APROVADO PELA RESOLUÇÃO CA BNDES Nº 20/2023

FOLHA DE INFORMAÇÕES GERAIS DO ATO NORMATIVO

Título	
POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO DO SISTEMA BNDES (PCSI)	
Unidade Gestora	**Unidade(s) Corresponsável(is)**
DEPARTAMENTO DE GESTÃO DE RISCO OPERACIONAL E CONTROLE INTERNO DA ÁREA DE INTEGRIDADE E COMPLIANCE (AIC/DEROC)	

Tipo de normativo				
☒ Política	☐ Regulamento	☐ Ato Organizacional	☐ Procedimento	☐ Circular

Previsão de delegação de competência		
☒ Não há	☐ Diretoria para Diretor / Presidente ☐ Diretoria para Comitês ☐ Diretoria para Superintendente	
☐ CA para Diretoria		
☐ Diretor para Superintendente	☐ Outro (especificar)	

Legislação de Referência

DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018 (INSTITUI A POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO E DISPÕE SOBRE A GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL)

DECRETO Nº 10.641, DE 2 DE MARÇO DE 2021 (ALTERA O DECRETO 9.637 DE 2018)

DECRETO Nº 10.222, DE 05 DE FEVEREIRO DE 2020 (QUE INSTITUI A ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA)

INSTRUÇÃO NORMATIVA Nº 1, DE 27 DE MAIO DE 2020 (DISPÕE SOBRE A ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS E NAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL)

INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021 (DISPÕE SOBRE OS PROCESSOS RELACIONADOS À GESTÃO DE SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS E NAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL, ESPECIALMENTE MAPEAMENTO DE ATIVOS DE INFORMAÇÃO E GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO)

INSTRUÇÃO NORMATIVA GSI/PR Nº 5, DE 30 DE AGOSTO DE 2021 QUE DISPÕE SOBRE OS REQUISITOS MÍNIMOS DE SEGURANÇA DA INFORMAÇÃO PARA UTILIZAÇÃO DE SOLUÇÕES DE COMPUTAÇÃO EM NUVEM PELOS ÓRGÃOS E PELAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

INSTRUÇÃO NORMATIVA GSI/PR Nº 6 DE 23 DE DEZEMBRO DE 2021 QUE ESTABELECE DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO PARA O USO SEGURO DE MÍDIAS SOCIAIS NOS ÓRGÃOS E NAS ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL.

RESOLUÇÃO CMN Nº 4.893, DE 26 DE FEVEREIRO DE 2021 (DISPÕE SOBRE A POLÍTICA DE SEGURANÇA CIBERNÉTICA E SOBRE OS REQUISITOS PARA A CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM A SEREM OBSERVADOS PELAS INSTITUIÇÕES AUTORIZADAS A FUNCIONAR PELO BANCO CENTRAL DO BRASIL)

Atos Internos Relacionados

APROVADO PELA RESOLUÇÃO CA BNDES Nº 20/2023

POLÍTICA CORPORATIVA DE PROTEÇÃO DE DADOS PESSOAIS DO SISTEMA BNDES (RESOLUÇÃO CA BNDES Nº 14/2021, DE 11/08/2021)

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI – RESOLUÇÃO CA BNDES Nº 03/2019, DE 23/04/2019, E ALTERAÇÕES)

Processos Associados

GESTÃO DE RISCOS, CONTROLES E COMPLIANCE - RCC GERIR SEGURANÇA DA INFORMAÇÃO

Parametrização em Sistema(s)

☒ Não há	☐ Habilitação	☐ Financiamento	☐ Acompanhamento

Vigência		**Prazo de Revisão**
Início	Data de publicação no Portal de Normas	Revisão anual a contar da entrada em vigor.
Fim	N/A	

Palavras-chave (indexação)

SEGURANÇA DA INFORMAÇÃO, RISCOS CIBERNÉTICOS, CIBERSEGURANÇA. PCSI.

Atendimento de dúvidas

GSEG@BNDES.GOV.BR

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO DO SISTEMA BNDES (PCSI)

1. OBJETIVO

1.1. Esta Política estabelece os princípios, as diretrizes, os papéis e as responsabilidades que devem ser observados por todos os colaboradores na execução de processos das Empresas do Sistema BNDES para preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações produzidas ou recebidas e sob a custódia do BNDES.

2. ABRANGÊNCIA E ESCOPO

2.1 Esta Política é aplicável às atividades do BNDES e de suas subsidiárias, a BNDES Participações S/A (BNDESPAR) e a Agência Especial de Financiamento Industrial S.A. (FINAME).

2.1.1 Esta Política se aplica a todos os Participantes do Sistema BNDES e aos seus prestadores de serviço.

2.1.2 O escopo da aplicabilidade de normas complementares ou de diretrizes dessa PCSI em contratos de prestação de serviços pode, por interesse das Empresas do Sistema BNDES e do prestador, ser delimitado para excetuar itens não aplicáveis no âmbito do serviço prestado mediante a reavaliação do risco de segurança da informação e da anuência da unidade gestora de segurança da informação.

2.2 Esta Política, alinhada à missão e aos objetivos da Instituição, estabelece objetivos, princípios e responsabilidades aplicáveis aos processos de gestão de segurança da informação.

2.3 A gestão de segurança da informação do Sistema BNDES orienta-se essencialmente pelo disposto na Resolução CMN nº 4.893, de 26/02/2021, pelo Decreto 9.637, de 26/12/2018 e pelas Instruções Normativas GSI-PR nº 01, de 27/05/2020, nº 03 de 28/05/2021 e nº 05 de 30/08/2021.

2.4 Toda informação produzida, recebida, adquirida ou custodiada pelas Empresas do Sistema BNDES é considerada patrimônio das Empresas do Sistema BNDES e deve ser usada exclusivamente para atender a interesses institucionais.

3. DEFINIÇÕES E ABREVIATURAS

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

a) **Autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado equipamento, sistema, órgão ou entidade.

b) **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, sistema, órgão ou à entidade não autorizados nem credenciados.

c) **Colaboradores:** todas aos Participantes do Sistema BNDES, o que inclui os empregados e estagiários do BNDES, bem como prestadores de serviço e aprendizes**.**

d) **Informações sensíveis:** são aquelas classificadas como confidenciais, reservadas ou secretas de acordo com o normativo interno que dispõe sobre a classificação e tratamento de informações.

e) **Disponibilidade:** propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade.

f) **Integridade:** propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

g) **Participantes do Sistema BNDES**: empregados integrantes dos quadros de pessoal permanente ou temporário, ainda que se encontrem cedidos ou requisitados ou em gozo de licença ou em outro afastamento equivalente, com ou sem remuneração, os cedidos às empresas do Sistema BNDES, os estagiários e os membros da Alta Administração das empresas do Sistema BNDES.

h) **Risco de Segurança da Informação:** potencial de perda associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo às Empresas do Sistema BNDES. O risco de segurança da informação é uma especialização de riscos operacionais.

i) **Risco Cibernético** – risco de segurança da informação que envolve ativo de tecnologia da informação e que pode implicar em perdas resultantes de incidentes cibernéticos.

j) **Serviços de tecnologia da informação relevantes**: são aqueles que manipulam informações sensíveis ou que suportam os sistemas principais de tecnologia da informação imprescindíveis para continuidade de processos críticos de negócio.

k) **Sistemas principais**: são aqueles referenciados no Plano Estratégico de Tecnologia da Informação[1]**.**

3.1 Para fins desta PCSI e seus anexos, consideram-se ainda as definições descritas no Manual de Conceitos, documento que é apresentado como o Anexo I desta Política e que é suficiente para o entendimento dos termos das demais Normas Complementares.

4. PRINCÍPIOS E DIRETRIZES

4.1 Os colaboradores devem observar os seguintes **princípios** de Segurança da Informação em suas decisões e na condução de suas atividades:

a) **privilégio mínimo:** os colaboradores devem possuir apenas os privilégios estritamente necessários ao desempenho das suas atribuições profissionais;

b) **proteção em camadas:** o uso de controles complementares deve ser incentivado com vistas a aumentar a efetividade e a tolerância a falhas do conjunto;

c) **adoção de padrões abertos**: as implementações de soluções de segurança devem priorizar a adoção de padrões abertos, de acordo com as orientações do ePING (Padrões de Interoperabilidade do Governo Eletrônico);

d) **controle pautado pelo risco**: a implantação de controles deve ser iniciada pelos mais simples e priorizada de acordo com o resultado de análises de riscos de segurança da informação;

e) **custo-benefício**: os custos associados aos controles não devem ser superiores aos benefícios esperados em decorrência de sua implementação; e

f) **viabilidade**: a aplicabilidade de controles deve ser ponderada diante de sua efetividade e do eventual impacto ao cumprimento das necessidades de negócio;

4.2 Os colaboradores devem observar as seguintes **diretrizes fundamentais** de Segurança da Informação em suas decisões e na condução de suas atividades:

4.2.1 Os ativos de TI e os ativos de informação sob gestão do Sistema BNDES, o que não inclui dispositivos pessoais, devem ser utilizados para exercício de atividades profissionais voltadas aos interesses corporativos das Empresas do Sistema BNDES e em consonância com as atribuições de cada colaborador.

[1] De acordo com o PETI, são considerados sistemas principais de TI o portal institucional do BNDES (site do Banco na Internet) e aqueles cuja indisponibilidade causa impacto significativo nos processos fundamentais à atuação do Sistema BNDES, no mercado financeiro e de capitais, a saber: captação e gestão do passivo; realização de operações diretas, indiretas ou de renda variável; e cumprimento de obrigações ao Banco Central do Brasil (BACEN) e à Comissão de Valores Mobiliários (CVM).

4.2.2 O acesso a informações sigilosas deve ser precedido da assinatura de um Termo de Confidencialidade baseado, conforme o caso, em um dos modelos anexos a essa Resolução e listados a seguir:

a) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Contratos Administrativos (Anexo II);

b) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Profissionais e Estagiários das Empresas do Sistema BNDES (Anexo III);

c) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Profissionais Terceirizados (Anexo IV);

d) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Empresas na Ausência de Contrato (Anexo V); e

e) Modelo de Termo de Confidencialidade e Tratamento de Dados Pessoais para Pessoa Física na Ausência de Contrato (Anexo VI).

4.2.3 Os colaboradores devem comunicar imediatamente a unidade gestora de Segurança da Informação sempre que tomarem conhecimento de vulnerabilidades, indícios de comprometimento de ativos de informação e casos de desrespeito à PCSI.

4.2.4 Todos os incidentes de Segurança da Informação, comunicados às Empresas do Sistema BNDES ou verificados por seus próprios colaboradores, devem ser analisados, classificados de acordo com sua relevância, contidos e tratados.

4.2.5 Os colaboradores que identificarem vulnerabilidades em ativos de TI não devem tentar testá-las ou explorá-las sem autorização da unidade gestora de Segurança da Informação.

4.2.6 As configurações dos ativos de TI não devem ser alteradas com a finalidade de burlar os controles aplicados ou de permitir acessos não autorizados.

4.3 A UF Gestora de Tecnologia da Informação deve observar as seguintes **diretrizes fundamentais** de Segurança da Informação em suas decisões e na condução de suas atividades:

4.3.1 A introdução de ativos de Tecnologia da Informação para execução em regime de produção, bem como a implementação de mudanças nesses ativos devem ser precedidas de homologação que inclua avaliação do impacto à segurança e verificação de conformidade com as diretrizes, normas e padrões internos.

4.3.2 Os ativos de Tecnologia da Informação utilizados pelas Empresas do Sistema BNDES devem ser inventariados, protegidos, possuir responsável definido para sua gestão e ter o acesso controlado para assegurar que

somente pessoas autorizadas possam deles se utilizar, em conformidade com o princípio do privilégio mínimo.

4.3.3 O processo de desenvolvimento de sistemas deve ser realizado em conformidade com as diretrizes, normas e padrões definidos internamente para este fim, bem como estar de acordo com as melhores práticas de Segurança da Informação.

