RESOLUÇÃO CRCRN Nº 183, DE 12 DE JANEIRO DE 2023.

Aprova a Política de Segurança da Informação (PSI) do Conselho Regional de Contabilidade do Rio Grande do Norte (CRCRN).

O Presidente do **CONSELHO REGIONAL DE CONTABILIDADE DO RIO GRANDE DO NORTE**, no uso de suas atribuições legais e regimentais, com supedâneo no Regimento Interno do CRC/RN,

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 do Rio Grande do Norte (CRCRN) 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 sigilo resguardado;

CONSIDERANDO que as informações no CRCRN 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 nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), 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 nº 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 nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO a Instrução Normativa nº 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 CRCRN nº 071, de 03 de junho de 2022, que criou o Comitê Gestor de Segurança da Informação (CGSI) no âmbito do CRCRN.

RESOLVE:

CAPÍTULO I
DEFINIÇÃO E COMPETÊNCIAS

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito do Conselho Regional de Contabilidade do Rio Grande do Norte (CRCRN), nos termos desta resolução.

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

CAPÍTULO II
DISPOSIÇÕES GERAIS

Seção I
OBJETIVOS

Art. 2º A PSI tem por finalidade estabelecer normas, diretrizes e procedimentos para a segurança no uso, tratamento, controle e 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 CRCRN.

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

Art. 3º A PSI trata do uso e do compartilhamento de dados, informações e documentos no âmbito do CRCRN, em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento,

transporte e descarte), objetivando a 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. 4º Para a segurança da informação no CRCRN, serão rigorosamente observados o compromisso institucional com a proteção das informações de sua propriedade e/ou sob a 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 II
PREMISSAS

Art. 5º São premissas da PSI:

I – proteger os dados pessoais, a privacidade e o acesso à informação, valorizando o princípio da autodeterminação informativa (sem prejuízo ao 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;
II – proteger as informações institucionais e cadastrais, 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;
III – garantir condições para que os empregados, estagiários, prestadores de serviços, conselheiros e, quando aplicável, terceiros e quaisquer outras pessoas que prestem serviços ao CRCRN sejam orientados sobre a existência e a utilização dos instrumentos normativos, dos procedimentos e dos controles de segurança adotados pelo CRCRN;
IV – capacitar as equipes envolvidas em tecnologias sensíveis;
V – criar, desenvolver e manter cultura relacionada à segurança da informação, alinhada às diretrizes nacionais de segurança da informação.

Seção III
PRINCÍPIOS BÁSICOS

Art. 6º A PSI do CRCRN orienta-se pelos seguintes princípios básicos:

I – Dispinibilidade: 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, propositalmente, acidentalmente ou sem autorização;
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.

Art. 7º As ações de Segurança da Informação, no âmbito do CRCRN, são norteados 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 deve ser assegurado;
VIII – Publicidade: determina que a divulgação das informações deve observar os critérios legais aplicáveis.

Art. 8º São observados, ainda, sem prejuízo dos demais, os princípios constitucionais e demais normativos que regem a matéria.

Seção IV
ABRANGÊNCIA

Art. 9º O disposto neste instrumento aplica-se a todos os empregados, estagiários, aprendizes, prestadores de serviços, conselheiros e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCRN 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 CRCRN.

§ 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 CRCRN.

§ 3º No caso de contratos de trabalho de empregados, serão utilizadas as cláusulas específicas de cumprimento de normativos, conforme disposto no Regulamento de empregados do CRCRN.

CAPÍTULO III
CONCEITOS E CLASSIFICAÇÃO DAS INFORMAÇÕES

Seção I
CONCEITOS E DEFINIÇÕES

Art. 10. Para os efeitos desta Política de Segurança, entende-se por:

