Cade.

§ 3º Os procedimentos de *backup*, manutenção, movimentação e descarte de computadores e *notebooks* deverão levar em consideração a classificação do equipamento para o tratamento adequado.

§ 4º Serão definidos os diretórios e tipos de arquivos a serem salvaguardados em ambiente de *backup*, considerando a necessidade para as atividades do Cade.

§ 5º O Cade não será responsável por *backups* de arquivos pessoais.

Seção III

Do uso de computadores e *notebooks* pessoais (BYOD)

Art. 11. Todos os computadores e *notebooks* particulares que são incorporados à rede de dados e usados para acessos às informações e infraestrutura do Cade são considerados como dispositivos corporativos, conforme determinação da Norma Complementar Nº 12/IN01/DSIC/GSIPR.

Art. 12. O uso de computadores e *notebooks* pessoais está condicionado à conformidade de configuração e adequação de segurança estabelecidos pela CGTI, devendo seguir os padrões e diretrizes de segurança impostos para os computadores e *notebooks* corporativos.

Art. 13. Todo colaborador que desejar utilizar um computador ou *notebook* pessoal para acessar recursos do Cade (ex: e-mail, sistemas e infraestrutura de TIC), deve procurar a CGTI para solicitar autorização e obter informações de configuração para seu dispositivo.

Art. 14. Em caso de perda, roubo ou furto de *notebooks*, a CGTI deve ser informada imediatamente para tomar as devidas providências de segurança, evitando o acesso indevido por terceiros.

Art. 15. É vedado o uso de computadores e *notebooks* pessoais no ambiente de rede cabeada do Cade.

Seção IV

Do registro e monitoramento

Art. 16. Mecanismos de monitoramento dos computadores e *notebooks* do Cade devem ser institucionalizados a fim de identificar e alertar sobre:

I - ações de instalação e remoção de *software*, assim como execuções de aplicações;

II - tentativas de ataques, como de varredura de portas, escuta de rede (*sniffing*), força bruta ou a exploração de alguma vulnerabilidade no ambiente corporativo do Cade;

III - uso de *softwares* de captura de informações passivos ou ativos;

IV - uso indevido do computador ou *notebook* do Cade; e

V - acesso indevido a conteúdo, conforme diretrizes das normas de Controle de acesso lógico e Conectividade e acessos à Internet.

Art. 17. Registros (log) de uso e de erros ou falhas devem ser utilizados para assegurar que os problemas de sistemas sejam identificados e alertados.

Art. 18. Registros de conexão e registro de acesso a aplicações devem ser mantidos por um período de 60 meses, contendo, minimamente:

I - identificação do usuário;

II - data, horário e detalhes de eventos;

III - identificação do *notebook*;

IV - registros de tentativas de acesso a recursos e dados aceitos e rejeitados;

V - alterações de configuração de sistemas;

VI - uso de escalonamento de privilégios;

VII - uso de aplicações ou utilitários do sistema;

VIII - arquivos acessados e tipo de acesso;

IX - endereço e protocolo de rede;

X - alarmes provocados por sistema de controle de acesso; e

XI - ativação e desativação de sistema de proteção.

Art. 19. Registros de log de auditoria devem ser de acesso restrito à equipe da ETIR.

Art. 20. Controles devem ser implementados para inibir a falsificação e acesso não autorizado aos registros de log.

Art. 21. O *backup* dos registros será realizado, mantendo os aspectos de segurança e criptografia.

Seção V

Da localização e proteção dos computadores e *notebooks*

Art. 22. Todos os computadores e *notebooks* do Cade devem ser identificados e inventariados.

§ 1º O inventário técnico deve possuir informações que possibilitem a recuperação do computador ou *notebook* em caso de perdas ou desastres com menor tempo possível.

§ 2º O inventário deve possibilitar a identificação do local e da pessoa e a sensibilidade das informações decorrentes do uso para as atividades do Cade.

§ 3º É necessário que seja possível a rastreabilidade ao nível de usuário, possibilitando recuperação de informações em caso de desastres ou eventos de segurança.

