RESOLUÇÃO CRCPE N.º 398, DE 27 DE OUTUBRO DE 2022.

Aprova a Política de Segurança da Informação (PSI) do Conselho Regional de Contabilidade em Pernambuco (CRCPE) e dá outras providências

O CONSELHO REGIONAL DE CONTABILIDADE EM PERNAMBUCO, no exercício de suas atribuições legais e regimentais,

Considerando a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico e não digital controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à classe contábil e à sociedade, com integridade, confidencialidade e disponibilidade;

Considerando que o Conselho Regional de Contabilidade em Pernambuco (CRCPE) recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado;

Considerando que as informações no CRCPE são armazenadas em diversas formas e veiculadas em diferentes meios físicos e eletrônicos, sendo, portanto, vulneráveis a incidentes, como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

Considerando o número progressivo de incidentes cibernéticos, no ambiente da rede mundial de computadores, e a necessidade de processos de trabalho orientados para a boa gestão da segurança a informação;

Considerando a Lei Federal n.º 13.709 (Lei Geral de Proteção de Dados Pessoais - LGPD), de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural";

Considerando o Decreto n.º 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, em especial, o inciso II do artigo 15;

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

Considerando a Instrução Normativa n.º 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Considerando as boas práticas preconizadas pelas normas ABNT NBR ISO/IEC, série 27000, e outras normas nacionais e internacionais relativas à Segurança da Informação;

Considerando a necessidade de estabelecer responsabilidades internas quanto à Segurança da Informação;

Considerando a Portaria CRCPE n.º 134, de 28 de julho de 2022, que cria o Comitê de Segurança da Informação (CSI) do Conselho Regional de Contabilidade em Pernambuco,

R E S O L V E:

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) no âmbito do Conselho Regional de Contabilidade em Pernambuco, nos termos do Anexo desta Resolução.

Paragrafo único. Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação do Conselho Regional de Contabilidade são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos.

Art. 2º A Política de Segurança da Informação se aplica a todos os conselheiros, funcionários, estagiários, menores aprendizes e colaboradores e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCPE e que tenham acesso a qualquer meio de informação e comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 3º A íntegra da Política de Segurança da Informação do CRCPE será disponibilizada em seu Portal.

Art. 4º Esta resolução entra em vigor a partir de sua data de publicação.

Contadora **MARIA DORGIVÂNIA ARRAES BARBARÁ**
Presidente

Aprovada na 1.559ª Reunião Plenária Extraordinária de 2022, realizada em 07 de novembro e 2022.

ANEXO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CRCPE

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

DAS PREMISSAS

Art. 1º Proteger os dados pessoais, a privacidade e o acesso à informação, valorizando o princípio da autodeterminação informativa, mas também o direito à informação, o legítimo interesse, a liberdade de expressão, o direito à opinião, a inviolabilidade da intimidade, da honra e da imagem dos titulares de dados pessoais, o desenvolvimento tecnológico e a inovação, a livre iniciativa, os direitos do consumidor, o livre desenvolvimento da personalidade e a cidadania;

Art. 2º Proteger a informação institucional e de cadastros, visando minimizar danos às finalidades institucionais, prevenir fraudes e maximizar o retorno dos investimentos e oportunidades, de acordo com a sua sensibilidade e exposição ao risco;

Art. 3º Garantir condições para que os empregados, estagiários, prestadores de serviços, conselheiros e, quando aplicável, terceiros e quaisquer outras pessoas que prestem serviços ao CRCPE sejam orientados sobre a existência e a utilização dos instrumentos normativos, dos procedimentos e dos controles de segurança adotados pelo CRCPE.

Seção II

DOS OBJETIVOS

Art. 4º A Política de Segurança da Informação (PSI) tem por finalidade estabelecer normas, diretrizes e procedimentos para a segurança no uso, tratamento e controle, proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio de informação e comunicação, de forma a garantir a disponibilidade, integridade e confidencialidade das informações no âmbito do Conselho Regional de Contabilidade de Pernambuco.

Parágrafo único. A PSI está alinhada às estratégias institucionais, com a política de governança, com a gestão de riscos e com os normativos que regem a matéria.

