Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 180 - DOU – 21/09/22 - Seção 1 – p.193

Entidades de Fiscalização do Exercício das Profissões Liberais
CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO

RESOLUÇÃO CREMESP Nº 354, DE 19 DE SETEMBRO DE 2022

Aprova a Política de Segurança da Informação (PSI) do Conselho Regional de Medicina do Estado de São Paulo e dá outras providências.

A Presidência do CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO - Cremesp, no uso de suas atribuições legais e regimentais em conformidade com a Lei nº 3.268/1957 e pelo Regimento Interno da Autarquia, aprovado pela Resolução Cremesp nº 325, de 12 de novembro de 2018;

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

CONSIDERANDO a Constituição Federativa do Brasil de 1988, em especial o art. 5º, LXXIX, que assegura o direito à proteção dos dados pessoais, inclusive nos meios digitais;

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

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

CONSIDERANDO a Portaria GSI/PR n.º 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

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

CONSIDERANDO a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

CONSIDERANDO a Instrução Normativa CFM nº 03, de 03 de março de 2021 - Institui a Política de Privacidade dos Dados das Pessoas Físicas no âmbito do Conselho Federal e nos Conselhos Regionais de Medicina;

CONSIDERANDO as boas práticas preconizadas pelas normas ABNT NBR ISO/IEC, série 27000, Tecnologia da Informação — Técnicas de Segurança —Código de Prática para controles de segurança da informação;

CONSIDERANDO as diretrizes estabelecidas pela norma ABNT NBR 16167:2013 - Segurança da Informação — Diretrizes para classificação, rotulação e tratamento da informação;

CONSIDERANDO os preceitos dispostos na norma ABNT NBR ISO 55000:2014 — gestão de ativos — visão geral, princípios e terminologia;

CONSIDERANDO que o Conselho Regional de Medicina do Estado de São Paulo (Cremesp) recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado;

CONSIDERANDO que as informações no Cremesp 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 necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico e físicocontrolado, eficiente e seguro, de forma a oferecer todas as informações necessárias à classe médica e à sociedade, com integridade, confidencialidade e disponibilidade;

CONSIDERANDO a necessidade de estabelecer responsabilidades internas quanto à segurança da informação;

CONSIDERANDO a Portaria Cremesp nº 79, de 5 de outubro de 2021, que institui a Comissão de Gestão de Segurança da Informação e Proteção de Dados Pessoais e a Designação do Encarregado de Proteção De Dados (EDP) ou Data Protection Office (DPO), resolve:

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) no âmbito do Conselho Regional de Medicina do Estado de São Paulo, nos termos desta Resolução.

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

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

DAS DEFINIÇÕES

Art. 2º Para fins do disposto nesta Instrução Normativa considera-se:

§ 1º - Política de segurança da informação (PSI)é um conjunto de princípios que norteia a gestão de segurança da informação, sendo a expressão formal das regras pelas quais são fornecidos acessos aos recursos tecnológicos de uma instituição.

§ 2º- A segurança da informação é um conjunto de ações que objetiva viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, constituindo-se importantes pilares de proteção da informação e intimamente relacionados aos títulos abordados nesta política.

§ 3º Demais termos e definições utilizados nesta norma estão conceituados no Anexo I - Termos e Definições, desta Resolução.

Seção II

DOS OBJETIVOS

Art. 3º O objetivo desta política é apresentar na forma de títulos, boas práticas em segurança da informação, estabelecendo regras gerais para uso apropriado e seguro dos recursos computacionais da instituição, garantindo a disponibilidade, a integralidade, a confidencialidade e a autenticidade das informações em meio computacional.

Seção III

DA ABRANGÊNCIA

Art. 4º A Política de Segurança da Informação se aplica a todos os empregados, estagiários, prestadores de serviços, conselheiros, delegados, convidados e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao Cremesp e que tenham acesso a qualquer meio de informação e comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Seção IV

DOS PRINCÍPIOS

Art. 5º A PSI do Cremesp orienta-se pelos seguintes princípios básicos:

I. Disponibilidade: é o que garante que os dados e sistemas estejam disponíveis para pessoas autorizadas no momento em que se tornar necessário;

II. Integridade: é o que garante a veracidade das informações, indicando que os dados não podem ser alterados sem autorização;

III. Confidencialidade: é o que garante o acesso das informações apenas às pessoas autorizadas, ou seja, não disponibiliza esse acesso a indivíduos, entidades ou processos não autorizados;

IV. Autenticidade: é o que garante a verdadeira autoria da informação, ou seja, que os dados são de fato provenientes de determinada fonte;

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

VI. capacitação das equipes envolvidas em tecnologias sensíveis;

VII. criação, desenvolvimento e manutenção de cultura relacionada à segurança da

informação, alinhadas às diretrizes nacionais de segurança da informação

CAPÍTULO II

DAS DIRETRIZES GERAIS

Art. 6º As diretrizes têm como objetivo prover orientação, direção e apoio para a segurança da informação de acordo com os requisitos do serviço e com as leis e regulamentações relevantes.

