



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 405, DE 20 DE MAIO DE 2019.

Regulamenta os direcionamentos de segurança da informação e comunicação para a contratação, permanência e desligamento de pessoas 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 os direcionamentos de segurança da informação e comunicação para a contratação, permanência e desligamento de pessoas 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 Gestão de Pessoal - CGESP:

- a) fomentar a aderência à legislação e normas que disciplinam os atos de pessoal, inclusive as relacionadas à segurança da informação e comunicação e gestão de riscos organizacionais;
- b) definir formas e ferramentas para identificação e avaliação do descumprimento de normativos de segurança da informação;
- c) propor e subsidiar a elaboração de diretrizes, normas e procedimentos;
- d) apoiar o Comitê de Segurança Institucional do Cade - CSIC no desenvolvimento de planos de divulgação, sensibilização, capacitação e conscientização dos assuntos de segurança da informação e comunicação e gestão de riscos, que devem ser parte da Política de Capacitação e Desenvolvimento do Cade;

- e) apoiar o CSIC nas ações para mensurar o nível de compreensão, de aderência e do uso de normativos de segurança da informação, regimento interno, código de conduta e demais pertinentes;
- f) garantir que todos os servidores, colaboradores e estagiários assinem os termos de conduta, confidencialidade e não repúdio relativos às suas funções, quando aplicável; e
- g) registrar e adotar medidas relativas ao afastamento, a remoção, a redistribuição, a disponibilidade, a requisição e a cessão de servidores, bem como exercício provisório.

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

- a) prover os recursos necessários e apoiar a implementação dos controles tecnológicos pertinentes, para o cumprimento das determinações descritas nesta norma;
- b) reportar à CGESP todo e qualquer incidente de segurança da informação ou desvio de conduta no âmbito do uso de recursos tecnológicos, segundo orientação dos normativos de segurança da informação e comunicação e código de conduta do Cade; e
- c) apoiar o monitoramento para identificação de desvios de condutas com o uso de recursos tecnológicos.

III - às unidades administrativas do Cade:

- a) encaminhar todos os servidores, colaboradores e estagiários para que a CGESP faça a ambientação e recolha assinatura dos termos pertinentes;
- b) manter a CGESP atualizada sobre o *status* e afastamento de servidores, colaboradores e estagiários;
- c) fomentar a aderência aos normativos de segurança da informação e comunicação para todos os seus servidores, colaboradores e estagiários; e
- d) monitorar as ações de seus servidores, colaboradores e estagiários quanto ao cumprimento das normas de segurança da informação.

IV - 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 requisitos de segurança para exercícios das funções, cargos ou atividades consideradas sensíveis devem ser estabelecidos em consonância com as unidades administrativas do Cade.

§ 1º O perfil de qualificação profissional e comportamental de servidores e colaboradores deve ser estabelecido de acordo com as atividades sensíveis desenvolvidas pela unidade organizacional em conjunto com a CGESP.

§ 2º Em caso de contratação de estagiários para atuação em atividades ou acessos a áreas sensíveis, somente o chefe imediato poderá solicitar a concessão de acessos, sendo necessária uma ambientação mais rigorosa e que seja estabelecido um perímetro de acessos específico, de forma a minimizar os acessos a informações sensíveis.

§ 3º O chefe imediato é corresponsável por dolos ou impactos causados pelo uso indevido de informações provenientes das concessões de acesso solicitados.

Art. 5º Todos os servidores, colaboradores e estagiários, independente de cargo ou função, devem possuir registro de sua lotação, descrição de cargo ou função, identificação de seu chefe imediato e unidade de lotação atualizados.

§ 1º O registro deverá ser feito na intranet, sendo de responsabilidade de cada servidor ou colaborador manter seus dados atualizados.

§ 2º A concessão de acessos físico e lógico do servidor ou colaborador está condicionada à completude de seu cadastro.

§ 3º Equipara-se o perfil de intercambista ao perfil de estagiário nos casos gerais de concessão de acessos físico e lógico.

§ 4º O registro da foto funcional é obrigatório e será realizado pela CGESP em conjunto com a Assessoria de Comunicação - Ascom, devendo a foto ser nítida, atual e impessoal.

§ 5º Para os casos de não conformidade do registro de servidores, colaboradores e estagiários com afastamento temporários (férias, viagens, treinamentos, dentre outros), o chefe imediato deverá ser comunicado do ocorrido para solicitação de providências.

