CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

PORTARIA COREN-SP/PLENÁRIO/024/2016

(Aprovada pelo Plenário na 995ª Reunião Ordinária de 22/12/2016*)*

Dispõe sobre a Política de Segurança da Informação e Comunicações no âmbito do Coren-SP.

O Plenário do Conselho Regional de Enfermagem de São Paulo – COREN-SP, neste ato, legal e regimentalmente representado pela Presidente e pelo Primeiro Secretário desta Autarquia,

CONSIDERANDO o disposto na Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008 e a Norma Complementar nº03 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 30 de junho de 2009,

CONSIDERANDO a deliberação do Plenário do Coren-SP em sua 995ª Reunião Ordinária,

RESOLVE:

CAPÍTULO I

ESCOPO

Art. 1º - Implementar a Política de Segurança da Informação e Comunicações (POSIC) no âmbito do Conselho Regional de Enfermagem de São Paulo – Coren-SP.

Parágrafo Único: A POSIC institui diretrizes, responsabilidades e competências que visam assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações do Conselho Regional de Enfermagem de São Paulo.

Art. 2º - Estão submetidos a esta Política todos os servidores, colaboradores, estagiários e prestadores de serviço que exerçam atividades no âmbito do Conselho Regional de Enfermagem de São Paulo, bem como qualquer pessoa que venha a ter acesso aos seus ativos de informação.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

Art. 3º - Para fins desta Portaria entende-se por:

1. **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do órgão;

2. **Agente Público**: toda pessoa que, por força de lei, contrato ou de qualquer outro ato jurídico, com ou sem remuneração, preste serviços de natureza permanente, temporária, excepcional ou eventual;

3. **Ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

4. **Ativo**: qualquer bem, tangível ou intangível, que tenha valor para a organização;

5. **Ativos de Informação**: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

6. **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

7. **Comitê de Segurança da Informação e Comunicações**: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito deste órgão;

8. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

9. **Criticidade**: grau de importância da informação;

10. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

11. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais**: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

12. **Gestor de área**: responsável pela área funcional onde a informação é criada, comunicada, manuseada, armazenada, custodiada, transportadas ou descartadas;

13. **Gestor de Segurança da Informação e Comunicações**: servidor responsável pelas ações de segurança da informação e comunicações no âmbito deste órgão;

14. **Incidente de segurança da informação**: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores;

15. **Informação**: é um ativo essencial para os negócios de uma organização e, por consequência, necessita ser adequadamente gerenciada e protegida independentemente de seu formato e meio;

16. **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

17. **Política de Segurança da Informação e Comunicações**: documento com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações neste órgão;

18. **Quebra de Segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações neste órgão;

19. **Recursos de TIC**: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

20. **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;

21. **Usuário**: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas, recursos computacionais e a rede corporativa disponibilizados por este órgão;

22. **Vulnerabilidade** : conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III

REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º - As ações de Segurança da Informação e Comunicações do Conselho Regional de Enfermagem de São Paulo deverão observar os seguintes requisitos legais e normativos:

1. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

2. Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008;

3. Norma Complementar nº 02 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 13 de outubro de 2008;

4. Norma Complementar nº 03 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 30 de junho de 2009;

5. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

6. Lei nº 12.527, de 18 de novembro de 2011, que 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;

7. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre 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;

8. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

9. Acórdão do Tribunal de Contas da União nº 461/2004, de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos "logs" com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;

10. Acórdão do Tribunal de Contas da União nº 1603/2009, de 13 de agosto de 2008 - Levantamento de Auditoria. Situação da Governança de tecnologia da Informação - TI na APF. Ausência de Planejamento estratégico Institucional. Deficiência na Estrutura de Pessoal. Tratamento Inadequado à Confidencialidade, Integridade e Disponibilidade das Informações. Recomendações;

11. Norma NBR ISO/IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação;

12. Acórdão do Tribunal de Contas da União nº 2308/2010, de 8 de setembro de 2010 - Avaliação da Governança de Tecnologia da Informação na Administração Pública Federal. Constatação de Precariedades e Oportunidades de Melhoria. Determinações, Recomendações e Comunicações;

13. ISO 31.000 - Diretrizes para a implementação da gestão de riscos;

CAPÍTULO IV

PRINCÍPIOS

Art. 5º - As ações relacionadas com a Segurança da Informação e Comunicações no Conselho Regional de Enfermagem de São Paulo são norteadas pelos seguintes princípios:

1. **Responsabilidade**: os agentes públicos devem conhecer e respeitar todas as normas de segurança da informação e comunicações do Coren-SP;

2. **Ética**: os direitos dos agentes públicos devem ser preservados sem comprometimento da segurança da informação e comunicações;

3. **Clareza**: as regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

4. **Privacidade**: informação que fira o respeito, à intimidade, à integridade e a honra dos cidadãos não podem ser divulgadas;

5. **Eficiência**: realizar um trabalho correto, sem erros e de boa qualidade;

6. **Eficácia**: realizar um trabalho que atinja totalmente os resultados esperados;

7. **Celeridade**: as ações de segurança da informação devem oferecer respostas rápidas a incidentes e falhas;

8. **Publicidade**: dar transparência no trato das informações, observado os critérios legais.

CAPÍTULO V

DIRETRIZES

Art. 6º - As diretrizes desta política aplicam-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação e implementam as seguintes ações de SIC:

a) Gerais

1. Atender as normas e legislação existentes sobre segurança;

2. Definir normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinadas à proteção da informação e à disciplina de sua utilização, no âmbito do Conselho Regional de Enfermagem de São Paulo.

b) Tratamento da Informação

1. Toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada é de propriedade do Conselho Regional de Enfermagem de São Paulo e deve ser

classificada e protegida, adequadamente, quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita;

2. O Agente Público deve ser capaz de identificar a classificação atribuída a uma informação e, a partir desta classificação, conhecer restrições de acesso e de divulgação associadas e obedecê-las;

3. O gestor da área na qual a informação é criada quando cedida a outrem, sempre que necessário, e assessorado juridicamente, deve providenciar a documentação relativa à cessão de direitos sobre as informações do Conselho Regional de Enfermagem de São Paulo, antes da sua disponibilização;

4. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso;

c) Tratamento de Incidentes em Rede

1. Instituir e manter no âmbito do Conselho Regional de Enfermagem de São Paulo, a Equipe de Tratamento de Incidentes em Redes Computacionais (ETIR), através de norma específica;

d) Gestão de Risco

1. Implementar e manter processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações. Esse processo deve possibilitar a seleção e priorização dos ativos a serem protegidos, bem como a definição e implantação de controles para a identificação e tratamento de problemas de segurança. Estas medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança;

e) Gestão de Continuidade

1. Implementar, manter e testar periodicamente processo de gestão da continuidade de negócios visando reduzir, para um nível aceitável, o tempo de interrupção causado por desastres ou incidentes de segurança que afetem os ativos de informação e comunicações;

f) Auditoria e Conformidade

1. O uso dos recursos computacionais e de informações disponibilizadas pelo Conselho Regional de Enfermagem de São Paulo será monitorado, respeitando os princípios legais;

2. Deverão ser mantidos procedimentos, tais como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede interna do Conselho Regional de Enfermagem de São Paulo;

g) Controles de Acesso

1. Os recursos computacionais disponibilizados pelo Conselho Regional de Enfermagem de São Paulo devem ser utilizados estritamente dentro do seu propósito, sendo vedados para uso próprio ou de terceiros, entretenimento, veiculação de opiniões político-partidárias ou religiosas;

2. A entrada e a saída de ativos de informação nas dependências do Conselho Regional de Enfermagem de São Paulo devem ser autorizadas e registradas por autoridade competente;

3. É obrigatório o uso de crachá, carimbo ou etiqueta de identificação, independentemente da forma, deve ser pessoal e intransferível, e possibilitar de maneira clara e inequívoca o reconhecimento de seu portador, de acordo com as orientações estabelecidas pela Gerência de Gestão de Pessoas;

4. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada Agente Público;

5. Os privilégios de acesso às informações devem ser definidos pelo gestor da área responsável pela informação;

6. Sempre que houver mudança nas atribuições de determinado Agente Público, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do Conselho Regional de Enfermagem de São Paulo;

7. Demais regras para o Controle de Acesso serão definidas em norma específica em conformidade com esta POSIC e demais orientações governamentais e legislação em vigor;

h) Uso de e-mail

1. O correio eletrônico é um meio de comunicação corporativa do Conselho Regional de Enfermagem de São Paulo. As regras de acesso e utilização serão definidas por norma específica, em conformidade com esta POSIC e demais orientações e diretrizes de governo;

i) Acesso à Internet

1. Este acesso, no ambiente de trabalho do Conselho Regional de Enfermagem de São Paulo, será regido por norma específica, em conformidade com esta POSIC e demais orientações governamentais e legislação em vigor.