4.3.4 O projeto de sistemas desenvolvidos ou adquiridos deve:

a) contemplar as funcionalidades relacionadas ao controle de acesso à informação e à comunicação de dados, em conformidade com as diretrizes, normas e padrões internos;

b) ser precedido de uma avaliação acerca do tratamento de informações sensíveis, que considere especialmente aos requisitos para proteção dos dados pessoais, inclusive a garantia ao direito de privacidade;

c) considerar a implementação dos controles necessários para tratar adequadamente riscos de segurança da informação e a titulares de dados pessoais, que tenham sido previamente mapeados, para os casos de uso em desenvolvimento; e

d) priorizar o uso das bases corporativas de credenciais e privilégios de acessos.

4.3.5 Os privilégios de acesso atribuídos aos colaboradores devem ser construídos de acordo com os papéis de negócio e atributos organizacionais reconhecidos pelas Empresas do Sistema BNDES.

4.4 As Unidades Administrativas e os colaboradores devem observar as seguintes **diretrizes fundamentais** ao classificar ou tratar informações das Empresas do Sistema BNDES:

4.4.1 A classificação de informações deve observar a publicidade como preceito geral e a atribuição do sigilo como exceção, conforme inciso I do artigo 3º da Lei 12.527, de 18/11/2011 (Lei de Acesso à Informação), e o princípio da transparência, conforme item 4 da Política de Transparência do Sistema BNDES, aprovada pela Resolução DIR BNDES nº 2.880, de 18/09/2015 e suas alterações.

4.4.2 As informações devem ser classificadas e tratadas segundo critérios e procedimentos estabelecidos em normativo próprio, atualmente a OS PRESI BNDES nº 01, de 22/01/2015, e suas eventuais alterações posteriores.

4.4.3 Na ausência de justificativas legais para a atribuição de restrição de acesso à informação, o seu gestor deve utilizar os instrumentos previstos no ato normativo referenciado no item 4.4.2 para tornar evidente o caráter público da informação.

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

4.4.4 Os colaboradores devem observar as orientações no ato normativo referenciado no item 4.4.2 para garantir o adequado tratamento às informações sigilosas, especialmente para evitar sua exposição indevida, o que começa com a adoção de cuidados básicos como, por exemplo, a guarda dos documentos em gavetas ou arquivos com tranca, a manutenção da mesa sem documentos ou informações sigilosas (mesa limpa) e a estação de trabalho bloqueada nos momentos de ausência de uso.

4.4.5 Os ativos de informação utilizados pelas Empresas do Sistema BNDES devem ser protegidos, possuir responsável definido para sua gestão e ter o acesso controlado para assegurar que somente pessoas autorizadas possam deles se utilizar, em conformidade com o princípio do privilégio mínimo.

4.4.6 O tratamento de informação relacionada à pessoa natural identificada ou identificável, especialmente de dados pessoais sensíveis, deve observar as diretrizes e regras estabelecidas na Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD), com destaque à necessidade de o tratamento de dados pessoais realizar-se com base em uma das situações admitidas na legislação; e do cumprimento dos princípios da finalidade, da adequação, da necessidade, da transparência, da segurança e da prevenção.

4.4.7 A disponibilidade e a proteção das informações devem ocorrer de acordo com a sua classificação e de forma a preservar a continuidade de negócios das Empresas do Sistema BNDES.

4.4.8 Cláusulas de sigilo e confidencialidade devem constar nos contratos estabelecidos com profissionais terceirizados, prestadores de serviços e estagiários.

4.5 Devem ser observadas as diretrizes corporativas para controles internos, gestão de riscos e continuidade do negócio, de forma a preservar os ativos de informação necessários à sustentação das operações das Empresas do Sistema BNDES.

4.6 A elaboração de cenários de incidentes considerados nos testes de continuidade de negócio deve contemplar riscos cibernéticos que possam afetar a disponibilidade dos processos críticos de negócio.

4.7 Periodicamente devem ser realizados treinamentos que incluam aspectos de segurança da informação ou avaliações sobre a prontidão dos colaboradores em identificar e em notificar tempestivamente a unidade gestora de segurança da informação sobre ameaças cibernéticas.

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

5. PAPÉIS E RESPONSABILIDADES

5.1 Cabe ao Conselho de Administração (CA):

a) deliberar para aprovação do Sistema de Gestão de Segurança da Informação (SGSI), da Política Corporativa de Segurança da Informação (PCSI), do Plano Estratégico de Segurança da Informação (PESI) e do Plano de Resposta a Incidentes de Segurança da Informação (PRISI), bem como atribuir as responsabilidades envolvidas, conforme estabelece o Decreto 9.637 de dezembro de 2018 e a Resolução CMN nº 4.893 de 2021 ou outros normativos que os substituam.

b) apoiar e promover as iniciativas para fortalecimento da segurança da informação.

c) acompanhar a execução dos planos e de indicadores que compõem o SGSI.

5.2 Cabe ao Comitê de Riscos (CR):

a) propor, com periodicidade mínima anual, recomendações ao Conselho de Administração sobre esta política e sobre os planos para gestão de segurança da informação que compõem o SGSI.

b) analisar o ambiente de riscos de segurança da informação do Sistema BNDES, mediante informações produzidas pela AIC

c) supervisionar a atuação e desempenho do Diretor Responsável por Segurança da Informação; e

d) avaliar o grau de aderência dos processos da estrutura de gerenciamento de riscos às políticas estabelecidas.

e) apoiar o Conselho de Administração com a avaliação dos planos de ação e tratamento de incidentes de segurança da informação, da política de segurança da informação e das demais normas que tratam do tema no âmbito interno; e

f) apreciar o relatório anual sobre a implantação dos planos de ação e de tratamento de incidentes de segurança da informação, relatório que atualmente compõe o RARO (Relatório Anual de Gestão de Risco Operacional, Controle Interno e Compliance).

5.3 Cabe à Diretoria Executiva:

a) manifestar-se acerca de propostas para aprovação das políticas, planos e normas que compõem o SGSI e sobre o próprio SGSI, submetendo-os para deliberação do Conselho de Administração;

b) apoiar e promover as iniciativas para fortalecimento da segurança da informação; e

c) promover a execução das ações para segurança da informação previstas no PESI.

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

5.4 Cabe ao Diretor Responsável por Segurança da Informação:

a) zelar pelo cumprimento desta PCSI;

b) deliberar sobre a criação, alteração ou eliminação de normas complementares a essa PCSI e de seus demais anexos;

c) acompanhar periodicamente os indicadores e os planos do SGSI;

d) orientar sobre a definição de prioridades nas ações previstas no PESI, bem como zelar por sua adequada execução.

e) garantir os recursos necessários para implantação e acompanhamento dos controles previstos nesta PCSI; e

f) atuar como responsável do Sistema BNDES junto ao Banco Central do Brasil nos assuntos afetos à Segurança da Informação, nos limites da Resolução CMN nº 4.893, de 26/02/2021 ou outro normativo que o substitua.

5.5 Cabe ao Comitê de Segurança da Informação (CSI):

a) propor ou avaliar alterações nas políticas, planos e normas que compõem o SGSI e encaminhá-la para deliberação da Diretoria Executiva;

b) deliberar sobre o tratamento de casos excepcionais encaminhados para apreciação do comitê;

c) assessorar na implementação das ações de segurança da informação;

d) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

e) acompanhar os indicadores e a execução dos planos que compõem o SGSI;

f) promover a governança de Segurança da Informação e o adequado alinhamento estratégico das ações de segurança da informação; e

g) apreciar os relatórios sobre a utilização de mídias sociais e os relacionados aos incidentes de segurança ocorridos em perfis institucionais em mídias sociais.

5.6 Cabe ao Comitê de Gestão de Riscos (CGR):

a) avaliar o processo de gestão dos riscos de segurança da informação;

b) apoiar a gestão de riscos de segurança da informação de forma integrada aos demais riscos, fomentando o desenvolvimento de metodologias para uma visão unificada de riscos e que possibilitem a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos resultantes das interações dos riscos de segurança da informação com os demais riscos;

c) analisar os trabalhos relativos à gestão de riscos de Segurança da Informação, com vistas a ratificar, alterar ou recomendar ações de tratamento e/ou aprimoramento dos controles e procedimentos, e acompanhar sua implementação pelas UFs envolvidas; e

d) analisar as propostas de criação e/ou alteração de políticas de gestão dos riscos de segurança da informação e encaminhá-las à alçada competente para validação ou deliberação.

5.7 Cabe à Unidade Fundamental Gestora de Tecnologia de Informação:

a) avaliar os potenciais impactos à segurança da informação que possam ocorrer na implementação de mudanças de TI, bem como verificar o resultado dessas mudanças e propor controles para mitigar os riscos de SI gerados por elas;

b) adotar as melhores práticas para segurança na implantação e no desenvolvimento de sistemas sob sua responsabilidade;

c) manter e acompanhar o inventário de Ativos de Informação em meio eletrônico e de Ativos de TI com o objetivo de manter atualizado um banco de dados de gerenciamento de configuração e promover a adequada identificação e classificação dos ativos; e

d) apoiar o Gestor de Licença de *Software* na realização do inventário da utilização de licenças e apoiar na geração de evidências para auditorias de licença de *software*.

5.8 Cabe à Unidade de Integridade e Compliance (AIC):

a) elaborar, manter e revisar periodicamente os documentos que compõem o SGSI, o que inclui a PCSI, o PRISI e o PESI, à luz das orientações do Gestor de Segurança da Informação, bem como zelar pela observância das políticas e a execução das ações de Segurança da Informação;

b) definir, medir e apresentar os indicadores selecionados do SGSI e os principais resultados das ações planejadas no PESI aos colegiados e integrantes da estrutura de gestão e governança de SI;

c) garantir a adequada resposta e tratamento de incidentes de Segurança da Informação, de acordo com o PRISI e a execução dos serviços de segurança previstos;

d) secretariar o Comitê de Segurança da Informação;

e) acompanhar os indicadores dos processos e dos planos que compõem o SGSI e apresentá-los periodicamente ao Gestor de Segurança da Informação e, quando demandado, aos demais colegiados que compõe a estrutura de gestão de Segurança da Informação;

f) apoiar o acionamento do Plano de Gerenciamento de Incidentes do Sistema BNDES (PGI) sempre que um incidente de segurança impacte em um incidente, contingência ou crise no escopo da continuidade de negócios, conforme define a Política de Gestão de Continuidade de Negócios (atualmente a Resolução CA BNDES nº 13/2022);

g) elaborar os planos e os relatórios para gestão de riscos de segurança da informação;

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

h) elaborar o relatório de incidentes de segurança ocorridos em perfis institucionais em mídias sociais e encaminhá-lo ao Gestor de Segurança da Informação;

i) coordenar a equipe de tratamento de incidentes de segurança da informação em rede do Sistema BNDES;

j) definir e adotar procedimentos para o adequado tratamento de incidentes de segurança da informação em rede do Sistema BNDES;

k) atuar como ponto focal para comunicação com entidades externas, ressalvada a atribuição do Encarregado de Proteção de Dados Pessoais do Sistema BNDES, nos termos definidos na PCPD, e com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV, nos assuntos relativos a incidentes de segurança da informação em rede do Sistema BNDES;

l) coordenar, quando demandado, as investigações, as avaliações dos danos decorrentes de quebras de segurança da informação e zelar pela adequada coleta de evidências;

m) disseminar a cultura de segurança da informação, com a implementação de programas de capacitação e de avaliação periódica de pessoal e apoiar as demais unidades na prestação de informações a clientes sobre riscos cibernéticos na utilização de produtos e serviços, inclusive na comunicação institucional por meio de mídias sociais;

n) acompanhar o processo de gestão de acessos a ativos de tecnologia da informação;

o) realizar estudos sobre novas tecnologias e seu potencial impacto à Segurança da Informação;

p) divulgar amplamente a PCSI a todos os colaboradores do Sistema BNDES, disponibilizar seu conteúdo integralmente para consulta interna e divulgar um resumo com as linhas gerais da norma ao público externo;

q) integrar o Comitê de Mudanças de Tecnologia da Informação, nos termos do normativo que regulamenta a atuação do Comitê (atualmente a Res DIR nº 3.944/2022-BNDES);

r) coordenar a execução do mapeamento de ativos de informações sensíveis e zelar por sua atualização periódica;

s) definir a metodologia para a execução do mapeamento de informações sensíveis, bem como consolidar as informações resultantes;

t) apoiar a avaliação dos riscos de segurança da informação e a elaboração dos planos de ação para tratamento de riscos cibernéticos, bem como promover seu adequado acompanhamento;

u) gerenciar, acompanhar e analisar, de forma contínua, as práticas de uso institucional seguro de mídias sociais, com relação aos aspectos de segurança da informação;

