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 407, DE 20 DE MAIO DE 2019.

Regulamenta o controle de acesso lógico 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 controle de acessos lógicos 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) administrar, gerenciar e monitorar as contas de acessos aos sistemas e serviços do Cade;

b) monitorar os acessos aos sistemas, serviços e informações afim de prevenir vazamentos, exclusão e modificações indevidas de informações;

c) apoiar a implantação dos recursos tecnológicos necessários para implementação de controles de acessos lógicos;

d) monitorar e avaliar a efetividade dos controles implementados, propondo melhorias, quando pertinente; e

e) propor novos controles de acessos lógicos considerando os aspectos operacionais.

II - à Coordenação-Geral de Gestão de Pessoas – CGESP:

a) administrar, gerenciar e monitorar o cadastro dos usuários;

b) apoiar a CGTI para a concessão adequada de acessos a informações, serviços e sistemas;

c) manter os registros de usuários atualizados; e

d) apoiar o Comitê de Segurança Institucional e a CGTI no desenvolvimento de campanhas de conscientização e sensibilização.

III - às unidades administrativas do Cade:

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

i. a CGESP e a Assessoria de Comunicação Social - Ascom devem 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 controle de acessos lógicos entre seus servidores, colaboradores e estagiários; e

b) solicitar concessões de acesso especiais.

V - aos servidores, colaboradores e estagiários do Cade:

a) zelar pelo sigilo das contas e senhas de acesso;

i. a responsabilização pelo uso de serviços, informações ou sistemas é pessoal de cada servidor, colaborador e estagiário do Cade.

b) 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 Esta norma abrange todos os servidores, colaboradores, estagiários e visitantes que necessitem da concessão de acessos lógicos às informações, serviços e sistemas do Cade.

Art. 5º Controles de acessos lógicos são implementados, monitorados e avaliados periodicamente, considerando os impactos organizacionais.

§ 1º O direito de acesso à informações, serviços e sistemas deve ser fortemente relacionado ao nível de classificação das informações do Cade.

§ 2º Critérios e requisitos para concessão de acesso devem ser estabelecidos, considerando os seguintes aspectos:

a) o estabelecimento de critérios e requisitos, levando em consideração o princípio do menor acesso, *i.e.*, “tudo é proibido a menos que expressamente permitido”;

b) a observação das necessidades de conhecimento e de uso de informações, serviços e sistemas para definição de critérios e requisitos de acessos;

c) o tratamento prioritário de acessos que dependa de aprovação especial deve ser formalizado via sistema de registro de chamados;

d) a segregação de função para o gerenciamento de acessos, assim como a atribuição da responsabilização por cada função;

e) a mudança de permissão de acesso, mediante avaliação periódica;

f) as especificidades, as necessidades e os limites operacionais considerados para a criação de controles de acesso; e

g) a responsabilização de cada usuário pelo agir e não agir, de acordo com os aspectos de segurança do Cade.

Art. 6º Os controles de acessos lógicos devem ser apoiados por procedimentos operacionais institucionalizados.

Art. 7º O acesso aos sistemas e aplicações deverá ser segregado, em consonância com a atribuição de cada usuário.

§ 1º Os chefes ocupantes de cargo ou função igual ou superior a DAS/FCPE 4 devem determinar, a partir dos critérios e requisitos de segurança, os direitos de acesso e restrições apropriadas para cada papel específico dos usuários para uso dos sistemas e aplicações ligadas aos objetivos de cada unidade operacional.

§ 2º Os chefes ocupantes de cargo ou função igual ou superior a DAS/FCPE 4 são corresponsáveis pelas ações de seus colaboradores nos acessos aos sistemas e aplicações.

§ 3º Os chefes ocupantes de cargo ou função igual ou superior a DAS/FCPE 4 são corresponsáveis pelas ações realizadas por meio de acesso aos sistemas e aplicações que tiverem autorizado.

Art. 8º É responsabilidade dos chefes ocupantes de cargo ou função igual ou superior a DAS/FCPE 4 a verificação do nível de exequibilidade e efetividade de todos os controles de acessos lógicos que tiver solicitado.

Art. 9º O acesso a sistemas e aplicações deverá ser avaliado e autorizado pela CGTI.

Seção III

Do Gerenciamento de Usuários e Acessos

Art. 10. Cada usuário terá uma conta única que dará acesso aos diversos serviços e sistemas do Cade.

Art. 11. A criação de contas de usuários deve seguir as diretrizes da norma de Contratação, permanência e desligamento de pessoas do Cade.

§ 1º O padrão e-ping deverá ser utilizado como referência para criação das contas, as quais devem usar o prenome.últimosobrenome, conforme demonstrado no exemplo do usuário Luiz Carlos Fraga da Silva, a conta criada será luiz.silva.

§ 2º Para os casos de existir um usuário homônimo previamente cadastrado, um usuário conhecido no seu meio social, inclusive profissional, pelo nome composto ou por outro sobrenome que não seja o definido pela regra padrão e, quando da utilização de nome social, é possível a alteração do padrão.

Art. 12. A assinatura de e-mail deverá respeitar o disposto na norma de Uso de correio eletrônico no Cade.

Parágrafo único. Colaboradores terceirizados utilizarão assinatura de sua respectiva empresa, salvo equipe de secretariado.

