MINISTÉRIO DA FAZENDA
Conselho Administrativo de Recursos Fiscais

PORTARIA CARF Nº 103, DE 14 JULHO DE 2016.

Dispõe sobre a Política de Segurança da Informação e Comunicações no âmbito do Conselho Administrativo de Recursos Fiscais.

O PRESIDENTE DO CONSELHO ADMINISTRATIVO DE RECURSOS FISCAIS, no uso da atribuição que lhe confere o inciso IV do art. 3º do Anexo I do Regimento Interno do Conselho Administrativo de Recursos Fiscais, aprovado pela Portaria MF nº. 343, de 09 de junho de 2015, **RESOLVE:**

Art. 1º Instituir, na esfera do Conselho Administrativo de Recursos Fiscais (CARF) a Política de Segurança da Informação e Comunicações (POSIC-CARF); com o objetivo de estabelecer princípios, diretrizes, responsabilidades e competências para implementar a Gestão da Segurança da Informação e Comunicações (SIC); visando assegurar a autenticidade, confidencialidade, integridade e disponibilidade da informação, bem como a conformidade, padronização e normatização das atividades relacionadas aos ativos de informação.

Parágrafo único. Deve ser observada, nas ações decorrentes da POSIC-CARF, a conformidade com a Política de Segurança da Informação e Comunicações estabelecidas pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR) pela Norma Complementar nº. 03/IN01/DSIC/GS1PR de 30 de junho de 2009.

Capítulo I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2ºA Política de Segurança da Informação e Comunicações aplica-se no âmbito interno do CARF e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas.

Art. 3º Para efeito desta Portaria entende-se por:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

II - agente público: todo aquele que exerce, ainda que transitoriamente, com ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal (APF) direta e indireta;

III - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

IV - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles tem acesso;

V - capacitação em SIC: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema;

VI - conformidade em SIC: cumprimento da legislação, normas e procedimentos relacionados à SIC da organização;

VII - conscientização em SIC: atividade que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar na instituição como Gestores de SIC;

VIII - credenciais ou contas de acesso: permissões concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso, podendo tal permissão ser física como crachá, cartão ou lógica como identificação de usuário e senha;

IX - desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período do tempo superior ao tempo objetivo de recuperação;

X - incidente: evento que tenha causado algum dano, colocado em risco ou interrompido execução de atividade de algum ativo de informação por um período de tempo inferior ao tempo necessário de recuperação;

XI - risco de SIC: potencial associado à probabilidade de exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto para a organização;

XII - sensibilização em SIC: atividade de ensino que tem como objetivo orientar sobre o que é Segurança da Informação e Comunicações (SIC) fazendo com que os participantes possam perceber em sua rotina pessoal e profissional ações que precisam ser corrigidas;

XIII - termo de responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que acessar, bem como assumir responsabilidades decorrentes de tal acesso;

XIV - o usuário: conselheiros, servidores, terceirizados, especialistas, estagiários e consultores que detenham autorização do responsável pela área interessada para acesso aos ativos da informação de um órgão ou entidade da APF formalizada por meio da assinatura de Termo de Responsabilidade;

XV - valor do ativo de informação: valor tangível e intangível que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado; e

XVI - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Capitulo II

DOS PRINCÍPIOS

Art. 4º São considerados princípios da SIC a serem observados por todos os agentes públicos, usuários, corpo técnico e gerencial:

I - confidencialidade: o princípio de segurança que trata da garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

II - integridade: o princípio de segurança que trata da salvaguarda da exatidão e confiabilidade da informação e dos métodos de processamento;

III - disponibilidade: o princípio de segurança que trata da garantia de que pessoas autorizadas obtenham acesso à informação e aos recursos correspondentes, sempre que necessário;

IV - autenticidade: o princípio de segurança que trata da garantia de que a informação foi produzida, expedida, modificada ou descartada por uma determinada pessoa física, órgão, entidade ou sistema..

Parágrafo único. A informação é um ativo que, como qualquer outro ativo necessário às atividades laborais, tem valor para a organização e consequentemente necessita ser adequadamente protegido.

Art. 5º As ações relacionadas à implementação e consolidação da POSIC-CARF são norteadas pelos seguintes princípios:

I - celeridade: as ações de SIC devem oferecer respostas rápidas;

II - clareza: as regras de SIC devem ser precisas e de fácil entendimento;

III - efetividade: as ações envolvendo a POSIC-CARF devem ser eficientes e eficazes quanto aos objetivos de SIC;

IV - ética: os direitos e interesses legítimos dos agentes públicos devem ser preservados, sem comprometimento da SIC;

V - interoperabilidade: deve haver esforço continuo para assegurar que sistemas sejam gerenciados e direcionados para maximizar oportunidades de troca e reuso de informações, interna e externamente, respeitando os princípios de SIC;

VI - responsabilidade: os agentes públicos devem conhecer e respeitar as normas de SIC, utilizando corretamente os ativos sob sua responsabilidade, monitorando e reportando o eventual uso indevido para que ações cabíveis sejam tomadas.

