MINISTÉRIO DA FAZENDA - MF
COMISSÃO DE VALORES MOBILIÁRIOS - CVM
Rua Sete de Setembro, 111 32º andar - Bairro Centro - Rio de Janeiro/RJ - CEP 20050-901
(21)3554-8245 - www.cvm.gov.br

PORTARIA/CVM/PTE/Nº 162, DE 14 DE OUTUBRO DE 2015

O Presidente da COMISSÃO DE VALORES MOBILIÁRIOS – CVM, no uso das atribuições que lhe confere o Regimento Interno aprovado pela Portaria MF nº 327, de 11 de julho de 1977 e considerando o disposto no art. 23 da Lei nº 8.159, de 8 de janeiro de 1991, o Decreto nº 4.553, de 27 de dezembro de 2002, e o Decreto nº 3.505, de 13 de junho de 2000, RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações - POSIC no âmbito da COMISSÃO DE VALORES MOBILIÁRIOS (CVM).

CAPÍTULO I - DO ESCOPO

Art. 2º A Política de Segurança da Informação e das Comunicações (POSIC) tem o objetivo de estabelecer diretrizes estratégicas, responsabilidades, competências, normas e procedimentos de uso, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações, sistemas, documentos, correspondências e publicações, bem como seus repositórios ou meios de armazenamento, reconhecidamente necessários ao desempenho das atribuições da Autarquia, contra ameaças que possam comprometer seus ativos e/ou sua imagem institucional.

§1º As diretrizes estabelecidas nesta política devem estar alinhadas ao Planejamento Estratégico Institucional, ao Plano Diretor de TI e em consonância com os valores institucionais.

§2º Os agentes públicos a serviço da CVM devem observar as diretrizes, normas, procedimentos, mecanismos, competências e responsabilidades estabelecidos nesta POSIC.

§3º Integram também a POSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

§4º A POSIC trata das diretrizes gerais acerca do uso e compartilhamento de ativos de informação durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade dos processos vitais da CVM, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como os valores éticos e as melhores práticas de Segurança da Informação e das Comunicações (SIC).

CAPÍTULO II - DOS CONCEITOS E DEFINIÇÕES

Art. 3º No âmbito da POSIC, considera-se:

I. **Acesso**: ato de ingressar, transitar, conhecer ou consultar dados ou informações, bem como a possibilidade de usar os ativos de informação;

II. **Agente público**: servidores, consultores, estagiários, prestadores de serviços que, por força de contratos, convênios, protocolos, acordos de cooperação e instrumentos congêneres, executem atividades vinculadas que os tornem autorizados a obter acesso a informações e sistemas da CVM;

III. **Ameaça**: conjunto de fatores internos, externos ou causa potencial de um incidente, que pode resultar em comprometimento da segurança dos ativos da organização;

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

V. **Ativo Crítico**: ativo do qual a organização depende, em maior ou menor grau, para a continuidade de suas atividades e serviços;

VI. **Ativos de informação**: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, materializadas ou não, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VII. **Autenticação**: confirmação acerca da identidade de um usuário ou sistema para fins de acesso ou execução de operações. Podem ser utilizados fatores múltiplos de autenticação, a exemplo de certificação digital, informações biométricas, login e senha;

VIII. **Autenticidade**: garantia de que o dado ou informação é verdadeiro e fidedigno na origem, em trânsito e no destino. Assevera a legitimidade e autoria do dado ou informação;

IX. **Avaliação de riscos**: procedimento de comparar um risco estimado com um critério, com o objetivo de determinar a sua relevância;

X. **Classificação da informação**: identificação dos níveis de proteção das informações e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

XI. **Comitê de Segurança da Informação e das Comunicações (CSIC)**: colegiado responsável pela normatização e supervisão da segurança da informação e comunicações na CVM;

XII. **Componente Organizacional**: parte integrante da estrutura organizacional da CVM, com atribuições definidas nos atos normativos aplicáveis;

XIII. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoas físicas, sistemas, órgãos ou entidades não autorizadas;