I – Ameaça: qualquer circunstância ou evento com 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 de fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere e é estabelecido pelo exame da completeza, da forma do documento e do grau de controle exercido no processo de sua produção;
XI – Comitê Gestor de Segurança da Informação (CGSI): grupo de pessoas designado com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do CRCRN;
XII – Computação em nuvem: modelo computacional que permite acesso, por demanda e independente 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, que objetiva 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. 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;
XXI – Gestão de Segurança da Informação: ações e métodos que têm como objetivo a integração das atividades de gestão de riscos, o tratamento de incidentes, o tratamento da informação, a conformidade, o credenciamento, a segurança cibernética, a segurança física, a segurança lógica, a segurança orgânica e a 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 CRCRN;
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, 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 Continuidade de Serviços Essenciais: 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;
XXXIV – Plano de Recuperação de Serviços Essenciais: documentação dos procedimentos e informações necessários para que se operacionalize o retorno das atividades criticas à normalidade;
XXXV – 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;
XXXVI – Público-alvo: conjunto de usuários internos e externos atendidos pela equipe de Tratamento e Resposta a Incidentes;
XXXVII – Recurso criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;
XXXVIII – Risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;
XXXIX – Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
XL – Serviços essenciais: são aqueles que são imprescindíveis à atividade finalística deste Conselho;
XLI – Spam: termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
XLII – Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XLIII – Termo de Confidencialidade: documento formal assinado por prestadores de serviço do CRCRN, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;
XLIV – Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
XLV – 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;
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 CRCRN;
XLIII – 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
CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 11. A classificação e o tratamento da informação, realizados por meio de procedimento definido, abrange informações provenientes dos serviços essenciais de Tecnologia da Informação do CRCRN.

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. 12. 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, 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 CRCRN 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, são informações associadas ao interesse estratégico do CRCRN e estão restritas ao presidente, ao diretor, aos gerentes e aos colaboradores cujas funções requeiram conhecê-las, tais como resultado da avaliação do desempenho, processo administrativo disciplinar, sanções e penalidades aplicadas e dados sensíveis.

CAPÍTULO IV
COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
COMPETÊNCIAS

Art. 13. Ao Comitê Gestor de Segurança da Informação (CGSI) 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 à aprovação do Conselho Diretor do CRCRN;
III – tratar dos assuntos de segurança da informação e assessorar diretamente as decisões do Conselho Diretor do CRCRN;
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 – acompanhar o gerenciamento do ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;
VI – coordenar as atividades de tratamento e resposta a incidentes de segurança, juntamente com o Comitê Gestor de Privacidade e Proteção de Dados e com o Encarregado de dados pessoais, quando se tratar de incidentes de segurança com dados pessoais, em conformidade com as Políticas de Incidentes de Segurança da Informação e de Notificação de Incidentes de Segurança com Dados Pessoais do CRCRN;
VII – 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;
VIII – realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e analise de sistemas comprometidos, buscando causas, danos e responsáveis, em conformidade com a Política de Incidentes de Segurança da Informação;
IX – receber e analisar as notificações e atividades relacionadas a incidentes de segurança em redes de computadores e em suportes físicos do CRCRN, em conformidade com a Política de Incidentes de Segurança da informação;

X – executar as ações necessárias para tratar quebras de segurança;
XI – obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
XII – planejar e coordenar a execução das ações de segurança da informação;
XIII – definir estratégias para a implementação desta PSI e suas normas complementares;
XIV – supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;
XV – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
XVI – encaminhar os fatos apurados, decorrentes de quebras de segurança, à autoridade competente, para a aplicação das penalidades previstas;
XVII – gerenciar a análise de risco de segurança da informação;
XVIII – verificar se os procedimentos de segurança da informação estão sendo aplicados de forma a atender à conformidade com legislações vigentes; e
XIX – providenciar a divulgação interna e permanente desta PSI e de suas normas complementares.

Art. 14. À Seção de Tecnologia da Informação (TI) compete:

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 metodologias e processos referentes à segurança da informação, como classificação de acessos à informação, avaliação de risco, análise de vulnerabilidade, entre outros;
IV – classificar e reclassificar o nível de acesso às informações sempre que necessário, em conformidade com a metodologia definida e com as restrições identificadas pelos responsáveis pelas Unidades Organizacionais ou pelo Comitê Gestor de Segurança da Informação;
V – gerenciar o ciclo de vida de incidentes de segurança, visando ao processo de melhoria contínua;
VI – promover a recuperação de sistemas;
VII – 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 CRCRN;
VIII – manter equipe, interna ou terceirizada, de segurança da informação com a responsabilidade de apoiar o Comitê Gestor de Segurança da Informação no cumprimento de suas atribuições;
VIX – definir as regras para instalação de software e hardware no CRCRN;
X – avaliar a possibilidade de utilização de equipamentos pessoais (smartphones e notebooks) para uso na rede do CRCRN, condicionado ao cumprimento dos requisitos de segurança que garantam a integridade das informações;
XI – supervisionar os acessos às informações e aos ativos de tecnologia (sistemas, banco de dados e recursos de rede), tendo como referência a PSI e as normas de segurança da informação;
XII – efetuar as alterações, exclusões, inclusões e manter registros 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;

XIII – promover, com o envolvimento da Direção Administrativa, palestras de conscientização dos colaboradores em relação à importância da segurança da informação;
XIV – manter comunicação efetiva com o Comitê Gestor de Segurança da Informação sobre possíveis ameaças e ações que deverão ser adotadas para mitigação dos riscos;
XV – buscar alinhamento com as diretrizes da organização, em especial com o planejamento estratégico, o Plano Diretor de Tecnologia da Informação (PDTI) e o o Plano de Integridade.

