PORTARIA N° 1247/2021

***Ementa**: Define a Política de Segurança da Informação do Conselho Regional de Farmácia do Estado do Rio de Janeiro, CRF-RJ.*

CONSIDERANDO a necessidade e importância de orientar funcionários, conselheiros e terceirizados na implementação de medidas voltadas à gestão de segurança da informação do CRF-RJ, com definição, análise e priorização de ações que correspondam aos objetivos e planejamento estratégico da instituição;

CONSIDERANDO a Lei n º 12.527 DE 2011, que dispõe sobre a Lei de Acesso à Informação;

CONSIDERANDO, por fim, as melhores práticas previstas na norma ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação;

A Presidente do Conselho Regional de Farmácia do Estado do Rio de Janeiro - CRF-RJ, no uso de suas atribuições legais;

RESOLVE:

Artigo 1º - A política de segurança da informação do Conselho Regional de Farmácia do Estado do Rio de Janeiro, CRF-RJ objetiva assegurar que seus ativos, possuídos ou custodiados sejam utilizados e protegidos de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a lei;

Parágrafo único - Fazem parte integrante desta Portaria os Anexos da Política de Segurança da Informação;

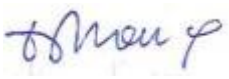
Artigo 2º - Aos funcionários, conselheiros e terceirizados não é escusável o descumprimento da Política de Segurança da Informação do CRF-RJ, alegando desconhecimento, devendo observar integralmente o que dispõe este documento. A inobservância destas regras acarretará a apuração das responsabilidades, podendo haver responsabilização penal, civil e administrativa;

Artigo 3º - As exceções, omissões e casos imprevistos sobre a Política de Segurança da Informação, estabelecida nesta Portaria, devem ser avaliados pelo Serviço de

Tecnologia e Informação do CRF-RJ, incumbida dos assuntos de tecnologia da informação;

Artigo 4º - Esta Portaria entrará em vigor na data de sua publicação e divulgação no site oficial da Instituição.

Rio de Janeiro, 25 de janeiro de 2021.



Tania Maria Lemos Mouço
Presidente CRF-RJ

Anexo da portaria Nº 1247/2021

1- ORIENTAÇÃO DA DIREÇÃO PARA SEGURANÇA DA INFORMAÇÃO

Política de Segurança da Informação – PSI 5 – Políticas de segurança da informação	
CRFRJ - Orientação da direção para segurança da Informação	Revisão: 00 Data: 11/01/2021

1. OBJETIVO

Prover orientação, direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ref. NBR27002:2013)

2. PÚBLICO ALVO

Esta norma é destinada aos FUNCIONÁRIOS, CONSELHEIROS , E TERCEIRIZADOS que exercem atividade no CRF-RJ.

3. REFERÊNCIAS LEGAIS E NORMATIVAS

I - ABNT NBR ISO/IEC 27002:2013 — Tecnologia da Informação — Técnicas de Segurança — Código de Prática para controles de segurança da informação.

II - Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

4. DIRETRIZES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Considerar informação como patrimônio

Assegurar que toda a informação, coletada, gerada, adquirida, utilizada, em trânsito e armazenada; própria, pessoal ou custodiada; por meio de tecnologias, procedimentos, pessoas e ambientes do CRF-RJ, deve ser tratada como parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, integridade e disponibilidade, bem como de proteção de dados pessoais, privacidade e conformidade legal.

5. Focar segurança na informação

Assegurar que essas diretrizes sejam aplicáveis aos ambientes, sistemas, pessoas e processos do CRF-RJ , tanto no meio digital quanto nos meios analógicos de processamento, comunicação e armazenamento de informações.

6. Proteger conforme riscos

Estabelecer medidas de segurança pelo valor do ativo e em função dos riscos de impacto nos negócios, atividades e objetivos institucionais do CRF-RJ , com vistas à proteção de dados

pessoais, à privacidade e à conformidade legal, considerando o balanceamento de aspectos como tecnologias, austeridade nos gastos, qualidade e velocidade.

7 - Responsabilizar proprietário dos ativos

Considerar o funcionário, o conselheiro ou terceirizado, , proprietário dos ativos de informação sob sua responsabilidade, bem como responsável pela liberação e cancelamento do acesso, classificação de segurança e medidas de proteção de informação e dados.