XIV. **Controle de acesso**: conjunto de procedimentos, recursos e meios

utilizados com a finalidade de conceder, monitorar ou bloquear o acesso;

XV. **Credencial de acesso**: recursos que identifiquem univocamente determinado usuário nos mais variados cenários: usuário/senha de rede, crachá, carimbo, correio eletrônico, certificado digital;

XVI. **Criptografia**: conjunto de técnicas pelas quais a informação pode ser transformada de sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, tornando impraticável a leitura por alguém não autorizado;

XVII. **Criticidade**: grau de importância da informação para a continuidade das atividades e serviços da CVM;

XVIII. **CTIR.GOV**: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e das Comunicações do Gabinete de Segurança Institucional da Presidência da República DSIC/GSI/PR;

XIX. **Custodiante do ativo de informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação, materializados ou não, que não lhe pertencem, mas que estão sob sua custódia;

XX. **Desastre**: catástrofes naturais, pandemias, incêndios, inundações, inacessibilidade ao local de trabalho, falhas nos sistemas de TI, dentre outros.

XXI. **Descarte**: eliminação de informações e documentos, em qualquer tipo de suporte, observando os procedimentos de segurança;

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

XXIII. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)**: equipe responsável por receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores na CVM;

XXIV. **Evento**: ocorrência identificada como uma possível violação da POSIC, falha de controles ou uma situação previamente conhecida que possa ter consequências para a segurança da informação;

XXV. **Gestão de ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XXVI. **Gestão de continuidade dos negócios**: processo que identifica desastres potenciais para uma organização e os possíveis impactos nas operações de negócio, caso esses desastres se concretizem. Esse processo fornece estrutura para que se desenvolva e mantenha o plano de continuidade de negócios, capaz de manter o funcionamento dos processos e salvaguardar a reputação e a marca da organização e suas atividades de valor agregado;

XXVII. **Gestão de Riscos**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXVIII. **Gestor do ativo de informação**: gestor do Componente Organizacional designado para responder pelo ativo como parte de sua atribuição regimental ou, nos casos omissos, por designação específica de superior hierárquico, tornando-se responsável pela sua segurança;

XXIX. **Grau de sigilo**: gradação atribuída aos ativos de informação em decorrência do teor e elementos intrínsecos das informações e dados sigilosos que contenham;

XXX. **Gestor de Segurança da Informação e das Comunicações (GSIC)**: responsável pelas ações de SIC no âmbito da CVM;

XXXI. **Impacto**: alteração no nível de disponibilidade, integridade, confidencialidade e autenticidade dos serviços e/ou ativos de informação disponíveis para os agentes públicos;

XXXII. **Incidentes de SIC**: eventos que tenham causado algum dano, colocado em risco algum ativo de informação ou interrompido a execução de alguma atividade por um período de tempo;

XXXIII. **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

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

XXXV. **Política de Segurança da Informação e das Comunicações (POSIC)**: documento aprovado pelo Comitê de Governança de TI e pelo Colegiado da CVM, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação e das Comunicações na Autarquia;

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

XXXVII. **Recursos criptográficos**: sistemas, programas, processos e equipamentos isolados ou em rede que utilizem algoritmo simétrico ou assimétrico para realizar a cifração ou decifração de informações;

XXXVIII. **Recursos de TI**: subgrupo dos ativos de informação dedicados à produção, armazenamento, transmissão e processamento de informações;

XXXIX. **Risco de SIC**: potencial impacto associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças;

XL. **SIC**: Segurança da Informação e das Comunicações;

XLI. **TCO**: Titular do Componente Organizacional;

XLII. **Tratamento de incidentes**: é o serviço de responsabilidade da ETIR que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XLIII. **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III - DOS PRINCÍPIOS

Art. 4º As ações relacionadas à SIC na CVM são norteadas pelos seguintes princípios:

I.**Legalidade**: a POSIC levará em consideração as leis, as normas, instruções, procedimentos e as políticas administrativas, organizacionais, técnicas e operacionais formalmente estabelecidas e emanadas da CVM;