Art. 15. À Seção de Recursos Humanos, compete:

I – comunicar à Seção de TI, por meio de Help Desk, o ingresso, a alteração de lotação ou localização e o desligamento de pessoal, inclusive postos terceirizados, no âmbito do CRCRN;
II – incluir, na análise e elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação com o objetivo de proteger os interesses do CRCRN;
III – assegurar que os colaboradores comprovem, por escrito, estar cientes deste regulamento.

Seção II
RESPONSABILIDADES

Subseção I
USUÁRIOS

Art. 16. Para o CRCRN, são considerados usuários todos os conselheiros, integrantes de Grupos de Estudos Técnicos, delegados representantes, empregados, estagiários, aprendizes, prestadores de serviços e terceiros que tenham acesso ao ambiente de tecnologia da informação, os quais têm as seguintes responsabilidades:

I – ter pleno conhecimento e cumprir fielmente a PSI, as normas e os procedimentos de segurança da informação do CRCRN;
II – solicitar esclarecimentos ao Comitê Gestor de Segurança da 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 CRCRN;
IV – acessar a rede de dados do CRCRN somente após tomar ciência das normas de Segurança da Informação e assinar Termo de Responsabilidade;
V – tratar a informação arquivística digital e impressa como patrimônio do CRCRN e como recurso que deva ter seu sigilo preservado;
VI – utilizar informações arquivísticas digitais e impressas disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do CRCRN exclusivamente para 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 CRCRN por terceiros;
XII – responder perante o CRCRN 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 CRCRN 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 CRCRN;
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 CRCRN 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 CRCRN deve obedecer a esse preceito.
XVIII – assinar o Termo de Responsabilidade, conforme Anexo I desta resolução, e declarar, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PSI;
XIX – utilizar as credenciais de acesso, login e senha, assim como os recursos computacionais em conformidade com a PSI do CRCRN e procedimentos estabelecidos em normas específicas do Conselho;
XX – comunicar, tempestivamente, ao gestor imediato ou ao Comitê Gestor 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. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não;
XXII – devolver as informações ou documentos sigilosos que estejam em seu poder;
XXIII – não manter armazenados, em seus equipamentos eletrônicos e softwares de uso particular e e-mails pessoais, os dados digitais de propriedade do CRCRN.

Subseção II
CUSTODIANTE

Art. 17. 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;
VII – comunicar prontamente ao seu gestor imediato e ao Comitê Gestor 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
GESTORES DAS UNIDADES ORGANIZACIONAIS

Art. 18. Os gestores das Unidades Organizacionais do CRCRN 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 dos prestadores de serviços ou outras entidades externas a assinatura do Termo de Confidencialidade referente a informações as quais terão acesso, quando aplicável;
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 V
DIRETRIZES E PROCEDIMENTOS

Seção I
DIRETRIZES

Art. 19. 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 CRCRN.

Art. 20. Os usuários deverão ser treinados e conscientizados nos procedimentos de segurança da informação.

Art. 21. Quando houver o afastamento ou a mudança de responsabilidade, de lotação ou de atribuições do usuário dentro da organização, será necessária a revisão imediata dos direitos de acesso e uso de 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 CRCRN, observadas as disposições da legislação aplicável.

Subseção I
PRESSUPOSTOS BÁSICOS

Art. 22. 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, aprendizes, conselheiros, prestadores de serviços, membros de grupos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do CRCRN e sejam usuários dos ativos sigilosos devem assinar o Termo de Responsabilidade quanto ao sigilo dos dados, informações e conhecimentos da administração do CRCRN.

Seção II
PROVIDÊNCIAS

Subseção I
TRATAMENTO DA INFORMAÇÃO

Art. 23. 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 CRCRN 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 CRCRN;

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 CRCRN;
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 CRCRN somente devem ser descartadas ou destruídas conforme o seu nível de classificação e atendendo às exigências legais;
VII – deve ser disponibilizada uma solução 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 CRCRN, que não sejam de domínio público, será condicionado a um termo de sigilo e responsabilidade, formal ou virtual.