Art. 13. A política de senhas obedecerá aos seguintes critérios:

§ 1º A senha deverá ser “forte” (suficientemente segura), atendendo os seguintes requisitos:

a) deve ter no mínimo 10 caracteres;

b) a senha deve conter pelo menos 3 dos 4 tipos de caracteres seguintes: letras maiúsculas, minúsculas, números e/ou caracteres especiais (!, @, #, $, %,=, +, ...);

c) não deve ser o próprio nome, partes dele ou a matrícula;

d) não deve ser registrada em papel;

e) deve ser fácil de lembrar, e difícil de ser adivinhada; e

f) deve evitar:

i. nome de membros de sua família ou de amigos íntimos;

ii. nomes de pessoas ou lugares em geral;

iii. nome do sistema operacional ou da máquina que está sendo utilizada;

iv. nomes próprios;

v. datas;

vi. números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;

vii. placas ou marcas de carros;

viii. palavras que constam de dicionários em qualquer idioma;

ix. letras seguidas do teclado do computador (ASDFG, YUIOP); e

x. objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela).

§ 2º A senha deverá ser trocada periodicamente, ou sempre que existir risco de comprometimento de sua confidencialidade.

a) a cada 120 (cento e vinte) dias o sistema solicitará a troca obrigatoriamente, com emissão de alertas diários prévios; e

b) a nova senha deverá ser diferente das últimas 3 senhas já cadastradas pelo usuário.

Art. 14. O desbloqueio de contas e reset de senhas seguirá os seguintes critérios:

I - o bloqueio da senha de acesso ocorrerá, automaticamente, quando identificada 3 (três) tentativas frustradas seguidas de acesso;

II - o desbloqueio deverá ser efetuado após a abertura de chamado para a Central de Serviços ou ferramenta específica; e

III - em caso de esquecimento de senhas, o usuário deverá solicitar nova senha através do portal de troca de senhas do Cade.

Parágrafo único. Caso o portal de troca de senhas não esteja disponível, nova senha temporária será enviada para o e-mail secundário cadastrado na intranet, mediante solicitação por meio de chamado na Central de Serviços.

Art. 15. Na retirada de acessos por encerramento de atividades, a CGTI impedirá o acesso do servidor, colaborador ou estagiário ao ambiente, mantendo suas informações por um período mínimo de 60 meses.

Art. 16. Contas inativas por mais de um ano serão excluídas pela CGTI.

Seção IV

Da Concessão de Acessos e Serviços de Rede

Art. 17. Um perfil mínimo deve ser estabelecido (Mapa de recursos mínimos), a fim de criar perímetros de segurança para acesso de arquivos, sistemas e todo e qualquer ambiente de tecnologia.

Art. 18. Os acessos adicionais deverão ser solicitados pelo chefe imediato para a CGTI, via sistema de registro de chamados.

Parágrafo único. O chefe imediato é corresponsável pelos impactos causados pela concessão de acessos por parte de servidores, estagiários e colaboradores.

Art. 19. Acessos remotos aos sistemas e serviços serão realizados mediante a utilização de fatores múltiplos de autenticação.

Art. 20. O acesso à rede corporativa e sistemas internos do Cade está restrito aos servidores, colaboradores e estagiários.

§ 1º A rede local cabeada é exclusiva para a utilização de computadores patrimoniados pelo Cade.

§ 2º O acesso será concedido após a data de contratação ou de entrada em exercício no Cade, conforme norma de Contratação, permanência e desligamento de pessoas do Cade.

§ 3º O desligamento do servidor, colaborador ou estagiário resultará na revogação de seu acesso.

§ 4º Acessos externos só serão permitidos por meio de canal de comunicação segura.

§ 5º O uso da rede WiFi Cade_Servidores é restrito a servidores, colaboradores e estagiários.

Art. 21. O acesso à rede WiFi para visitantes será concedido mediante solicitação de senha de acesso no ato de seu credenciamento e identificação.

§ 1º A rede Cade_Visitantes dará acesso restrito para uso da internet, sendo vedado o uso de serviços internos.

§ 2º A senha de acesso terá validade de 12 meses a partir de sua criação.

§ 3º A senha será bloqueada após 90 dias sem uso. Em caso de bloqueio, o visitante, caso necessário, deverá solicitar o desbloqueio da senha de acesso.

Art. 22. A CGTI deverá monitorar e auditar periodicamente os acessos aos sistemas e aplicações do Cade.

§ 1º O sistema de monitoramento de acessos deverá permitir a identificação e rastreabilidade dos endereços de origem e destino, os usuários e os serviços utilizados, emitindo alertas para casos de uso ou comportamento indevidos e gravando os logs para posterior auditoria.

§ 2º Todos os acessos devem ser registados de forma a permitir a rastreabilidade e a identificação do usuário pelo período mínimo de 3 anos.

Seção V

Das Sanções e Penalidades

Art. 23. O servidor, colaborador ou estagiário que não zelar pela implementação e execução das diretrizes descritas nesse normativo será responsabilizado 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 VI

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?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0616609** e o código CRC **8828C0A6**.

Referência: Processo nº 08700.000342/2014-58 SEI nº 0616609