Parágrafo único. São também aplicáveis às ações mencionadas no **caput,** os princípios constitucionais e legais atinentes à Administração Pública.

Capitulo III

DAS DIRETRIZES

Art. 6º As diretrizes constituem os principais pilares da Gestão de SIC, norteando a elaboração de normas supervenientes no âmbito do CARF.

Art. 7º Procedimentos próprios de tratamento da informação corporativa deverão ser fixados em norma complementar, considerando-se as seguintes diretrizes gerais:

I - tratamento da informação: a informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades do CARF;

II - tratamento de Incidentes de Rede: os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes documentados e comunicados;

III - gestão de risco: devem ser identificados e implementadas as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, considerando, prioritariamente, os objetivos estratégicos do CARF e de forma continua;

IV - gestão de continuidade: compreende o processo permanente destinado a preparar o CARF a resistir aos efeitos de emergências ou interrupções e minimizar os danos operacionais, legais, financeiros e à imagem da instituição.

V - auditoria: o uso de recursos computacionais e de informações disponibilizadas pelo CARF deve ser monitorado, respeitando os princípios legais;

VI - conformidade: conjunto de medidas disciplinares que será estabelecido para fazer cumprir as normas legais e regulamentares, as diretrizes, a POSIC, as normas internas e os procedimentos estabelecidos para as atividades do CARF, bem como evitar, detectar e tratar qualquer desvio que possa ocorrer;

VII - controles de acesso: as regras de controle de acesso a todo sistema corporativo, Intranet, Internet, Informações, dados e às instalações do CARF deverão ser definidas e regulamentadas pelo Serviço de Tecnologia da Informação (SEINF) do CARF;

VIII - correio eletrônico: as regras de acesso e utilização de correio eletrônico (e-mail) serão fixadas em norma específica, a ser elaborada pelo SEINF, em conformidade com esta POSIC e demais orientações e diretrizes do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR);

IX - acesso a internet: o acesso a Internet, no ambiente de trabalho da será regido por norma especifico, a ser elaborada pela Coordenação correspondente, em conformidade com esta POSIC e demais orientações e diretrizes governamentais.

§1º Para cumprimento do disposto no inciso V deste artigo, o Serviço de Tecnologia da Informação (SEINF) deve manter registros e procedimentos, como trilhas de auditória e outros que assegurem a conformidade por meio do rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos e da rede computacional interna.

§2º A iniciativa para a edição de normas complementares relativas à Segurança da Informação e Comunicação será de cada unidade pertencente à estrutura administrativa do CARF, no limite de suas atribuições estabelecido no Regimento Interno da CARF.

Capítulo IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 8º A POSIC-CARF compreende os seguintes papéis:

I – Gestor de Segurança da Informação e Comunicações com as seguintes responsabilidades:

a) promover cultura de segurança da informação e comunicações;

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor recursos necessários às ações de segurança da informação e comunicações;

d) coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

e) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

f) manter contato permanente e estreito com o Programa de Modernização Integrada do Ministério da Fazenda (PMIMF) para o trato de assuntos relativos à segurança da informação e comunicações;

g) propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da Administração Pública Federal (APF).

II - Comitê de Gestão da Tecnologia de Informação com as seguintes responsabilidades:

a) assessorar na implementação e consolidação das ações de SIC;

b) propor a constituição de equipes de trabalho para tratar de temas e propor soluções específicas sobre SIC.

c) propor normas e procedimentos relativos a SIC no âmbito do CARF inclusive alterações.

III – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do CARF:

a) receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Parágrafo único. Caberá a cada membro do Comitê de Gestão da Tecnologia da Informação incluir em pauta as questões de Segurança da Informação e Comunicações relativas à sua unidade de origem.

Art. 9º. Todo usuário é responsável pela segurança dos ativos, credenciais ou contas de acesso, e processos que estejam sob sua responsabilidade e por todos os atos executados com sua identificação.

Art. 10. É vedada, e considerada prática grave, a exploração de falhas ou vulnerabilidades porventura existentes nos ativos de informação do CARF.

DAS PENALIDADES

Art. 11. As ações que violem esta POSIC-CARF ou os controles determinados em normas específicas caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

DAS DISPOSIÇÕES FINAIS

Art. 12. Os contratos de prestação de serviços e convênios celebrados a partir da data de publicação desta portaria, devem contemplar, no que couber, as orientações desta POSIC-CARF.

Art. 13. A POSIC-CARF bem como todos os instrumentos normativos gerados a partir dela, deve ser revisada, sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal, havendo necessidade de atualização obrigatória após o decurso do prazo de três anos.

Art. 14. Esta Portaria entra em vigor na data de sua publicação.

CARLOS ALBERTO FREITAS BARRETO