§ 3º As informações deverão ser classificados de forma a permitir tratamento diferenciado de acordo com o seu grau de importância, criticidade, sensibilidade, e em conformidade com requisitos legais.

Subseção II
CONTROLE DE ACESSO

Art. 24. 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 na Política de Controle de Acesso Lógico do CRCRN, em comformidade com as diretrizes desta PSI.

Parágrafo único. 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.

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 CRCRN.

Subseção III

POLÍTICA DE SENHAS

Art. 26. A política de senhas de acessos aos sistemas e informações do CRCRN deve ser definida na Política de Controle de Acesso Lógico do CRCRN, em conformidade com as diretrizes desta PSI.

Subseção IV
USO DE E-MAIL

Art. 27. O uso de e-mail no âmbito do CRCRN deve ser definido na Política de Controle de Acesso Lógico do CRCRN, em conformidade com as diretrizes desta PSI, e deve tratar, entre outras coisas, do controle de acesso.

Subseção V
ACESSO À INTERNET

Art. 28. O acesso à rede mundial de computadores, no âmbito do CRCRN, deve ser definido na Política de Controle de Acesso Lógico do CRCRN, em conformidade com as diretrizes desta PSI, orientações governamentais e legislações específicas em vigor.

Subseção VI
TRATAMENTO DE INCIDENTES DE REDE

Art. 29. 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, em conformidade com a Política de Incidentes de Segurança da Informação e com Política de Notificação de Incidentes de Segurança com Dados Pessoais do CRCRN.

Parágrafo único. O CRCRN manterá equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em rede de computadores, sendo a criação, a estrutura e o modelo de implementação desta equipe definidos em portaria que deverá estar em conformidade com as diretrizes desta PSI.

Subseção VII
GESTÃO DE RISCOS

Art. 30. A gestão de riscos é realizada por meio de processo formalizado, contendo as fases de análise, avaliação e tratamento dos riscos. 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.

§ 1º 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 CRCRN.

§ 2º 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 VIII
GESTÃO DE CONTINUIDADE

Art. 31. As diretrizes para a Gestão de Continuidade de TI, conforme procedimentos definidos em norma específica, devem minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades críticas, além de recuperar perdas de ativos e informação em nível aceitável e em tempo hábil, por intermédio de ações de prevenção e recuperação.

Parágrafo único. As informações de propriedade ou custodiadas pelo CRCRN, 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 da instituição, em conformidade com a Política de Backup. Já as informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Subseção IX
AUDITORIA E CONFORMIDADE

Art. 32. 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 se os controles estão 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.

Art. 33. O CRCRN 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. Sobre a auditoria de conformidade:

I – deve ser realizada com periodicidade mínima anual, para a verificação de conformidade das práticas de Segurança da Informação aplicadas no CRCRN com esta PSI, bem como com a legislação específica em vigor;
II – a verificação de conformidade pode ser estendida para os contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o CRCRN;
III – a verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros e logs, análise de código-fonte, entrevistas e testes de invasão;

IV – os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade;
V – deverão ser tomadas medidas de proteção para que administradores de sistemas não tenham permissão de exclusão ou desativação de registros de log de suas próprias atividades;
VI – os recursos e informações de registro de log deverão ser protegidos contra falsificação e acesso não autorizado;
VII – compete ao Sistema de Gestão de Qualidade do CRCRN o acompanhamento da Auditoria de Segurança da Informação.

§ 1º Os procedimentos e as metodologias utilizados na auditoria no âmbito do CRCRN serão definidos em norma específica, em conformidade com as diretrizes desta PSI e demais legislações em vigor.

§ 2º A realização de auditoria especial deverá ser, obrigatoriamente, solicitada pelo gestor da área e aprovada pela diretoria correspondente. Durante a sua execução, deverão ser resguardados os direitos quanto à privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do CRCRN, de forma que se misturem ou impeçam o acesso às informações de propriedade ou sob a responsabilidade do CRCRN.

Subseção X
INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 34. 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, para a Gestão de Riscos de Segurança da Informação, para a 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. O processo de Inventário e Mapeamento de Ativos de Informação será regulamentado por meio da Política de Gestão de Ativos do CRCRN.

Subseção XI
DISPOSITIVOS MÓVEIS

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

Subseção XII
BACKUP

Art. 36. Todo sistema ou informação relevante para a operação das finalidades institucionais do CRCRN deve possuir cópia de seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar ao impactos nas operações da instituição, devendo a implementação dos procedimentos de backups ser definida na Política de Backup do CRCRN.