Art. 23. Todos os computadores e notebooks devem possuir termos de custódia assinados, conforme descrito na norma de Contratação, permanência e desligamento de pessoas no âmbito do Cade.

Parágrafo único. Os termos de custódia são responsabilizações pessoais e forma de não repúdio para o uso de computadores e *notebooks*, não substituindo os termos de responsabilidade já assinados pelos chefes ocupantes de cargo ou função igual ou superior a DAS/FCPE 4 de cada área.

Art. 24. Computadores devem ser posicionados cuidadosamente para que se reduza o risco de que as informações sejam vistas por pessoas não autorizadas durante a sua utilização.

Art. 25. Consumo de sólidos e líquidos deve ser ponderado, afim de prevenir danos aos computadores e *notebooks*.

Art. 26. Travas de segurança devem ser instalados nos computadores, fixando-as nas mesas e impedindo movimentações não autorizadas ou furtos.

Parágrafo único. Controles complementares devem ser implementados para prevenção de furtos.

Seção VI

Do uso e controle de software

Art. 27. É vedado o uso de qualquer sistema ou *software* que não esteja no Mapa de Recursos Mínimos do Cade ou no catálogo de serviços de TI.

§ 1º A equipe CGTI, apoiada pelas demais unidades administrativas do Cade, deverá produzir um Mapa de Recursos Mínimos, que conterá a lista de *softwares* homologados e ofertados pelo Cade.

§ 2º O Mapa de Recursos Mínimos deverá refletir a visão institucional e será atualizado a cada aquisição ou descontinuidade de uso de *softwares* pelas unidades administrativas do Cade.

§ 3º O Mapa de Recursos Mínimos será utilizado como insumo para os instrumentos de planejamento de TI.

Art. 28. É vedada a instalação de *softwares* pessoais em *notebooks* e computadores patrimoniados pelo Cade.

Art. 29. É vedado o uso de *softwares*, de qualquer natureza, adquirido pelo Cade, para atividades de interesse e ganhos econômicos pessoais.

Art. 30. Toda e qualquer instalação ou demanda de aquisição de *softwares* deverá ser solicitada à CGTI, a qual analisará a solicitação considerando a aderência aos instrumentos de planejamento, a capacidade de entrega, o nível de sustentação operacional, os riscos de segurança da informação e os aspectos operacionais.

Parágrafo único. Mesmo que as áreas finalísticas possuam recursos, toda aquisição de *softwares* deverá ser apoiada pela CGTI para construção dos artefatos da contratação.

Art. 31. Um ambiente de teste e homologação de *softwares* deve ser estabelecido para aprovação de novos sistemas e aplicações e atualização de versões.

Seção VII

Da segurança dos *notebooks* para teletrabalho e atividades remotas

Art. 32. Todos os integrantes do teletrabalho e atividades remotas receberão *notebooks* patrimoniados pelo Cade, sendo vedado o uso de computadores e notebooks pessoais para exercício das atividades.

Art. 33. Os notebooks do teletrabalho e atividades remotas deverão ser monitorados e auditados constantemente e com maior rigor.

Art. 34. Será estabelecido duplo fator de autenticação para o uso de *notebooks* usados no teletrabalho.

Art. 35. Todos os *notebooks* deverão possuir controles mais rigorosos quanto ao uso de criptografia, controle de uso de *softwares*, uso de recursos e acessos à internet e para abertura e remoção de suas unidades de armazenamento.

Parágrafo único. Serão criadas barreiras físicas que inibam a abertura dos notebooks, preservando a integridade do equipamento.

Art. 36. Os acessos aos sistemas e ambiente de tecnologia do Cade deverão respeitar as diretrizes da norma de Controle de acessos lógicos no âmbito do Cade.

§ 1º O acesso à internet será através do túnel criptográfico estabelecido com o Cade, seguindo as definições de acesso, monitoramento e auditoria estabelecidos pela CGTI.

§ 2º É vedado qualquer outro acesso à internet sem o devido tratamento dos controles de acessos estabelecidos pela CGTI.

§ 3º É vedado o acesso a sites ou sistemas que não façam parte do teletrabalho.