Art. 5º A PSI trata do uso e do compartilhamento de dados, informações e documentos no âmbito do CRCPE, em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), objetivando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação.

Art. 6º Para a segurança da informação no CRCPE, serão rigorosamente observados o compromisso institucional com a proteção das informações de sua propriedade e/ou sob sua guarda, a participação e o cumprimento por todos os colaboradores em todo o processo e o disposto neste normativo, nas disposições constitucionais, legais e regimentais vigentes.

Seção III

DOS PRINCÍPIOS BÁSICOS

Art. 7º A PSI do CRCPE orienta-se pelos seguintes princípios básicos:

I - Disponibilidade: garante que a informação esteja sempre acessível para uso legítimo de pessoas físicas, sistemas e entidades autorizadas;

II - Integridade: garante que a informação esteja correta, confiável e sem a ocorrência de mudanças. Além disso, assegura que a informação não seja modificada, gravada ou excluída sem autorização ou acidentalmente;

III - Confidencialidade: garante que a informação seja acessível apenas às pessoas físicas, ao sistema e às entidades autorizadas;

IV - Autenticidade: garante a identificação de pessoa física, sistema e entidade que produziu, expediu, modificou ou excluiu a informação;

V - Proteção: assegura o direito individual e coletivo das pessoas à inviolabilidade da sua intimidade e ao sigilo da informação, nos termos previstos na Constituição Federal.

VI - Capacitação das equipes envolvidas em tecnologias sensíveis;

VII - criação, desenvolvimento e manutenção de cultura relacionada à segurança da informação, alinhadas às diretrizes nacionais de segurança da informação.

Art. 8º As ações de Segurança da Informação, no âmbito do CRCPE, são norteadas pelos seguintes princípios:

I - Criticidade: define a importância da informação para a continuidade da execução das finalidades institucionais;

II - Celeridade: garante respostas rápidas a incidentes e falhas de segurança;

III - Clareza: define que as regras e a documentação sobre segurança da informação devam ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;

IV - Ética: preserva o direito do empregado, colaborador, terceirizado, conselheiro, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação;

V - Legalidade: devem ser levadas em consideração as leis, as normas e as políticas organizacionais, administrativas, técnicas e operacionais vigentes;

VI - Responsabilidade: define que os usuários são responsáveis pelo cumprimento desta PSI e devem respeitar a legislação e normas pertinentes à Segurança da Informação vigentes.

VII - Privacidade: estabelece que o direito do cidadão de não ter registros pessoais e da vida privada divulgados sem sua prévia autorização devem ser assegurados; e

VIII - Publicidade: determina que a divulgação das informações deve observar os critérios legais aplicáveis.

Art. 9º São observados, ainda, sem prejuízo dos demais, os princípios constitucionais e demais normativos que regem a matéria.

Seção IV

DA ABRANGÊNCIA

Art. 10. O disposto neste instrumento aplicar-se-á a todos os empregados, estagiários, prestadores de serviços, conselheiros e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCPE e que tenham acesso a qualquer informação ou comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

§ 1º Os contratos, convênios e instrumentos congêneres conterão cláusulas específicas que imponham aos contratados e convenentes a obrigação de observarem o disposto nesta PSI, para o exercício de suas atividades no âmbito do CRCPE.

§ 2º Os termos aditivos dos contratos, convênios e instrumentos congêneres celebrados após a aprovação desta PSI deverão incluir cláusulas específicas que imponham aos contratados/convenentes a obrigação de observarem o disposto nesta Política, para o exercício de suas atividades no âmbito do CRCPE.

CAPÍTULO II
DOS CONCEITOS E CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I
DOS CONCEITOS E DAS DEFINIÇÕES

Art. 11. Para os efeitos desta Política de Segurança, entende-se por:

I - Ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, integridade, autenticidade e disponibilidade da informação;

II - Assinatura digital: conjunto de dados criptografados, associados a determinado documento ou arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;

III - Acessibilidade: facilidade no acesso ao conteúdo e ao significado de um objeto digital;

IV - Ativo de informação: patrimônio composto de dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;

V - Metadados: dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

VI - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por um determinado indivíduo, entidade ou processo;

VII - Banco de Dados (ou Base de Dados): um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

VIII - Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

IX - Cópia de Segurança (backup): guarda de dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade.