II.**Impessoalidade**: a POSIC visará ao interesse público no tratamento das informações, buscando evitar que estas sejam utilizadas para finalidades particulares ou para a obtenção de benefícios pessoais;

III.**Moralidade**: a elaboração da POSIC, bem como sua posterior aplicação, deverá observar os preceitos da boa administração pública, pautando-se pela atuação ética e nos ideais de honestidade e justiça;

IV.**Publicidade**: as diretrizes, normas e procedimentos da POSIC definidos pela CVM devem ser publicados e amplamente divulgados para o balizamento dos agentes públicos no pleno desempenho de suas atribuições;

V.**Responsabilidade**: a POSIC deverá ser seguida pelos agentes públicos no exercício de suas atividades, pautando-se por atitudes e comportamentos condizentes com as diretrizes, normas e procedimentos de SIC;

VI.**Proporcionalidade**: a aplicação da POSIC, no que abrange o nível, a complexidade e o custo das ações deverá ser adequada ao entendimento administrativo e aos valores dos ativos a serem protegidos.

CAPÍTULO IV - DA ESTRUTURA E GESTÃO DA SIC

Art. 5º Fica instituído o Gestor de Segurança da Informação e das Comunicações (GSIC), a ser designado pelo PTE, subordinado ao Superintendente de Informática, com mandato de 3 (três) anos, passível de recondução.

Art. 6º Fica instituído o Comitê de Segurança da Informação e das Comunicações (CSIC), órgão colegiado, de natureza consultiva e executiva, com os seguintes integrantes:

I.Superintendência Geral – SGE;

II.Gestor de Segurança da Informação e das Comunicações (GSIC);

III.Superintendência Administrativo-Financeira – SAD;

IV.Assessoria de Comunicação Social – ASC;

V.Assessoria de Análise e Pesquisa – ASA;

VI.Superintendência de Proteção e Orientação aos Investidores – SOI;

§1º A coordenação do CSIC compete à SGE e a coordenação técnica ao GSIC.

§2º Nas hipóteses de ausência, afastamento ou impedimento de qualquer integrante do CSIC, poderá ser designado substituto.

§3º O CSIC poderá convidar para assessorá-lo, quando necessário, qualquer servidor da CVM, bem como consultar especialistas e representantes de outras instituições.

§4º O CSIC poderá atribuir a responsabilidade por projetos específicos a um de seus membros, bem como instituir grupos de trabalho com representantes dos componentes organizacionais que o integram.

Art. 7º Fica instituída a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), a ser regulamentada pelo CSIC, com a responsabilidade de receber, analisar e responder a eventos relacionados à SIC.

Parágrafo único. A ETIR deverá ser composta pelo Gestor de SIC, ou por servidor por ele indicado, além de servidores da área de TI indicados pelo Superintendente de Informática e aprovados pelo Superintendente Geral, nos termos da regulamentação mencionada no *caput* deste artigo.

CAPÍTULO V - DAS DIRETRIZES

Seção I – Das Diretrizes Gerais

Art. 8º As informações criadas, armazenadas, manuseadas, transportadas, custodiadas ou descartadas, referentes à CVM, são patrimônio da Autarquia, classificadas e manipuladas de acordo com normas e legislação específica em vigor, mantendo a segurança durante todo o seu ciclo de vida.

Parágrafo único. O uso das informações deverá ser feito apenas para o desempenho das atividades profissionais.

Art. 9º Todos os contratos celebrados pela CVM com prestadores de serviços devem conter cláusulas que determinem a observância da POSIC e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência.

Art. 10. Os prestadores de serviços sob contrato com a CVM serão obrigados a assinar Termo de Aceitação, em obediência ao estabelecido na POSIC.

Seção II – Do uso de recursos de TI

Art. 11. Os recursos de tecnologia da informação vinculados às unidades da CVM,

colocados à disposição para uso como ferramenta de trabalho, devem ser utilizados em atividades primordialmente relacionadas às funções institucionais desempenhadas pela Autarquia.