Art. 37. Em caso de perda ou roubo, o usuário deverá comunicar imediatamente às equipes da CGTI, CGOFL e CGESP, que tratarão o evento como incidente de segurança da informação.

Art. 38. O uso de *notebooks* do teletrabalho deve ser feito em ambiente privado, preservando os princípios da privacidade e do sigilo das informações.

Parágrafo único. Caso o uso em ambiente público seja necessário, o equipamento não pode ser deixado em momento algum sem supervisão de seu custodiante.

Art. 39. Devem ser implementados controles que inibam o acesso remoto não autorizado aos *notebooks*.

Seção VIII

Da manutenção de computadores e *notebooks*

Art. 40. A CGTI deve estabelecer procedimentos operacionais para manutenção, instalação e suporte de computadores e *notebooks*.

Art. 41. A CGTI deverá prover equipamentos e recursos necessários para os processos de manutenção de computadores e *notebooks*.

Parágrafo único. O uso de dispositivo de armazenamento externo (pen-drive, HD externos e afins) para manutenção e demais atividades de suporte técnico ao Cade, deverá ser restrito aos dispositivos providos pela autarquia, sendo vedado o uso de dispositivos de armazenamento externo de terceiros ou pessoais.

Art. 42. Somente a equipe da CGTI ou empresa contratada deverá fazer manutenção nos computadores e *notebooks*.

§1º Imagens de instalações devem ser usadas, considerando as atribuições ou áreas operacionais, estabelecendo um padrão de instalações e reduzindo erros nas entregas de equipamentos.

§2º Instalações que utilizem licenças de *software* deverão ser documentadas para fins de gerenciamento de itens de configuração.

§3º Toda manutenção deverá ser solicitada por meio de sistema próprio para atendimento de solicitações e demandas.

§4º Registros de falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva ou corretiva realizadas devem ser armazenados.

Art. 43. Durante a manutenção é necessário que sejam salvaguardadas as informações do usuário, a fim de manter as condições originais de confidencialidade, integridade e disponibilidade das informações;

§ 1º Dados pessoais de usuários deverão ser tratados com sigilo e discrição.

§ 2º Efetuar cópias indevidas de arquivos pessoais de usuários ou informações do Cade durante processo de manutenção, será considerado como incidente de segurança da informação, sendo tratado da forma cabível.

§ 3º Somente o chefe ocupante de cargo ou função igual ou superior a DAS/FCPE 4 poderá solicitar a destruição dos dados em processo de manutenção.

§ 4º Sempre que necessário, os arquivos contidos no dispositivo serão salvos para posterior restabelecimento em seus locais de destino após conclusão do procedimento de manutenção.

Art. 44. As manutenções devem ser feitas, sempre que possível, na presença do usuário solicitante. Quando não for possível, o computador ou notebook será encaminhado até o laboratório da CGTI para que seja efetuado o procedimento adequado, de acordo com os normativos vigentes.

§ 1º Somente os chefes imediatos podem autorizar a retirada de computadores de suas unidades administrativas, mediante registro no chamado.

§ 2º Colaboradores da empresa contratada e estagiários devem possuir treinamento adequado quanto aos aspectos de segurança.

Art. 45. Antes de colocar o computador ou *notebook* em operação após processo de manutenção, haverá checagem para avaliar o perfeito funcionamento e restabelecimento pleno dos serviços.

Seção IX

Da reutilização de computadores e *notebooks*

Art. 46. Uma imagem de instalação deverá ser produzida a fim de prover um padrão de instalação homologado, minimizando erros, além de reduzir o tempo de entrega em caso de reinstalações futuras.

§ 1º Criada e homologada a imagem de instalação, esta deverá ser usada em todas as instalações futuras.

§ 2º Todos os computadores e *notebooks* custodiados no patrimônio do Cade deverão, obrigatoriamente, ser formatados e configurados com o padrão mínimo de instalação.

§ 3º Para fins de controle, a CGTI deverá registrar quais máquinas foram formatadas ou destruídas logicamente e instaladas com o padrão mínimo, notificando a CGOFL para que os computadores e *notebooks* possam ser salvaguardados da forma adequada.

