Código de Serviços Qualificados

ANBIMA

TÍTULO II – PRINCÍPIOS, REGRAS E PROCEDIMENTOS PARA AS ATIVIDADES DE SERVIÇOS QUALIFICADOS

(...)

CAPÍTULO V – REGRAS E PROCEDIMENTOS

(...)

Seção III – Privacidade e proteção de dados pessoais~~Segurança e Sigilo das Informações~~

~~**Art. 12.** As Instituições Participantes devem estabelecer mecanismos para:~~

~~I. Propiciar o controle de informações confidenciais, reservadas ou privilegiadas a que tenham acesso os seus sócios, diretores, administradores, profissionais e terceiros contratados; e~~

~~II. Assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico;~~

~~III. Assegurar meios eletrônicos seguros para envio e recepção de informações; e~~

~~IV. Manter seus manuais operacionais atualizados, com a descrição de arquivos e atividades, matrizes de risco, documentação dos programas, controles de qualidade e regulamentos de segurança.~~

Art. 12. ~~§1º.~~ As instituições participantes devem implementar e manter, em documento~~(s)~~ escrito~~(s)~~ e com base em critérios próprios, regras, ~~e~~ procedimentos e controles internos

que trate de privacidade e dos dados pessoais a que a instituição tenha acesso ~~para assegurar o disposto no caput,~~ incluindo, no mínimo:

I. Como se dá o controle de privacidade e dados pessoais a que a instituição tem acesso, identificando, no mínimo: controlador, processador, bases legais, finalidade, duração de tratamento, compartilhamento e responsabilidades.

II. Critérios adotados para a proteção da confidencialidade dos ativos de informação e dos dados pessoais tratados durante todo o seu ciclo de vida, conforme classificação da informação, abordando desde a sua geração até o seu descarte, incluindo armazenamento, acesso, criptografia, tratamento, transmissão e transporte.

III. Regras aplicáveis aos colaboradores para o gerenciamento de identidade e acesso aos ativos de informação e dados pessoais a que tenham acesso, desde o início até o término do relacionamento do colaborador com a instituição, inclusive nos casos de mudança de atividade dentro da mesma instituição, de forma a garantir o adequado tratamento dos dados.

IV. Prazo para atualização do documento de que trata o caput, que não deve ser superior a 24 (vinte e quatro) meses, ou sempre que necessário se a regulamentação exigir.

~~I. Regras de acesso às informações confidenciais, reservadas ou privilegiadas, indicando como se dá o acesso e controle de pessoas autorizadas e não autorizadas a essas informações, inclusive nos casos de mudança de atividade dentro da mesma instituição ou desligamento do profissional;~~

~~II. Regras sobre concessão de senhas para acesso aos sistemas e restrição de acesso à área responsável pela prestação das Atividades, de forma a garantir a integridade das informações e impedir o acesso de pessoas não autorizadas formalmente, bem como a periodicidade para a realização da revisão de acesso aos sistemas, áreas e diretórios;~~

III. Regras específicas sobre proteção da base de dados e procedimentos internos para tratar casos de vazamento de informações confidenciais, reservadas ou privilegiadas mesmo que oriundos de ações involuntárias;

IV. Regras sobre gravações de ligações telefônicas, monitoramento de mensagens eletrônicas para funcionários que sejam autorizados e/ou terem contato com clientes para realizar a validação das informações das operações com as instituições intermediárias, quando esta validação não for automatizada, bem como o prazo para manutenção das gravações; e

V. Regras de restrição ao uso de sistemas, acessos remotos e qualquer outro meio/veículo que contenham informações confidenciais, reservadas ou privilegiadas no exercício de suas atividades.

§2º. As Instituições Participantes devem implementar treinamento para os sócios, diretores, alta administração e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas.

§3º. As Instituições Participantes devem estar aptas a enviar e receber informações por meio de arquivo padrão, disponibilizado pela ANBIMA em seu site na internet e atualizado nos meses de maio e de outubro de cada ano, e de acordo com as regras e prazos definidos pela Diretoria.

Art. 13. As Instituições Participantes devem exigir que seus profissionais assinem, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei.

Parágrafo único. Os terceiros contratados que tiverem acesso às informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas no exercício de

~~suas atividades, devem assinar o documento previsto no caput, podendo tal documento ser excepcionado quando o contrato de prestação de serviço possuir cláusula de confidencialidade.~~

Seção IV – Plano de Continuidade de Negócios

Art. 1~~3~~4. As instituições participantes devem implementar e manter, em documento escrito, plano de continuidade de negócios observando-se, no mínimo:

I. Formas alternativas para processamento em situações de contingência, assegurando a continuidade das atividades em tempo hábil para cumprimento de suas responsabilidades.