Parágrafo único. É vedado o uso de recursos computacionais para armazenar ou transmitir conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso.

Art. 12. É vedada a utilização dos recursos de tecnologia da informação com o objetivo de praticar ações prejudiciais ao funcionamento e à utilização de quaisquer recursos da rede de computadores da CVM ou redes externas.

Parágrafo único. A Superintendência de Informática (SSI) pode autorizar terceiros ou efetuar testes controlados de sistemas e de infraestrutura com o objetivo de identificar vulnerabilidades e mensurar riscos, adotando as medidas preventivas cabíveis a fim de evitar quaisquer efeitos danosos ou impactos indesejáveis ao ambiente computacional e ao trabalho dos usuários.

Art. 13. O uso dos recursos computacionais pelos agentes públicos da rede da CVM está sujeito à monitoração, respeitando-se os princípios constitucionais e legais aplicáveis.

Art. 14. É vedado aos agentes públicos não autorizados alterar, física ou logicamente, as estações de trabalho disponibilizadas pela Autarquia.

Art. 15. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento das informações, de acordo com a sua classificação.

Seção III – Da gestão de ativos de informação

Art. 16. As informações e dados produzidos ou recebidos pela CVM, em decorrência do desempenho de seu mandato, serão considerados públicos, ressalvadas as exceções previstas na legislação aplicável.

Art. 17. Os ativos de informação devem:

I. ser inventariados e protegidos;

II. ter identificados os seus proprietários e custodiantes;

III. ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV. ter a sua entrada e saída nas dependências da CVM autorizadas e registradas por autoridade competente;

V. ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI. ser regulamentados por norma específica quanto a sua utilização; e

VII. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 18. Cada ativo de informação da CVM deverá ter um gestor designado pelo CSIC.

Art. 19. A definição do custodiante do ativo de informação deve ser feita formalmente pelo gestor do ativo de informação.

Parágrafo único. A ausência desta designação pressupõe que o gestor é o próprio custodiante.

Art. 20. O CSIC deve criar, gerir e avaliar critérios de tratamento e classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 21. Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 22. Durante todo o ciclo de vida de um ativo de informação, sua manipulação e uso observarão medidas especiais de segurança compatíveis com seu grau de sigilo e em conformidade com a legislação vigente e normas complementares adotadas pela CVM.

Art. 23. O acesso dos agentes públicos aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a termo de sigilo e responsabilidade.

Seção IV – Do tratamento de incidentes de segurança

Art. 24. Nos contratos de serviços relacionados ao provimento, gerenciamento e suporte da infraestrutura computacional de TI, deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de SIC por parte do prestador.

Parágrafo único. Em relação aos contratos mencionados no *caput*, cabe à ETIR supervisionar o tratamento de incidentes de SIC para o fiel cumprimento das suas atribuições.

Art. 25. A ETIR tem autonomia para tomar ações emergenciais para a resposta aos incidentes de SIC e deverá manter mecanismos de articulação com o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov).

Seção V – Da gestão de risco

Art. 26. A gestão de riscos em SIC constitui um processo contínuo de planejamento, execução, verificação e revisão das ações que visem manter em níveis aceitáveis os riscos de SIC a que estão sujeitos os ativos de informação da CVM.

Art. 27. Deverá ser definida, em normatização complementar, a metodologia de análise e avaliação de riscos, que será realizada periodicamente no levantamento de risco nos ativos de informação da CVM, visando à proteção destes ativos.

Art. 28. A normatização mencionada no art. 27 deverá assegurar que as atividades de análise e avaliação produzam resultados comparáveis e reproduzíveis, de modo a permitir a priorização no tratamento dos maiores riscos.

§1º A normatização de que trata o *caput* deverá contemplar a definição de níveis aceitáveis de riscos, de acordo com requisitos legais, regulatórios ou internos da CVM.

