

Resolução BCB nº 287 de 24/I/2023

RESOLUÇÃO BCB Nº 287, DE 24 DE JANEIRO DE 2023

Divulga a Política de Segurança da Informação do Banco Central do Brasil (PSIBC).

O Comitê de Governança, Riscos e Controles (GRC) do Banco Central do Brasil, no uso das suas atribuições, com base no art. 11, parágrafo único, e art. 132, inciso VII, alínea “a”, do Regimento Interno, anexo à Portaria nº 84.287, de 27 de fevereiro de 2015, e tendo em vista o disposto no Voto GRC 71/2023, de 24 de janeiro de 2023,

R E S O L V E :

Art. 1º Fica divulgada a Política de Segurança da Informação do Banco Central do Brasil (PSIBC), anexa a esta Resolução.

Art. 2º O Presidente do Comitê de Segurança (Coseg) pode editar os atos complementares necessários para o cumprimento da PSIBC.

Art. 3º Fica revogada a Resolução BCB nº 115, de 14 de julho de 2021.

Art. 4º Esta Resolução entra em vigor em 1º de fevereiro de 2023.

Carolina de Assis Barros
Diretora de Administração

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO BANCO CENTRAL DO BRASIL (PSIBC), ANEXA À RESOLUÇÃO BCB Nº 287, DE 24 DE JANEIRO DE 2023

CAPÍTULO I DAS FINALIDADES

Seção I Dos Objetivos

Art. 1º A Política de Segurança da Informação do Banco Central do Brasil (PSIBC) estabelece diretrizes, responsabilidades e ações para a sua gestão e tem por objetivo assegurar:

- I- a segurança cibernética;
- II- a segurança física e a proteção de dados organizacionais; e
- III- a disponibilidade, a integridade, a confidencialidade, a autenticidade da informação e a proteção de dados pessoais.

Art. 2º A PSIBC tem os seguintes propósitos:

- I- atender às exigências legais e normativas aplicáveis à Administração Pública Federal;
- II- orientar as ações necessárias à garantia da segurança da informação;
- III- definir competências e atribuições decorrentes; e
- IV- servir de referência para efeitos de auditoria e corregedoria.

Art. 3º A PSIBC abrange:

- I- as áreas de negócio do Banco Central do Brasil em todas as praças;
- II- os conhecimentos tácitos e os explícitos;
- III- os meios físicos;
- IV- a Tecnologia da Informação e Comunicação (TIC) do Banco Central do Brasil;
- V- os projetos, as ações e as atividades de trabalho exercidos dentro ou fora das instalações do Banco Central do Brasil; e
- VI- os dirigentes, os servidores, os terceirizados, os estagiários, os aprendizes, os prestadores de serviço e os visitantes.

Seção II

Das Definições

Art. 4º Para os fins da PSIBC, consideram-se as seguintes definições:

I- administrador de recurso de TIC: pessoa responsável pela administração e manutenção de um recurso de TIC;

II- ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;

III - ativo de informação: os meios, os locais, os equipamentos e os sistemas de armazenamento, transmissão e processamento da informação;

IV- autenticidade: propriedade pela qual se assegura que a informação foi produzida ou expedida, modificada ou destruída por uma pessoa natural, equipamento, sistema, órgão ou entidade;

V - autoridade de monitoramento da Lei de Acesso à Informação (LAI): autoridade diretamente subordinada ao dirigente máximo do órgão ou entidade da Administração Pública Federal direta e indireta, indicada para acompanhar o cumprimento da LAI e de seus regulamentos, na forma do art. 40 da Lei nº 12.527, de 18 de novembro de 2011;

VI - ciclo de vida da informação: conjunto de fases composto por planejamento ou pré-produção, produção, divulgação, transporte, armazenamento e descarte de informação ou documento;

VII- classificação: atribuição, pela autoridade competente, de grau de sigilo reservado, secreto ou ultrassecreto a informação que necessite de restrição de acesso temporária, na forma do art. 23 da Lei nº 12.527, de 2011;

VIII - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizados nem credenciados;

IX- credencial de segurança: certificado que autoriza pessoa para o tratamento de informação classificada;

X - criptografia: conjunto de técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, tornando impraticável a leitura por pessoa não autorizada;

XI - dado: forma primária de informação, que não foi processada, correlacionada, integrada, avaliada, interpretada ou atribuída qualquer sentido inerente em si mesma;