X - Fidedignidade: credibilidade de um documento arquivístico como uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;

XI - Comitê de Segurança da Informação: grupo de pessoas designado com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do CRCPE;

XII - Computação em nuvem: modelo computacional que permite acesso, por demanda e independentemente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

XIII - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XIV - Custódia: responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade.

XV - Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, ou seja, recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

XVI - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por indivíduo, entidades ou processos;

XVII - Dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre eles, notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

XVIII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ou Comitê de Gestão de Riscos: grupo de pessoas designado com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança;

XIX - Evento: Acontecimento que acarrete a mudança do estado atual de um processo;

XX - Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas finalidades institucionais, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e seu valor agregado. O Plano de Contingência e Continuidade dos Serviços de TI do CRCPE tem o objetivo de garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas, softwares, hardwares, infraestrutura, etc.) por ele utilizados;

XXI - Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação;

XXII - Gestão de Riscos em Segurança da Informação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXIII - Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do CRCPE;

XXIV - Incidente de segurança: evento ou conjunto de eventos de segurança da informação, indesejados ou inesperados, confirmados ou sob suspeita, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

XXV - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

XXVI - Integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

XXVII - Documento arquivístico: documento produzido ou recebido no curso de uma atividade prática como instrumento ou resultado dessa atividade, retido para ação ou referência;

XXVIII - Inventário e Mapeamento de Ativos de Informação: processo interativo e evolutivo, composto de três etapas:

a) identificação e classificação de ativos de informação;

b) identificação de potenciais ameaças e vulnerabilidades; e

c) avaliação de riscos.

XXIX - Malwares: o nome malware vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao seu dispositivo;

XXX - Preservação digital: conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário;

XXXI - Repositório digital: complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos;

XXXII - Repositório arquivístico digital: repositório digital que armazena e gerencia documentos arquivísticos, seja nas idades corrente e intermediária, seja na idade permanente;

XXXIII - Plano de Contingência e Continuidade dos Serviços de TI do CRCPE: documentação dos procedimentos e informações necessários para manter os ativos de informação críticos e a continuidade de suas atividades em local alternativo previamente definido, em casos de

incidentes. Também apresenta os procedimentos e informações necessários para que se operacionalize o retorno das atividades críticas à normalidade;

XXXIV - Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

XXXV - Público-Alvo: conjunto de usuários internos e externos atendidos pela Equipe de Tratamento e Resposta a Incidentes;

XXXVI - Recurso Criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXXVII - Risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XXXVIII - Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXIX - Serviços Essenciais: são aqueles que são imprescindíveis à atividade finalística deste Conselho;

XL - Spam: termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

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

XLII - Termo de Confidencialidade: documento formal assinado por prestadores de serviço do CRCPE, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;

XLIII - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XLIV - Trilhas de Auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

XLV - Unidade Gestora de Segurança da Informação: é a unidade responsável pela gestão de segurança da informação no CRCPE;

XLVI - Unidades Organizacionais: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz;

XLVII - Usuários: pessoa física ou jurídica que opera algum sistema informatizado do Conselho Regional de Contabilidade de Pernambuco (CRCPE);

XLVIII - Vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças;

XLIX - Phishing: também conhecido como roubo de identidade. É uma fraude eletrônica, na qual o criminoso cibernético tenta obter informações confidenciais de forma fraudulenta. Normalmente, é realizado por falsificação de e-mail ou mensagem instantânea, e, muitas vezes, direciona usuários a inserir informações pessoais em um site falso, que corresponde à aparência do site legítimo. Esse método é muito usado para roubar senhas e números de cartões de crédito, entre outros dados confidenciais.

Seção II

DA CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 12. A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrange informações provenientes dos serviços essenciais de Tecnologia da Informação do CRCPE.

Parágrafo único. As informações devem ser classificadas de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade e em conformidade com requisitos legais.