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

5.9 Cabe aos gestores de sistemas e de processos:

a) definir os requisitos de segurança da informação dos sistemas e processos sob sua responsabilidade e buscar assegurar-se de que tais exigências sejam cumpridas;

b) priorizar a correção de problemas e vulnerabilidades de segurança descobertas nos sistemas e processos sob sua responsabilidade;

c) aprovar os privilégios dos colaboradores que utilizam os sistemas ou atuam nos processos sob sua responsabilidade, bem como revisar periodicamente esses privilégios com vistas a revogar aqueles que não são mais necessários;

d) aprovar as declarações de aplicabilidade e o plano de tratamento de riscos de sistemas ou processos sob sua responsabilidade e acompanhar a execução do plano de tratamento de riscos;

e) fornecer periodicamente para a unidade gestora de Segurança da Informação e para a UF Gestora de Tecnologia da Informação a lista de privilégios dos colaboradores que utilizam os sistemas ou atuam nos processos sob sua responsabilidade, quando o sistema em questão não for integrado com a base corporativa de credenciais e acessos;

f) fornecer à unidade gestora de Segurança da Informação informações referentes aos ativos com informações sensíveis envolvidos em processos sob sua gestão, seja na sua criação ou atualização e sempre que demandados; e

g) identificar e avaliar o risco de segurança da informação aos ativos de informação sensíveis tratados no âmbito do processo sob sua gestão;

5.10 Cabe às Unidades Fundamentais (UF) e seus executivos:

a) observar, na execução de suas atividades, as disposições desta Política;

b) reportar tempestivamente ao AIC/DEROC informações relativas aos riscos de segurança das informações dos seus processos de trabalho e às perdas deles oriundas, bem como sobre o andamento dos planos de ação ou outras iniciativas para a mitigação desses riscos, prioritariamente por meio de seus Agentes de Conformidade;

c) incentivar a participação dos colaboradores da UF nas ações de capacitação relacionadas à gestão de segurança da informação, bem como providenciar para que conheçam integralmente e atuem em conformidade com esta Política; e

d) revisar periodicamente os privilégios de acesso dos colaboradores sob sua responsabilidade, com vistas a revogar aqueles que não são mais necessários.

5.11 Cabe à Unidade Fundamental Responsável pela Comunicação Institucional:

a) criar, alterar, excluir e controlar os perfis institucionais em mídias sociais do órgão ou da entidade;

b) remover, tão logo tome conhecimento, postagens que atentem contra a segurança da informação;

c) elaborar relatório mensal sobre a utilização de mídias sociais sob sua administração e apresentar ao gestor de segurança da informação;

d) fornecer à unidade gestora de Segurança da Informação informações referentes aos eventos, no âmbito do uso e gestão de perfis institucionais em mídias sociais, que possam implicar em comprometimento da segurança das informações do Sistema BNDES.

5.12 Cabe aos gestores de informação: efetuar a classificação das informações das quais foi indicado como gestor, bem como avaliar os controles e procedimentos relativos às atividades ligadas ao ciclo de vida dessas informações.

5.13 Cabe aos gestores de licença de *software*:

a) estabelecer regras para a autorização e revogação do uso das licenças do *software*;

b) autorizar o uso das licenças do *software* para novos usuários, bem como eventuais remanejamentos das licenças;

c) autorizar o uso de recursos que alterem o quantitativo da licença de *software*, por exemplo, o aumento da capacidade de processamento;

d) controlar o quantitativo de licenças em uso;

e) inventariar periodicamente a utilização das licenças do *software*;

f) zelar para que o uso esteja em conformidade com a licença e os direitos de uso do *software*, bem como o respectivo contrato de aquisição do *software* quando aplicável; e

g) responder tempestivamente a auditorias internas e externas que se refiram à licença de *software*, bem como gerar as eventuais evidências solicitadas.

5.14 Cabe aos gestores de contrato:

a) providenciar para que os colaboradores terceirizados que atuem no âmbito de contratos sob sua gestão observem as orientações da PCSI aplicáveis;

b) providenciar a assinatura do termo de confidencialidade e acesso a dados pessoais pertinente por todos os colaboradores terceirizados que eventualmente atuem no âmbito de contratos sob sua gestão;

c) revisar periodicamente os privilégios de acesso dos colaboradores sob sua responsabilidade, com vistas a revogar aqueles que não são mais necessários; e

d) difundir e promover no âmbito de sua atuação e competência as boas práticas de segurança da informação definidas nesta PCSI e em suas normas complementares.

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

5.15 Cabe ao responsável pelo Processo Gerenciar Mudanças de Tecnologia da Informação estabelecido nos termos da IS SUP/ATI nº 04/2022 (e alterações posteriores):

a) coordenar a gestão de mudanças de Tecnologia da Informação;

b) garantir, no âmbito do processo de gestão de mudanças, a apreciação dos aspectos de segurança da informação;

c) garantir o alinhamento do processo de gestão de mudanças, no tocante aos aspectos de segurança da informação e aos resultados do processo de gestão de riscos; e

d) assegurar o registro de auditoria de todas as informações relevantes relacionadas com as mudanças.

5.16 Cabe especificamente ao Gestor de Segurança da Informação:

a) propor e encaminhar para deliberação as políticas, planos e normas que compõem o SGSI;

b) manter contato com o Departamento de Segurança da Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional da Presidência da República (GSIPR), para o trato de assuntos relativos à Segurança da Informação;

c) remeter, quando demandado, os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação para o GSIPR;

d) promover a cultura de segurança da informação;

e) acompanhar, quando demandado, as investigações, as avaliações dos danos decorrentes de quebras de segurança e zelar pela adequada coleta de evidências;

f) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

g) acompanhar a atuação da equipe de tratamento e resposta a incidentes de segurança da informação na rede do Sistema BNDES – ETIR-BNDES, bem como zelar por sua adequada coordenação;

h) promover a gestão de riscos de segurança da informação;

i) avaliar o plano para gestão de riscos de segurança da informação e dos relatórios para identificação, análise, avaliação e tratamento dos riscos de segurança da informação;

j) zelar pela adequada execução do processo de mapeamento de ativos de informação sensíveis e acompanhar seus indicadores;

k) zelar pela adequada avaliação dos aspectos de segurança da informação na execução do processo de mudanças de TI;

l) propor recursos necessários para as ações de Segurança da Informação em consonância com o Plano Estratégico de Segurança da Informação (PESI) das empresas do Sistema BNDES;

m) zelar pela atualização dos processos de Segurança da Informação e dos procedimentos de trabalho;

n) apresentar ao Comitê de Segurança da Informação os relatórios sobre a utilização de mídias sociais e de eventuais incidentes de segurança ocorridos em perfis institucionais em mídias sociais;

o) aprovar, acompanhar e dar publicidade aos indicadores do SGSI, bem como submeter os relatórios com dados relativos à gestão de Segurança da Informação para apreciação dos colegiados pertinentes que compõem a estrutura de gestão de Segurança da Informação; e

p) coordenar o Comitê de Segurança da Informação.

5.17 Cabe aos colaboradores:

a) zelar pela segurança das informações das Empresas do Sistema BNDES;

b) participar na realização de testes e treinamentos de segurança da informação, quando solicitado pelo AIC/DEROC; e

c) atuar em conformidade com esta PCSI.

5.18 Os papéis e responsabilidades atribuídos nesta seção não excluem os previstos em outros normativos internos ou externos.

6. MONITORAÇÃO

6.1 As Empresas do Sistema BNDES podem, a seu critério e, observadas as disposições da Lei nº 13.709, de 2018, bem como as regras estabelecidas pela PCPD, monitorar e registrar a manipulação de Ativos de Informação armazenados ou em trânsito, com o objetivo de zelar pelo fiel cumprimento da PCSI.

6.2 Os colaboradores usuários de Ativos de TI do Sistema BNDES devem ser informados da possibilidade de registro e monitoramento das atividades realizadas por meio desses ativos.

7. NORMAS COMPLEMENTARES

7.1 As normas apresentadas a seguir e apensadas a este documento complementam essa PCSI com diretrizes para procedimentos e controles específicos, além de regularem e atribuírem responsabilidades adicionais sobre os temas que endereçam, a saber:

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

7.1.1 Norma de Segurança da Informação para Acesso a Áreas com Ativos Críticos de Tecnologia da Informação (Anexo VII): estabelece que os ativos de Tecnologia da Informação considerados críticos ao desempenho das atividades das Empresas do Sistema BNDES devem ser armazenados em áreas apropriadas, com acesso restrito, e dispõe sobre:

a) autorização de acesso;
b) registro e monitoração de acesso; e
c) execução de procedimentos técnicos.

7.1.2 Norma de Segurança da Informação para Acesso Remoto a Ativos de Tecnologia da Informação (Anexo VIII): estabelece as responsabilidades e condições que devem ser observadas no acesso remoto a ativos de TI das Empresas do Sistema BNDES e dispõe sobre:

a) restrições para o uso;
b) solicitação e autorização;
c) controles necessários; e
d) auditoria do acesso.

7.1.3 Norma de Segurança da Informação para Controle de Acesso à Informação (Anexo IX): estabelece os requisitos para o controle de acesso à informação no âmbito das Empresas do Sistema BNDES e dispõe sobre:

a) credenciais de acesso;
b) senhas;
c) uso de dispositivos criptográficos;
d) autorização de acesso;
e) revisão e revogação de acessos;
f) auditoria; e
g) acesso a ativos de tecnologia da informação.

7.1.4 Norma para Gestão dos Serviços de Segurança da Informação (Anexo X): estabelece as diretrizes para a gestão dos processos de Segurança da Informação e dispõe sobre:

a) gestão de riscos cibernéticos;
b) gestão de vulnerabilidades;

c) gestão de incidentes;

d) coleta de evidências e artefatos; e

e) intervenções em ativos de TI.

7.1.5 Norma de Segurança da Informação para Uso da Internet (Anexo XI): estabelece a conduta adequada para uso da Internet nas Empresas do Sistema BNDES e dispõe sobre:

a) uso aceitável da Internet;

b) controles empregados; e

c) monitoração dos acessos.

7.1.6 Norma de Segurança da Informação para Uso de Ativos de Tecnologia da Informação (Anexo XII): estabelece as responsabilidades e condições que devem ser observadas para uso de ativos de TI das Empresas do Sistema BNDES e dispõe sobre:

a) uso adequado dos ativos de TI;

b) uso dos ativos de TI por terceiros; e

c) uso das redes corporativas.

7.1.7 Norma de Segurança da Informação para Administração de Ativos de Tecnologia da Informação (Anexo XIII): estabelece as responsabilidades e condições que devem ser observadas para administração de ativos de TI das Empresas do Sistema BNDES e dispõe sobre:

a) administração de ativos de TI;

b) administração das redes corporativas;

c) inventário de ativos de TI; e

d) inventário de licenças de *software*.

7.1.8 Norma de Segurança da Informação para Uso do Correio Eletrônico (Anexo XIV): estabelece a conduta adequada dos colaboradores das Empresas do Sistema BNDES na utilização do correio eletrônico corporativo e dispõe sobre:

a) uso aceitável do serviço de correio eletrônico;

b) restrições quanto à comunicação externa;

c) arquivos anexos;

d) monitoração; e

e) conteúdo malicioso.

7.1.9 Norma de Segurança da Informação para Uso de Dispositivos Pessoais (Anexo XV): estabelece as responsabilidades e condições para uso de dispositivos pessoais conectados à infraestrutura de Tecnologia da Informação das Empresas do Sistema BNDES e dispõe sobre:

a) condição para uso de dispositivos pessoais na infraestrutura de TI do Sistema BNDES;

b) restrições quanto ao uso de dispositivos pessoais para acesso a recursos internos;

c) gerenciamento e controle;

d) monitoração; e

e) suporte.

