RESOLUÇÃO CRC/PI N.º 564, DE 27 DE JANEIRO DE 2023.

Institui a Política de Segurança em Recursos Humanos.

A **PRESIDENTE DO CONSELHO REGIONAL DE CONTABILIDADE DO PIAUÍ**, no uso de suas atribuições legais e regimentais em vigor,

Considerando o Decreto n.º 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

Considerando o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

Considerando as normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança – Segurança em recursos humanos;

Considerando que o Plano Diretor de Tecnologia da Informação (PDTI) 2022-2023 do Conselho Regional de Contabilidade do Piauí estabelece o objetivo estratégico de "Garantir que o acesso, o tratamento e o armazenamento de informações do Conselho Regional de Contabilidade do Piauí ocorram em conformidade com políticas e normas que assegurem a confidencialidade e a integridade das informações";

Considerando a Resolução CRC/PI n.º 561/2023, que dispõe sobre a Política de Segurança da Informação do CRC/PI;

Considerando a necessidade de estabelecer princípios e diretrizes de segurança da informação para a validação dos sistemas desenvolvidos, mantidos, adquiridos ou em produção, resolve:

CAPÍTULO I

DA INSTITUIÇÃO, DO OBJETIVO E DA APLICAÇÃO

Art. 1º Fica instituída a Política de Segurança em Recursos Humanos no âmbito do Conselho Regional de Contabilidade do Piauí.

Art. 2º Esta Política tem por objetivo assegurar que os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários:

I – compreendam suas responsabilidades com relação ao cumprimento da Política de Segurança da Informação do CRC/PI;

II – estejam conscientes das ameaças relativas à segurança da informação do CRC/PI;

III – estejam aptos a apoiar a Política de Segurança da Informação do CRC/PI;

IV – denunciem os usuários que descumprirem a Política de Segurança da Informação do CRC/PI.

Art. 3º A Política de Segurança em Recursos Humanos é o documento que estabelece princípios, conceitos, diretrizes e define os papéis e as responsabilidades que devem ser observadas na seleção e contratação de pessoal, conscientização, no processo de educação e treinamento em segurança da informação e na instauração de processo administrativo disciplinar, naquilo que for cabível.

Art. 4º Esta norma se aplica a todos os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários.

Art. 5º Esta norma não substitui a Política de Gestão de Pessoas adotada pelo CRC/PI, mas a complementa quanto aos aspectos de segurança da informação.

Art. 6º A elaboração e atualização deste documento são de responsabilidade do Comitê de Segurança da Informação.

CAPÍTULO II
DOS TERMOS E DAS DEFINIÇÕES

Art. 7º Para os efeitos desta Política são estabelecidos os seguintes conceitos e definições:

I – Ameaça: qualquer circunstância ou evento com o potencial de causar incidente indesejado que pode resultar em dano para um sistema ou instituição;

II – Análise de Risco: uso sistemático de informações de identificação de fontes para estimar o risco;

III – Atividade: ação ou conjunto de ações executadas por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

IV – Ativos de informação: qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRC/PI, assim como também os locais onde se encontram estes dispositivos, gestão do pessoal que a eles possuem acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

V – Colaboradores: são todos os empregados, aprendizes, estagiários e os profissionais contratados em cargos em comissão de livre nomeação e exoneração;

VI – Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

VII – Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado;

VIII – Integridade: propriedade de salvaguarda da exatidão e completeza das informações contra alterações, intencionais ou acidentais, em seu estado e atividades;

IX – Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

X – Sigilo: segredo de conhecimento restrito a pessoas credenciadas, proteção contra revelação não autorizada;

XI – Sistema de informação: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando aperfeiçoar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação;

XII – Usuários: os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários que acessam ou utilizam informações custodiadas ou de propriedade do CRC/PI.