XII- dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

XIII - dado pessoal sensível: dado pessoal sobre 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, quando vinculado a uma pessoa natural;

XIV- disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;

XV - encarregado de dados pessoais: pessoa indicada pelo controlador ou pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XVI - Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes Computacionais (Etir): grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XVII- gestor de segurança e credenciamento: responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e nos postos de controle, devidamente credenciado;

XVIII - gestor de segurança da informação: coordenador, no âmbito do Comitê de Segurança (Coseg), nos assuntos relacionados à segurança da informação;

XIX- incidente de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XX - incidente cibernético: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança cibernética;

XXI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXII - informação sigilosa: informação submetida à restrição de acesso público por estar abrangida por hipótese de sigilo legal;

XXIII - informação classificada: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada;

XXIV - informação de acesso restrito: informação sigilosa, informação classificada e as demais informações que devem ser protegidas de forma a preservar os princípios da PSIBC, sem prejuízo das legislações específicas;

XXV - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVI - irretratabilidade: princípio de segurança da informação por meio do qual é garantido o não repúdio às informações fornecidas;

XXVII - necessidade de conhecer: condição segundo a qual o conhecimento da informação de acesso restrito é indispensável para o adequado exercício de cargo, função, emprego ou atividade;

XXVIII - privilégio mínimo: conjunto mínimo de permissões necessárias em um ativo de informação para que um usuário possa realizar suas atividades de trabalho;

XXIX - recurso de TIC: qualquer ativo de informação usado para o tratamento de dados e informações em meio digital;

XXX - regime não presencial: modalidade em que o usuário executa suas atribuições integral ou parcialmente fora das dependências físicas do Banco Central do Brasil;

XXXI - regime presencial: modalidade em que o usuário executa suas atribuições integralmente nas dependências físicas do Banco Central do Brasil;

XXXII - resiliência cibernética: capacidade de identificação, prevenção, detecção, resposta e recuperação a incidentes cibernéticos;

XXXIII - risco: definido como a quantificação da incerteza, no contexto da segurança da informação pode ser entendido como o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto desses ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXXIV - risco cibernético: exposição a danos e perdas resultantes da ocorrência de incidentes cibernéticos;

XXXV - rotulação: atribuição, por pessoa competente, de rótulo a dado ou informação visando ao estabelecimento de níveis adequados de proteção;

XXXVI - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXXVII - segurança cibernética: ações voltadas para preservar a disponibilidade, a integridade, a confidencialidade e a autenticidade, bem como os demais princípios da PSIBC, dos recursos de TIC do Banco Central do Brasil e de dados e informações tratados nesses recursos;

XXXVIII - tratamento: toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XXXIX - usuários: dirigentes, servidores, terceirizados, estagiários, aprendizes, prestadores de serviço e visitantes que de alguma forma possam ter acesso a ativos de informação do Banco Central do Brasil; e

XL - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou organização e que podem ser evitados por uma ação interna de segurança da informação.

Seção III

Das Referências Legais e Normativas

Art. 5º Os conceitos e as ações desenvolvidas no âmbito da PSIBC são regidos pelas seguintes normas:

I - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI) e dispõe sobre a governança da segurança da informação;

II - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

III - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV - Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal, bem como sua Norma Complementar nº 01/IN02/DSIC/GSIPR, de 27 de junho de 2013;

V - Instrução Normativa GSI/PR nº 3, de 6 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

VI - Normas Técnicas NBR ISO/IEC 27001 e NBR ISO/IEC 27002, da Associação Brasileira de Normas Técnicas (ABNT), que instituem o código de melhores práticas para gestão de segurança da informação;

VII - Código de Conduta dos Servidores do Banco Central do Brasil;

VIII - Código de Conduta da Alta Administração Federal;

IX- Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, anexo ao Decreto nº 1.171, de 22 de junho de 1994;

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

XI- Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (LAI);

XII- Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 2011;

XIII- Decreto nº 7.845, 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; e

XIV- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

CAPÍTULO II DOS PRINCÍPIOS

Art. 6º A PSIBC é regida pelos seguintes princípios da segurança da informação:

I- disponibilidade;

II- integridade;

III- confidencialidade;

IV- autenticidade;

V- irretratabilidade;

VI- privilégio mínimo;

VII- necessidade de conhecer;

VIII- proteção de dados pessoais; e

IX- proteção da privacidade.