7.1.10 Norma de Segurança da Informação para Uso de Serviços de Processamento, Armazenamento e Transmissão de Dados e Computação em Nuvem (Anexo XVI): estabelece os procedimentos e requisitos para uso de serviços de Tecnologia da Informação em nuvem para guarda, processamento ou transmissão de informações corporativas e dispõe sobre:

a) categorias de serviço de computação em nuvem;

b) restrições para o uso e análise preliminar de riscos;

c) autenticação, provisionamento e autorização;

d) auditoria e tratamento de incidentes de segurança;

e) controles exigidos;

f) continuidade do serviço; e

g) proteção dos dados e da comunicação.

7.1.11 Norma de Segurança da Informação para Uso Institucional de Mídias Sociais (Anexo XVII): estabelece a conduta adequada para uso e gestão de perfis institucionais das Empresas do Sistema BNDES mantidos em mídias sociais e dispõe sobre:

a) responsabilidades;

b) diretrizes e orientações para uso institucional seguro de mídias sociais; e

c) controles exigidos.

APROVADO PELA RESOLUÇÃO CA BNDES nº 20/2023

8. PENALIDADES

8.1 O descumprimento da PCSI pode acarretar responsabilização, nos termos dos respectivos regulamentos de pessoal dos Planos de Cargos e Salários das Empresas do Sistema BNDES e nos termos dos contratos ou convênios para estagiários, menores aprendizes, empresas prestadoras de serviço e seus empregados, sem prejuízo das responsabilidades civis e penais eventualmente cabíveis.

9. DISPOSIÇÕES FINAIS

9.1 Casos excepcionais ou não contemplados pela PCSI devem ser tratados individualmente, mediante orientação da unidade gestora de Segurança da Informação.

9.1.1 Eventualmente, por decisão da unidade gestora de Segurança da Informação ou para resolução de conflitos, o Comitê de Segurança da Informação poderá ser envolvido e chamado a manifestar-se em casos excepcionais.

9.1.2 O Comitê de Contingência, quando instaurado, poderá excepcionalizar temporariamente controles de Segurança da Informação, quando tais controles inviabilizarem a execução dos procedimentos de recuperação necessários.

9.2 A unidade gestora de Segurança da Informação pode propor a implantação de controles adicionais para atingir os objetivos definidos na seção 1, desde que de acordo com os princípios desta PCSI.

9.3 Havendo modificação na nomenclatura ou na competência das Unidades Fundamentais e Unidades Administrativas Principais da estrutura organizacional do Sistema BNDES, ou a atualização de normativos, o presente ato normativo permanecerá em vigor, adequando-se a sua aplicação às novas normas da organização interna.

9.4 O prazo previsto para revisão desta Política é anual, em conformidade com a Resolução CMN nº 4.893 de 2021.

9.4.1 A revisão anual será submetida diretamente à manifestação do Conselho de Administração do BNDES sempre que não houver necessidade de alteração na Política em vigência ou nas situações em que a proposta se enquadrar nas seguintes hipóteses:

a) a alteração tiver como finalidade mera adequação a normativo externo de reprodução obrigatória; e/ou

b) a alteração tiver como finalidade a correção de erro material; e/ou
c) a alteração tiver como finalidade adequar a redação da Política às modificações realizadas na estrutura organizacional do Sistema BNDES, desde que a proposta se limite a alterar siglas/nomes de unidades e/ou sugira a redistribuição dos papéis e responsabilidades já previstos no normativo, de forma a adaptar a Política ao disposto na Organização Interna Básica do Sistema BNDES em relação às atribuições das Unidades Fundamentais (UF) e/ou das Unidades Administrativas Principais (UAP).

9.4.1.1 Previamente à manifestação do Conselho de Administração, será feito comunicado à Diretoria Executiva, ao Comitê de Riscos e, eventualmente a outro órgão colegiado sempre que exigido por normativo externo.

9.4.1.2 A proposta de revisão não seguirá este trâmite nos casos em que, ao se manifestar sobre a matéria, o Conselho de Administração entenda pela impossibilidade de adoção do fluxo de aprovação simplificada.

9.5 O presente ato normativo entrará em vigor na data de sua publicação no Portal de Normas, revogando-se a Resolução CA nº 22/2022, de 26/12/2022.

Manual de Conceitos da Política Corporativa de Segurança da Informação

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Este manual tem o objetivo de esclarecer os conceitos necessários à plena compreensão da Política Corporativa de Segurança da Informação do Sistema BNDES (PCSI) e de seus documentos complementares.

Art. 2º - O presente manual aplica-se a todos os colaboradores que exercem atividades no âmbito das empresas do Sistema BNDES e demais pessoas que têm acesso a informações de propriedade ou sob custódia das empresas do Sistema BNDES.

CAPÍTULO II - CONCEITOS

I - **Acesso remoto** – Uso de ativos de Tecnologia da Informação (TI) de acesso normalmente restrito à rede corporativa, a partir de redes públicas, compartilhadas ou de terceiros.

II - **Agente de tratamento** – o controlador e o operador, conforme definição dos respectivos termos.

III - **Ameaça** – Qualquer perigo em potencial de exploração de uma vulnerabilidade por um agente.

IV - **API** – Interface de Programação de Aplicação, cujo acrônimo provém do inglês *Application Programming Interface*, é um conjunto de rotinas e padrões estabelecidos por um *software* para a utilização das suas funcionalidades por outros aplicativos.

V - **Arquivos executáveis** – Arquivos cujo conteúdo pode ser interpretado (e executado) por um computador como um programa. Algumas extensões comuns para esse tipo de arquivo são: EXE, COM, BAT, SCR, CMD, PIF e LNK.

VI - **Artefato** – Programa de computador, equipamento, documento, arquivo ou código malicioso associado a um incidente de segurança.

VII - **Assinatura digital –** Assinatura em meio eletrônico, que permite aferir a origem e a integridade de informações digitais.

VIII - **Ativo crítico de Tecnologia da Informação –** Ativo de Tecnologia da Informação extremamente relevante para a execução de processos de negócio das empresas do Sistema BNDES, tais como: servidores de banco de dados, equipamentos de infraestrutura de rede que suportam o núcleo da rede, servidores que suportam sistemas cuja disponibilidade é crítica, ativos de TI classificados como críticos por seus gestores, ativos de TI que implementam controles de segurança da informação e ativos de TI que armazenam ou manipulam informações sigilosas.

IX - **Ativo de informação** – Dado ou informação que tem valor para as Empresas do Sistema BNDES, bem como meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal e locais onde se encontram esses meios.

X - **Ativo de Tecnologia da Informação** – Elementos computacionais *(hardware e software)* e de infraestrutura de Tecnologia da Informação (circuitos de dados, redes de computadores e telefonia), com exceção dos dispositivos pessoais particulares, utilizados na execução dos processos das empresas do Sistema BNDES.

XI - **Autenticação** – Processo de verificação da identidade de uma entidade (usuário, equipamento, sistema etc.).

XII - **Autenticação de dois fatores** – Processo de verificação da identidade digital de entidades (usuários, equipamentos, sistemas etc.) mediante uso combinado de dois critérios (ou fatores) de autenticação distintos, os quais podem ser divididos em três categorias: baseados no que se conhece (ex.: senha), no que se detém (ex.: crachá) ou no que se é, ou seja, numa característica pessoal (ex.: impressão digital).

XIII - **Autorização** – Processo que determina se uma entidade (usuário, equipamento, sistema etc.), depois de devidamente autenticada, possui permissão para realizar determinada operação.

XIV - **Certificado digital** – Arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade.

XV - **Classificação –** Atribuição, por agente competente, de grau de sigilo ou nível de proteção a ativos de informação, áreas ou instalações.

XVI - **Código malicioso** – Termo que define o *software* destinado a infiltrar-se em um sistema de computador de forma ilícita, com o intuito de causar algum dano ou roubar informações. São exemplos de códigos maliciosos os vírus de computador, os cavalos de Troia (*trojan horses*) e os programas espiões (*spywares*).

XVII - **Colaboradores** – todos os Participantes do Sistema BNDES, incluindo, além de empregados, estagiários e membros da Alta Administração, os prestadores de serviço, os consultores e menores aprendizes.

XVIII - **Comprometimento** – Violação de segurança resultante de acesso não-autorizado.

XIX - **Conteúdo malicioso –** Artefato utilizado para disseminar código malicioso.

XX - **Controlador** – sob o aspecto da Lei Geral de Proteção de Dados Pessoais (LGPD), é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

XXI - **Controle de acesso** – Estrutura de processos que permite negar ou conceder privilégios de acesso a um recurso (entidade passiva que pode ser um sistema, um arquivo, um serviço, um ambiente etc.) por um sujeito (entidade ativa, como um indivíduo ou processo computacional).

XXII - **CPADS** – Sigla utilizada para referir-se à Comissão Permanente de Avaliação e Destinação de Documentos Sigilosos, grupo multidisciplinar encarregado da avaliação de documentos de arquivo das empresas do Sistema BNDES, no que tange ao grau de sigilo. A constituição, as competências e o funcionamento da CPADS constam da Política Corporativa de Arquivo.

XXIII - **Credencial de acesso** – Conjunto de informações e dispositivos necessários à realização de acesso controlado a determinado recurso, por exemplo um par identificador de acesso e senha ou um certificado digital.

XXIV - **Criptografia** – Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É

usada, entre outras finalidades, para autenticar usuários e transações, proteger a integridade de transferências eletrônicas de fundos e preservar o sigilo em comunicações pessoais e comerciais.

XXV - **Custódia** – Responsabilidade pela guarda e proteção de ativos de informação, independentemente de vínculo de propriedade. A custódia não permite automaticamente o acesso aos ativos, nem o direito de conceder acesso a outrem.

XXVI - **Dado** – Qualquer elemento identificado em sua forma bruta, que em determinado contexto não conduz, por si só, à compreensão de determinado fato ou situação.

XXVII - **Dado pessoal –** Qualquer informação relacionada à pessoa natural identificada ou identificável.

XXVIII - **Dado pessoal sensível** – Qualquer dado pessoal sobre a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou à 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.

XXIX - **Desclassificação** – Cancelamento, por autoridade competente ou por decurso de prazo, de classificação previamente atribuída.

XXX - **Dispositivo de filtragem de tráfego** – Sistema computacional que controla o fluxo de tráfego entre redes por meio da verificação de um conjunto de regras previamente definidas.

XXXI - **Dispositivos móveis** – Dispositivos computacionais portáteis, cuja mobilidade é facilitada por natureza e que permitem o armazenamento ou o processamento de informações. São exemplos de dispositivos móveis: *laptops*, dispositivos de reprodução multimídia, telefones celulares e câmeras digitais.

XXXII - **Documento** – Ativo de informação que consiste em unidade de registro de informações, qualquer que seja o suporte ou formato utilizados.

XXXIII - **Documento eletrônico –** Documento mantido em suporte eletrônico, acessível por meio de sistema computacional.

XXXIV - **Documento físico –** Documento mantido em suporte papel ou microforma, como microfilmes e microfichas.

XXXV - **Empresas do Sistema BNDES** – o conjunto de entidades constituído pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e suas subsidiárias ou, ainda, qualquer das entidades isoladamente, quando utilizada de forma a referir-se a apenas uma delas:

a) Agência Especial de Financiamento Industrial S.A. (FINAME);

b) BNDES Participações S.A. (BNDESPAR);

c) demais instituições que vierem a ser constituídas pelo BNDES no País ou no exterior.

XXXVI - **Encarregado (DPO)** – pessoa indicada pelo agente de tratamento que atua como canal de comunicação entre ela, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD), bem como exerce outras atribuições relacionadas à proteção de dados pessoais como definidas pelo Agente de Tratamento.

XXXVII - **Estação de Trabalho** – Microcomputador, inclusive portátil, disponibilizado pelas empresas do Sistema BNDES para apoiar a realização das atividades profissionais.

XXXVIII - **ETIR BNDES** – Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação em Redes do BNDES.

XXXIX - **Evento** – Qualquer mudança no estado da infraestrutura, sistemas ou serviços de Tecnologia da Informação.

XL - **Evidência** – Tudo aquilo que pode ser usado para provar que uma determinada afirmação é verdadeira ou falsa.

XLI - **Gestor da informação** – Empregado titular de função executiva responsável por Unidade Gestora de informação.