§ 4º Os computadores e *notebooks* não adequados ao padrão mínimo deverão ser separados e não poderão ser usados em movimentações.

Art. 47. Em caso de chegada de computadores e *notebooks*, a CGTI deverá adequar todos os equipamentos com os parâmetros mínimos de segurança e instalação de softwares, considerando o Mapa de Recursos Mínimos.

Art. 48. Em casos de movimentação interna de computadores e notebooks, os equipamentos deverão ser formatados e reinstalados com o uso dos discos de imagem de instalação.

§ 1º Para os computadores e *notebooks* do Lab-SG, ou quando solicitado pelo usuário e autorizado pelo CGTI, será exigido maior rigor para destruição dos dados, através da técnica de *wipe*, para posterior reinstalação do sistema, conforme Mapa de Recursos Mínimos.

Art. 49. Para os casos de desfazimentos (doações), todos os computadores e notebooks deverão ser destruídos logicamente de forma mais criteriosa.

§ 1º O uso da técnica de *wipe* deverá ser adotado para limpeza dos dados contidos nos discos e adequação do equipamento às instalações de fábrica.

§ 2º Quando pertinente, será realizada a verificação de dispositivos de leitura de mídias afim de resguardar que nenhuma mídia esteja nos dispositivos.

Art. 50. Para descarte de computadores e *notebooks*, os discos e as mídias internas de armazenamento de dados deverão ser danificados fisicamente, a fim de impedir o reuso, e os demais periféricos devem ser descartados como lixo eletrônico.

Seção X

Do tratamento de *malware*

Art. 51. Controles de detecção, prevenção e recuperação devem ser implementados para proteção contra *malwares*.

Parágrafo único. Como forma complementar de controle, haverá, periodicamente, campanha de conscientização e sensibilização periódica para todos os servidores, colaboradores e estagiários do Cade.

Art. 52. É vedado o uso de qualquer software executável do tipo portátil (*portable*) diretamente de pelo usuário ou através de mídia de armazenamento externo (*pendrive*, HD externo e afins).

Parágrafo único. Quando necessário o uso de softwares de execução direta, a CGTI deverá ser informada da necessidade de uso.

Art. 53. Todos os aplicativos usados e homologados pelo Cade serão atualizados periodicamente.

Art. 54. Sistemas de varreduras *antimalware* devem ser executados e atualizados periodicamente.

§ 1º Serão criados controles que impeçam usuários de desativar ou desabilitar os mecanismos de varredura.

§ 2º Serão adotados controles para mitigação de ameaças especializadas no ambiente corporativo.

§ 3º O sistema de varredura verificará todos os discos e todas as extensões de arquivos.

§ 4º Sempre que aplicável, arquivos infectados devem ser descontaminados.

§ 5º Quando pertinente, o Cade poderá usar mecanismos complementares de varredura para contraprova do sistema usado institucionalmente.

§ 6º O sistema de varredura *antimalware* deve verificar automaticamente arquivos anexados aos *e-mails* e obtidos pela internet.

Seção XI

Sanções e Das Penalidades

Art. 55. Os colaboradores que não zelarem pela implementação e execução das diretrizes descritas neste normativo serão responsabilizados em caso de vazamento, total ou parcial, de informações sensíveis decorrentes de seus atos.

Art. 56. A violação ou a não aderência a este normativo será considerado um incidente de segurança da informação e acarretará a aplicação das penalidades previstas em lei.

Seção XII

Das Disposições Finais

Art. 57. Os casos omissos serão resolvidos no âmbito da Diretoria de Administração e Planejamento.

Art. 58. Esta Portaria entra em vigor 30 dias após a data de sua publicação.

ALEXANDRE BARRETO DE SOUZA
Presidente
(assinado eletronicamente)

Documento assinado eletronicamente por **Alexandre Barreto de Souza**, **Presidente**, em 20/05/2019, às 19:10, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0616610** e o código CRC **2AC16B15**.

Referência: Processo nº 08700.000342/2014-58 SEI nº 0616610