~~I. Ambiente alternativo para processamento em situações de contingência com estrutura física e tecnológica adequadas, assim como versões de sistemas idênticas às do local de processamento principal, e que esteja localizado a uma distância razoável do local de processamento principal, assegurando a continuidade das Atividades;~~

~~II.~~ Análise de riscos potenciais, os quais a instituição esteja exposta com a indicação da medida de contingência a ser adotada para mitigação. ~~, sendo que nesta indicação devem constar, no mínimo:~~

~~III. Opções de deslocamento até o ambiente alternativo que deve possuir rotas diferentes das utilizadas para acesso ao ambiente principal;~~

~~IV. Tempo necessário para deslocamento até o ambiente alternativo, sendo que esse tempo não deve afetar a continuidade das Atividades; e~~

~~Em caso de uso de filial da instituição situada em outra cidade como ambiente alternativo, a Instituição Participante deve possuir profissional nesta filial~~

~~devidamente treinado e habilitado para assumir as Atividades durante o tempo de deslocamento dos profissionais responsáveis.~~

~~V. Avaliação quanto à localidade dos ambientes, principal e alternativo, a fim de verificar se a área é propensa a protestos, invasões, movimentos paredistas (greve) e incidentes naturais;~~

~~VI. Avaliação quanto aos horários dos edifícios que os ambientes, principal e alternativo, estão locados, identificando se possuem restrições;~~

~~VII. Acesso a dados e informações armazenadas em locais e instalações diferentes do local de processamento principal e que permitam a ativação e continuidade do processamento de suas Atividades;~~

~~VIII.~~II. Planos de contingência, detalhando os procedimentos de ativação, o estabelecimento de prazos para a implementação e a designação das equipes que ficarão responsáveis pela operacionalização dos referidos planos.~~;~~

~~IX. Validação ou testes, no mínimo, a cada 12 (doze) meses, ou em prazo inferior se exigido pela Regulação em vigor; e~~

~~X. Documento que descreva a metodologia utilizada pela auditoria dos sistemas, bem como a periodicidade de sua aplicação.~~

~~**Parágrafo único.** A validação ou testes de que trata o inciso VII do caput tem como objetivo avaliar se os Planos de Continuidade de Negócios desenvolvidos são capazes de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da instituição e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se tais planos podem ser ativados tempestivamente.~~

Seção V – Segurança da informação e cibersegurança~~Cibernética~~

Art. 1~~45~~. As instituições participantes devem implementar e manter, em documento escrito, regras, procedimentos e controles de segurança da informação e de cibersegurança ~~cibernética~~ que sejam compatíveis com o seu porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas.

§1º. O documento de que trata o caput deve ser formulado com base em princípios que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pelas instituições participantes e deve conter, no mínimo:

I. Indicação dos procedimentos adotados para controle de informações consideradas pela instituição como confidenciais, reservadas ou privilegiadas a que tenham acesso os seus sócios, diretores, administradores, colaboradores e terceiros contratados.

~~I.~~II. Avaliação de riscos, que deve identificar os ativos considerados relevantes~~, sejam pela instituição, sejam~~ eles equipamentos, sistemas, dados ou processos, suas vulnerabilidades considerando a identificação de probabilidades e impactos de possíveis ameaças cibernéticas~~e possíveis cenários de ameaças;~~.

~~II.~~III. Ações de proteção e prevenção, visando mitigar os riscos identificados~~;~~.

~~III.~~IV. Descrição dos mecanismos de supervisão para cada risco identificado, de forma a verificar sua efetividade e identificar eventuais incidentes~~;~~.

~~IV. Criação de um plano de resposta a incidentes, considerando os cenários de ameaças previstos durante a avaliação de riscos, que permita a continuidade dos negócios ou a recuperação adequada em casos mais graves; e~~

~~V. Indicação de responsável dentro da instituição para tratar e responder questões de segurança cibernética.~~

~~**§2º.** As Instituições Participantes podem usar o documento que preveja as regras, procedimentos e controles de segurança cibernética de seu Conglomerado ou Grupo Econômico.~~

§2~~3~~º. É recomendável que as instituições participantes observem, na elaboração do documento de que trata o caput, o ~~Manual~~guia ANBIMA de Segurança Cibernética disponível no site da Associação na internet.