Parágrafo único: Para fins desta Resolução consideram-se as seguintes diretrizes:

I. 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 Conselho Regional de Medicina do Estado de São Paulo, devem ser tratados 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;

II. Focar segurança na informação: Assegurar que essas diretrizes sejam aplicáveis aos ambientes, sistemas, pessoas e processos do Conselho Regional de Medicina do Estado de São Paulo, tanto no meio digital quanto nos meios analógicos de processamento, comunicação e armazenamento de informações;

III. 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 Conselho Regional de Medicina do Estado de São Paulo, 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;

IV. Responsabilizar proprietário dos ativos: Considerar o conselheiro, delegado, colaborador ou terceirizado, registrado no inventário de ativos, proprietário dos ativos de informação sob sua responsabilidade, bem como responsável pelas medidas de proteção de informação e dados dos quais possui acesso;

V. Segregar funções: Segregar a administração e a execução de funções conflitantes ou áreas de responsabilidade críticas, visando reduzir os riscos de mau uso, acidental ou deliberado, dos ativos do Conselho Regional de Medicina do Estado de São Paulo;

VI. Responsabilizar uso da credencial: Liberar o acesso e uso de ativos por meio de credencial, de forma pessoal e intransferível, qualificando o titular como responsável por todas as atividades desenvolvidas por meio dela, sendo pré-requisito o preenchimento do Termo de Responsabilidade e Sigilo;

VII. 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 conselheiros, servidores e terceirizados autorizados e utilizados no estrito interesse do Conselho Regional de Medicina do Estado de São Paulo, apenas para as finalidades profissionais, lícitas, éticas, administrativamente aprovadas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização;

VIII. Usar ativos seguros: Permitir somente o uso de ativos homologados e autorizados pelo Conselho Regional de Medicina do Estado de São Paulo, desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário responsável. Os ativos devem ter documentação atualizada, riscos mapeados, capacidade, manutenção e contingência adequadas e sua operação deve estar de acordo com a Política de Segurança da Informação do Conselho Regional de Medicina do Estado de São Paulo, cláusulas contratuais e legislação em vigor;

IX. 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;

X. 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;

XI. 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 Conselho Regional de Medicina do Estado de São Paulo;

XII. Assegurar continuidade dos serviços críticos: Assegurar a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos de trabalho do Conselho Regional de Medicina do Estado de São Paulo, por intermédio de ações de administração de crise, prevenção e recuperação, estabelecendo uma estratégia de continuidade de serviço para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas.

XIII. 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;

XIV. Conscientizar de forma contínua: Assegurar que conselheiros, servidores e terceirizados sejam continuamente capacitados e conscientizados sobre os procedimentos de proteção e uso correto dos ativos do Conselho Regional de Medicina do Estado de São Paulo quando da realização de suas atividades, bem como estejam conscientes e cumpram suas responsabilidades, de forma a minimizar riscos;

XV. Notificar via canal único: Notificar a área responsável por tratamento de incidentes, caso o colaborador identifique qualquer quebra ou fragilidade na segurança da informação;

XVI. 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 conselheiros, servidores, terceirizados e partes externas relevantes.

CAPÍTULO III

POLÍTICA DE ATUALIZAÇÃO

Art. 7º A elaboração e a adoção da Política de Segurança da Informação interna evidenciam o comprometimento da alta administração com vistas a promover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão de segurança da informação na organização, devendo observar as seguintes premissas nesta política:

§ 1º Periodicidade da Revisão: Cada espécie normativa da Política de Segurança da Informação deve ser revista em intervalos planejados, não superiores a 02(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).

§ 2º Monitoramento Periódico: A Política de Segurança da Informação é complementada por normas, metodologias e procedimentos conforme legislação, cabendo aos responsáveis a sua manutenção, atualização e monitoramento periódico delas.

§ 3º Aprovação das Alterações: A aprovação das alterações nas normas que compõe a Política de Segurança da Informação competirá à Diretoria do CREMESP.

§ 4ºProcesso de Análise Crítica: O processo 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.

CAPÍTULO IV

DA COMPUTAÇÃO EM NUVEM

Art. 8º No cumprimento de suas atribuições legais, O Cremesp adota, no que couber, os requisitos mínimos e as boas práticas de segurança da informação para contratação, implementação e utilização de soluções de computação em nuvem, inclusive os especificados na Instrução Normativa GSI/PR nº 5/2021 e suas eventuais atualizações.