XLII - **Gestor de Recursos Humanos (GRH) –** Empregado titular de função executiva responsável por uma Unidade Administrativa ou empregado designado para desempenhar a atividade de gestão de contrato que envolve prestação de serviço executado por colaborador externo.

XLIII - **Gestor de Recurso Técnico (GRT) –** Empregado responsável pela gestão de um ativo de informação ao qual o acesso deve ser controlado.

XLIV - **Grau de sigilo** – Gradação de sigilo atribuída a uma informação em razão da natureza de seu conteúdo, com o objetivo de limitar sua divulgação a quem tenha necessidade de conhecê-la.

XLV - **Hypervisor** – É um sistema monitor de máquinas virtuais, ou seja, é uma camada de *software* que permite a criação e execução de vários sistemas operacionais em um mesmo computador por meio do compartilhamento dos recursos do *hardware* (CPU, memória, periféricos etc).

XLVI - **Identificador de acesso** – Nome que permite identificar inequivocamente uma entidade durante a realização de um acesso. Também conhecido como identificador de usuário, *login* ou *userid*.

XLVII - **Incidente de Segurança da Informação** – Evento adverso, confirmado ou sob suspeita, que ameace os objetivos da PCSI, tais como: o acesso não autorizado a ativos de informação; ataques de negação de serviço; distribuição de *software* malicioso; etc.

XLVIII - **Incidente cibernético** – Incidentes de segurança da informação que produz efeito adverso ou represente ameaça a ativos de tecnologia da informação ou à informação durante o processamento, armazenamento ou transmissão por meio desses ativos.

XLIX - **Informação** – Dados organizados e inseridos em um contexto, de maneira a propiciar retorno a quem os acessa ou a conduzir a um resultado.

L - **Informação interna** – Informação produzida pelas empresas do Sistema BNDES e por seus empregados e estagiários.

LI - **Informação externa** – Informação recebida ou adquirida de entidades externas pelas empresas do Sistema BNDES.

LII - **Informação ostensiva** – Informação pública, portanto sem qualquer restrição de acesso, cujo uso pode transcender o âmbito das empresas do Sistema BNDES.

LIII - **Informação sigilosa –** Informação com restrição de acesso devido a sua natureza e/ou conteúdo.

LIV - ***Internet*** – Rede de computadores interconectados em escala mundial e de acesso público. A Internet disponibiliza diversos serviços, como o correio eletrônico e o *World Wide Web* (documentos e informações disponíveis em hipertextos relacionados).

LV - **IPSec** – Conjunto de protocolos que implementa segurança em comunicações via redes de pacotes IP, com autenticação das partes envolvidas e criptografia dos dados transmitidos. O IPSec implementa ainda um protocolo para troca de chaves de criptografia.

LVI - **Levantamento de Vulnerabilidades** – Atividade necessária para identificar e monitorar fragilidades em ativos de Tecnologia da Informação (TI) decorrentes de falhas técnicas que, se exploradas, podem comprometer a confidencialidade, a disponibilidade, a integridade e a autenticidade das informações processadas, armazenadas ou transmitidas por meio desses ativos.

LVII - **Manipulação de Informações –** Atividades de armazenamento, processamento ou transmissão de informações.

LVIII - **Material de divulgação** – ativo de informação produzido com finalidade de comunicar as atividades das empresas do Sistema BNDES para um público amplo, de endereçamento não individualizado e cuja distribuição não pode ser monitorada. São exemplos: folhetos, cartazes, livros, revistas, lâminas, *folders*, boletins, *banners*, *banners* eletrônicos e convites eletrônicos.

LIX - **Medidas especiais de segurança –** Medidas destinadas a garantir sigilo, inviolabilidade, confidencialidade, integridade, autenticidade, legitimidade e disponibilidade de informações. Também objetivam prevenir, detectar, anular e registrar ameaças às informações.

LX - **Necessidade de conhecer –** Condição pessoal, inerente ao efetivo exercício, no âmbito das empresas do Sistema BNDES, de cargo, função, emprego ou atividade, indispensável para que uma pessoa autorizada tenha acesso a informações sigilosas.

LXI - **Operador** – sob o aspecto da Lei Geral de Proteção de Dados Pessoais (LGPD) é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

LXII - **OVF –** Sigla que provém do inglês *Open Virtualization Format*, que se refere ao padrão aberto para empacotamento e distribuição de *appliances* virtuais ou, de forma mais genérica, *software* para ser executado em máquinas virtuais.

LXIII - **Padrão *Syslog* –** Padrão criado pela *Internet Engineering Task Force* (IETF) para a transmissão em redes IP de registros utilizados na formação de trilhas de auditoria. O termo é geralmente usado para identificar tanto o protocolo de rede quanto a aplicação ou biblioteca de envio de mensagens no protocolo *syslog*.

LXIV - **Participantes do Sistema BNDES**: empregados integrantes dos quadros de pessoal permanente ou temporário, ainda que se encontrem cedidos ou requisitados ou em gozo de licença ou em outro afastamento equivalente, com ou sem remuneração, os cedidos às empresas do Sistema BNDES, os estagiários e os membros da Alta Administração das empresas do Sistema BNDES.

LXV - **Plano de continuidade do negócio –** Conjunto de ações de prevenção e procedimentos de recuperação a serem seguidos para proteger os processos críticos de trabalho contra efeitos de falhas em equipamentos, acidentes, ações intencionais ou desastres naturais significativos, assegurando a disponibilidade das informações.

LXVI - **Política Corporativa de Segurança da Informação do Sistema BNDES (PCSI) –** Conjunto de documentos composto pelas diretrizes da Política Corporativa de Segurança da Informação (documento da Política – nível estratégico) e por seus documentos complementares (normas de segurança – nível tático, além dos modelos de termos de confidencialidade). A implementação da PCSI contempla também procedimentos e instruções (nível operacional).

LXVII - **Privilégio de acesso –** Autorização para utilizar um ou mais ativos de informação.

LXVIII - **Privilégio administrativo –** Privilégio de acesso atribuído a usuário com permissão para administrar os recursos de um sistema computacional. Usuários com privilégios administrativos podem instalar ou remover *software*, adicionar ou remover usuários em sistemas computacionais, bem como alterar configurações. Normalmente, privilégios administrativos relacionados a recursos de Tecnologia da Informação são restritos à Unidade Gestora de Tecnologia da Informação.

LXIX - **Programa de computador –** Sequência completa de instruções a serem executadas por computador. A definição abrange tanto a versão em código-fonte (escrita em linguagem simbólica) quanto o código executável (já convertido em linguagem de máquina).

LXX - **Reclassificação –** Alteração, pela autoridade competente, de classificação previamente atribuída.

LXXI - **Recurso de tecnologia de informação –** Qualquer equipamento, dispositivo, serviço, infraestrutura ou sistema de processamento da informação, bem como instalações físicas que os abriguem.

LXXII - **Rede interna –** Parte da infraestrutura de rede de computadores das Empresas do Sistema BNDES potencialmente com acesso aos seus ativos críticos de Tecnologia da Informação.

LXXIII - **Rede sem fio corporativa -** Rede sem fio que provê acesso à rede interna das Empresas do Sistema BNDES.

LXXIV - **Restrição de acesso –** Limitação da possibilidade de obtenção, consulta ou utilização da informação.

LXXV - **Risco à Segurança da Informação –** potencial de violação da integridade, confidencialidade, disponibilidade ou autenticidade da informação de propriedade ou custodiada pelo Sistema BNDES em decorrência da exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo às Empresas do Sistema BNDES. Esta definição inclui o risco cibernético, que é o risco à segurança da informação que envolve ativo de tecnologia da informação.

LXXVI - **Rotulagem –** Ação ou efeito de rotular um ativo de informação.

LXXVII - **SAML –** Sigla utilizada para referir-se a Security Assertion Markup Language, protocolo para permitir a integração entre sistemas de autenticação e autorização de acessos.

LXXVIII - **Sigilo bancário –** Resguardo, por instituições financeiras, de informações relacionadas a suas operações e serviços, conforme disposto na Lei Complementar nº 105/ 2001, de 10/01/2001.

LXXIX - **Sistema de informação –** Conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, sistemas de informática, especificações e procedimentos para sua operação, uso e manutenção.

LXXX - **Sistema de informática –** Conjunto de programas de computador destinados a realizar funções específicas.

LXXXI - **Sistema operacional –** Programa de computador responsável por realizar a interface entre o *software* e os diversos dispositivos de *hardware* existentes em um computador, bem como gerenciar seus recursos.

LXXXII - **Secure Sockets Layer (SSL) –** Protocolo criptográfico que provê comunicação segura na *Internet* para serviços como correio eletrônico, navegação por páginas web (HTTP) e outros tipos de transferência de dados. Também pode ser utilizado como protocolo para o estabelecimento de canais VPN.

LXXXIII - **Sub-rede –** Divisão de uma rede de computadores. A divisão de uma rede grande em redes menores resulta em tráfego de rede reduzido, administração simplificada e melhor desempenho.

LXXXIV - **Suporte –** Material no qual são registradas as informações.

LXXXV - **Tabela de Temporalidade e Destinação de Documentos (TTD) –** Instrumento aprovado pela autoridade competente, que determina prazos e condições de guarda de documentos tendo em vista a transferência ao arquivo intermediário, recolhimento ao arquivo permanente, migração de suporte e eliminação segura de documentos.

LXXXVI - **Teste de Invasão (ou teste de penetração ou *pentest*) –** simulação de ataques cibernéticos contra ativos de Tecnologia da Informação ou processos de uma organização, realizados em condições controladas, para a identificação de vulnerabilidades.

LXXXVII - **Trilha de auditoria –** Registros históricos com detalhes das tentativas de autenticação (bem-sucedidas ou não) e das ações que envolvam criação, alteração, remoção, leitura ou reprodução de informações, bem como movimentação (entrada e saída) de pessoal e material.

LXXXVIII - **Unidade administrativa –** Órgão das empresas do Sistema BNDES, o que inclui Conselho de Administração, Conselho Fiscal, Presidência, Vice-Presidência, Diretorias, Unidades Fundamentais (Áreas), Unidades Administrativas Principais (Departamentos), Gerências Executivas, Gerências e Coordenações de Serviço.

LXXXIX - **Unidade gestora de informação –** Unidade administrativa responsável por gerir as informações produzidas, recebidas, adquiridas ou custodiadas pelas empresas do Sistema BNDES durante todas as fases envolvidas na gestão da informação.

XC - **Usuário –** Indivíduo que utiliza um sistema de informação.

XCI - ***Universal Time – Coordinated*** **(UTC) –** Fuso horário de referência, a partir do qual se calculam todas as outras zonas horárias do mundo. É equivalente ao Tempo Médio de Greenwich (GMT - Greenwich Mean Time).

XCII - ***Virtual Private Network*** **(VPN) –** Rede de comunicações privada estabelecida sobre rede de comunicações pública (como a Internet, por exemplo) ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados em trânsito.

XCIII - **Vulnerabilidade –** Ausência ou fraqueza de proteção, que pode ser explorada para fins maliciosos.

TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS PARA CONTRATOS ADMINISTRATIVOS

_____*(Identificação da empresa – CNPJ, Razão Social, etc)*_____, por intermédio de seu representante legal, _____(*identificação do representante legal – Nome e CPF)*_____, doravante designado simplesmente **RESPONSÁVEL**, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O **RESPONSÁVEL** reconhece que, em razão da sua prestação de serviços às **EMPRESAS DO SISTEMA BNDES** – Contrato OCS nº _____/_____, celebrado em _____/_____/_____, estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES**, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES** e do **RESPONSÁVEL**, sem a expressa e escrita autorização do representante legal signatário do Contrato ora referido.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas ou confidenciais a que venha a ter acesso;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Documentos e informações utilizados na execução dos serviços do contrato OCS nº _____/_____.

CLÁUSULA TERCEIRA

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza confidencial de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal das **EMPRESAS DO SISTEMA BNDES**, signatário do Contrato OCS nº _____/_____, a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

O **RESPONSÁVEL** recolherá, ao término do Contrato OCS nº _____/_____, para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse seja de seus empregados, prepostos, prestadores de serviço seja de fornecedores, com vínculo empregatício ou eventual com o **RESPONSÁVEL**, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial, dado pessoal a que teve acesso enquanto contratado pelas **EMPRESAS DO SISTEMA BNDES**.