CAPÍTULO III
DAS DIRETRIZES

Art. 8º Para assegurar que os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários entendam as suas responsabilidades, visando preservar a segurança da informação, serão observadas as seguintes diretrizes e procedimentos:

I – disponibilizar as políticas, normas e procedimentos de segurança da informação do CRC/PI antes da nomeação e contratação de empregados, estagiários, aprendizes e profissionais em cargos em comissão;

II – manter, continuamente, ampla divulgação das políticas, normas e procedimentos de segurança da informação do CRC/PI para assegurar que todos os usuários estejam conscientes das ameaças e das suas responsabilidades para preservar a segurança da informação;

III – realizar treinamentos e atualizações periódicas sobre a segurança da informação para os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários;

IV – comunicar área responsável pela Gestão de TI todas as contratações, desligamentos, transferências e modificações no quadro de pessoal efetivo do CRC/PI, bem como contratações e desligamentos/términos de contratos de aprendizes e estagiários e contratações/exonerações de ocupantes de cargos em comissão de livre nomeação e exoneração;

V – garantir que os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários assinem o Termo de Ciência da Política de Segurança da Informação no processo de integração;

VI – manter atualizados e arquivados os Termos de Responsabilidade da Política de Segurança da Informação;

VII – desenvolver campanha de conscientização para promoção de mudanças de comportamento e, também, de cultura, de modo a se estabelecer a necessidade da segurança da informação;

VIII – avaliar, periodicamente, o nível de maturidade do CRC/PI nos aspectos relacionados à segurança da informação;

IX – instaurar processo administrativo disciplinar para apuração de responsabilidades e aplicação das sanções previstas em regulamentações internas e legislação em vigor, em caso de descumprimento ou violação, pelo usuário, das regras previstas nas políticas, normas e procedimentos de segurança da informação do CRC/PI.

CAPÍTULO IV
DOS PROCEDIMENTOS E DAS RESPONSABILIDADES

Art. 9º Este capítulo define os responsáveis e um conjunto de procedimentos que deverão ser seguidos para garantir a segurança da informação do CRC/PI.

Art.10. Cabe ao **Departamento de Gestão de Pessoas**:

I – incluir, no edital do concurso público para seleção e contratação de empregados, a fim de preencher o quadro próprio de pessoal, em observância aos Princípios de Legalidade, Impessoalidade, Moralidade e Publicidade constantes no Art. 37 da Constituição Federal:

a) obrigatoriedade de entrega do Termo de Responsabilidade com a Política de Segurança da Informação (Anexo I), no item que trata dos requisitos para investidura no cargo.

II – recepcionar, do candidato habilitado no concurso e convocado para preenchimento de cargo no CRC/PI, juntamente com os documentos para formalização da contratação, o Termo de Responsabilidade com a Política de Segurança da Informação (Anexo I), que deve ser arquivado nos autos funcionais;

III – disponibilizar, para análise e ciência, a Política de Segurança da Informação ao estudante ou profissional selecionado, respectivamente, para ocupar a vaga de estagiário ou aprendiz ou de cargo comissionado de livre nomeação e exoneração;

IV – recepcionar, do estudante ou profissional selecionado, respectivamente, para ocupar a vaga de estagiário ou aprendiz ou de cargo comissionado de livre nomeação e exoneração, juntamente com os documentos para formalização da contratação, o Termo de Responsabilidade com a Política de Segurança da Informação (Anexo I), que deve ser arquivado nos autos funcionais;

V – atualizar, a cada dois anos, mediante assinatura por todos os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários do Termo de Responsabilidade com a Política de Segurança da Informação, ou sempre que houver atualização do normativo, e arquivar nos autos funcionais;

VI – elaborar, implantar e divulgar o Plano Anual de Treinamento de Tecnologia da Informação, em conjunto com a área de TI, para desenvolver as competências gerenciais e técnicas necessárias à operacionalização da governança, gestão e atualização tecnológica;

VII – inserir, no Plano Anual de Treinamento, a realização de evento de capacitação para atualização regular das políticas e procedimentos relacionados à segurança da informação a todos os usuários;

VIII – instruir o processo de contratação e/ou de realização dos eventos de capacitação sobre segurança da informação:

a) efetuar a inscrição dos participantes no evento de capacitação;

b) divulgar e convocar os colaboradores a participar do evento de capacitação;

c) acompanhar a realização do evento de capacitação.

IX – realizar treinamento de integração para todos os novos contratados, em até 30 (trinta) dias do início da admissão, para orientar sobre as políticas, normas e procedimentos de segurança da informação do CRC/PI;

X – pesquisar, no mercado, a oferta de cursos e eventos sobre segurança da informação, solicitar proposta de preços e submeter ao Comitê de Segurança da Informação para análise e definição de contratação;

XI – comunicar ao responsável pelo setor de TI sempre que ocorrerem admissões, desligamentos ou remanejamentos de empregados, aprendizes ou estagiários;

XII – recepcionar as representações de denúncias a quaisquer violações a esta Política e a políticas, normas e procedimentos de segurança da informação e providenciar a instrução do processo administrativo disciplinar para apuração das responsabilidades, com base nos normativos internos que tratam da matéria.