8. Restringir acesso e uso de ativos

Assegurar que o acesso e o uso dos ativos sejam controlados e limitados às atribuições necessárias para cumprimento das atividades de funcionários, conselheiros e terceirizados autorizados e utilizados no estrito interesse do CRF-RJ , apenas para as finalidades profissionais, lícitas, éticas, administrativamente aprovadas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação.

- **Usar ativos seguros**

Permitir somente o uso de ativos homologados e autorizados pelo CRF-RJ , capacidade, manutenção e contingência adequadas e sua operação deve estar de acordo com a legislação, e desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário responsável. Os ativos devem ter documentação atualizada, riscos mapeados, a Política de Segurança da Informação do ente, cláusulas contratuais e legislação em vigor.

9. Tratar informações e dados conforme classificação

Tratar as informações e dados segundo sua classificação de segurança, aposta de maneira a serem adequadamente protegidos quando da sua coleta, criação, utilização, custódia e descarte, para assegurar sua confidencialidade, integridade, disponibilidade.

10. Assegurar a proteção de dados pessoais e a privacidade

Proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa afetar a privacidade do titular (ref. Lei Federal 13709/2018).

11. Manter segurança nos serviços em nuvem

Assegurar que toda a cadeia de suprimentos de TI baseada em provedores de serviços no ambiente de computação em nuvem seja avaliada por todos os aspectos da segurança, incluindo o cumprimento da legislação e regulamentação local e global, o gerenciamento de identidades, o monitoramento e auditoria regulares e as restrições de localização geográfica para proteger dados, metadados, informações e conhecimentos produzidos ou custodiados pelo CRF-RJ.

12. Dar continuidade de uso dos serviços críticos

Assegurar a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos do CRF RJ , por intermédio de ações de administração de crise, prevenção e recuperação, estabelecendo uma estratégia de continuidade de negócio para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas.

13. Monitorar e auditar permanentemente

Monitorar e auditar periodicamente o cumprimento da Política de Segurança da Informação, pelas áreas competentes, respeitando-se os princípios legais e normativos.

14. Conscientizar de forma contínua

Assegurar que funcionários, conselheiros e terceirizados sejam continuamente capacitados e conscientizados sobre os procedimentos de proteção e uso correto dos ativos do CRF-RJ quando da realização de suas atividades, bem como estejam conscientes e cumpram suas responsabilidades, de forma a minimizar riscos.

15. Notificar via canal único

Notificar a área responsável por tratamento incidentes caso o funcionário, conselheiro ou terceirizado identifique qualquer quebra ou fragilidade na segurança da informação.

16.Comunicar no âmbito interno e externo

Recomendar que diretrizes, normas e procedimentos da política de segurança da informação sejam definidos, aprovados pela Direção, publicados e comunicados para todos os funcionários, conselheiros e terceirizados e partes externas relevantes (ref. NBR27002:2013).

17.ANÁLISE CRÍTICA DAS ESPÉCIES NORMATIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Cada espécie normativa da Política de Segurança da Informação – diretrizes, normas e procedimentos - deve ser revista em intervalos planejados, não superiores a 2 (dois) anos, a partir de sua data de publicação, ou em caso de condições obrigatórias de atualização do documento, como:

I - Edição ou alteração de leis e/ou regulamentos;

II - Mudança estratégica da instituição;

III - Expiração da data de validade do documento;

IV - Mudanças de tecnologia na organização; ou

V - A partir dos resultados das análises de risco que estabeleçam a necessidade de mudança da norma para readequação da instituição aos riscos (mitigação).

Competirá ao Sistema de Tecnologia da Informação o monitoramento de periódico das normas, bem como sua complementação por intermédio dos demais instrumentos que compõem a Política de Segurança da Informação CRF-RJ. A aprovação das alterações nas normas que compõe a Política de Segurança da Informação competirá aos gestores do CRF-RJ. O risco de análise crítica para determinar a adequação, suficiência e eficácia das normas deve ser suportado por procedimento formal com registro das sugestões de melhorias e das decisões tomadas em documento específico.

1 - Termos e definições

Política de Segurança da Informação – PSI 3 – Termos e definições	
CRF-RJ-PSI-03.01 - Termos e definições	Revisão: 00
	Data: 11/01/2020

1. OBJETIVO

1.1. Descrever termos e expressões usados na Política de Segurança da Informação, documentando de maneira clara quaisquer termos, classificações ou expressões, cujo significado possa causar dúvidas ou permitir interpretação diversa do que se pretende. Corresponde ao jargão utilizado pela Política de Segurança da Informação e precisa ser observado para que os normativos de segurança sejam entendidos.

