



**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 416, DE 20 DE MAIO DE 2019.

Regulamenta o uso de ativos de infraestrutura
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 Regular o uso de ativos de infraestrutura no âmbito do Conselho Administrativo de Defesa Econômica – Cade, em consonância com o inciso VII do art. 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 Coordenação-Geral de Tecnologia da Informação – CGTI:

- a) prover os recursos necessários para o gerenciamento dos ativos de tecnologia do Cade;
- b) estabelecer as políticas e critérios para o gerenciamento dos ativos de tecnologia da informação;
- c) manter a documentação de infraestrutura e procedimentos de administração de rede atualizados; e
- d) estabelecer e gerir os processos de gestão de mudança, gestão de configuração e gestão de incidentes.

II - às unidades administrativas do Cade:

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

III - à Assessoria de Comunicação Social – Ascom:

a) apoiar o processo de divulgação, avaliação e sensibilização dos assuntos referentes à segurança da informação e comunicação.

IV - 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.

V - aos servidores, colaboradores e estagiários do Cade:

a) cumprir 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 Os recursos de tecnologia, assim como a infraestrutura são de uso exclusivo para as atividades finalísticas do Cade.

Art. 5º O uso do servidor de arquivos é exclusivo para as atividades do Cade.

Parágrafo único. As pastas corporativas de cada setor serão de responsabilidade do chefe da unidade ocupante de cargo ou função igual ou superior a DAS/FCPE 4.

Art. 6º As informações contidas nos sistemas de banco de dados são exclusivas para atividades do Cade, sendo vedada a cópia ou uso não-autorizado para outros fins que não sejam de interesse do Cade ou situações previstas em lei.

Art. 7º O consumo de serviços de *streaming* será monitorado pela CGTI, ficando a cargo dessa Coordenação-Geral administrar a liberação ou limitação de banda desse tráfego, a fim de manter a disponibilidade de serviços críticos do Cade.

Art. 8º O ambiente de tecnologia do Cade deve ser segregado, promovendo, sempre que possível, isolamento físico e lógico.

§1º A rede deve segregar os andares, serviços e ambientes operacionais.

§2º O acesso lógico entre os andares deve ser controlado através de regras de segurança e conectividade com autorização da CGTI, sendo impedida a livre comunicação entre eles.

§3º O acesso lógico para gestão dos servidores, ativos de conectividade (roteadores e *switches*) e demais ambientes estruturantes de tecnologia serão feitos, exclusivamente, através de uma rede de gestão, segregada das demais redes corporativas.

§4º O monitoramento dos ativos de conectividade deve ser feito com o uso do protocolo SNMP.

Seção III

Da Concessão de Acesso de Administração

Art. 9º Os acessos para gestão de serviços e sistemas operacionais serão feitos através de conta nominal e estão restritos aos servidores e colaboradores designados pela CGTI.

Art. 10. Cada serviço deve possuir uma equipe de administração responsável formada por um servidor do Cade e um colaborador da empresa contratada para sustentação dos serviços.

§1º A responsabilidade pela sustentação e bom funcionamento do serviço é do servidor do Cade, que deve solicitar ao colaborador apoio operacional para mantê-lo.

§2º Em caso de falhas em horário fora do expediente normal, o servidor do Cade deve ser acionado, solicitando ao preposto da empresa contratada apoio, quando pertinente.

§3º O acesso originado fora da rede do Cade, deve ser autorizado pela CGTI.

Art. 11. É vedado o uso de equipamentos pessoais ou não patrimonizados pelo Cade para acesso de administração dos servidores e ativos de tecnologia.

§1º Servidores, colaboradores, consultores e prestadores de serviços de empresas fornecedoras devem usar equipamento do Cade para manutenção, atualização e demais operações de ativos de infraestrutura; e

§2º Para os casos de uso de ferramentas específicas ou ambiente específico de fornecedores, será permitido o uso de computadores do fornecedor, desde que autorizados pela CGTI.

Art. 12. Um plano de execução deve ser apresentado para aprovação de um servidor do Cade antes de qualquer manutenção do ambiente tecnológico.

§1º Quando houver planejamento de ações no ambiente de produção, é necessário que seja apresentado um plano de execução demonstrando, minimamente, o que será feito, resultados esperados, riscos da execução, plano de recuperação do ambiente em caso de resultados não esperados, janela de execução.

§2º O planejamento da mudança deverá seguir procedimentos específicos de gerenciamento de mudanças.

§3º Um servidor do Cade deve acompanhar a execução do planejamento apresentado.

Seção IV

Da Gestão de *Backups*

Art. 13. O sistema de gerenciamento de *backup* deverá ser gerenciado e monitorado por um servidor do Cade.