CAPÍTULO III DAS DIRETRIZES

Seção I Das Diretrizes Gerais

Art. 7º A PSIBC deve ser conhecida e observada por todos os usuários.

Art. 8º Os níveis gerenciais devem zelar pelo cumprimento da PSIBC no âmbito de sua competência.

Art. 9º Os segmentos de pessoas, de áreas e instalações, de TIC, de documentação e materiais, bem como de gestão de riscos e continuidade de negócios, devem dedicar especial atenção aos aspectos de segurança da informação dispostos na PSIBC.

Art. 10. O Banco Central do Brasil deve contribuir para a evolução do ecossistema de segurança da informação, mediante a colaboração e o compartilhamento de informações com as autoridades competentes, a sociedade e o Sistema Financeiro Nacional (SFN), na forma da legislação de regência.

Art. 11. Durante todo o ciclo de vida da informação, devem ser observados o atendimento à PSIBC e os princípios definidos no art. 6º.

Seção II Da Rotulação e Classificação dos Dados e da Informação

Art. 12. Toda informação tratada no âmbito do Banco Central do Brasil deve ser considerada pública, salvo as informações de acesso restrito e os dados pessoais, inclusive os sensíveis, que devem ser devidamente rotulados ou classificados de forma a indicar essa condição.

Parágrafo único. A informação tratada pelo Banco Central do Brasil pode ser classificada como reservada, secreta ou ultrassecreta, observado o seu teor, em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, na forma da legislação vigente.

Art. 13. O acesso e o tratamento da informação de acesso restrito ficam limitados às pessoas que tenham necessidade de conhecê-la.

Parágrafo único. No caso de informação classificada, o acesso e o tratamento ficam condicionados ainda ao prévio credenciamento ou à assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS), na forma da legislação própria.

Seção III Do Segmento de Pessoas

Art. 14. Os servidores do Banco Central do Brasil devem receber orientações ou instruções sobre segurança da informação por meio de ações educacionais no período de ambientação, formação inicial e continuada.

Parágrafo único. Os demais usuários do Banco Central do Brasil devem receber, no que couber, instruções e orientações relacionadas à segurança da informação.

Art. 15. Os contratos, acordos, convênios e demais ajustes do Banco Central do Brasil com pessoas naturais ou entidades privadas devem conter cláusulas referentes ao cumprimento da PSIBC e à observância dos procedimentos de segurança para tratamento da informação de acesso restrito, dos dados pessoais e dos dados pessoais sensíveis pelos seus empregados, prepostos ou representantes, sem prejuízo da participação em orientações complementares de segurança da informação.

Parágrafo único. O disposto neste artigo aplica-se, no que couber, aos contratos, acordos, convênios e demais ajustes do Banco Central do Brasil com órgãos e entidades públicos e com organismos internacionais.

Art. 16. Medidas e procedimentos de segurança da informação devem ser observados em todo o processo de admissão, alocação, transferência, remanejamento, promoção, substituição, afastamento, sucessão e desligamento de dirigentes, servidores, terceirizados, prestadores de serviço, aprendizes e estagiários.

Seção IV

Do Segmento de Áreas e Instalações

Art. 17. As áreas e instalações que contiverem informação de acesso restrito, dados pessoais ou dados pessoais sensíveis têm seu acesso limitado apenas às pessoas autorizadas.

Art. 18. Devem ser adotadas medidas para definição, demarcação, sinalização, segurança e autorização de acesso às áreas restritas.

Art. 19. As pessoas que necessitam ingressar em ambientes para a realização de obras ou para a prestação de serviços dependem de autorização prévia e, sempre que necessário, são acompanhadas por servidor do Banco Central do Brasil ou outro agente autorizado, inclusive fora dos horários de expediente.

Art. 20. A entrada e a saída de pessoas, documentos, objetos e materiais nas áreas e nas instalações do Banco Central do Brasil obedecem a medidas e procedimentos de segurança que auxiliem na mitigação dos riscos à segurança da informação.

Art. 21. As áreas de acesso público são, preferencialmente, isoladas fisicamente das áreas de trabalho ou devem possuir medidas de segurança complementares.