§2º Todos os riscos identificados, mesmo os que forem considerados aceitáveis, deverão ter sua evolução acompanhada para permitir a detecção de possíveis mudanças no seu impacto ou probabilidade de ocorrência.

Seção VI – Da gestão de continuidade de negócios

Art. 29. A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e procedimentos que visem assegurar o funcionamento continuo ou recuperação antecipada da CVM quando da ocorrência de indisponibilidade de recursos de infraestrutura, de tecnologia ou de recursos humanos, isolada ou simultaneamente.

Art. 30. O Plano de Continuidade de Negócios da CVM, baseado em metodologias e boas práticas e aprovado pelo CSIC, deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

Seção VII – Da auditoria e conformidade

Art. 31. A CVM manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos de informação, considerando sua criticidade.

Art. 32. Os processos de negócio, em todas as áreas da CVM, deverão ser auditados na conformidade com as normas de SIC e a pertinente legislação em vigor.

Art. 33. É vedada ao prestador de serviços a responsabilidade de executar a verificação da conformidade dos próprios serviços prestados.

Art. 34. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo GSIC e aprovado pelo CSIC.

Parágrafo único. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo GSIC ao CSIC, e será montado um plano de ação para a tomada das ações cabíveis.

Seção VIII – Dos controles de acesso

Art. 35. As instalações, equipamentos, redes e sistemas de computadores, exceto os sistemas destinados a atendimento ao público, deverão possuir mecanismos adequados de controle de acesso físico e/ou lógico, que possibilitem a identificação das pessoas.

Art. 36. O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa.

Art. 37. Para utilização dos recursos de TI da CVM será sempre necessária a autenticação do agente público, mediante credencial de acesso.

§1º As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimento sobre a CVM.

§2º As credenciais de acesso deverão delegar a seu portador somente os níveis de privilégio mínimos ao exercício de sua função.

Art. 38. Os equipamentos e softwares utilizados na administração dos recursos de TI deverão ser protegidos por senha, que será de conhecimento exclusivo dos técnicos da SSI e/ou terceiros responsáveis pela administração destes recursos.

Parágrafo único. Os administradores dos recursos de TI da CVM são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade, disponibilidade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Art. 39. Na ocorrência de afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da Autarquia, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos.

Parágrafo único. Na efetivação do desligamento do usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos de informação a ele atribuídos.

Art. 40. A senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio agente público, a qualquer tempo, ou por determinação da SSI, especialmente quando houver suspeita de sua violação.

Parágrafo Único. Qualquer utilização dos sistemas e demais recursos de informática da CVM é de responsabilidade do agente público ao qual estejam associadas as credenciais de acesso utilizadas.

Art. 41. A senha de rede valerá por prazo determinado, em normatização complementar estabelecida pela SSI, ressalvado o caso da certificação digital, regida por regra específica.

Parágrafo único. A SSI divulgará as regras a serem seguidas na definição da senha de rede dos agentes públicos, além de recomendações que visem assegurar a maior privacidade possível da senha.

Art. 42. Deverão ser implementados controles de acesso físico para o acesso às dependências da CVM, com a disponibilização de credenciais que permitam o acesso dos agentes públicos às instalações da Autarquia.

Art. 43 Deverão ser disponibilizadas credenciais de acesso físico também aos visitantes, que permitirão o acesso destes às instalações da CVM, sempre mediante autorização de servidor da área visitada.

§1º Os visitantes não poderão possuir credenciais de acesso a redes e sistemas de computadores da CVM, exceto nos casos de redes destinadas para tais pessoas, autorização expressa da SSI e casos previstos em lei.

§2º Nos casos de invalidação temporária ou definitiva das credenciais de acesso de agentes públicos, o acesso aos ativos de informação da Autarquia dar-se-á mediante as condições estabelecidas para os visitantes.

Seção IX – Do desenvolvimento de sistemas

Art. 44. O CSIC deverá estabelecer critérios de segurança para desenvolvimento de sistemas de informação, de forma a abranger todas as fases do ciclo de desenvolvimento e atividades de manutenção.

