CONSELHO REGIONAL DE NUTRIÇÃO 10ª REGIÃO

Rua Felipe Schimdt, 321, Florianópolis/SC, CEP 88010-000
Telefone: (48) 3222 - 1967 - http://crn10.org.br/ - E-mail: crn10@crn10.org.br

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

1.1. O CONSELHO REGIONAL DE NUTRIÇÃO DA DÉCIMA REGIÃO (CRN-10) tem como missão contribuir para a garantia do Direito Humano à Alimentação Adequada e Saudável, normatizando e disciplinando o exercício profissional do Nutricionista e do Técnico em Nutrição e Dietética, para uma prática pautada na ética e comprometida com a Segurança Alimentar e Nutricional, em benefício da sociedade.

1.2. O CRN-10 entende que a informação é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços oferecidos aos profissionais e a população.

1.3. O CRN-10 compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações.

1.4. Dessa forma, o CRN-10 estabelece sua Política Geral de Segurança da Informação (PGSI), como parte integrante do seu sistema de gestão, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações do Órgão ou sob sua responsabilidade

2. PROPÓSITO

2.1. Esta política e documentos complementares tem por proposito estabelecer diretrizes e normas de segurança da informação que permitam funcionários, assessorias, conselheiros, membros da diretoria e estagiários do CRN-10 adotar padrões de comportamento seguro, adequados às suas funções institucionais.

2.2. Orientar e divulgar quanto à adoção de controles e processos para atendimento dos requisitos para segurança da informação, visando a sua disponibilidade para todos que se relacionam com o CRN-10, ou que, direta ou indiretamente, são impactados.

2.3. Resguardar as informações do CRN-10, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade.

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal do Órgão e seus funcionários, assessorias, conselheiros, membros da diretoria e estagiários representantes e inscritos.

2.5. Minimizar os riscos de perdas financeiras, da confiança de inscritos, da população ou de qualquer outro impacto negativo para o CRN-10 como resultado de falhas de segurança.

3. ESCOPO

3.1. Esta política se aplica a todos os usuários de informação do CRN-10, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com o CRN-10, tais como empregados, ex-empregados, conselheiros, ex-conselheiros, prestadores de serviço, ex-prestadores de serviço, que possuíram, possuem ou virão a possuir acesso às informações do CRN-10 e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do CRN-10.

4. **DIRETRIZES**

4.1. O objetivo da gestão de segurança da informação do CRN-10, é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas e minimizando riscos identificados e seus eventuais impactos ao Órgão.

4.2. A Diretoria e a COMISSÃO DE PROTEÇÃO DE DADOS E PRIVACIDADE estão comprometidas com uma gestão efetiva de segurança da informação no CRN-10. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis do Órgão.

4.3. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação as necessidades do CRN-10.

4.4. É política do CRN-10:

4.4.1. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação do CRN-10 sejam atingidos por meio da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas.

4.4.2. Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: funcionários, assessorias, conselheiros, membros da diretoria, estagiários e terceiros contratados, onde pertinente, aos inscritos.

4.4.3. Garantir a educação e conscientização sobre as práticas adotadas pelo CRN-10 de segurança da informação para funcionários, assessorias, conselheiros, membros da diretoria, estagiários e terceiros contratados e, onde pertinente, aos inscritos.

4.4.4. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais.

4.4.5. Tratar integralmente incidentes de segurança da informação, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas.

4.4.6. Garantir a continuidade do negócio por meio da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.

4.4.7. Melhorar continuamente a gestão de segurança da informação com a definição e revisão sistemática de objetivos de segurança em todos os níveis do Órgão.

5. **PAPÉIS E RESPONSABILIDADES**

5.1. **COMISSÃO DE PROTEÇÃO DE DADOS E PRIVACIDADE – CPDP**

5.1.1. Fica constituído a COMISSÃO DE PROTEÇÃO DE DADOS E PRIVACIDADE (CPDP), contando com a participação de, pelo menos, um representante da diretoria e um membro das seguintes áreas: Assessoria Jurídica, Área Técnica, Setor Tecnologia da Informação, Gestão de Pessoas, Setor de Ética, Setor de Administração.

5.1.2. É responsabilidade da CPDP:

5.1.2.1. Analisar, propor a aprovação de políticas e normas relacionadas à segurança da informação.

5.1.2.2. Revisar periodicamente a política de segurança e normas a ela relacionadas, sugerindo possíveis alterações.

5.1.2.3. Solicitar, sempre que necessário, a realização de auditorias referentes à conformidade com normas complementares, procedimentos e legislação relacionada à Segurança da Informação.

5.1.2.4. Avaliar relatórios e resultados de auditorias apresentados relativos à Segurança da Informação.

5.1.2.5. Propor a abertura de sindicância para investigar e avaliar os danos decorrentes de quebra de segurança da informação.

5.1.2.6. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação.

5.1.2.7. Garantir que as atividades de segurança da informação sejam executadas em conformidade com esta Política Geral de Segurança da Informação.

5.1.2.8. Promover a divulgação da Política Geral de Segurança da Informação e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do CRN-10.