Art. 13.As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

I - Pública: são informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete a execução das finalidades institucionais e que, por isso, não necessitam de proteção efetiva ou tratamento específico, em especial, editais de licitação, agendas e rotinas;

II - Interna: são informações disponíveis aos colaboradores do CRCPE para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo, em especial, memorandos, procedimentos internos, avisos e campanhas internas;

III - Confidencial: são informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros, em especial, processos judiciais e dados cadastrais de colaboradores;

IV - Confidencial/Restrita: são informações de acesso restrito a um colaborador ou grupo de colaboradores que, obrigatoriamente, são delas destinatários. Em geral, informações associadas ao interesse estratégico do CRCPE e estão restritas a presidente, à diretoria, as chefias e aos colaboradores, cujas funções requeiram conhecê-las, em especial, resultado da avaliação de desempenho.

CAPÍTULO III
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
DAS COMPETÊNCIAS

Art. 14. Ao Comitê de Segurança da Informação compete:

I - propor melhorias e atualizar a Política de Segurança da Informação (PSI);

II - propor, analisar e revisar normas complementares relativas à segurança da informação, em conformidade com as legislações vigentes e submeter a aprovação ao Conselho Diretor do CRCPE;

III - tratar dos assuntos de Segurança da Informação e assessorar diretamente as decisões do Conselho Diretor do CRCPE;

IV - propor investimentos relacionados à segurança da informação com o intuito de fortalecer o ambiente tecnológico e não digital e minimizar os riscos causados em virtude de possíveis vulnerabilidades;

V - classificar e reclassificar o nível de acesso às informações sempre que necessário;

VI - acompanhar o gerenciamento do ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;

VII - coordenar as atividades de tratamento e resposta a incidentes de segurança;

VIII - promover a recuperação de sistemas;

IX - agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de Segurança da Informação e avaliando condições de segurança de rede por meio de verificações de conformidade;

X - realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

XI - receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores e em suportes físicos do CRCPE;

XII - executar as ações necessárias para tratar quebras de segurança;

XIII - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes.

XIV - planejar e coordenar a execução das ações de Segurança da Informação;

XV - definir estratégias para a implementação desta Política de Segurança da Informação (PSI) e suas normas complementares;

XVI - supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de Segurança da Informação;

XVII - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;

XVIII - encaminhar os fatos apurados, decorrentes de quebras de segurança, para a aplicação das penalidades previstas;

XIX - gerenciar a análise de risco;

XX - verificar se os procedimentos de Segurança da Informação estão sendo aplicados de forma a atender à conformidade com legislações vigentes; e

XXI - providenciar a divulgação interna e permanente desta PSI e de suas normas complementares.

Art. 15.À Chefia de TI e ao Departamento de Informática competem:

I - planejar, coordenar, supervisionar, executar e controlar as atividades de TI em conformidade com as diretrizes desta PSI;

II - elaborar, implementar e atualizar normas internas específicas em conformidade com esta PSI e demais diretrizes do Conselho;

III - propor as metodologias e processos referentes à segurança da informação, como classificação de acessos à informação, avaliação de risco, análise de vulnerabilidade, entre outros;

IV - gerenciar o ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;

V - manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais do CRCPE;

VI - manter equipe interna, de Segurança da Informação com a responsabilidade de apoiar o Comitê de Segurança da Informação no cumprimento de suas atribuições.

VII - definir as regras para instalação de software e hardware no CRCPE;

VIII - avaliar a possibilidade de utilização de equipamentos pessoais (smartphones e notebooks) para uso na rede do CRCPE, condicionado ao cumprimento dos requisitos de segurança que garantam a integridade das informações;

IX - supervisionar os acessos às informações e aos ativos de tecnologia (sistemas, banco de dados, recursos de rede), tendo como referência a PSI e as normas de segurança da informação;

X - efetuar as alterações, exclusões, inclusões e manter registro e controles atualizados de todos os acessos sempre que demandado formalmente pelas Unidades Organizacionais acerca de admissão, demissão e movimentação de pessoal e/ou entrada/saída de novos processos;

XI - promover, com o envolvimento do Departamento de Pessoal, palestras de conscientização dos colaboradores em relação à importância da segurança da informação;

XII - manter comunicação efetiva com o Comitê de Segurança da Informação sobre possíveis ameaças e ações que deverão ser adotadas para mitigação dos riscos;

XIII - buscar alinhamento com as diretrizes da organização, em especial com o planejamento estratégico, Plano Diretor de Tecnologia da Informação (PDTI), Plano de Integridade e governança de tecnologia.