Seção V

Do Segmento de TIC

Art. 22. O segmento de TIC compreende os ativos de informação do Banco Central do Brasil usados para o tratamento da informação em meio digital.

§ 1º Normas complementares pertinentes ao segmento de TIC podem ser publicadas pelo Departamento de Tecnologia da Informação (Deinf) e disponibilizadas aos usuários como parte integrante da PSIBC.

§ 2º O uso seguro dos recursos de computação em nuvem deve ser objeto de norma específica.

§ 3º As normas devem ter como prioridade a segurança das informações da organização, bem como o atendimento aos princípios e diretrizes que norteiam a PSIBC.

Art. 23. Todas as soluções de TIC desenvolvidas ou adquiridas pelo Banco Central do Brasil, inclusive as que se encontram em uso, devem considerar os princípios previstos no art. 6º.

Art. 24. Os recursos de TIC do Banco Central do Brasil são disponibilizados visando ao atendimento das atividades voltadas aos objetivos institucionais.

Parágrafo único. É vedada a utilização dos recursos de TIC do Banco Central do Brasil para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos de ordem moral, econômica ou financeira a qualquer pessoa natural ou jurídica, ou para veicular opiniões político-partidárias.

Art. 25. O usuário tem acesso autorizado apenas aos recursos de TIC necessários e indispensáveis ao seu trabalho.

Art. 26. O usuário de recursos de TIC deve ter identificação pessoal e intransferível.

Art. 27. Não há privacidade em relação a informações contidas em arquivos, bases de dados, mensagens ou em qualquer outro recurso de TIC utilizado para seu tratamento, à exceção de eventuais informações de acesso restrito, dados pessoais ou dados pessoais sensíveis.

§ 1º A Corregedoria-Geral do Banco Central do Brasil (Coger), a Procuradoria-Geral do Banco Central (PGBC), a Comissão de Ética do Banco Central do Brasil (CEBCB) ou as comissões disciplinares podem ter acesso a quaisquer dados e informações tratados nos recursos de TIC do Banco Central do Brasil, desde que haja sindicância investigativa ou acusatória ou outro procedimento disciplinar ou ético instaurado, em qualquer de suas modalidades.

§ 2º O conteúdo dos aplicativos e programas de mensagens instantâneas e o conteúdo dos e-mails recebidos ou enviados a partir das caixas corporativas, de uso individual ou compartilhado, bem como o conteúdo dos arquivos de dados criados pelos aplicativos usados para ler e-mails, independentemente do local de armazenamento, somente pode ser acessado pelo Deinf mediante solicitação formal da Coger, da PGBC, da CEBCB ou das comissões de sindicância ou disciplinares, para esclarecimentos de fatos que, em tese, configurem irregularidade funcional ou ética, ou da PGBC, para comunicação de crimes ou contravenções às autoridades competentes ou para o cumprimento de preceito legal ou ordem judicial ou emanada de outra autoridade competente, na forma da legislação de regência.

Art. 28. Os administradores dos recursos de Tecnologia da Informação (TI) devem ter apenas os acessos necessários à execução das atividades de trabalho sob sua responsabilidade.

Art. 29. Devem ser mantidas cópias atualizadas das contas do correio eletrônico do Banco Central do Brasil, incluindo todas as mensagens trafegadas, por pelo menos cinco anos.

Art. 30. As informações do Banco Central do Brasil em meio digital devem ser armazenadas em locais autorizados e com as proteções recomendadas pelo Deinf, conforme definido em norma específica.

Art. 31. O Deinf pode restringir o acesso a recursos de TIC do Banco Central do Brasil, como o acesso a sítios e o recebimento de e-mails, quando houver indício de risco à segurança da informação, considerando os princípios previstos no art. 6º, ou quando necessário ao tratamento de incidentes cibernéticos.

Art. 32. O uso dos recursos de TI do Banco Central do Brasil é monitorado e registrado.

§ 1º Norma específica deve indicar os requisitos mínimos aplicáveis aos dados que devem ser registrados e guardados para fins de tratamento e resposta a incidentes de segurança.

§ 2º O acesso aos registros de que trata este artigo deve ser disponibilizado à Etir, aos desenvolvedores e aos administradores e equipes de suporte dos recursos de TIC, para execução das atividades de sua competência.

