MINISTÉRIO DA ECONOMIA - ME
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 155, DE 31 DE AGOSTO DE 2021

Dispões sobre a Política de Segurança da Informação – PoSIn no âmbito da Comissão de Valores Mobiliários.

O Presidente da COMISSÃO DE VALORES MOBILIÁRIOS – CVM, no uso das atribuições que lhe confere o Regimento Interno aprovado pela Resolução CVM nº 24, de 5 de março de 2021 e considerando o Decreto nº 9.637, de 26 de dezembro de 2018,

Resolve:

Art. 1º Instituir a Política de Segurança da Informação – PoSIn no âmbito da CVM.

CAPÍTULO I
DO ESCOPO

Art. 2º A PoSIn 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 ou sua imagem institucional.

§1º As diretrizes estabelecidas nesta política devem estar alinhadas ao Planejamento Estratégico Institucional, ao Plano Diretor de TI, à Política de Gestão de Documentos 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 PoSIn.

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

§4º A PoSIn 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 – SI.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3º No âmbito da PoSIn, serão consideradas as definições apresentadas na Portaria GSI/PR nº 93, de 26 de setembro de 2019:

CAPÍTULO III
DOS PRINCÍPIOS

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

I - Legalidade: a PoSIn 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 PoSIn 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 PoSIn, 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 PoSIn definidos pela CVM devem ser publicados e amplamente divulgados para o balizamento dos agentes públicos no pleno desempenho de suas atribuições;

V - Responsabilidade: a PoSIn 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 SI;

VI - Proporcionalidade: a aplicação da PoSIn, 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; e

VII - Privacidade: os dados pessoais de pessoas naturais, quando tratados pela CVM no âmbito de suas atividades, devem estar consoantes com o interesse público ou com o consentimento do titular para assegurar-lhe a inviolabilidade da intimidade, da honra e da imagem.

CAPÍTULO IV
DA ESTRUTURA E GESTÃO DA SI

Art. 5º A PoSIn é proposta pelo Gestor de Segurança da Informação – GSIN e aprovada pelo Comitê de Gestão de Segurança da Informação – CGSIN e pelo Comitê de Governança e Gestão Estratégica – CGE.

§1º Por iniciativa do GSIN, grupos de trabalho podem ser formados para conceber, planejar ou realizar atividades específicas de SI.

§ 2º A recepção, a análise e o tratamento de eventos de SI será realizada pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

CAPÍTULO V

DAS DIRETRIZES

Seção I - Das Diretrizes Gerais

Art. 6º 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. 7º Todos os contratos celebrados pela CVM com prestadores de serviços devem conter cláusulas que determinem a observância da PoSIn e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência.

Art. 8º. Os prestadores de serviços sob contrato com a CVM serão obrigados a assinar Termo de Aceitação, em obediência ao estabelecido na PoSIn.

Seção II - Do uso de recursos de TI

Art. 9º. 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. 10. 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 Tecnologia da Informação 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. 11. 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. 12. É vedado aos agentes públicos não autorizados alterar, física ou logicamente, as estações de trabalho disponibilizadas pela Autarquia.

Art. 13. 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. 14. 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. 15. 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. 16. Cada ativo de informação da CVM deverá ter um gestor designado pelo CGSIN.

Art. 17. 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. 18. O CGSIN 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. 19. 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. 20. 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. 21. 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. 22. 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 SI por parte do prestador.

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

Seção V - Da gestão de risco

Art. 23. A gestão de riscos em SI constitui um processo contínuo de planejamento, execução, verificação e revisão das ações que visem

manter em níveis aceitáveis os riscos de SI a que estão sujeitos os ativos de informação da CVM.

Art. 24. 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. 25. A normatização mencionada no art. 24 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. 26. A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e procedimentos que visem assegurar o funcionamento contínuo ou recuperação antecipada da CVM quando da ocorrência de indisponibilidade de recursos de infraestrutura, de tecnologia ou de recursos humanos, isolada ou simultaneamente.

Art. 27. O Plano de Continuidade de Negócios da CVM, baseado em metodologias e boas práticas e aprovado pelo CGSIN, deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

Seção VII - Da auditoria e conformidade

Art. 28. 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. 29. Os processos de negócio, em todas as áreas da CVM, deverão ser auditados na conformidade com as normas de SI e a pertinente legislação em vigor.

Art. 30. É vedada ao prestador de serviços a responsabilidade de executar a verificação da conformidade dos próprios serviços prestados.

Art. 31. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo GSIN e aprovado pelo CGSIN.

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

Seção VIII - Dos controles de acesso

Art. 32. 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. 33. O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa.

Art. 34. 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. 35. Os equipamentos e softwares utilizados na administração dos recursos de TI deverão ser protegidos por senha, que será de conhecimento exclusivo dos técnicos da STI 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. 36. 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. 37. 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 STI, 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. 38. A senha de rede valerá por prazo determinado, em normatização complementar estabelecida pela STI, ressalvado o caso da certificação digital, regida por regra específica.

Parágrafo único. A STI 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. 39. 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. 40. 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 STI 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. 41. O CGSIN 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. 42. Os desenvolvimentos e aquisições de sistemas e aplicações corporativas devem atender a requisitos de segurança previstos em norma específica.

CAPÍTULO VI
DAS PENALIDADES

Art. 43. Ações que violem a PoSIn ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SI serão devidamente apuradas e aos responsáveis poderão ser aplicadas as sanções administrativas, penais e civis em vigor.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 44. Compete à STI:

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 PoSIn, no limite de suas atribuições, à Autoridade competente para as providências cabíveis;

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

IV - informar ao CGSIN situações que eventualmente comprometam a SI;

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 SI.

Art. 45. Compete à Superintendência Administrativo-Financeira – SAD:

I - notificar a STI 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 SI adotadas pela CVM.

Art. 46. Compete aos Titulares de Componentes Organizacionais - TCOs:

I - indicar as necessidades de treinamento dos agentes públicos lotados no CO pelo qual é responsável no que diz respeito às normas de SI 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. 47. Compete aos agentes públicos:

I - conhecer e disseminar institucionalmente a PoSIn e as normas complementares de SI, 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 SI.

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.

Art. 48. As competências do GSIN e do CGSIN serão definidas em portarias específicas.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 49. A PoSIn será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 50. As propostas de alteração ou criação de normas internas sobre SI deverão ser encaminhadas ao CGSIN.

Art. 51. Após sua publicação, o CGSIN deverá dar ampla divulgação da PoSIn a todos os agentes públicos.

Art. 52. A PoSIn 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. 53. O descumprimento de qualquer dispositivo desta PoSIn e demais normas e procedimentos estabelecidos relativos à SI 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 SI, bem como das penalidades a que estarão sujeitos em caso de descumprimento ou violação da PoSIn.

Art. 54. Os casos omissos e as dúvidas surgidas na aplicação desta Portaria serão dirimidos pelo CGSIN.

Art. 55. Esta Portaria entra em vigor em 1 de outubro de 2021.

MARCELO BARBOSA

Presidente

Documento assinado eletronicamente por **Marcelo Santos Barbosa**, **Presidente**, em 31/08/2021, às 19:10, com fundamento no art. 6º 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 **1336273** e o código CRC **2E60B86F**.

*This document's authenticity can be verified by accessing https://sei.cvm.gov.br/conferir_autenticidade, and typing the "Código Verificador" **1336273** and the "Código CRC" **2E60B86F**.*