Art. 16. Ao responsável pelo Departamento Pessoal (DP) compete:

I - comunicar ao Comitê de Segurança da Informação o ingresso, a alteração de localização, bem como o desligamento de pessoal, inclusive postos terceirizados, no âmbito do CRCPE.

Seção II
DAS RESPONSABILIDADES

Subseção I
DOS USUÁRIOS

Art. 17. Para o Conselho Regional de Contabilidade de Pernambuco, são considerados usuários todos os conselheiros, integrantes de grupos de trabalhos,

empregados, estagiários, prestadores de serviços e terceiros que tenham acesso ao ambiente de tecnologia da informação e têm as seguintes responsabilidades:

I - ter pleno conhecimento e cumprir fielmente a PSI, as normas e os procedimentos de segurança da informação do CRCPE;

II - solicitar esclarecimentos ao Comitê de Segurança de Informação em caso de dúvidas relacionadas à PSI;

III - gerenciar os ativos sob sua responsabilidade e garantir que os documentos e arquivos impressos ou digitais, equipamentos e recursos tecnológicos à sua disposição sejam utilizados, exclusivamente, para uso a serviço do CRCPE;

IV - acessar a rede de dados do CRCPE somente após tomar ciência das normas de Segurança da Informação e assinar o Termo de Responsabilidade;

V - tratar a informação arquivística digital e impressa como patrimônio do CRCPE e como recurso que deva ter seu sigilo preservado;

VI - utilizar as informações arquivísticas digitais e impressas disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do CRCPE exclusivamente para o interesse do serviço;

VII - preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

VIII - não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança ou cujo teor não tenha autorização ou necessidade de conhecer;

IX - não se fazer passar por outro usuário usando a identificação com login e senha de acesso;

X - no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;

XI - não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional do CRCPE por terceiros;

XII - responder perante o CRCPE pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil;

XIII - não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

XIV - não transferir qualquer tipo de arquivo que pertença ao CRCPE para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

XV - estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não são permitidos na rede computacional do CRCPE;

XVI - estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional e nos arquivos setoriais, intermediários e permanentes impressos ou digitais do CRCPE pode ser auditada;

XVII - estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional do CRCPE deve obedecer a esse preceito;

XVIII - assinar o Termo de Responsabilidade - Anexo I e declarar, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PSI;

XIX - utilizar as credenciais de acesso, login e senha, e os recursos computacionais, em conformidade com a PSI do CRCPE e procedimentos estabelecidos em normas específicas do Conselho;

XX - comunicar, tempestivamente, ao gestor imediato ou ao Comitê de Segurança da Informação qualquer violação a esta política, suas normas e procedimentos;

XXI - fazer uso da política de mesa limpa e tela protegida para garantir a proteção das informações de maneira eficaz e reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho.

XXII - devolução das informações ou documentos sigilosos que estejam em seu poder.

XXIII - eliminação completa de dados digitais que porventura foram armazenados em seus equipamentos eletrônicos e softwares de uso particular e e-mails pessoais.

Subseção II

DO CUSTODIANTE

Art. 18. Ao Custodiante da Informação cabem as seguintes responsabilidades:

I - Cumprir e zelar pela observância integral das diretrizes desta PSI e demais normas e procedimentos decorrentes;

II - Zelar pela disponibilidade, integridade e confidencialidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta PSI e demais normas e procedimentos decorrentes, mediante assinatura do Termo de Responsabilidade;

III - Participar de capacitação e treinamento em segurança da informação, quando convocado;

IV - Utilizar os recursos sob sua responsabilidade, exclusivamente, para o fim a que se destinam;

V - Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

VI - Preservar a classificação do grau de sigilo de documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções; e

VII - comunicar prontamente ao seu gestor imediato e ao Comitê de Segurança da Informação qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade e a confidencialidade das informações.