5.2. **TECNOLOGIA DA INFORMAÇÃO**

5.2.1. É responsabilidade do Setor de Tecnologia da Informação:

5.2.1.1. Conduzir a gestão e operação da segurança da informação, tendo como base esta política e demais resoluções da CPDP.

5.2.1.2. Apoiar a CPDP em suas deliberações.

5.2.1.3. Elaborar e propor a CPDP as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a Política Geral de Segurança da Informação.

5.2.1.4. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco.

5.2.1.5. Tomar as ações cabíveis para se fazer cumprir os termos desta política.

5.2.1.6. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

5.3. **COORDENADORES**

5.3.1. É responsabilidade dos Coordenadores de cada setor:

5.3.1.1. Gerenciar as informações geradas ou sob a responsabilidade da sua área durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo CRN-10.

5.3.1.2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pelo CRN-10.

5.3.1.3. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área, ajustando a classificação e rotulagem delas conforme necessário.

5.3.1.4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade.

5.3.1.5. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo CRN-10.

5.4. **USUÁRIOS DA INFORMAÇÃO**

5.4.1. É responsabilidade dos Usuários da Informação:

5.4.1.1. Ler, compreender e cumprir integralmente os termos desta política, bem como as demais documentos complementares, normas e procedimentos de segurança aplicáveis.

5.4.1.2. Proteger ativos de informação e dados, evitando perda e modificação indevida de forma proposital ou acidental.

5.4.1.3. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a PGSI, suas normas e procedimentos ao Setor de TI ou, quando pertinente, a CPDP.

5.4.1.4. Comunicar ao Setor de TI, tempestivamente, qualquer evento que viole esta política, coloque ou possa a vir a colocar em risco a segurança das informações ou dos recursos computacionais do CRN-10.

5.4.1.5. Assinar o Termo de Responsabilidade de Uso de Recursos Tecnológicos do CRN-10, formalizando a ciência e o aceite integral das disposições da PGSI, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento.

5.4.1.6. Responder pela inobservância da PGSI, normas e procedimentos de segurança, conforme definido no item sanções e punições

6. SANÇÕES E PUNIÇÕES

6.1. As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades previstas pelas leis brasileiras e/ou normas e regulamentos disciplinares do CRN-10.

6.2. No caso de terceiros contratados ou prestadores de serviço, deve-se considerar, em adição, os termos previstos em contrato.

6.3. A aplicação de sanções e punições serão realizadas pelo CRN-10 conforme a análise e parecer da CPDP, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e outros aspectos passíveis de identificação.

6.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao CRN-10, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 7.1 e 7.2 desta política.

7. CASOS OMISSOS

7.1. Os casos omissos serão avaliados pela CDPD para posterior deliberação.

7.2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do CRN-10 adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações do CRN-10.

8. DAS DISPOSIÇÕES FINAIS

8.1. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo CRN-10 devem observar, no que couber, o constante desta PGSI.

8.2. Esta política entra em vigor na data de sua publicação.

9. GLOSSÁRIO

9.1. **Ameaça**: Causa potencial de um incidente, que pode vir a prejudicar o CRN-10.

9.2. **Ativo:** Tudo aquilo que possui valor para o CRN-10.

9.3. **Ativo de informação:** Patrimônio intangível do CRN-10, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao CRN-10 por , inscritos, empregados, conselheiros e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do CRN-10 ou por infraestrutura externa contratada pelo Órgão, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

9.4. **COMISSÃO DE PROTEÇÃO DE DADOS E PRIVACIDADE – CPDP:** Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria do CRN-10, que tem por finalidade tratar questões ligadas à Segurança da Informação e Privacidade.

9.5. **Confidencialidade:** Propriedade dos ativos da informação do CRN-10, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

9.6. **Controle:** Medida de segurança adotada pelo CRN-10 para o tratamento de um risco específico.

9.7. **Disponibilidade:** Propriedade dos ativos da informação do CRN-10, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

9.8. **Gestor da Informação:** Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

9.9. **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do CRN-10.

9.10. **Integridade:** Propriedade dos ativos da informação do CRN-10, de serem exatos e completos.

9.11. **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação do CRN-10.

9.12. **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do CRN-10.

9.13. **Usuário da informação:** Empregados de qualquer área do CRN-10 ou terceiros alocados na prestação de serviços ao CRN-10, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação do CRN-10 para o desempenho de suas atividades profissionais.

9.14. **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as atividades ou ameaçar as informações do CRN-10.

10. **REVISÕES**

10.1. Esta política é revisada com periodicidade anual ou conforme o entendimento da CPDP.

11. **GESTÃO DA POLÍTICA**

11.1. A Política Geral de Segurança da Informação é aprovada pela COMISSÃO DE PROTEÇÃO DE DADOS E PRIVACIDADE, em conjunto com a Diretoria do CRN-10.

11.2. A presente política fica aprovada no dia 30/08/2024 pelo presidente do CRN-10.

Vânia Passero

Presidente do CRN-10

CRN-10/0520

Documento assinado eletronicamente por **Vânia Passero**, **Presidente**, em 30/08/2024, às 16:40, conforme horário oficial de Brasília, com fundamento no §2°, do art. 4°, do Decreto n° 10.543, de 13 de novembro de 2020.