Parágrafo único. A operação de rotinas de *backup* deverá ser realizada somente por servidores e colaboradores que realizem atividades de sustentação de infraestrutura.

Art. 14. Serão gerados relatórios automatizados pela própria ferramenta de *backup* para a CGTI, no mínimo, uma vez ao mês.

Art. 15. Para os *backups* que apresentarem falhas, o operador do *backup* deverá criar relatório de acompanhamento, no qual deverá constar a data, os horários de início e término, os objetos e os clientes de *backup*, a causa da falha, a ação corretiva adotada e qual parte do *backup* ficou comprometida.

Art. 16. A configuração e a monitoração das funcionalidades relativas ao banco de dados serão de responsabilidade do administrador do recurso.

Art. 17. Os *backups* deverão seguir políticas diferenciadas de acordo com o tipo de dado e o ambiente computacional, como disposto a seguir:

§ 1º - Quanto ao período de realização do *backup*:

I - diário crítico: deverá ser programado para execução no intervalo entre 5h e 20h do dia, de segunda a sexta;

II - diário: deverá ser programado para execução no intervalo entre 20h e 5h do dia seguinte, de segunda a sexta;

III - semanal: deverá ser programado para execução no intervalo entre 20h de sábado e 12h do domingo; e

IV - mensal: deverá ser programado para execução no intervalo entre 20h em dia fixo do mês e 8h do dia seguinte.

§ 2º - Quanto à aplicação do *backup*:

I - sistemas de informação críticos terão o agendamento de tarefas de *backups*:

- a) incrementais diários críticos;
- b) completos sintéticos diários; e
- c) completos semanais.

II - sistemas de informação de apoio terão o agendamento de tarefas de *backups*:

- a) incrementais diários ou completos semanais.

III - os sistemas operacionais dos servidores terão o agendamento de tarefas de *backups*:

- a) completos mensais.

IV - cópias auxiliares para fins de arquivamento de dados serão realizadas em regime de 24 (vinte e quatro) horas, por 7 (sete) dias por semana, desde que não impacte no desempenho das demais tarefas; e

V - expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, conforme políticas de armazenamento de dados e de descarte de mídias vigentes.

§ 3º - *Backups* de registros de acesso serão mantidos por no mínimo 12 meses, salvo para critérios específicos contidos na Posic-Cade e suas demais normas complementares.

Art. 18. Os *backups* de histórico de sistemas (log) e bancos de dados dos demais aplicativos de infraestrutura deverão seguir a mesma política especificada para o *backup* do sistema de arquivos.

Art. 19. A recuperação de *backups* deverá obedecer às seguintes orientações:

I - o usuário que necessitar recuperar arquivos deverá entrar em contato com o setor de suporte ao usuário, registrar o pedido no sistema de gestão de chamados com, obrigatoriamente, as informações sobre o usuário, o arquivo a ser recuperado, o subdiretório de localização e a data da versão que deseja recuperar;

II - o chamado será encaminhado à CGTI que, após a conclusão da tarefa, realizará o fechamento do chamado indicando ao solicitante a restauração do arquivo;

III - deverá ser mantido registro de todos os arquivos restaurados juntamente com a solicitação inicial; e

IV - os bancos de dados serão restaurados pelo administrador do banco.

Art. 20. As regras de *backup* devem ser atualizadas quando houver novas aplicações desenvolvidas ou adquiridas, novos locais de armazenamento de dados ou arquivos, novas instalações de banco de dados, ou alterações nas necessidades de negócio.

Art. 21. O *backup* deve considerar o impacto da perda parcial ou total da informação, a sensibilidade das informações e resiliência dos processos finalísticos.

Art. 22. Todos os *backups* criados deverão ser testados, observando a restauração e integridade dos arquivos e dados.

Art. 23. Os *backups* realizados em mídias do tipo cartucho de fita que necessitem de armazenamento para recuperação de desastres serão guardados em ambiente seguro, segregado do ambiente de processamento de dados.

Seção V

Das Sanções e Penalidades

Art. 24. Os servidores e 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. 25. 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 VI

Das Disposições Finais

Art. 26. Os logs de ativos de infraestrutura devem ser criptografados e salvaguardados por um período de 3 anos.

Parágrafo único. O acesso aos arquivos de log deve ser controlado e de uso exclusivo para casos de auditoria ou previstos em lei.

Art. 27. Os casos omissos serão resolvidos no âmbito da Diretoria de Administração e Planejamento.

Art. 28. 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](http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0616622** e o código CRC **CF6F21D0**.