CAPÍTULO V

DAS DISPOSIÇÕES GERAIS

Art. 9º A íntegra da política de segurança da informação do Cremesp será disponibilizada em seu Portal e em sua intranet.

Art. 10. O Conselho Regional de Medicina do Estado de São Paulo estabelece o prazo de 24 (vinte e quatro meses) para implementaçãodas ações propostas por esta Política de Segurança da Informação.

Art. 11. Esta Resolução entra em vigor na data da sua aprovação.

IRENE ABRAMOVICH
Presidente

ANEXO I

TERMOS E DEFINIÇÕES

Para os efeitos desta Política de Segurança da Informação, as expressões, as classificaçõese os termos técnicos adotados nesta normativa, serão entendidos por:

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

Algoritmo Criptográfico- função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente nas informações classificadas.

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).

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

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.

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).

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).

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

Autenticação de Multifatores (MFA) - utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como: as digitais, os padrões de retina, o reconhecimento facial, dentre outros); e onde o usuário está (quando o acesso só pode ser feito em uma máquina específica, cujo acesso é restrito).

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.

Chave Criptográfica - valor que trabalha com um algoritmo criptográfico para cifração ou decifração.

Cibernética - é um termo que pode ser usado como substantivo ou adjetivo. No primeiro caso (como substantivo) refere-se à especialidade científica que compara o funcionamento de uma máquina e o de um ser vivo, principalmente em relação aos mecanismos de comunicação e regulação. No segundo caso (como adjetivo), cibernética refere-se ao que está ligado à realidade virtual e ao que foi produzido ou é controlado por um computador.

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).

Cloud Computing - Computação em nuvem -é um termo coloquial para a disponibilidade sob demanda de recursos do sistema de computador, especialmente armazenamento de dados e capacidade de computação.

CloudBroker- indivíduo ou organização que oferece consultoria, medeia e facilita a seleção de soluções de computação em nuvem em nome de uma organização. Um cloudbroker serve como um terceiro entre um provedor de serviço de nuvem (PSN) e uma organização que contrata serviços de computação em nuvem. Para as infraestruturas de multi-nuvem, o cloudbroker proporciona uma visão mais centralizada de todos os fornecedores e soluções, o que auxilia no gerenciamento dos recursos disponíveis e também dos custos. Em geral, consideram-se quatro tipos de cloudbroker: a) serviços de agregação, que garantem a interoperabilidade entre diversos provedores de serviço de nuvem, por meio da agregação de todos os serviços contratados em uma única interface; b) serviços de integração, que adicionam valor automatizando fluxos de trabalho em ambientes híbridos, por meio de uma única orquestração, para melhorar o desempenho e reduzir o risco de negócios; c) serviços de personalização (ou customização), que modificam os serviços de nuvem existentes, a fim de atender às necessidades dos negócios da contratante, podendo inclusive desenvolver recursos adicionais para executar corretamente os serviços desejados; d) serviços de arbitragem, fornecendo flexibilidade ao contratante por intermédio da oferta de vários serviços semelhantes para avaliação e seleção.

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).

Cookies - são arquivos de texto que contêm pequenas quantidades de informações que são armazenadas no seu dispositivo quando você visita um site. Essas informações podem ser sobre você, as suas preferências ou sobre o seu dispositivo. Os cookies podem ter diferentes objetivos, como permitir que você navegue entre as páginas com eficiência, lembrando suas preferências e, geralmente, melhorando a experiência do usuário.

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

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).

Criticidade - nível de crise (ou impacto) que pode advir da divulgação ou uso indevido da informação (ref. NBR16167:2013).

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. Geralmente não faz parte do grupo de acesso e, portanto, não está autorizado a acessar a informação (ref. NBR16167:2013).

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).

Dado pessoal - informação relacionada à pessoa natural identificada ou identificável (ref. Lei Federal 13.709/2018). Se uma informação permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, então ela é considerada um dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, retrato em fotografia, prontuário de saúde, cartão bancário, histórico de pagamentos, endereço de IP (Protocolo da Internet), entre outros.

Dado pessoal sensível - dado relacionado à 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, que, quando vinculado a uma pessoa natural e usados de forma inadequada podem gerar constrangimentos ou a discriminação de uma pessoa (ref. Lei 13.709/2018).

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).

Dados de crianças e adolescentes - informação relacionada a criança de até 12 anos de idade incompletos e adolescente, aquela entre 12 e 18 anos (ref. Lei 8.069/1990).