§ 6º Cabe à CGESP a validação periódica dos dados e, em casos de não conformidade do cadastro, um e-mail deverá ser enviado ao servidor, colaborador ou estagiário, informando a ocorrência encontrada e solicitando que seja tomada providência, com cópia para o chefe imediato.

§ 6º Cabe ao chefe imediato solicitar que os servidores, colaboradores e estagiários mantenham seus dados atualizados.

§ 7º A foto de perfil é de livre escolha do servidor, colaborador ou estagiário, desde que atenda às regras de ética e conduta da Administração Pública Federal.

Art. 6º A CGESP deve ser informada sobre novos servidores, colaboradores e estagiários, independentemente do tempo de permanência, cargo ou função exercidos.

Art. 7º No caso de identificação de incidentes decorrentes do descumprimento dos controles de proteção e custódia de ativos, deve-se informar ao chefe imediato da área afetada sobre tal ilícito.

§ 1º É de responsabilidade do chefe imediato informar à CGESP sobre incidentes de desvio de conduta de segurança da informação e comunicação.

§ 2º Cabe à CGESP analisar e avaliar os incidentes de segurança da informação e comunicação por desvio de conduta e proceder conforme as legislações vigentes.

§ 3º Incidentes de segurança da informação e comunicação que envolvam desvio de conduta serão formalizados, assim como as medidas adotadas para o tratamento desse desvio.

a) os registros de eventos de desvio de conduta, não classificados como incidentes de segurança da informação e comunicação, devem ser realizados junto à CGESP; e

b) os registros de incidentes de segurança da informação e comunicação devem ser avaliados periodicamente como forma de identificar fragilidades e desenvolver um plano de ação para melhoria contínua do processo.

Art. 8º Devem ser desenvolvidas campanhas de conscientização e treinamentos para os assuntos de segurança da informação e comunicação, com apoio da Ascom.

Parágrafo único. A Auditoria Interna e o chefe imediato devem realizar avaliação do nível de aderência e da efetividade dos normativos de segurança da informação e comunicação, levando em consideração o nível de sensibilidade de suas atividades e informações.

Seção III

Da Recepção e Entrada de Servidores, Colaboradores e Estagiários

Art. 9º A CGESP deve desenvolver ambientação para todos os servidores, colaboradores e estagiários, independente de cargo ou função, apresentando, minimamente:

I - legislação relacionada ao Cade;

II - planejamento Estratégico;

III - regimento Interno do Cade;

IV - código de Conduta dos Agentes Públicos do Cade;

V - a política e os normativos de segurança da informação e comunicação, e gestão de riscos; e

VI - a responsabilização por seus atos.

Art. 10. Todos os servidores, colaboradores e estagiários do Cade devem assinar os termos de conduta, confidencialidade e não repúdio relativos às suas funções, condizentes com a execução de suas atividades na autarquia.

§ 1º Todos os termos deverão ser salvuardados em um único local para fácil acesso:

a) em caso de armazenamento lógico dos termos, os documentos devem conter nomenclatura para fácil identificação, considerando o tipo do termo e nome do colaborador assinante; e

b) a CGESP custodiará uma cópia dos termos assinados, organizando-os individualmente em pastas ou repositórios com demais documentos e termos assinados pelos servidores, colaboradores e estagiários.

Art. 11. Todos os servidores e colaboradores que receberem ativos de tecnologia e dispositivos móveis patrimoniados pelo Cade devem cumprir, obrigatoriamente, as normas de Controle de acesso lógico, Dispositivos móveis e Uso de computadores.

§ 1º A CGESP, CGOFL e CGTI devem consultar o Mapa de recursos mínimos para que sejam preparados os recursos necessários.

§ 2º Um representante da CGOFL, CGTI e CGESP devem ser designados para entrega das credenciais e recursos, no momento de ambientação.

§ 3º No ato do recebimento, o servidor ou colaborador deve verificar o perfeito funcionamento dos equipamentos, sendo de sua responsabilidade a salvaguarda e o zelo desses.

§ 4º Todos os servidores e colaboradores que receberem ativos de tecnologia e dispositivos móveis patrimoniados pelo Cade devem assinar o termo de custódia dos ativos e dispositivos móveis.

Art. 12. As concessões de acessos deverão preceder conforme diretrizes das normas de Controle de acessos físico e lógico.