2. PÚBLICO ALVO

2.1. Este normativo é destinado aos funcionários, conselheiros e terceirizados que exercem alguma atividade profissional no CRFRJ.

3. REFERÊNCIAS LEGAIS E NORMATIVAS

I - ABNT NBR 16167:2020 - Segurança da Informação — Diretrizes para classificação, rotulação e tratamento da informação.

II - ABNT NBR ISO 55000:2014 — Gestão de ativos — Visão geral, princípios e terminologia.

III - ABNT NBR ISO/IEC 27002:2013 — Tecnologia da Informação — Técnicas de Segurança — Código de Prática para controles de segurança da informação.

IV - Constituição da República Federativa do Brasil de 1988

V - Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

VI - Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

4. TERMOS E DEFINIÇÕES

4.1. Agentes de tratamento – o controlador e o operador (ref. Lei Federal 13.709/2018).

4.2. Anonimização – utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (ref. Lei Federal 13.709/2018).

4.3. Ativo – item, algo ou entidade que tem valor real ou potencial para uma organização (ref. ABNT NBR ISO 55000).

4.4. Ativos de informação - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso.

4.5. Atributos biográficos – dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios (ref. Decreto nº 10.046/2019).

4.6. Atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar (ref. Decreto 10046/2019)

4.7. Atributos genéticos – características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas (ref. Decreto nº 10.046/2019).

4.8. Autoridade Classificadora – autoridade, designada pela organização, responsável pelas decisões no que diz respeito à classificação, à reclassificação, ao acesso e à proteção de uma informação sigilosa.

4.9. Classificação da informação – ação de definir o nível de sensibilidade da informação a fim de assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização (ref. NBR16167:2013)

4.10. Controlador – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (ref. Lei Federal 13.709/2018).

4.11. Cracker – termo usado para designar quem pratica a quebra (ou cracking) de um sistema de TI, de forma ilegal ou sem ética.

4.12. Credencial (ou conta de acesso) – permissão, concedida por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como um crachá), ou lógica (como a identificação de usuário e senha).

4.13. Criticidade – nível de crise (ou impacto) que pode advir da divulgação ou uso indevido da informação (ref. NBR16167:2020).

4.14. Custodiante da informação ou custodiante – usuários, grupos de trabalho ou áreas delegadas pelo proprietário do ativo de informação para cuidar da manutenção e guarda do ativo de informação no dia a dia.

4.15. Dado anonimizado – dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (ref. Lei 13.709/2018).

4.16. Dado pessoal – informação relacionada a pessoa natural identificada ou identificável (ref. Lei Federal 13.709/2018).

4.17. Dado pessoal sensível – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (ref. Lei 13.709/2018).

4.18. Dados cadastrais – informações identificadoras perante os cadastros de órgãos públicos, tais como os atributos biográficos, o número de inscrição no Cadastro de Pessoas Físicas – CPF, o número de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ, o Número de Identificação Social – NIS, o número de inscrição no Programa de Integração Social – PIS, o número de inscrição no Programa de Formação do Patrimônio do Servidor Público – Pasep, o número do Título de Eleitor, a razão social, o nome fantasia e a data de constituição da pessoa jurídica, o tipo societário, a composição societária atual e histórica e a Classificação Nacional de Atividades Econômicas - CNAE e outros dados públicos relativos à pessoa jurídica ou à empresa individual (ref. Decreto nº 10.046/2019)

4.19. Encarregado – pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (ref. Lei Federal 13.709/2018)

4.20. Grupo de acesso – pessoas, grupos de trabalho ou áreas autorizadas a terem acesso à determinada informação (ref. NBR16167:2013).