Art. 11. Cabe ao Comitê de Segurança da Informação:

I – avaliar o nível de maturidade dos usuários do CRC/PI nos aspectos relacionados à segurança da informação:

a) elaborar os quesitos que deverão compor a pesquisa de comportamento dos usuários quanto à segurança da informação;

b) formatar a pesquisa com as orientações para preenchimento;

c) encaminhar a pesquisa ao responsável pelo setor de Tecnologia da Informação, para aplicação aos usuários;

d) avaliar o resultado da pesquisa de comportamento dos usuários quanto à segurança da informação e apresentar proposição de melhoria das políticas, normativos e procedimentos.

II – analisar as propostas de cursos e eventos sobre segurança da informação, definir a realização do treinamento e submetê-las ao Departamento de Gestão de Pessoas para instrução do processo de contratação e/ou execução;

III – analisar e aprovar o projeto da campanha para divulgação, sensibilização e conscientização das políticas, normas e procedimentos de segurança da informação e submetê-lo ao Comitê de Segurança da Informação para aprovação;

IV – analisar a efetividade das ações implementadas voltadas ao estabelecimento da cultura e ampliação do nível de maturidade da segurança da informação;

V – analisar as proposições apresentadas pelos usuários para alteração das políticas, normas ou procedimentos relacionados à segurança da informação;

VI – impedir a execução operacional de uma atividade crítica, exclusivamente, por único empregado;

VII – prestar esclarecimento imediato aos usuários sobre dúvidas relacionadas à política, às normas e aos procedimentos de segurança da informação.

Art. 12. Cabe ao Responsável pelo Setor de Tecnologia da Informação:

I – divulgar, aplicar, tabular e apresentar o resultado da pesquisa, elaborada pelo Comitê de Segurança da Informação, para aferir o nível de maturidade dos usuários do CRC/PI nos aspectos relacionados à segurança da informação:

a) divulgar e orientar os usuários sobre os procedimentos para preenchimento da pesquisa de comportamento dos usuários quanto à segurança da informação;

b) aplicar a pesquisa de comportamento dos usuários quanto à segurança da informação, aprovada pelo Comitê de Segurança da Informação;

c) tabular a pesquisa e apresentar o resultado ao Comitê de Segurança da Informação para proposição de melhoria.

II – identificar a necessidade e propor a contratação de novos cursos aos empregados lotados na Coordenadoria de Gestão de TI para manter o alto nível de maturidade em segurança da informação;

III – desativar e/ou liberar acessos aos sistemas e equipamentos, conforme previstos nas políticas e nos procedimentos relacionados à segurança da informação, sempre que houver admissão, desligamento ou remanejamento de empregado, estagiário ou aprendiz;

IV – vedar o uso de credenciais de terceiros, que não sejam empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários, para acessar computadores, sistemas, internet, intranet, correio eletrônico e a rede do CRC/PI, para o desempenho de qualquer tipo de atividade;

V – prestar esclarecimento imediato aos usuários sobre dúvidas relacionadas à política, às normas e aos procedimentos de segurança da informação.

Art. 13. Cabe à Assessoria de Comunicação do CRC/PI:

I – desenvolver o projeto da campanha para divulgação, sensibilização e conscientização das políticas, normas e dos procedimentos de segurança da informação e submeter ao Comitê de Segurança da Informação para aprovação:

a) o projeto da campanha deverá ser elaborado anualmente para execução durante o ano em curso;

b) a campanha deve incentivar e engajar os usuários para a prática da segurança da informação em suas atividades;

c) a campanha deve contemplar a conscientização dos usuários quanto às ameaças externas, tais como vírus, interceptação de mensagens e dados, grampos, fraudes e tentativas que ensejam o roubo de senhas e que possam afetar ou ameaçar a segurança das informações do CRC/PI;

d) a campanha deve abordar as penalidades em caso de descumprimento das políticas, normas e procedimentos de segurança da informação;

e) incluir na campanha o Dia da Segurança da Informação no CRC/PI;

f) executar a campanha de divulgação das políticas, normas e procedimentos de segurança da informação aprovada pelo Comitê de Segurança da Informação.