Art. 45. Os desenvolvimentos e aquisições de sistemas e aplicações corporativas devem atender a requisitos de segurança previstos em norma específica.

CAPÍTULO VI - DAS PENALIDADES

Art. 46. Ações que violem a POSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aos responsáveis poderão ser aplicadas as sanções administrativas, penais e civis em vigor.

CAPÍTULO VII - DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 47. A CVM deverá prover os recursos humanos e materiais necessários à aplicação da POSIC.

Art. 48. Compete ao GSIC:

I. promover cultura de SIC;

II. acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de SIC;

III. propor recursos necessários às ações de SIC;

IV. coordenar tecnicamente o CSIC;

V. coordenar a ETIR, podendo delegar essa função a um agente responsável;

VI. acompanhar estudos de novas tecnologias, quanto a possíveis

impactos na SIC;

VII. manter contato permanente e estreito com o Departamento de Segurança da Informação e das Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIG/GSI/PR, para o trato de assuntos relativos à SIC;

VIII. propor normas e procedimentos relativos à SIC no âmbito da CVM;

IX. elaborar, com a colaboração dos demais integrantes do CSIC, um relatório das atividades do Comitê, a ser emitido com periodicidade semestral;

X. propor a capacitação dos servidores em SIC, inclusive a participação em fóruns, redes, congressos, grupos de discussões e afins;

XI. coordenar a instituição, a implementação e a manutenção da infraestrutura necessária à ETIR; e

XII. decidir sobre os casos omissos relativos à SIC.

Art. 49. Compete ao CSIC:

I. estabelecer padrões e procedimentos necessários para assegurar a implementação da POSIC;

II. propor a constituição de grupos de trabalho para tratar de temas e apresentar soluções específicas sobre SIC;

III. atualizar a POSIC e as normas complementares;

IV. propor normas complementares e procedimentos internos relativos à SIC;

V. propor a implementação de mecanismos que permitam a quantificação, a qualificação e o levantamento de custos dos incidentes de SIC e do mau funcionamento e vulnerabilidades de sistemas;

VI. definir critérios para verificação técnica periódica destinada a aferir o cumprimento da POSIC da CVM, suas Normas Complementares e Procedimentos Operacionais;

VII. definir responsáveis por projetos específicos; e

VIII. coordenar a elaboração do Plano de Continuidade de Negócios.

Art. 50. Compete à ETIR:

I. receber, filtrar, classificar e responder as solicitações e alertas relacionados a incidentes de SIC;

II. realizar as análises dos incidentes de SIC;

III. propor e recomendar ações de SIC;

IV. executar medidas de recuperação relacionadas a incidentes de SIC;

V. assessorar o CSIC na proposição de normas relacionadas a incidentes de SIC;

VI. realizar monitoração de uso e inspeções para avaliação de conformidade do uso dos recursos computacionais com as normas de SIC em vigor;

VII. prestar suporte em SIC aos diversos Componentes Organizacionais da CVM.

Art. 51. Compete à Gerência de Recursos Humanos (GAH) da CVM:

I. notificar a SSI sobre qualquer alteração de cargo, função ou lotação de agentes públicos da CVM, bem como sobre afastamentos destes por períodos superiores a 30 (trinta) dias; e

II. promover a capacitação dos agentes públicos nas normas de SIC adotadas pela CVM.

Art. 52. Compete à SSI:

I. implantar ações técnicas para os controles de segurança dos ativos de informação, de acordo com a sua classificação;

II. encaminhar solicitação dos recursos necessários para implantação da POSIC, no limite de suas atribuições, à Autoridade competente para as providências cabíveis;

III. prestar assessoria técnica aos gestores de ativos e ao CSIC nos temas relacionadas a TI;

IV. informar ao CSIC situações que eventualmente comprometam a SIC;

V. operacionalizar a ETIR no âmbito de suas atribuições;

VI. monitorar o uso dos recursos computacionais; e

VII. promover o aperfeiçoamento constante de seu corpo técnico quanto às boas práticas e tecnologias de SIC.

Art. 53. Compete aos TCO:

I. indicar as necessidades de treinamento dos agentes públicos lotados no CO pelo qual é responsável no que diz respeito às normas de SIC adotadas pela CVM;

II. indicar as necessidades de concessão/revogação de credenciais de acesso para os agentes públicos nos ativos de informação de sua responsabilidade, de acordo com sua classificação.