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).

Firewall - Em informática, um firewall (em português: parede de fogo), raramente traduzido como corta-fogo ou corta-fogos, é um dispositivo de uma rede de computadores, na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP.

Governança de TIC - conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam assegurar que as decisões e ações relativas à gestão e ao uso de TIC mantenham-se harmoniosas às necessidades institucionais e contribuam para o cumprimento da missão e o alcance das metas organizacionais.

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

Hipervisor- é um software que cria e executa máquinas virtuais (VMs). Também chamado de monitor da máquina virtual (VMM), ele isola o sistema operacional do hipervisor e os recursos das máquinas virtuais e permite a criação e o gerenciamento dessas máquinas. Quando usado como hipervisor, o hardware físico é chamado de host, enquanto as diversas máquinas virtuais que utilizam seus recursos são chamadas de guests.

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 a outras vítimas em potencial, que também fazem o mesmo.

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 12.527/2018).

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.

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 email, senhas, números de cartões de crédito e contas bancárias, endereços e outros dados privados.

Metadados - O prefixo "Meta" vem do grego e significa "além de". Assim, Metadados são informações que acrescem aos dados e que têm como objetivo informar-nos sobre eles para tornar mais fácil a sua organização. Um item de um metadado pode informar do que se trata aquele dado numa linguagem inteligível para um computador. Os metadados têm a função de facilitar o entendimento dos relacionamentos e evidenciar a utilidade das informações dos dados.

Malware - software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits.

NetBus é um trojan. Ferramenta de administração remota com uma interface muito simples e muito fácil de utilizar que utiliza a porta 12345. Tem funções como abrir e fechar drive de cd, iniciar algum programa, controlar mouse entre outras. O Indivíduo que controla a máquina infectada remotamente, pode fazer download, abrir programas, deletar arquivos e formatar partições. Um perigo se cair em mãos mal-intencionadas, porém sendo muito útil em assistência remota.

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).

Objetivos Estratégicos - resultados que a TIC pretende atingir, com vistas à concretização da missão e ao alcance da visão, observando as diretrizes estratégicas do planejamento institucional do órgão.

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).

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 email, mensagem instantânea, SMS, dentre outros.

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).

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

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).

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.

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 ciber criminosos. Um único computador em um botnet pode automaticamente enviar milhares de mensagens de spam por dia. As mensagens de spam mais comuns vêm de computadores zumbis.

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).

Rótulo - identificação física ou eletrônica da classificação atribuída à informação.

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).

Segurança de Rede - Consiste em uma série de medidas que visam garantir que o acesso aos dados compartilhados pela empresa seja feito apenas por quem tiver autorização. As medidas servem, também, para assegurar que apenas o administrador da rede tenha controle sobre ela, impedindo que outros façam alterações que comprometam o sistema.

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

Sigilo - é a condição de algo que é mantido como oculto e secreto, fazendo com que poucas pessoas saibam da sua existência. Quando uma pessoa pede sigilo sobre determinado assunto, está implícito que a informação não deve ser reproduzida para outras pessoas, mas sim reservada exclusivamente para aquela que a está recebendo.

Sigilo Profissional - proibição legal de divulgar informações obtidas no exercício de uma atividade profissional, dever ético de não revelar dados confidenciais obtidos no âmbito da profissão; segredo profissional.

Grau de Sigilo - é a gradação atribuída a dados, informações, documentos, áreas ou edificações, considerados sigilosos em decorrência de sua natureza ou conteúdo. Normalmente são classificados em: ultra-secreto, secreto, confidencial, reservado e de conheço público.

Single SignOn (SSO) - é uma solução tecnológica que permite que diversos aplicativos com senhas de acesso diferentes possam ser acessados de forma transparente e segura pela utilização de uma única senha principal ou meio de identificação pessoal (como a biometria ou um personalidentificationnumber- PIN, por exemplo). Ou seja,

com o SSO, o usuário digita apenas uma senha quando faz o primeiro acesso e depois vai abrindo os demais aplicativos sem necessidade de digitar a senha específica do aplicativo.

Smartcard - 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.

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 email, 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.

Spammer- pessoa que envia diversos emails ou mensagens (geralmente propaganda eletrônica) sem autorização do receptor.

Spyware- tipo de malware. 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.

TCP/IP -(TCP - sigla de transmissioncontrol protocole IP - sigla de Internet protocol) trata-se de um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede.

Tecnologia da Informação e Comunicação (TIC) - 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.

Termo de Classificação da Informação (TCI) - 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.

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

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

Trojan (ou Cavalo de Troia) - tipo de malware que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

IRENE ABRAMOVICH
Presidente do Conselho