Subseção XIII
CRIPTOGRAFIA

Art. 37. A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico, conforme procedimentos definidos na Política de Controle de Ativos e em legislações específicas em vigor.

Parágrafo único. Qualquer sistema próprio do CRCRN que contenha tabelas com senhas deve ter esses dados armazenados de forma criptografada.

Subseção XIV
REDES SOCIAIS

Art. 38. O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades, definidas em norma complementar, em conformidade com as diretrizes desta PSI.

Subseção XV
CONTRATAÇÃO DE SERVIÇOS

Art. 39. Nos editais de licitação e nos contratos de empresas prestadoras de serviços com o CRCRN, deverá constar cláusula específica sobre 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, quando cabível.

Parágrafo único. A empresa contratada também deverá demonstrar que possui mecanismos que assegurem a segurança das informações do CRCRN por ela acessadas, direta ou indiretamente, no acesso aos ativos que contêm informações, e cumprir o disposto nesta PSI, quando aplicável.

Art. 40. Não poderá ser objeto de contratação a Gestão de Processos de Tecnologia da Informação ou a Gestão de Segurança da Informação.

§ 1º 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 CRCRN.

§ 2º Os termos e procedimentos para contratação de serviços terceirizados serão detalhados em norma complementar específica.

Seção III
DIREITOS DE PROPRIEDADE

Art. 41. Todo produto resultante do trabalho dos funcionários e colaboradores, tal como coleta de dados e documentos, sistema, metodologia, entre outros, é propriedade do CRCRN. Em caso de extinção ou rescisão do contrato de prestação de serviços, por qualquer motivo, deverá o colaborador devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços ao CRCRN, ou emitir declaração de que as destruiu.

CAPÍTULO VI
VIOLAÇÕES E SANÇÕES

Art. 42. A inobservância de dispositivos constantes nesta Política de Segurança da Informação, normas ou procedimentos de segurança da informação do CRCRN é considerada falta grave, podendo acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 43. São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, entre outras:

I – quaisquer ações ou situações que possam expor o CRCRN à perda financeira e causar danos à sua imagem, direta ou indiretamente, de modo real ou potencial, comprometendo seus ativos de informação;
II – utilização indevida de dados corporativos, divulgação não autorizada de informações ou outras informações sem a permissão expressa do gestor;
III – uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do CRCRN;
IV – a não comunicação imediata à Seção de Tecnologia da Informação de quaisquer descumprimento deste regulamento;
V – o uso ilegal de software;
VI – a introdução (intencional ou não) de vírus de informática;
VII – as tentativas de acesso não autorizado a dados e sistemas;
VIII – a cópia, o compartilhamento ou a impressão de informações restritas ao CRCRN para uso próprio;
IX – a divulgação de informações sigilosas.

Art. 44. Será de inteira responsabilidade de cada colaborador todo prejuízo ou dano que vier a sofrer ou causar ao CRCRN e/ou a terceiros, em decorrência da não obediência às diretrizes e normas definidas neste regulamento.

CAPÍTULO VII
DIVULGAÇÃO E ATUALIZAÇÃO

Art. 45. Esta PSI e suas atualizações, após publicação, deverão ser amplamente divulgadas aos usuários e disponibilizadas no portal do CRCRN, sendo consideradas um documento de relevante interesse público.

Art. 46. Esta Política de Segurança da Informação deverá ser revisada sempre que se fizer necessário, não excedendo ao período máximo de 3 (três) anos, a contar da data de sua publicação.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 47. Os casos omissos desta PSI serão resolvidos pelo Comitê Gestor de Segurança da Informação do CRCRN.

Art. 48. O CRCRN tem o prazo de o prazo de 24 (vinte e quatro) meses para implementação de todas as ações propostas nesta Política de Segurança da Informação.

Art. 49. Esta Resolução entra em vigor na data de sua assinatura.

Contador **Anailson Márcio Gomes**
Presidente

ANEXO I

Termo de Responsabilidade

Pelo presente termo, eu _____, declaro ter conhecimento da Política de Segurança da Informação do Conselho Regional de Contabilidade do Rio Grande do Norte (CRCRN), disponível para consulta no portal do CRCRN, no menu “Governança”, submenu “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 CRCRN 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 CRCRN, 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.

Natal/RN, ____de_____de 20___.

Nome:
Matrícula:
Unidade Organizacional:

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