III. classificar os ativos de informação sob sua responsabilidade;

IV. determinar o nível de acesso dos seus subordinados e terceiros frente aos ativos de informação sob sua responsabilidade; e

V. solicitar o credenciamento e descredenciamento de colaboradores associados a contratações sob sua responsabilidade;

Art. 54. Compete aos agentes públicos:

I. conhecer e disseminar institucionalmente a POSIC e as normas complementares de SIC, propondo, inclusive, sugestões de melhoria;

II. cumprir e fazer cumprir as normas e procedimentos relativos à segurança da informação e das comunicações da CVM;

III. informar imediatamente à ETIR qualquer evento relacionado à SIC.

IV. zelar pelo sigilo das suas credenciais de acesso aos ativos de informação da CVM;

V. comunicar a perda ou o comprometimento das suas credenciais de acesso;

VI. responder pela quebra de segurança ocorrida com a utilização da sua credencial de acesso; e

VII. manter o nível de proteção da informação a que tem acesso.

CAPÍTULO VIII - DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 55. A POSIC está em consonância, entre outros, com os seguintes atos normativos:

I. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

II. 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 caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

III. Decreto nº 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação e das Comunicações nos órgãos e entidades da Administração Pública Federal;

IV. Decreto nº 7845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

V. Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159, de 8 de janeiro de 1991;

VI. Decreto nº 1048, de 21 de janeiro de 1994, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, do Poder Executivo Federal;

VII. 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;

VIII. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

IX. Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que define a metodologia de gestão de Segurança da Informação e Comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

X. Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações - POSIC nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XI. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – Etir nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XII. Norma Complementar nº 07/IN01/DSIC/GSIPR, de 6 de maio de

2010, que estabelece diretrizes para o implemento de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XIII. Normas ABNT NBR ISO/IEC 27001, 27002 e 27005, que instituem melhores práticas para gestão da segurança da informação.

CAPÍTULO IX - DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 56. A POSIC será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 57. As propostas de alteração ou criação de normas internas sobre SIC deverão ser encaminhadas ao CSIC.

Art. 58. Após sua publicação, o CSIC deverá dar ampla divulgação da POSIC a todos os agentes públicos.

Art. 59. A POSIC deverá ser revisada e atualizada sempre que eventos ou mudanças significativas relativas ao tema assim o exigirem ou a cada período de 3 (três) anos.

Art. 60. O descumprimento de qualquer dispositivo desta POSIC e demais normas e procedimentos estabelecidos relativos à SIC configura descumprimento do dever inserido no art. 116, inciso III, da Lei nº 8.112, de 1990.

§1º Caso se verifique o descumprimento previsto no *caput* por funcionários de prestadores de serviços terceirizados, eventuais colaboradores ou estagiários, a CVM poderá determinar a respectiva substituição ou o desligamento, sem prejuízo das eventuais sanções penais e civis previstas na legislação aplicável.

§2º Os agentes públicos registrarão em Termo de Responsabilidade o conhecimento de todas as normas e procedimentos de SIC, bem como das penalidades a que estarão sujeitos em caso de descumprimento ou violação da POSIC.

Art. 61. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo CSIC.

Art. 62. Esta Portaria entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Leonardo Porciúncula Gomes Pereira**, **Presidente**, em 20/10/2015, às 14:08, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.cvm.gov.br/conferir_autenticidade, informando o código verificador **0050145** e o código CRC **826E096F**.
*This document's authenticity can be verified by accessing https://sei.cvm.gov.br/conferir_autenticidade, and typing the "Código Verificador" **0050145** and the "Código CRC" **826E096F**.*