Art. 1~~5~~~~6~~. As instituições participantes devem exigir que seus colaboradores e/ou terceiros contratados assinem, de forma manual ou eletrônica, documento de confidencialidade sobre as informações confidenciais, reservadas ou privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei.~~O conteúdo dos documentos exigidos neste capítulo pode constar de um único documento, inclusive por Conglomerado ou Grupo Econômico, desde que haja clareza a respeito dos procedimentos e regras exigidos em cada seção, e deve ser atualizado em prazo não superior a 24 (vinte e quatro) meses, ou quando houver alteração na Regulação que demande modificações.~~

Parágrafo único. As instituições participantes estão dispensadas de assinar o documento de que trata o caput, caso o contrato de prestação de serviço do profissional ou terceiro contratado possua cláusula de confidencialidade.

Art. 16. As instituições participantes devem assegurar que suas regras e procedimentos de contratação de terceiros contemplem a contratação de serviços de processamento e

armazenamento de dados e de computação em nuvem, no País ou no exterior, classificados como críticos e/ou de maior risco conforme metodologia de cada instituição.

Parágrafo único. A contratação de serviços de processamento e armazenamento de dados de que trata o caput deve assegurar a verificação da capacidade do potencial prestador de serviço, incluindo, no mínimo:

I. o cumprimento da regulamentação em vigor.
II. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço.
III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço.
IV. a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado, caso aplicável.
V. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados.
VI. a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos.
VII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

Seção VI – Tratamento de incidentes

Art. 17. As instituições participantes devem estabelecer plano de ação e de resposta a incidentes visando à implementação das regras, procedimentos e controles internos de privacidade, proteção de dados pessoais, segurança da informação, segurança cibernética e contingência.

§1º. O plano mencionado no caput deve considerar os incidentes cibernéticos previstos durante a avaliação de riscos, e garantir a continuidade dos negócios ou a recuperação adequada em casos mais graves.

§2º. O plano mencionado no caput deve abranger, no mínimo:

I. as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes das regras, procedimentos e controles internos de privacidade, proteção de dados pessoais, segurança da informação, segurança cibernética e contingência.

II. as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes indicadas acima.

III. a área responsável pelo registro e controle dos efeitos de incidentes considerados relevantes pela instituição.

IV. alçada de reporte dos incidentes identificados.

§3º. O plano de resposta a incidentes indicado deverá prever, minimamente, o procedimento de comunicação com órgãos reguladores e titulares dos dados comprometidos pelo incidente, incluindo cenários, processo de decisão de comunicação e prazo para efetivação da comunicação.

Seção VII – Governança

Art. 18. As instituições participantes devem instituir mecanismos de acompanhamento com vistas a assegurar a implementação e a efetividade das regras, procedimentos e controles internos de que trata as seções deste capítulo.

Parágrafo único. Os mecanismos de acompanhamento de que trata o caput devem conter, no que couber:

I. definição das áreas e/ou profissionais responsáveis por assegurar o cumprimento das obrigações previstas em cada seção.

II. quais processos e controles são adotados no acompanhamento de que trata o caput, incluindo, mas não se limitando, a trilha de auditoria.

III. definição de metodologias, métricas, critérios e indicadores utilizados.

IV. mapeamento dos cenários de estresse, incidentes e risco e formas de tratamento.

V. realização de testes com plano de ação para tratamento e correção de eventuais deficiências encontradas.

Art. 19. Os instrumentos referidos no artigo anterior deverão incluir mecanismos de validação e testes, no mínimo, anuais, ou em prazo inferior se exigido pela regulamentação em vigor.

Parágrafo único. Os mecanismos de validação ou testes descritos tem como objetivo avaliar se as medidas de sigilo, proteção de dados, segurança cibernética e os planos de continuidade de negócios e plano de prevenção de incidentes desenvolvidos são capazes de suportar, de modo satisfatório, os processos operacionais, sistemas e bancos de dados críticos, manter sua integridade, segurança e consistência na infraestrutura adotada, e verificar se tais políticas ou planos podem ser ativados tempestivamente.

Art. 20. As instituições participantes deverão implementar e manter programa de conscientização para todos seus profissionais, incluindo terceiros, sobre práticas gerais de proteção de informações confidenciais, reservadas ou privilegiadas e dados pessoais, segurança da informação e cibersegurança, e sobre os protocolos de continuidade de negócios e prevenção de incidentes.

Art. 21. No mínimo anualmente, ou em prazo inferior se exigido pela regulamentação em vigor, as instituições participantes deverão realizar a revisão das políticas, documentos, conteúdo do programa de conscientização e planos indicados neste capítulo.

Art. 22. O conteúdo dos documentos exigidos neste capítulo pode constar de um único documento, inclusive por conglomerado ou grupo econômico, desde que haja clareza a respeito dos procedimentos e regras exigidos em cada seção.