4.21. Hoax – mensagem que tenta convencer o leitor de sua veracidade por um embuste ou farsa e depois tenta convencê-lo a realizar uma ação específica. A disseminação de um hoax depende do envio deliberado da mensagem à outras vítimas em potencial, que também fazem o mesmo

4.22. Informação – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (ref. Lei Federal nº 12.527/2011).

4.23. Informação de natureza pública – bem público, tangível ou intangível, com forma de expressão gráfica, sonora ou iconográfica, que consiste num patrimônio cultural de uso comum da sociedade e de propriedade das entidades/instituições públicas da administração centralizada, das autarquias e das fundações públicas. A informação de natureza pública pode ser produzida pela administração pública ou, simplesmente, estar em poder dela, para que esteja disponível ao interesse público ou coletivo da sociedade

4.24. Keylogger – Software que rastreia ou registra as teclas pressionadas em um teclado, geralmente de forma encoberta para que a pessoa usando o teclado não esteja ciente de que suas ações estão sendo monitoradas. Isso geralmente é feito por pessoas mal-intencionadas para coletar informações, incluindo mensagens instantâneas, textos e endereços de e-mail, senhas, números de cartões de crédito e contas bancárias, endereços e outros dados privado

4.25. Nível de classificação – categoria a ser definida para cada informação ou classe de informação, que estabelece a sensibilidade da informação em termos de preservação de sua confidencialidade, integridade e disponibilidade (ref. NBR16167:2013).

4.26. Operador – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (ref. Lei Federal 13.709/2018).

4.27. Phishing – forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais, ao se fazer passar como uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial. Isto ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros.

4.28. Privacidade – inviolabilidade do direito a intimidade, a vida privada, a honra e a imagem das pessoas (ref. Constituição da República Federativa do Brasil de 1988).

4.29. Proprietário do ativo de informação – refere-se à parte interessada do CRF-RJ, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

4.30. Proteção de dados pessoais – 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 (ref. Lei Federal 13.709/2018).

4.31. Proxy anônimo – ferramenta que se esforça para fazer atividades na Internet sem vestígios: acessa a Internet a favor do usuário, protegendo as informações pessoais ao ocultar a informação de identificação do computador de origem.

4.32. Redes de bots ou botnet – Forma curta de "rede de robôs", é uma rede de computadores pirateados controlada remotamente por um hacker. O hacker pode usar a rede para enviar spam e lançar ataques de negação de serviço (DoS) e pode alugar a rede para outros cibercriminosos. Um único computador em um bonet pode automaticamente enviar milhares de mensagens de spam por dia. As mensagens de spam mais comuns vêm de computadores zumbis.

4.33. Relatório de impacto à proteção de dados pessoais (RIPD) – documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (ref. Lei Federal 13.709/2018).

4.34. Rótulo – identificação física ou eletrônica da classificação atribuída à informação.

4.35. Segurança da informação - implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware (ref. NBR 27002:2013).

4.36. Sensibilidade – grau de sigilo necessário para informação (ref. NBR16167:2013).

4.37. Smart card – cartão de plástico que geralmente assemelha-se em forma e tamanho a um

cartão de crédito convencional de plástico com um chip de computador embutido.

4.38. Spam – uma mensagem eletrônica indesejada, geralmente não solicitada, enviada por mala-direta. Normalmente, o spam é enviado para vários destinatários que não pediram para recebê-lo. Dentre os tipos de spam estão o spam por e-mail, spam por mensagens instantâneas, spam por mecanismos de pesquisa da Web, spam em blogs e spam por mensagens em telefones celulares. O spam pode conter publicidade legítima, publicidade enganosa e mensagens de phishing que tentam defraudar os destinatários para obter informações pessoais e financeiras. As mensagens não são consideradas spam caso o usuário tenha feito a solicitação para recebê-las.

4.39. Spyware – tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware.

4.40. Setor da Tecnologia e da Informação – ativo estratégico que suporta processos institucionais, por meio da conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, fazer uso e disseminar informações.

4.41. Termo de Classificação da Informação – Documento usado para formalizar a decisão da autoridade competente sobre a classificação da informação, que registra, entre outros dados, o nível de classificação, a categoria na qual se enquadra a informação, o tipo de documento, as datas da produção e da classificação, a indicação de dispositivo legal que fundamenta a classificação, as razões da classificação, o prazo de sigilo ou evento que definirá o seu término e a identificação da autoridade classificadora. O TCI deve ser anexado à informação classificada.

4.42. Titular – pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (ref. Lei Federal 13.709/2018).

4.43. Token – dispositivos físicos geradores aleatórios de código para uso como forma de autenticação.

4.44. Transparência ativa – princípio que exige de órgãos e entidades públicas a divulgação de informações de interesse geral, independentemente de terem sido solicitadas (ref. Lei 12527/2011).

4.45. Visão – declaração de propósito e futuro desejado, com perspectiva de longo prazo.