Art. 13. As credenciais de acesso aos ambientes de TI e ao ambiente físico do Cade, o crachá de identificação, ou bóton para os casos aplicáveis, serão entregues ao final da ambientação, mediante assinatura dos termos de conduta, confidencialidade e não repúdio relativos às suas funções.

Art. 14. O servidor, colaborador ou estagiário terá seu perfil divulgado em área específica de “boas vindas” e “até logo” no portal da intranet no momento de sua entrada e saída, respectivamente.

Seção IV

Das Mudanças de Atribuições

Art. 15. Em caso de mudança de atribuições de servidores e colaboradores, o responsável pela área de lotação vigente deve informar à CGESP, com cópia para a CGTI e CGOFL, a data de saída do servidor ou colaborador.

§ 1º Na data especificada, quando pertinente, serão encerrados os acessos atuais.

§ 2º Os acessos às informações da atribuição vigente serão mantidos caso haja solicitação do chefe imediato.

§ 3º Ao servidor ou colaborador, será concedido acesso mínimo para a nova atribuição, conforme diretrizes das normas de Controle de acessos físico e lógico.

§ 4º Os termos de conduta, confidencialidade e não repúdio assinados englobam migrações verticais (de atribuições com menores restrições de acessos para atribuições com maiores restrições de acessos).

Art. 16. Quando pertinente, deve-se estabelecer processo de avaliação de perfil e enquadramento para a nova atribuição, conforme Art. 4º.

Parágrafo único. Para solicitações de novas concessões de acesso, será obrigatório que a CGESP seja informada da nova lotação do servidor ou colaborador, conforme determinação do Art. 14.

Seção V

Do Encerramento das Atividades

Art. 17. A CGESP deve ser informada com antecedência sobre o encerramento das atividades do servidor, colaborador ou estagiário, para que sejam tomadas as medidas cabíveis.

§ 1º A CGESP deve solicitar a retirada das concessões de acessos à infraestrutura de tecnologia da informação e comunicação e ao ambiente físico do Cade.

§ 2º A CGTI deve retirar os direitos de acessos do servidor, colaborador ou estagiário, na data marcada, conforme diretrizes da norma de Controle de acesso lógico.

§ 3º A CGOFL deve retirar as concessões de acessos físicos do servidor, colaborador ou estagiário, conforme diretrizes da norma de Controle de acesso físico.

§ 4º Em caso de suspeita de ilícitos de segurança da informação e comunicação, a CGTI deverá proceder conforme legislação vigente.

Art. 18. O registro de termos assinados pelo servidor, colaborador ou estagiário deve ser consultado para que seja solicitada a devolução de todos os ativos sob a sua responsabilidade.

Parágrafo único. Os servidores e colaboradores em desligamento devem assinar os termos de devolução dos dispositivos de tecnologia da informação e dos dispositivos móveis, conforme diretrizes das normas de Uso de dispositivos móveis e demais de uso de recursos de tecnologia da informação.

Art. 19. O servidor, colaborador ou estagiário deverá entregar para a CGESP o crachá de identificação, carteira funcional, os ativos de TIC, dispositivos móveis corporativos e cartão de acesso à garagem, quando aplicável.

Parágrafo único. No ato da entrega, a CGTI deve fazer a análise dos ativos de TIC e a CGOFL deve fazer a análise da integridade dos dispositivos móveis entregues, observando o estado e o funcionamento desses.

Art. 20. O servidor, colaborador ou estagiário deverá assinar os termos de entrega e ciência da retirada de concessão, comprometendo-se a manter o sigilo das informações, quando pertinente.

Art. 21. Uma resposta automática de e-mails será configurada, conforme diretrizes da norma de Uso do correio eletrônico do Cade, informando sobre o desligamento do servidor ou colaborador, redirecionando as suas mensagens para o seu chefe imediato ou pessoa designada.

Parágrafo único. Após 30 dias do desligamento do servidor ou colaborador, deve-se encerrar as respostas automáticas, mantendo o redirecionamento.

Art. 22. Servidores, colaboradores e estagiários desligados do Cade devem proceder como visitantes para acessos físicos e lógicos, conforme normas de Controle de acessos físico e lógico do Cade.

Seção VI

Das Sanções e Penalidades

Art. 23. 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. 24. 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 VII

Das Disposições Finais

Art. 25. Os casos omissos serão resolvidos no âmbito da Diretoria de Administração e Planejamento.

Art. 26. 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?](http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[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 **0616606** e o código CRC **9165DDE8**.