Subseção III

DAS CHEFIAS DAS UNIDADES ORGANIZACIONAIS

Art. 19. As chefias das unidades organizacionais do CRCPE são responsáveis por:

I - Ter postura exemplar em relação à segurança da informação para servir como modelo de conduta para os colaboradores sob sua gestão;

II - Cumprir e fazer cumprir esta PSI;

III - Exigir das entidades relacionadas, prestadores de serviços ou outras entidades externas, a assinatura do Termo de Confidencialidade referente às informações as quais terão acesso;

IV - Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

V - Adotar os procedimentos necessários sempre que identificar descumprimentos da PSI.

CAPÍTULO IV

DAS DIRETRIZES E PROCEDIMENTOS

Seção I

DAS DIRETRIZES

Art. 20. Esta PSI tem como principal diretriz a preservação da disponibilidade, integridade e confiabilidade dos dados, informações e conhecimentos que compõem o ativo da informação do CRCPE.

Art. 21. Os usuários deverão ser treinados e conscientizados nos procedimentos de segurança da informação.

Art. 22. Quando do afastamento, da mudança de responsabilidade, de lotação ou de atribuições do usuário dentro da organização, far-se-á necessária a revisão imediata dos direitos de acesso e uso dos ativos.

§ 1º Os direitos de acesso e o uso dos ativos atribuídos ao usuário deverão ser extintos quando da efetivação de seu desligamento.

§ 2º Todo ativo produzido pelo usuário desligado será de propriedade do CRCPE, observadas as disposições da legislação aplicável.

Subseção I

DOS PRESSUPOSTOS BÁSICOS

Art. 23 Esta Política de Segurança da Informação é constituída dos seguintes pressupostos básicos:

I - O sucesso das ações nos assuntos de segurança da informação está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas;

II - a informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado;

III - a Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, de disponibilidade e de confidencialidade;

IV - todos os empregados, estagiários, conselheiros e prestadores de serviços, membro de grupos ou particulares que, oficialmente, executem atividade vinculada à

atuação institucional do CRCPE e sejam usuários dos ativos sigilosos devem assinar o Termo de Responsabilidade quanto ao sigilo dos dados, informações e conhecimentos da administração do CRCPE.

Seção II

DAS PROVIDÊNCIAS

Subseção I

DO TRATAMENTO DA INFORMAÇÃO

Art. 24. Esta Política de Segurança da Informação considera os seguintes requisitos para o Tratamento da Informação:

I - Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade do CRCPE e deve ser protegida segundo as diretrizes descritas nesta PSI e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços institucionais e preservar sua imagem;

II - É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo CRCPE;

III - os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos das finalidades institucionais do CRCPE;

IV - As informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e legislação específica em vigor;

V - Todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas;

VI - As informações produzidas ou custodiadas pelo CRCPE somente devem ser descartadas ou destruídas conforme o seu nível de classificação e atendendo às exigências legais;

VII - deve ser disponibilizada uma solução de Gestão Eletrônica de Documentos com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa;

VIII - a manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor;

§ 1º Qualquer outra forma de uso das informações que extrapole as atribuições necessárias ao desempenho das atividades dos usuários, internos ou colaboradores, necessitará de prévia autorização formal.

§ 2º O acesso, quando autorizado, dos usuários internos ou externos às informações produzidas ou custodiadas pelo CRCPE, que não sejam de domínio público, será condicionado a um termo de sigilo e responsabilidade, formal ou virtual.

Parágrafo único. As informações deverão ser classificadas de forma a permitir tratamento diferenciado de acordo com seu grau de importância, criticidade, sensibilidade, e em conformidade com requisitos legais.

Subseção II

DA UTILIZAÇÃO DA REDE

Art. 25. O ingresso à rede interna deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados, devendo os procedimentos serem definidos em normas específicas, em especial, a Política de Controle de Acesso Lógico do CRCPE.

Subseção III

DO TRATAMENTO DE INCIDENTES DE REDE

Art. 26. Tratamento de Incidentes de Rede:

I - A gestão de incidentes de segurança da informação deverá ser realizada por meio de processo formalizado, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança;

II - A Coordenadoria de TI e o Departamento de Informática manterão Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, com a responsabilidade de receber, analisar e responder a notificações e a atividades relacionadas a incidentes de segurança em rede de computadores;

III - sua criação, sua estrutura e seu modelo de implementação serão definidas em Portaria que deverá estar em conformidade com as diretrizes desta PSI.