§ 3º O acesso aos registros relativos a atividades de usuários e ao uso de recursos de TIC somente podem ser solicitados:

I- pelos usuários, no caso de seus próprios registros;

II- pelos respectivos gestores, no caso de uso de recursos de TIC;

III- pela Auditoria Interna do Banco Central do Brasil (Audit), no caso de uso de recursos de TIC; e

IV- pela Coger, pela PGBC, pela CEBCB e pelas comissões de sindicância e outras de natureza disciplinar, no caso dos registros das atividades de usuários e de uso de recursos de TIC.

§ 4º As solicitações de que trata o § 3º devem ser devidamente formalizadas ao Deinf e devem conter a justificativa motivada para tal solicitação.

Art. 33. O acesso a qualquer recurso de TIC pode ser suspenso, sempre que necessário à preservação da segurança da informação do Banco Central do Brasil, visando ao atendimento dos princípios previstos no art. 6º.

Seção VI

Do Segmento de Documentação e Materiais

Art. 34. As informações rotuladas ou classificadas devem observar medidas e procedimentos de segurança próprios, definidos em norma específica, aplicando-se, no que couber, o disposto na PSIBC.

Art. 35. Os ativos de informação destinados ao descarte, seja o papel ou outras mídias, devem ser devidamente inutilizados visando à segurança da informação e ao atendimento dos princípios que regem a PSIBC.

Seção VII

Da Gestão de Riscos e Continuidade de Negócios

Art. 36. A segurança da informação deve orientar os processos de levantamento, avaliação e tratamento das vulnerabilidades e das ameaças capazes de deixar os ativos de informação em situação de risco considerada inaceitável pelo Banco Central do Brasil.

CAPÍTULO IV

DAS COMPETÊNCIAS E ATRIBUIÇÕES

Art. 37. Compete ao Presidente do Banco Central do Brasil designar o Gestor de Segurança da Informação (GSI) e o Gestor de Segurança e Credenciamento (GSC), bem como seus suplentes, na forma da legislação vigente.

Art. 38. Compete ao Coseg:

I- assessorar as instâncias competentes na implementação de ações de segurança da informação;

II - deliberar sobre temas e propor soluções específicas sobre segurança da informação, podendo constituir grupos de trabalho;

III- propor alterações na PSIBC e em normas de segurança da informação no âmbito do Banco Central do Brasil; e

IV - deliberar sobre normas internas de segurança da informação que não estejam no âmbito de competência das demais instâncias do Banco Central do Brasil.

Parágrafo único. Ressalvadas as competências específicas da Diretoria Colegiada, do Presidente, dos Diretores, do GSI e do GSC, o Coseg é o órgão máximo de decisão em questões relativas à gestão da segurança da informação no âmbito do Banco Central do Brasil.

Art. 39. Compete ao GSI:

I- coordenar o Coseg, nos assuntos relacionados à segurança da informação;

II- coordenar a elaboração da PSIBC e das normas internas de segurança da informação;

III- assessorar a Alta Administração na implementação da PSIBC;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V- incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VI- propor recursos necessários às ações de segurança da informação;

VII- aprovar e acompanhar a execução de ações, metas e planos estratégicos relacionados à segurança da informação;

VIII - encaminhar periodicamente à Diretoria Colegiada relatórios sobre a execução dos planos e sobre os incidentes cibernéticos relevantes;

IX- verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; e

X - comunicar tempestivamente ao encarregado de dados pessoais a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

Art. 40. Compete ao GSC:

I- propor normas relacionadas aos processos de rotulação e classificação da informação;

II- propor normas relacionadas aos processos de credenciamento de segurança para tratamento da informação classificada, com base na legislação e nas normas vigentes;

III- credenciar ou dispor sobre o credenciamento dos usuários que podem ter acesso à informação classificada;

IV- fiscalizar o cumprimento da legislação e das normas de credenciamento e de tratamento da informação; e

V - assessorar a Diretoria Colegiada do Banco Central do Brasil em assuntos relacionados ao tratamento de informação classificada, em qualquer grau de sigilo.

Art. 41. Compete à Autoridade de Monitoramento da LAI, no âmbito da segurança da informação:

I- orientar as unidades no que se refere ao cumprimento do disposto na LAI e em seus regulamentos; e

II - acompanhar os pedidos de acesso à informação e os processos de classificação, reclassificação e desclassificação da informação.