Art. 14. Cabe aos gestores das Unidades Organizacionais (Uos):

I – ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;

II – cumprir e fazer cumprir esta Política e demais políticas, normas e procedimentos de segurança da informação;

III – desenvolver e difundir uma mentalidade de segurança institucional, fazendo com que os colaboradores sob sua gestão compreendam as necessidades das medidas adotadas e incorporem o conceito de que todos são responsáveis por garantir a segurança da informação;

IV – prestar esclarecimento imediato aos colaboradores sob sua gestão sobre dúvidas relacionadas à política, às normas e aos procedimentos de segurança da informação;

V – adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender à política de segurança da informação e aos demais normativos correlatos;

VI – autorizar o acesso e definir o perfil e a mudança de perfil do usuário junto ao Responsável pelo Setor de TI;

VII – propor melhorias e alterações nas políticas, normas e nos procedimentos de segurança da informação;

VIII – identificar a necessidade e propor ao Departamento de Gestão de Pessoas a contratação de novos cursos para os empregados sob sua gestão, visando manter o alto nível de maturidade em segurança da informação;

IX – intercambiar com as demais Uos e os empregados sob sua gestão informações necessários à produção de conhecimentos relacionados com as atividades de segurança da informação;

X – acompanhar, permanentemente, os cenários de interesse do CRC/PI no que se refere à segurança da informação do Conselho, de modo a proporcionar suporte adequado ao desenho das funções da instituição;

XI – relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento e presença de vírus;

XII – relatar para seu superior hierárquico e ao Responsável pelo Setor de TI o surgimento da necessidade de um novo software para o desenvolvimento de suas atividades;

XIII – denunciar ao Departamento de Gestão de Pessoas, ainda que por mera suspeita, qualquer usuário que violar esta Política e demais políticas, normas e procedimentos de segurança da informação;

XIV – desenvolver outras atividades correlatas visando à efetiva segurança da informação.

Art. 15. Cabe aos empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários:

I – cumprir as políticas, normas e procedimentos que tratem da segurança da informação;

II – tomar ciência e conhecimento de todo material referente à segurança da informação disponibilizado pelo CRC/PI;

III – firmar, obrigatoriamente, o Termo de Responsabilidade com a Política de Segurança da Informação e demais políticas, normas e procedimentos do CRC/PI;

IV – estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes sobre a segurança da informação do CRC/PI;

V – adquirir conhecimento necessário para a correta utilização dos recursos relacionados à segurança da informação;

VI – solicitar esclarecimentos à chefia imediata ou ao Responsável pelo Setor de TI sempre que houver dúvidas acerca das políticas, normas e procedimentos de segurança da informação;

VII – participar, sempre que convocado pelo CRC/PI, de campanhas, eventos, cursos ou atualizações relacionadas à Segurança da Informação do CRC/PI;

VIII – proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizadas, conforme disposto nas políticas internas do CRC/PI;

IX – atuar de forma responsável, pessoal e intransferível, na utilização dos recursos, tecnológicos ou não, disponibilizados pelo CRC/PI para o desempenho de suas atividades na prestação de serviços para o Conselho;

X – adotar a prática de não abordagem e não discussão em ambientes públicos e áreas expostas sobre assuntos relacionados ao trabalho;

XI – denunciar ao gestor imediato ou ao Departamento de Gestão de Pessoas ou ao Responsável pelo Setor de TI ou ao Comitê de Segurança da Informação, quaisquer eventos ou incidentes potenciais ou reais que causem riscos à segurança da informação, ou ainda sua mera suspeita;

XII – relatar ao Responsável pelo Setor de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento ou presença de vírus;

XIII – relatar ao gestor imediato e ao responsável pelo Setor de TI o surgimento da necessidade de nova ferramenta ou software para o desenvolvimento de suas atividades;

XIV – denunciar ao Departamento de Gestão de Pessoas quaisquer usuários que violarem esta Política e as políticas, normas e procedimentos de segurança da informação, ainda que mera suspeita;

XV – apresentar ao gestor imediato ou responsável pelo Setor de TI ou ao Comitê de Segurança da Informação sugestões de melhorias para as políticas, normas e procedimentos de segurança da informação;

XVI – responder pelo prejuízo ou dano que vier a provocar ao CRC/PI ou a terceiros, em decorrência da não obediência às diretrizes e normas;

XVII – atuar de forma responsável, pessoal e intransferível, pelo sigilo, privacidade e uso de senhas de acesso aos recursos computacionais, não podendo estas ser compartilhadas, divulgadas, anotadas em papel ou em sistema visível ou de acesso não protegido:

a) as senhas utilizadas para acesso aos recursos são pessoais, intransferíveis e devem ser escolhidas atendendo às melhores práticas definidas na Política de Controle de Acesso Lógico do Conselho Regional de Contabilidade do Piauí;

b) troca imediata das senhas, nos casos de perda de sigilo ou mesmo suspeita.