Subseção IV

DA GESTÃO DE RISCOS

Art. 27 Gestão de Riscos:

I - A gestão de riscos é realizada por meio de processo formalizado, contendo as fases de análise, avaliação e tratamento dos riscos;

II - Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação;

III - Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito do CRCPE;

IV - O processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade, conforme procedimentos definidos em norma específica sobre o tema.

Subseção V

DA GESTÃO DE CONTINUIDADE

Art. 28. Gestão de Continuidade:

I - O CRCPE deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

II - As informações de propriedade ou custodiadas pelo CRCPE, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança atualizada e guardada em local remoto, de forma a garantir a continuidade das atividades do órgão.

III - As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

IV - As diretrizes para a Gestão de Continuidade de TI em Segurança da Informação, conforme procedimentos definidos em norma específica, deve minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades críticas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Subseção VI

DA AUDITORIA E CONFORMIDADE

Art. 29. Auditoria e Conformidade:

I - A Auditoria em Segurança da Informação é uma atividade devidamente estruturada para examinar criteriosamente a situação dos controles que se aplicam à segurança da informação, especialmente por meio da análise de objetos e respectivos pontos de controle. Para tanto, é preciso verificar que os controles estejam de acordo com as normas e políticas de segurança estabelecidas para esses ativos, bem como se o que está em operação alcança os objetivos de segurança;

II - O CRCPE deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos sistemas corporativos e rede interna da entidade;

Subseção VII

DO CONTROLE DE ACESSO

Art. 30. Controle de Acesso:

I - O controle de acesso aos sistemas internos e externos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico e serão definidos em norma específica, em conformidade com as diretrizes desta PSI;

II - As medidas de proteção serão adotadas para evitar que usuários dos ativos de Tecnologia da Informação não tenham permissão para instalar, remover, modificar, criar ou desenvolver softwares sem a devida autorização.

Subseção VIII

DA POLÍTICA DE SENHAS

Art. 31. A política de senhas de acessos aos sistemas e informações do CRCPE deve ser definida em norma específica, em conformidade com as diretrizes desta PSI.

Subseção IX

DO USO DE E-MAIL

Art. 32. O uso de e-mail no âmbito do CRCPE deve ser definido em norma específica, em conformidade com as diretrizes desta PSI, e deve tratar, entre outras coisas, do controle de acesso.

Subseção X

DO ACESSO À INTERNET

Art. 33. O acesso à rede mundial de computadores, no âmbito do CRCPE, deve ser definido em norma específica, em conformidade com as diretrizes desta PSI, orientações governamentais e legislações específicas em vigor.

Subseção XI

DO INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 34. Inventário e Mapeamento de Ativos de Informação:

I - Nos aspectos relacionados à Segurança da Informação, o processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios para a Gestão de Segurança da Informação, Gestão de Riscos de Segurança da Informação, Gestão de Continuidade de TI, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de geração da base de dados sobre os ativos de informação;

II - O processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação;

III - O inventário deve documentar e classificar a importância do ativo para as finalidades institucionais, o impacto para atividades finalísticas em caso de comprometimento e a estratégia que permita a recuperação do ativo em caso de desastre;

IV - Todos os ativos críticos devem ter um proprietário formalmente designado.

V- O proprietário dos ativos de informação é a parte interessada do CRCPE, ou indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

VI - O proprietário é responsável por:

a) assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificadas;

b) definir e periodicamente analisar criticamente as classificações e as exigências de segurança da informação para os ativos de informação;

c) identificar os riscos e comunicar as exigências de segurança da informação para os ativos sob sua responsabilidade aos custodiantes e usuários;

d) implementar controles internos a fim de verificar se as exigências estão sendo cumpridas.

VII - o proprietário do ativo pode delegar formalmente as tarefas de rotina a um custodiante que cuida do ativo no dia a dia, porém a responsabilidade permanece do proprietário;

VIII - o custodiante dos ativos de informação é qualquer indivíduo ou estrutura que tenha a responsabilidade formal de proteger um ou mais ativos de informação. É responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação informadas pelo proprietário dos ativos de informação;

IX - as regras para uso dos ativos associados com a informação e dos recursos de processamento da informação devem ser identificadas, documentadas e implementadas;

X - os usuários que têm acesso aos ativos do CRCPE devem estar conscientes dos requisitos de segurança da informação;

XI - a informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada;

XII - o proprietário do ativo de informação deve ser responsável por sua classificação.