Art. 42. Compete ao encarregado de dados pessoais, no âmbito da segurança da informação, sem prejuízo das demais atribuições:

I- orientar os dirigentes, servidores e contratados no que diz respeito às práticas a serem tomadas em relação à proteção de dados pessoais; e

II- comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a esses dados.

Art. 43. Compete ao Deinf:

I- propor alterações na PSIBC;

II - elaborar e publicar Manuais e Procedimentos, como parte integrante da PSIBC, relativos aos aspectos de segurança cibernética do uso dos recursos de TIC do Banco Central do Brasil;

III- revisar os Manuais e Procedimentos, ao menos anualmente;

IV- propor a norma específica sobre o uso seguro dos recursos de computação em nuvem;

V- realizar ações para o desenvolvimento da cultura de segurança cibernética;

VI- prover os recursos de TIC necessários à devida execução da PSIBC;

VII - realizar e acompanhar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança cibernética;

VIII- mensurar, ao menos anualmente, a resiliência cibernética e os riscos cibernéticos; e encaminhar ao Departamento de Riscos Corporativos e Referências Operacionais (Deris), após a mensuração, relatório com a avaliação do risco cibernético e da resiliência cibernética;

IX- propor ao GSI metas e planos relacionados à segurança cibernética;

X- executar ações que visam ao cumprimento das metas e dos objetivos estabelecidos nos planos aprovados pelo GSI, sem prejuízo das demais ações relacionadas à segurança cibernética, e encaminhar, ao menos semestralmente, ao GSI relatórios sobre o andamento dessas ações;

XI - fornecer as informações necessárias para a área responsável pela elaboração do Relatório de Impacto à Proteção de Dados Pessoais;

XII- fornecer mensalmente ao Deris relatórios com os incidentes cibernéticos relevantes;

XIII- manter a Etir;

XIV- fornecer as informações sobre os incidentes cibernéticos relevantes, oriundas da Etir, necessárias ao GSI para a tomada de decisões; e

XV- fomentar o aprimoramento da resiliência cibernética do SFN.

Art. 44. Compete ao Departamento de Segurança (Deseg):

I- assessorar na implantação das ações relacionadas com a PSIBC;

II- planejar as ações necessárias para assegurar a proteção física de áreas e instalações, visando ao cumprimento da PSIBC;

III- propor alterações na PSIBC;

IV- disseminar a cultura de segurança da informação no Banco Central do Brasil;

V- prover os equipamentos e a infraestrutura necessários à devida aplicação da PSIBC, no âmbito de sua competência; e

VI - elaborar e publicar normas complementares relativas aos aspectos de segurança da informação que não estejam no âmbito de competência das demais unidades do Banco Central do Brasil.

Art. 45. Compete ao Departamento de Infraestrutura e Gestão Patrimonial (Demap):

I- prover os equipamentos e a infraestrutura necessários à devida aplicação da PSIBC, no âmbito de sua competência;

II - implantar as ações necessárias para assegurar a proteção e a recuperação das informações disponíveis no sistema de arquivamento e transporte de documentos; e

III- assessorar na implantação das ações relacionadas com a PSIBC.

Art. 46. Compete ao Departamento de Gestão de Pessoas, Educação, Saúde e Organização (Depes) implantar, no seu âmbito de atuação, as ações educacionais destinadas aos servidores do Banco Central do Brasil necessárias ao cumprimento da PSIBC.

Art. 47. Compete à Coger, à PGBC e à CEBCB, no âmbito de suas atribuições, aplicar as ações corretivas e disciplinares cabíveis nos casos de descumprimento das disposições da PSIBC e das normas a ela relacionadas.

Art. 48. São atribuições do Procurador-Geral, do Secretário-Executivo, do Chefe de Gabinete do Presidente, dos Procuradores-Gerais Adjuntos, dos Secretários-Executivos Adjuntos, dos Chefes de Unidade e titulares de funções equivalentes e dos Gerentes Administrativos:

I- contribuir para o cumprimento da PSIBC pelos servidores lotados em componentes a eles subordinados e demais usuários dos ativos de informação de sua unidade;

II - observar as medidas e os procedimentos de segurança e acesso à informação nos processos de admissão, alocação, transferência, remanejamento, promoção, substituição, afastamento, sucessão e desligamento de servidores, terceirizados, prestadores de serviço, aprendizes e estagiários;