Parágrafo Único

O **RESPONSÁVEL** determinará a todos os seus empregados, prepostos e prestadores de serviço que estejam, direta ou indiretamente, envolvidos com a prestação de serviços objeto do Contrato OCS nº _____/_____, a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA QUINTA

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA SEXTA

O RESPONSÁVEL obriga-se a tratar os dados pessoais que tiver acesso em razão de seu relacionamento com as EMPRESAS DO SISTEMA BNDES unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD, observando a Política Corporativa de

Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver, por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

   a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais 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; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

CLÁUSULA SÉTIMA

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação, bem como do **RESPONSÁVEL**, no que for cabível.

CLÁUSULA OITAVA

As obrigações a que alude este instrumento perdurarão inclusive após a cessação do vínculo contratual entre o **RESPONSÁVEL** e as **EMPRESAS DO SISTEMA BNDES** e abrangem as informações presentes e futuras.

[OBS.: A CLÁUSULA ABAIXO DEVE SER INCLUÍDA QUANDO FOR POSSÍVEL DELIMITAR OS PROFISSIONAIS QUE IRÃO PRESTAR OS SERVIÇOS OBJETO DO CONTRATO]

CLÁUSULA NONA

O **RESPONSÁVEL** se compromete no âmbito do Contrato objeto do presente Termo, a apresentar às **EMPRESAS DO BNDES** declaração individual de adesão e aceitação das cláusulas do **Termo de Confidencialidade para Profissionais Terceirizados**, de cada integrante ou participante da equipe que prestar ou vier a prestar os serviços especificados no Contrato OCS nº _____/_____.

DE ACORDO,

Rio de Janeiro, ____ de _____ de 20____.

_____

RESPONSÁVEL

Modelo de Termo de Confidencialidade e de Tratamento de Dados Pessoais para Profissionais e Estagiários das Empresas do Sistema BNDES

TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS PARA PARTICIPANTES DO SISTEMA BNDES

(identificação – Nome e CPF), doravante designado simplesmente **RESPONSÁVEL**, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. – FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O **RESPONSÁVEL** reconhece que, em razão de seu relacionamento funcional e de seu vínculo empregatício ou contratual com as **EMPRESAS DO SISTEMA BNDES**, estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES** e de seus clientes e parceiros comerciais, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES**, sem a expressa e escrita autorização do representante legal das **EMPRESAS DO SISTEMA BNDES**.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas, inclusive aquelas relativas ao sigilo bancário que as **EMPRESAS DO SISTEMA BNDES** devem observar, por imposição legal;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Documentos e informações utilizados no relacionamento com as **EMPRESAS DO SISTEMA BNDES**.

CLÁUSULA TERCEIRA

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham a ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza sigilosa de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal das **EMPRESAS DO SISTEMA BNDES** a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

O **RESPONSÁVEL** recolherá para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade destas, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial e dados pessoais a que teve acesso enquanto em contato com as **EMPRESAS DO SISTEMA BNDES**.

Parágrafo Único

O **RESPONSÁVEL** adotará todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA QUINTA

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA SEXTA

O RESPONSÁVEL obriga-se a tratar os dados pessoais que tiver acesso em razão de seu relacionamento com as EMPRESAS DO SISTEMA BNDES unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD (conforme Guia de Bases Legais do Sistema BNDES), observando a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver, por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

   a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais 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; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, a Unidade Responsável pela gestão da base de dados e ao GOPD, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

CLÁUSULA SÉTIMA

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal do **RESPONSÁVEL** que, comprovadamente, estiver envolvido no descumprimento ou violação e ensejará, quando for o caso, a aplicação do disposto no subitem "Penalidades" dos regulamentos gerais de pessoal dos respectivos planos de cargos e salários.

CLÁUSULA OITAVA

As obrigações a que alude este instrumento perdurarão inclusive após a cessação do relacionamento entre o **RESPONSÁVEL** e as **EMPRESAS DO SISTEMA BNDES,** e abrangem as informações presentes ou futuras.

DE ACORDO,

Rio de Janeiro, ____ de _____ de 20____.

_____

RESPONSÁVEL

TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS PARA PROFISSIONAIS TERCEIRIZADOS

_____(*identificação – Nome e CPF)*_____, doravante designado simplesmente **RESPONSÁVEL**, compromete-se, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O **RESPONSÁVEL** reconhece que, em razão da sua prestação de serviços às **EMPRESAS DO SISTEMA BNDES** – Contrato OCS nº _____/_____, celebrado em _____/_____/_____, estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES**, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES** e do **RESPONSÁVEL**, sem a expressa e escrita autorização do representante legal signatário do Contrato ora referido.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas ou confidenciais a que venha a ter acesso enquanto contratado por empresa que preste serviço às **EMPRESAS DO SISTEMA BNDES**;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Documentos e informações utilizados na execução dos serviços do contrato OCS nº _____/_____.

CLÁUSULA TERCEIRA

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham a ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza confidencial de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal das **EMPRESAS DO SISTEMA BNDES**, signatário do Contrato OCS nº _____/_____, a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

O **RESPONSÁVEL** recolherá, ao término do Contrato OCS nº _____/_____, para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade destas, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial e dados pessoais a que teve acesso enquanto contratado pelas **EMPRESAS DO SISTEMA BNDES**.

Parágrafo Único

O **RESPONSÁVEL** adotará todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA QUINTA

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA SEXTA

O RESPONSÁVEL obriga-se a tratar os dados pessoais a que tiver acesso em razão do Contrato OCS nº _____/_____, com as EMPRESAS DO SISTEMA BNDES unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD, observando a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver,

por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais 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; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, as EMPRESAS DO SISTEMA BNDES, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

CLÁUSULA SÉTIMA

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

CLÁUSULA OITAVA

As obrigações a que alude este instrumento perdurarão inclusive após a cessação da prestação de serviços objeto do Contrato OCS nº _____/_____, e abrangem as informações presentes e futuras.

DE ACORDO,

Rio de Janeiro, ____ de _____ de 20____.

_____

RESPONSÁVEL

TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS

_____*(Identificação da empresa – CNPJ, Razão Social, etc)*_____, por intermédio de seu representante legal, _____(*identificação do representante legal – Nome e CPF)*_____, doravante designado simplesmente **RESPONSÁVEL**, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. - FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O RESPONSÁVEL reconhece que, em razão de (_____*DESCRIÇÃO RESUMIDA DO EVENTO, FATO OU ATIVIDADE*), verificado(a) em___/____/____ (ou a partir de / /), estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES**, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES** e do **RESPONSÁVEL**, sem a expressa e escrita autorização do representante legal das **EMPRESAS DO SISTEMA BNDES**.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas ou confidenciais a que venha a ter acesso;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Documentos e informações utilizados, obtidos ou produzidos durante o fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA**.

CLÁUSULA TERCEIRA

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza confidencial de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente por representante legal das **EMPRESAS DO SISTEMA BNDES**, a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

O **RESPONSÁVEL** recolherá, ao término do fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA**, para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, seja de seus empregados, prepostos, prestadores de serviço, seja de fornecedores, com vínculo empregatício ou eventual com o **RESPONSÁVEL**, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial e dados pessoais a que teve acesso durante o referido fato, evento ou atividade.

Parágrafo Único

O **RESPONSÁVEL** determinará a todos os seus empregados, prepostos e prestadores de serviço que estejam, direta ou indiretamente, envolvidos no fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA**, a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas, responsabilizando-se pelo seu eventual descumprimento, por parte de qualquer integrante ou participante da equipe envolvida no referido fato, evento ou atividade.

CLÁUSULA QUINTA

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA SEXTA

O RESPONSÁVEL obriga-se a tratar os dados pessoais que tiver acesso em razão do fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA,** unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD, observando a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver, por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

   a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais 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; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, as EMPRESAS DO SISTEMA BNDES, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

CLÁUSULA SÉTIMA

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal do **RESPONSÁVEL** que, comprovadamente, estiver envolvido no descumprimento ou violação.

CLÁUSULA OITAVA

As obrigações a que alude este instrumento perdurarão inclusive após a cessação da execução da atividade referida na **CLÁUSULA PRIMEIRA** por período não inferior a 20 (vinte) anos, salvo se expressamente autorizado por representante legal das **EMPRESAS DO SISTEMA BNDES**.

Parágrafo Único

As obrigações a que a alude este instrumento são extensíveis aos integrantes ou participantes envolvidos no fato, evento ou atividade aludido na CLÁUSULA PRIMEIRA, cabendo ao RESPONSÁVEL as medidas jurídicas cabíveis para assegurar a observância dessas obrigações.

DE ACORDO,

Rio de Janeiro, ____ de _____ de 20____.

_____

RESPONSÁVEL

TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS

_____(*identificação – Nome e CPF)*_____, doravante designado simplesmente **RESPONSÁVEL**, compromete-se, por intermédio do presente TERMO DE CONFIDENCIALIDADE E TRATAMENTO DE DADOS PESSOAIS, a tratar adequadamente os dados pessoais e a não divulgar sem autorização quaisquer informações de propriedade do Banco Nacional de Desenvolvimento Econômico e Social - BNDES e de suas Subsidiárias BNDES Participações S.A. - BNDESPAR e Agência Especial de Financiamento Industrial S.A. FINAME, doravante simplesmente designados como **EMPRESAS DO SISTEMA BNDES**, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA

O **RESPONSÁVEL** reconhece que, em razão de (_____*DESCRIÇÃO RESUMIDA DO EVENTO, FATO OU ATIVIDADE*), verificado(a) em___/____/____ (ou a partir de / /), estabelece contato com informações privadas das **EMPRESAS DO SISTEMA BNDES**, que podem e devem ser conceituadas como segredo de indústria ou de negócio. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios empregados das **EMPRESAS DO SISTEMA BNDES** e do **RESPONSÁVEL**, sem a expressa e escrita autorização do representante legal das **EMPRESAS DO SISTEMA BNDES**.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no âmbito das **EMPRESAS DO SISTEMA BNDES** e que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Listagens e documentações com informações sigilosas ou confidenciais a que venha a ter acesso enquanto contratado por empresa que preste serviço às **EMPRESAS DO SISTEMA BNDES**;

II. Documentos relativos a estratégias econômicas, financeiras, de investimentos, de captações de recursos, de marketing, de clientes e respectivas informações, armazenadas sob qualquer forma, inclusive informatizadas;

III. Metodologias e ferramentas de desenvolvimento de produtos e serviços elaborados pelas **EMPRESAS DO SISTEMA BNDES** ou por terceiros para as **EMPRESAS DO SISTEMA BNDES**;

IV. Valores e informações de natureza operacional, financeira, administrativa, contábil e jurídica;

V. Documentos e informações utilizados, obtidos ou produzidos durante o fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA**.

CLÁUSULA TERCEIRA

O **RESPONSÁVEL** reconhece que as referências dos incisos I a V da **CLÁUSULA SEGUNDA** deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham a ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único

Em caso de dúvida acerca da natureza confidencial de determinada informação, o **RESPONSÁVEL** deverá mantê-la sob sigilo até que venha a ser autorizado expressamente por representante legal das **EMPRESAS DO SISTEMA BNDES**, a tratá-la diferentemente. Em hipótese alguma a ausência de manifestação expressa das **EMPRESAS DO SISTEMA BNDES** poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

O **RESPONSÁVEL** recolherá, ao término do fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA**, para imediata devolução às **EMPRESAS DO SISTEMA BNDES**, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, , dados pessoais, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial, dados pessoais a que teve acesso durante o referido fato, evento ou atividade.