Subseção XII

DOS DISPOSITIVOS MÓVEIS

Art. 35. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito do CRCPE deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário e ser definido em norma específica em conformidade com as diretrizes desta PSI.

Subseção XIII

DA COMPUTAÇÃO EM NUVEM

Art. 36. A implementação ou contratação de computação em nuvem no âmbito do CRCPE deve ser definida em norma específica, em conformidade com as diretrizes desta PSI e com as demais legislações vigentes sobre o tema.

Subseção XIV

DO BACKUP

Art. 37. Todo sistema ou informação relevante para a operação das finalidades institucionais do CRCPE deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição, devendo a implementação dos procedimentos de backups ser definida em norma específica.

Subseção XV

DA CRIPTOGRAFIA

Art. 38. Criptografia:

I - A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico, conforme procedimentos definidos em norma e legislações específicas em vigor;

II - qualquer sistema próprio do CRCPE que contenha tabelas com senhas devem ter essas tabelas armazenadas de forma criptografada.

Subseção XVI

DA CONTRATAÇÃO DE SERVIÇOS

Art. 40. Contratação de Serviços:

I - Nos editais de licitação e nos contratos de empresas prestadoras de serviços com o CRCPE, deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta PSI, bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade e do Termo de Confidencialidade;

II - A empresa contratada também deverá demonstrar que possui mecanismos que

assegurem a segurança das informações do CRCPE por ela acessadas, direta ou indiretamente, acesso aos ativos que contêm informações, e cumprir o disposto nesta PSI quando aplicável;

III - Não poderá ser objeto de contratação a Gestão de Processos de Tecnologia da Informação ou a Gestão de Segurança da Informação;

IV - O apoio técnico aos processos de planejamento e a avaliação da qualidade das soluções de tecnologia da informação poderão ser objetos de contratação, desde que sob supervisão exclusiva de empregados do CRCPE;

V - Os termos e procedimentos para contratação de serviços terceirizados serão detalhados em norma complementar específica.

CAPÍTULO V

DA DIVULGAÇÃO E ATUALIZAÇÃO

Art. 41.Esta PSI e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal do CRCPE, sendo consideradas documentos de relevante interesse público.

Art. 42.Esta Política de Segurança da Informação deverá ser revisada a cada 2 (dois) anos ou sempre que se fizer necessário, não excedendo ao período máximo de 3 (três) anos, a contar da data de sua publicação.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 43. A inobservância dos dispositivos constantes desta Política de Segurança da Informação pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 44. Os casos omissos desta PSI serão resolvidos pelo Comitê de Segurança da Informação do CRCPE.

Art. 45. O Conselho Regional de Contabilidade de Pernambuco tem o prazo de 24 (vinte e quatro) meses para implementação de todas as ações propostas por esta Política de Segurança da Informação.

ANEXO I

Termo de Responsabilidade

Pelo presente termo, eu, _____, declaro ter conhecimento da Política de Segurança da Informação do Conselho Regional de Contabilidade de Penambuco (CRCPE), disponível para consulta no portal do CRCPE, no menu “Governança - LGPD”.

Declaro que estou recebendo uma conta com privilégios adequados ao exercício das atividades que executo, a qual será utilizada somente para tal fim.

Declaro estar ciente de que minhas ações serão monitoradas nos termos da Política de Segurança da Informação do CRCPE e de que qualquer alteração será de minha responsabilidade, feita a partir de minha identificação, autenticação e autorização.

Estou ciente, ainda, que serei responsável pelo dano que possa causar em caso de descumprimento da Política de Segurança da Informação do CRCPE, ao realizar uma ação de iniciativa própria de tentativa quanto à modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Recife/PE, ____ de _____ de 20____.

Nome:
Matrícula:
Unidade Organizacional:

Nome:
Unidade Organizacional:
(titular da Unidade Organizacional ou gestor do contrato, para o caso dos terceirizados)