XVIII – utilizar crachá de identificação durante a permanência nas dependências do CRC/PI, caso determinado;

XIX – acompanhar toda e qualquer manutenção preventiva ou corretiva realizada em equipamentos sob sua responsabilidade;

XX – desenvolver outras atividades correlatas visando à efetiva segurança da informação.

Art. 16. É vedado aos empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários:

I – conectar na rede do CRC/PI equipamentos não autorizados;

II – abrir ou executar arquivos de origem desconhecida;

III – acessar informação institucional que não seja explicitamente autorizado;

IV – transportar informações confidenciais do CRC/PI sem as devidas autorizações e proteções e em qualquer meio, como CD, DVD, HD, pen drive, compartilhamento em nuvem, papel, entre outros;

V – alterar normas padronizadas dos ativos;

VI – acessar e divulgar informações que contenham material obsceno, apologia ao fanatismo, práticas religiosas, político-partidário, qualquer forma de discriminação ou material que, explícita ou implicitamente, se refira à conduta imoral;

VII – fazer cópias de materiais da internet, inclusive desenhos, artigos, gráficos e fotografias, sem autorização do proprietário ou citação da fonte;

VIII – alimentar-se próximo aos servidores de rede, equipamentos e estações de trabalho;

IX – fazer cópia não autorizada de softwares adquiridos ou desenvolvidos pelo CRC/PI;

X – instalar e/ou desabilitar qualquer ferramenta ou aplicativo nos recursos tecnológicos de propriedade do CRC/PI sem a expressa autorização do responsável pelo Setor de TI;

XI – Utilizar sistemas e aplicativos instalados localmente ou que funcionem de forma on-line através da internet que não tenham sido expressamente autorizados ou disponibilizados pelo responsável pelo Setor de TI;

XII – utilizar recursos tecnológicos fornecidos pelo CRC/PI para fins particulares.

CAPÍTULO V
DAS VIOLAÇÕES E SANÇÕES

Art. 17. O não cumprimento desta Política e/ou das demais políticas, normas e procedimentos de segurança da informação constitui falta grave, e os empregados ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários estarão sujeitos a penalidades definidas no Manual de Políticas de Gestão de Pessoas e nos normativos que tratam do processo administrativo disciplinar, podendo acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, assegurando aos envolvidos o contraditório e a ampla defesa.

Art.18. O não cumprimento desta Política e/ou das demais políticas, normas e procedimentos de segurança da informação poderá implicar:

I - a exoneração do cargo em comissão;

II - a rescisão antecipada do contrato de aprendizagem por motivo de dispensa por justa causa do aprendiz, depois das devidas apurações dos fatos; e

III - o término antecipado do contrato de estágio, bem como, nos termos da legislação aplicável, sanções civis e penais e eventuais ressarcimentos por danos causados ao CRC/PI.

Art. 19. Além das sanções, caso o gestor entenda necessário e viável, poderá aplicar aos empregados, ocupantes de cargos efetivos, ocupantes de cargos em comissão de livre nomeação e exoneração, aprendizes e estagiários uma medida educativa, que consistirá na realização de cursos, workshops e treinamentos, que serão disponibilizados pelo CRC/PI.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 20. Os casos omissos desta Política serão resolvidos pelo Comitê de Segurança da Informação do CRC/PI.

Art. 21. A presente resolução entra em vigor na data de sua assinatura.

ADRIANA DE ALMEIDA PAULA DA GRACA:70556547349

Assinado digitalmente por ADRIANA DE ALMEIDA PAULA DA GRACA:70556547349
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A3, OU=(EM BRANCO), OU=22949096000171, OU=presencial, CN=ADRIANA DE ALMEIDA PAULA DA GRACA:70556547349
Razão: Eu concordo com os termos definidos por minha assinatura neste documento
Localização: sua localização de assinatura aqui
Data: 2023-02-06 11:31:22
Foxit Reader Versão: 9.5.0

Contadora Adriana de Almeida Paula da Graça

Presidente do CRC/PI

Aprovada na 906ª Reunião Plenária do CRC/PI, realizada em 27 de janeiro de 2023.