Parágrafo Único

O **RESPONSÁVEL** adotará todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA QUINTA

O **RESPONSÁVEL** obriga-se a informar imediatamente às **EMPRESAS DO SISTEMA BNDES** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA SEXTA

O RESPONSÁVEL obriga-se a tratar os dados pessoais que tiver acesso em razão do fato, evento ou atividade aludido na **CLÁUSULA PRIMEIRA** unicamente para as finalidades informadas e/ou autorizadas e se o tratamento fundamentar-se em uma das situações previstas no art. 7º ou 11 da LGPD, observando a Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e a Politica Corporativa de Segurança da Informação do Sistema BNDES (PCSI), ambas das EMPRESAS DO SISTEMA BNDES, bem como o seguinte:

a) Os dados pessoais sensíveis só poderão ser compartilhados com terceiros nas hipóteses previstas na legislação de proteção de dados pessoais, quando houver,

por exemplo, o consentimento específico do titular de dados pessoais, quando necessário ao cumprimento de obrigação legal ou regulatória, à execução de política pública, ao exercício regular de direito e para garantia da prevenção à fraude e da segurança do titular de dados pessoais.

a.1) São entendidos como dados pessoais sensíveis, nos termos do inciso III do artigo 7º da LGPD, os dados pessoais 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; e

b) O RESPONSÁVEL deve comunicar, sem prejuízo de tomar outras medidas indicadas na PCSI, prontamente, sobre qualquer incidente com dados pessoais, aos quais teve acesso em razão da assinatura deste Termo, inclusive sobre o vazamento de dados pessoais.

CLÁUSULA SÉTIMA

O descumprimento de quaisquer das cláusulas do presente Termo acarretará responsabilização civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

CLÁUSULA OITAVA

As obrigações a que alude este instrumento perdurarão inclusive após a cessação da execução da atividade referida na **CLÁUSULA PRIMEIRA**, por período não inferior a

20 (vinte) anos, salvo se expressamente autorizado por representante legal das **EMPRESAS DO SISTEMA BNDES**.

DE ACORDO,

Rio de Janeiro, ____ de _____ de 20____.

_____

RESPONSÁVEL

Política Corporativa de Segurança da Informação

Norma de Segurança da Informação para

Acesso a Áreas com Ativos Críticos de TI

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem por objetivo disciplinar os controles e procedimentos para acesso a centros de processamento de dados e salas de telecomunicações com ativos críticos de Tecnologia da Informação (TI) das Empresas do Sistema BNDES.

Art. 2º - As áreas com ativos críticos de TI devem ser protegidas e ter o acesso controlado para assegurar que somente pessoas autorizadas possam nelas ingressar, bem como devem conter avisos informativos sobre a restrição de acesso de pessoal não autorizado.

§ 1º O acesso a centros de processamento de dados deve ser condicionado à autenticação de dois fatores.

§ 2º As demais salas de telecomunicações com ativos críticos de TI devem ser mantidas trancadas.

CAPÍTULO II - AUTORIZAÇÃO DE ACESSO

Art. 3º - Apenas os colaboradores autorizados pela UAP gestora de Infraestrutura de TI podem acessar áreas com ativos críticos de TI sem acompanhamento.

Parágrafo Único - As autorizações devem ser registradas e justificadas, referenciando o colaborador autorizado, o motivo, a data de início da autorização e o seu prazo de validade.

Art. 4º - A UAP gestora da Infraestrutura de TI deve revisar periodicamente a lista de pessoas autorizadas a ingressar em áreas com ativos críticos de TI e deve revogar as autorizações que não forem mais necessárias.

CAPÍTULO III - REGISTRO E MONITORAÇÃO DE ACESSO

Art. 5º - A UAP gestora da Infraestrutura de TI deve manter registro de cada acesso a áreas com ativos críticos de TI.

Parágrafo Único - O registro de acesso deve incluir dados que permitam identificar nome, empresa e horário de cada acesso.

Art. 6º - Os centros de processamento de dados devem ser monitorados por meio de câmeras de vídeo integradas a um sistema de gravação.

CAPÍTULO IV - EXECUÇÃO DE PROCEDIMENTOS TÉCNICOS

Art. 7º - Todo procedimento executado por prestadores de serviço em áreas com ativos críticos de Tecnologia da Informação deve ser acompanhado por um agente de segurança ou por um colaborador autorizado da UAP gestora de Infraestrutura de TI.

Art. 8º - A movimentação de equipamentos em áreas com ativos críticos de TI deve ser precedida de autorização formal da UAP gestora de Infraestrutura de TI, com a identificação dos equipamentos, bem como o horário e o propósito da atividade.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Acesso Remoto a Ativos de Tecnologia da Informação

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Art. 1º - Esta norma tem o objetivo de estabelecer as responsabilidades e condições que devem ser observadas no acesso remoto a ativos de Tecnologia da Informação (TI) das Empresas do Sistema BNDES.

Art. 2º - Para efeitos dessa norma, define-se acesso remoto como o uso de ativos de TI de acesso normalmente restrito à rede corporativa, a partir de redes públicas, compartilhadas ou de terceiros.

Art. 3º - O acesso remoto a ativos de TI das Empresas do Sistema BNDES, desde que em conformidade com os demais termos dessa norma, pode ocorrer:

I - por meio de uma rede privada virtual (*Virtual Private Network* – VPN), passível de ser estabelecida de duas formas:

a) direta, quando um dispositivo remoto a partir do qual será realizado o acesso estabelece uma conexão segura diretamente com a infraestrutura de acesso remoto do BNDES; ou

b) entre redes, quando uma conexão segura é estabelecida entre uma rede remota (externa à infraestrutura de TI das Empresas do Sistema BNDES) e uma rede do BNDES;

II - através de um portal *web* seguro, administrado pela UF gestora de Tecnologia da Informação, que permita o acesso a aplicações corporativas e a operação remota de estações de trabalho.

CAPÍTULO II - REGRAS GERAIS

Art. 4º - Todo colaborador que fizer uso de acesso remoto a ativos de TI das Empresas do Sistema BNDES é responsável por zelar pela segurança dos ativos expostos por consequência desse acesso.

Art. 5º - O acesso remoto deve ser restrito aos colaboradores autorizados e apenas aos ativos de TI necessários ao desempenho de suas atividades profissionais.

CAPÍTULO III - SOLICITAÇÃO E AUTORIZAÇÃO

Art. 6º - O acesso remoto para colaboradores deve ser justificado e precedido de autorização do chefe da UAP do solicitante ou por executivo que ocupe função hierarquicamente superior.

§ 1º - Os colaboradores com as funções de coordenador, gerente, gerente executivo, chefe de departamento, superintendente, assessor, diretor, presidente ou conselheiro não necessitam de autorização para realização do acesso remoto.

§ 2º - A autorização para o uso de dispositivos móveis corporativos, cuja concessão implicará necessariamente na viabilidade de realizar acessos remotos por meio de tais dispositivos, deve seguir o disposto na OS PRESI 04/2017 – BNDES.

CAPÍTULO IV - ACESSO REMOTO

Art. 7º - O acesso remoto somente pode ser realizado através de canais de comunicação seguros, utilizando protocolos aprovados pela unidade gestora de Segurança da Informação, com a infraestrutura de acesso remoto administrada pela UF gestora de Tecnologia da Informação.

Art. 8º - O uso de dispositivos corporativos deve ser privilegiado para realização do acesso remoto.

§ 1º - É proibido o uso de equipamentos compartilhados, disponibilizados em ambientes públicos (*LAN houses*, *cibercafés* e afins), para realização do acesso remoto.

§ 2º - O acesso remoto por meio de dispositivos pessoais deve ser limitado de acordo com regras definidas pela unidade gestora de Segurança da Informação em consonância com a percepção do risco associado.

Art. 9º - Convém que os dispositivos utilizados para realizar acesso remoto disponham de mecanismos habilitados e atualizados de filtragem de tráfego de rede (firewall) e de proteção contra software malicioso (antivírus).

Art. 10º - O acesso remoto deve ser condicionado à autenticação por dois fatores.

Parágrafo Único - No caso de acesso de prestadores de serviço, o gestor do contrato pode designar responsável pela guarda e ativação dos dispositivos utilizados como segundo fator.

Art. 10 - As sessões de acesso remoto devem ser desconectadas automaticamente após um período de inatividade definido pela unidade gestora de Segurança da Informação.

Art. 11 - A transferência de informações controladas para dispositivos pessoais através do acesso remoto somente é permitida em condições excepcionais, com a anuência do gestor da informação e desde que seja realizada por meio de recursos institucionais disponibilizados pela UF gestora de Tecnologia da Informação para esse fim.

CAPÍTULO V - AUDITORIA

Art. 12 - Os acessos remotos devem ser registrados apropriadamente para permitir a formação de trilhas de auditoria, de acordo com a Norma de Segurança da Informação para Administração de Ativos de TI.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Controle de Acesso à Informação

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Art. 1º - Esta norma tem o objetivo de regulamentar o controle de acesso à informação no âmbito das Empresas do Sistema BNDES.

Art. 2º - A presente norma aplica-se a todos os colaboradores que têm acesso próprio ou viabilizem o acesso de outrem a informações produzidas, obtidas ou custodiadas pelas Empresas do Sistema BNDES.

Art. 3º - O controle de acesso à informação no âmbito das Empresas do Sistema BNDES deve considerar a segregação de funções e estar em conformidade com o princípio do privilégio mínimo, segundo o qual cada colaborador deve possuir apenas o conjunto de privilégios estritamente necessários ao desempenho das suas atribuições profissionais.

Art. 4º - Não é permitida a utilização não autorizada de credenciais e privilégios de acesso, bem como de quaisquer recursos, físicos ou lógicos, no sentido de suprimir controles de acesso vigentes.

Art. 5º - Cabe ao executivo titular de unidade administrativa ou ao empregado designado como gestor de contrato de prestação de serviço, doravante identificado como **Gestor do Recurso Humano (GRH)**, a gestão dos privilégios de acesso dos colaboradores sob sua responsabilidade.

Art. 6º - Cabe ao empregado ou ao grupo de empregados responsável pela gestão de um ativo de informação, doravante identificado como **Gestor do Recurso Técnico (GRT)**, a gestão dos privilégios de acesso a esse ativo de informação.

§ 1º Chefes imediatos e mediatos do GRT podem autorizar acesso aos ativos de informação sob a responsabilidade de seus subordinados.

§ 2º Em casos excepcionais, mediante apresentação de justificativa, o acesso a ativos de informação poderá ser autorizado, conjuntamente, pelo Diretor responsável pela Área Jurídica do BNDES e pelo Diretor responsável por Segurança da Informação.

CAPÍTULO II - CREDENCIAIS DE ACESSO

Art. 7º - As credenciais de acesso dos colaboradores devem ser individuais e o seu compartilhamento não é permitido.

Art. 8º - Os colaboradores são responsáveis por toda e qualquer ação realizada mediante utilização de suas credenciais de acesso.

Art. 9º - O cadastro de credenciais de acesso dos colaboradores deve, sempre que possível, utilizar repositório centralizado, de forma a possibilitar o aproveitamento de base única de credenciais para o acesso a ativos distintos.

§ 1º As informações referentes a credenciais de acesso devem ser mantidas atualizadas com exatidão.

§ 2º As informações incluídas em bases de credenciais distintas, quando tal implementação for inevitável, devem ser mantidas consistentes e homogêneas quanto a padrões de preenchimento.

§ 3º O cadastro de credenciais de acesso dos empregados e estagiários deve incluir nome completo, lotação, telefone comercial, localização e endereço de correio eletrônico corporativo.

§ 4º O cadastro de credenciais de acesso dos prestadores de serviço e profissionais externos que desempenham atividades de caráter eventual deve incluir os seguintes dados do credenciado: nome completo, documento oficial, instituição de origem, telefone comercial, endereço de correio eletrônico e identificação do contrato de prestação de serviços (quando aplicável).

Art. 10 - As credenciais de acesso de uso pessoal de colaboradores não devem ser incluídas em programas, rotinas e procedimentos para acesso automatizado a ativos de Tecnologia da Informação.

Art. 11 - As credenciais de acesso destinadas à execução de programas, rotinas e procedimentos que demandem acesso automatizado a ativos de Tecnologia da Informação devem ser utilizadas exclusivamente para tal fim e seu uso ordinário por colaboradores não é permitido.

Art. 12 - O reaproveitamento de credenciais de uso pessoal de colaboradores para acesso a ativos de Tecnologia da Informação não é permitido, salvo quando destinado ao mesmo colaborador para o qual a credencial foi originalmente concedida.

Art. 13 - As credenciais de acesso de uso pessoal de colaboradores devem, sempre que possível, ser automaticamente bloqueadas após período de noventa dias consecutivos sem utilização.