III - dar ciência ao Coseg de qualquer ato que possa causar risco relevante à segurança da informação no âmbito do Banco Central do Brasil;

IV - definir e implantar, em conjunto com o Deseg, eventuais necessidades de restrição de acesso a áreas e instalações sob sua responsabilidade, visando à proteção dos ativos de informação nelas armazenados;

V- indicar a concessão de credencial de segurança para funções, cargos ou postos de trabalho sob sua responsabilidade que possuam a necessidade de conhecer as informações classificadas;

VI - implantar as ações necessárias para assegurar a proteção e a recuperação das informações em meio físico sob a guarda da unidade;

VII- fazer constar, nos contratos sob sua responsabilidade, cláusulas necessárias ao cumprimento da PSIBC; e

VIII - definir diretrizes para a realização de trabalho em regime não presencial na unidade, considerando a sensibilidade das informações e os riscos à segurança da informação.

CAPÍTULO V DOS USUÁRIOS

Art. 49. Os usuários são responsáveis:

I- pela segurança das informações a que tiverem acesso, inclusive quando em regime não presencial;

II- pelo tratamento adequado das informações de acesso restrito, dos dados pessoais e dos dados pessoais sensíveis aos quais tiverem acesso;

III- pela assinatura do Termo de Responsabilidade, anexo à PSIBC, como condição para acesso aos ativos de informação do Banco Central do Brasil;

IV- pelo cumprimento da PSIBC e das demais normas relacionadas à segurança da informação;

V- no caso de servidor, por dar ciência ao respectivo Chefe de Unidade de qualquer ato que possa causar um risco relevante à segurança da informação;

VI - pela comunicação à Etir, caso tenha conhecimento, de incidente cibernético ou suspeita de incidente cibernético relacionado a recurso de TIC do Banco Central do Brasil;

VII- pelos acessos realizados com sua conta de identificação na rede de computadores e demais recursos de TIC do Banco Central do Brasil; e

VIII- pela manutenção do sigilo de suas senhas de acesso aos recursos, sistemas e serviços da rede de computadores, sendo vedada a utilização da conta de identificação do usuário por terceiros.

CAPÍTULO VI DO TERMO DE RESPONSABILIDADE

Art. 50. Os usuários que necessitam de acesso aos ativos de informação do Banco Central do Brasil devem assinar o Termo de Responsabilidade anexo à PSIBC.

§ 1º O descumprimento do disposto no **caput**, em prazo a ser estabelecido, enseja a suspensão do acesso a determinados ativos de informação.

§ 2º A não-assinatura do Termo de Responsabilidade não exime o usuário dos deveres e responsabilidades de que trata a PSIBC.

CAPÍTULO VII DISPOSIÇÕES FINAIS

Art. 51. A PSIBC, bem como a estrutura de governança dos riscos cibernéticos, deve ser revisada, no máximo, a cada três anos.

Art. 52. Os manuais, regulamentos e atos normativos internos do Banco Central do Brasil devem estar em conformidade com a PSIBC.

Art. 53. Devem ser promovidas campanhas de conscientização para a divulgação da PSIBC.

Art. 54. O descumprimento das disposições estabelecidas na PSIBC pode ensejar a instauração de procedimento disciplinar pela Coger ou pela PGBC, a depender do caso, bem como a aplicação das penalidades cabíveis, assim como de procedimento ético pela CEBCB.

Art. 55. Os casos omissos são resolvidos pelo Coseg, sem prejuízo do disposto no Regimento Interno do Banco Central do Brasil.

ANEXO À PSIBC TERMO DE RESPONSABILIDADE

Por meio do presente Termo de Responsabilidade, declaro-me ciente de que:

I- as normas gerais de segurança da informação do Banco Central do Brasil estão consignadas na Política de Segurança da Informação do Banco Central (PSIBC), anexa à Resolução BCB nº 287, de 24 de janeiro de 2023, a cujo inteiro teor tive acesso;

II- o uso indevido ou fraudulento das informações e dos recursos de Tecnologia da Informação (TIC) do Banco Central do Brasil enseja apuração de responsabilidade, nos termos da legislação vigente.

Responsabilizo-me por agir de modo a preservar a segurança das informações às quais tenho acesso e pelo correto uso dos ativos de informação do Banco Central do Brasil e comprometo-me a cumprir as determinações e recomendações contidas na PSIBC.