CAPITULO VI

PENALIDADES

Art. 7º - Todos os Agentes Públicos do Conselho Regional de Enfermagem de São Paulo são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: *login*, crachá, carimbo, endereço de correio eletrônico ou assinatura digital.

Art. 8º - O desrespeito ou violação de um ou mais itens desta Política de Segurança da Informação e Comunicações resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas penais e/ou cíveis.

Art. 9º - Deverá ser implantado e mantido o Termo de Responsabilidade, documento que tem por propósito sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações, em conformidade com esta POSIC e demais orientações e diretrizes governamentais e legislação em vigor.

Parágrafo Único: Este Termo deverá ser preenchido pela área responsável pela autorização de acesso aos ativos de informação, conta de serviço ou credencial e assinado pelo usuário beneficiado do acesso.

CAPITULO VII

COMPETÊNCIAS E RESPONSABILIDADES

Art. 10 O Presidente do Conselho Regional de Enfermagem de São Paulo designará agente público que atuará como Gestor de Segurança da Informação e Comunicações (GSIC), com as seguintes competências:

1. Promover cultura de segurança da informação e comunicações;
2. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
3. Propor recursos necessários às ações de segurança da informação e comunicações;
4. Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
5. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
6. Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do Conselho Regional de Enfermagem de São Paulo.

Art. 11 O Comitê de Segurança da Informação e Comunicações (CSIC) será integrado por, pelo menos, 01 (um) representante das áreas funcionais do Conselho Regional de Enfermagem de São Paulo, a saber:

1. Plenário;
2. Gabinete da Presidência;
3. Procuradoria Jurídica;
4. Controladoria Geral;
5. Gerência de Administração e Logística (GEAD);
6. Gerência de Atendimento ao Profissional (GAP);
7. Gerência de Compras e Contratação (GCC);
8. Gerência de Comunicação (GECOM);
9. Gerência de Fiscalização (GEFIS);
10. Gerência de Gestão de Pessoas (GGP);
11. Gerência de Tecnologia da Informação (GTI);
12. Gerência do Coren-SP Educação; e
13. Gerência Financeira (GEFIN).

Art. 12 O Comitê de Segurança da Informação e Comunicações (CSIC) terá as seguintes competências:

1. Assessorar na implementação das ações de segurança da informação e comunicações no Conselho Regional de Enfermagem de São Paulo;

2. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

3. Propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do Conselho Regional de Enfermagem de São Paulo;

4. Revisar e analisar periodicamente as diretrizes e normas estabelecidas nesta política visando a sua aderência e concordância aos objetivos institucionais deste Conselho e as legislações vigentes;

Art. 13 O Agente Público deve comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações ou o descumprimento da POSIC ao Gestor de Segurança da Informação e Comunicações.

CAPITULO VIII

ATUALIZAÇÃO

Art. 14 Todos os instrumentos normativos gerados a partir da POSIC e a própria POSIC, devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 02 anos.

CAPITULO IX

DIVULGAÇÃO

Art. 15 Difundir, a todos os Agentes Públicos do Conselho Regional de Enfermagem de São Paulo por processo permanente de conscientização de segurança da informação, as diretrizes e normas estabelecidas nessa política.

Art. 16 Os contratos firmados pelo Conselho Regional de Enfermagem de São Paulo devem conter cláusulas que determinem a observância da política disposta nesta Portaria e suas respectivas normas.

Art. 17 Em caso de quebra de segurança da informação por meios eletrônicos, a Gerência de Tecnologia da Informação (GTI) deverá ser imediatamente acionada para adotar as providências necessárias.

CAPITULO X

VIGÊNCIA

Art. 18 Esta Portaria entra em vigor na data de sua publicação.

São Paulo, 22 de dezembro de 2016.

FABÍOLA DE CAMPOS BRAGA MATTOZINHO
COREN-SP 68.336
Presidente

MARCUS VINICIUS DE LIMA OLIVEIRA
COREN-SP 51.063
Primeiro Secretário