Art. 14 - O acesso a redes sociais para gestão de perfis institucionais ou publicação institucional de conteúdo, sempre que disponibilizado pelo provedor do serviço, deve ser condicionado à autenticação por, no mínimo, dois fatores.

Art. 15 - O acesso a dispositivos móveis e estações de trabalho corporativos deve ser controlado e condicionado à apresentação de uma senha, sequência secreta ou fator biométrico que permita o desbloqueio do dispositivo.

Parágrafo Único - O acesso ao dispositivo deve ser automaticamente bloqueado após, no máximo, dez tentativas sucessivas de desbloqueio sem sucesso.

CAPÍTULO III - SENHAS

Art. 16 - As senhas associadas a identificadores de acesso pessoais não podem ser compartilhadas.

Art. 17 - Os colaboradores são responsáveis pela preservação da confidencialidade das senhas associadas aos identificadores de acesso que utilizam.

Art. 18 - As senhas em uso devem atender minimamente aos seguintes requisitos:

I - ter tamanho mínimo de oito caracteres;

II - conter letras e números; e

III - conter símbolos (caracteres especiais) ou a combinação de letras maiúsculas e minúsculas.

§ 1º Excepcionalmente, esses requisitos não serão exigidos quando:

I - decorrente de restrição tecnológica (exemplo: teclado exclusivamente numérico etc.); ou

II - for possível a aplicação de controles tecnológicos adicionais, definidos pela unidade gestora de Segurança da Informação, que busquem evitar a ocorrência de acessos não autorizados.

§ 2º Quando as senhas estiverem associadas à autenticação de dois fatores ou mais, o tamanho mínimo pode ser reduzido para quatro caracteres e sem restrição quanto à composição.

Art. 19 - As senhas associadas a identificadores de acesso pessoais de colaboradores devem ser alteradas pelo menos a cada 180 (cento e oitenta) dias.

§ 1º O procedimento de troca de senhas deve, sempre que possível, impedir a reutilização das quatro últimas senhas.

§ 2º A utilização de um segundo fator para autenticação dispensa a troca da senha nessa frequência.

Art. 20 - A reinicialização da senha associada a determinado identificador de acesso somente pode ser solicitada pelo próprio responsável por seu uso.

§ 1º Excepcionalmente, em caso de incidente de segurança da informação, a reinicialização poderá ocorrer mediante solicitação da unidade gestora de Segurança da Informação ou da UF gestora de Tecnologia da Informação.

§ 2º Para prestadores de serviço, a solicitação poderá ser realizada pelo gestor do contrato ou outro empregado delegado pelo gestor.

Art. 21 - As senhas reinicializadas ou inicialmente atribuídas a identificadores de acesso devem respeitar as presentes regras de formação, ser aleatórias e alteradas na primeira ocasião em que forem utilizadas.

Art. 22 - As senhas utilizadas pelos colaboradores no âmbito das Empresas do Sistema BNDES não devem ser utilizadas em sistemas não administrados exclusivamente pelo Banco.

CAPÍTULO IV - DISPOSITIVOS CRIPTOGRÁFICOS CORPORATIVOS

Art. 23 - Os dispositivos criptográficos para armazenamento de certificados digitais pessoais, tais como e-CPF, são de uso exclusivo de cada colaborador e não podem ser compartilhados.

Art. 24 - Os dispositivos criptográficos devem ser protegidos com uma senha PIN (*Personal Identification Number*) de conhecimento exclusivo do colaborador responsável por seu uso.

Art. 25 - A senha administrativa para recuperação ou desbloqueio do PIN (PUC ou PUK – *Personal Unblocking Code* ou *Pin Unlock Key*) deve ser armazenada pela UF gestora de Tecnologia da Informação e não deve ser alterada pelos colaboradores.

Art. 26 - Os colaboradores devem zelar pela proteção dos dispositivos criptográficos e pelo sigilo do PIN.

Art. 27 - Certificados armazenados em dispositivos criptográficos adquiridos pelo BNDES para uso do colaborador devem incluir o endereço de correio eletrônico institucional.

Art. 28 - Os colaboradores devem notificar à UF gestora de Tecnologia da Informação eventos de perda, furto ou roubo de dispositivos criptográficos, bem como devem proceder ao aviso e à revogação do certificado junto à Autoridade Certificadora ou de Registro emitente conforme orientações indicadas no "Termo de Titularidade de Certificado Digital de Pessoa Física".

§ 1º Em caso de furto ou roubo fora do ambiente das Empresas do Sistema BNDES, o colaborador deve apresentar à UF gestora de Tecnologia da Informação cópia do registro de ocorrência expedido pelo órgão competente.

§ 2º Caso o furto ou roubo tenha ocorrido nas dependências das Empresas do Sistema BNDES, o colaborador deve fazer um registro formal do fato à UF responsável pela administração do condomínio.

CAPÍTULO V - AUTORIZAÇÃO DE ACESSO

Art. 29 - A concessão de acesso a ativos de informação deve ser condicionada à autorização prévia devidamente registrada.

§ 1º O Gestor do Recurso Técnico deve avaliar o risco associado ao acesso para definir o fluxo de autorização de acordo com uma das seguintes opções:

I - autorizações do Gestor do Recurso Humano e do Gestor do Recurso Técnico;

II - autorização apenas do Gestor do Recurso Humano;

III - autorização apenas do Gestor do Recurso Técnico; ou

IV - não há necessidade de autorização.

§ 2º O Gestor do Recurso Técnico pode estabelecer regras pré-aprovadas para concessão e revogação automática de acessos, por exemplo, a definição de que determinado privilégio pode ser automaticamente concedido a executivos de certa unidade.

§ 3º As solicitações de acesso tendo como alvo chefes de UAP ou superiores dispensam a aprovação do Gestor do Recurso Humano, salvo quando o Gestor do Recurso Técnico explicitamente exigir alçada de autorização por empregado com função hierarquicamente superior.

§ 4º O Gestor do Recurso Técnico pode, a seu critério, estabelecer a alçada do Gestor do Recurso Humano necessária para autorização do acesso.

§ 5º O Gestor do Recurso Técnico deve considerar as limitações tecnológicas e processuais na definição do fluxo de aprovação.

§ 6º Quando o ativo de informação manipular informações que não estejam exclusivamente sob gestão do Gestor do Recurso Técnico, a sua aprovação deve estar pautada em uma avaliação conjunta com os gestores das informações, nos termos do normativo interno que dispõe sobre a classificação e tratamento de informações.

Art. 30 - A concessão dos privilégios de acesso a ativos de informação deve, sempre que possível, ser realizada mediante a associação do colaborador com os perfis estritamente relacionados a seus papeis desempenhados profissionalmente.

Art. 31 - A concessão e a revogação de privilégios de acesso devem ser realizadas em conformidade com instruções documentadas, que incluam a descrição do fluxo macro dos procedimentos estabelecidos e as responsabilidades pela execução de cada atividade.

CAPÍTULO VI - REVISÃO E REVOGAÇÃO DE ACESSOS

Art. 32 - O afastamento ou desligamento de colaboradores deve resultar na revogação dos privilégios de acesso e no bloqueio das suas credenciais de acesso.

§ 1º De acordo com o motivo do afastamento, podem ser mantidos privilégios de acesso básicos definidos pela UF gestora de recursos humanos.

§ 2º A manutenção excepcional de acessos de usuários afastados ou desligados deve ser autorizada pelo Superintendente da Unidade Fundamental de lotação do usuário ou por executivo com função hierarquicamente superior.

Art. 33 - O Gestor do Recurso Humano deve revisar os privilégios de acesso dos colaboradores na unidade sob sua responsabilidade e promover a revogação dos privilégios que não forem mais necessários.

§ 1º A revisão deve ser realizada pelo menos uma vez por ano e sempre que um novo colaborador for lotado na unidade.

§ 2º A revisão dos privilégios de acesso de chefes de UAP e superiores poderá ser realizada pelo próprio colaborador ocupante da função, sendo facultado aos membros da Diretoria Executiva delegar a revisão a um assessor.

Art. 34 - Os sistemas ou aplicações cuja gestão de acesso não esteja integrada à base centralizada de usuários e credenciais de acesso das Empresas do Sistema BNDES devem ter seus acessos revisados pelo Gestor do Recurso Técnico pelo menos uma vez por ano.

Parágrafo Único - Nesses casos fica dispensada a revisão do Gestor do Recurso Humano.

CAPÍTULO VII - AUDITORIA

Art. 35 - A concessão e a revogação de privilégios de acesso devem ser registradas de modo que seja possível determinar a data na qual ocorreram, os colaboradores afetados, bem como os privilégios concedidos e revogados.

Art. 36 - As tentativas de autenticação de colaboradores devem ser registradas, independente de resultarem em sucesso ou fracasso, de modo que seja possível determinar a data e a hora na qual ocorreram, os identificadores de acesso utilizados e o ativo de informação associado.

Art. 37 - Devem ser mantidos registros que permitam identificar os colaboradores responsáveis pelas ações realizadas por meio de credenciais de acesso, mesmo depois de bloqueadas ou revogadas.

Art. 38 - Os registros para auditoria indicados neste Capítulo devem permanecer disponíveis para consulta *online* por, no mínimo, seis meses e mantidos em *backup* por, no mínimo, cinco anos, com vistas ao adequado tratamento de incidentes de segurança.

Art. 39 - Os registros de auditoria relacionados a acessos a sistemas e outros recursos de TI realizados por colaborador utilizando-se da infraestrutura de TI das Empresas do Sistema BNDES podem ser solicitados pelo Diretor ou pelo Superintendente da

Unidade Fundamental de lotação do colaborador, desde que justificadamente e que não implique em violação à privacidade do colaborador.

Parágrafo Único - Cumpridas as disposições do caput a unidade gestora de Segurança da Informação ou a UF gestora de Tecnologia da Informação podem disponibilizar os registros de auditoria ao executivo demandante.

CAPÍTULO VIII - ACESSO A ATIVOS DE TI

Art. 40 - O uso de ativos de TI que viabilizam acesso a informações sigilosas deve ser condicionado à apresentação de credenciais de acesso de uso individual.

§ 1º O acesso a serviços de computação em nuvem contratados pelas Empresas do Sistema BNDES deve, sempre que tecnicamente viável, ser precedido de autenticação por pelo menos dois fatores distintos e de acordo com os demais controles aplicados pela Unidade Gestora de Tecnologia da Informação.

§ 2º Excepcionalmente, é dispensado o segundo fator de autenticação previsto no § 1º quando a credencial de acesso for destinada à execução de programas, rotinas e procedimentos que demandem acesso automatizado, desde que seja possível a aplicação de controles tecnológicos compensatórios, definidos pela unidade gestora de Segurança da Informação, que busquem evitar a ocorrência de acessos não autorizados.

Art. 41 - Os sistemas utilizados nas Empresas do Sistema BNDES devem dispor de ambientes segregados, voltados ao seu desenvolvimento (quando interno), à sua homologação e à sua execução em regime de produção.

Art. 42 - O acesso a ambiente de execução de sistemas em regime de produção por colaboradores que atuam nas atividades de desenvolvimento de sistemas deve ser rigorosamente limitado.

Art. 43 - A intervenção, em ambiente de execução de sistemas em regime de produção, por colaboradores que atuam nas atividades de desenvolvimento de sistemas, somente deve ser permitida em caso de exceção, transitoriamente, com o objetivo de viabilizar operação específica e preferencialmente com o acompanhamento de colaborador responsável pela gestão desse ambiente.

Art. 44 - Os sistemas acessíveis a partir da *Internet* devem, sempre que possível, utilizar mecanismos de proteção contra tentativas automatizadas de acesso indevido.

Política Corporativa de Segurança da Informação

Norma para Gestão dos Serviços de Segurança da Informação

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Art. 1º - Esta norma tem o objetivo de estabelecer as diretrizes que devem ser seguidas para a gestão dos Serviços de Segurança da Informação.

CAPÍTULO II - GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 2º - Os riscos de segurança da informação e cibernéticos, por se tratarem de riscos operacionais, devem compor uma base única de riscos das Empresas do Sistema BNDES e sua gestão deve seguir alinhada ao estabelecido na Política Corporativa de Gestão de Risco Operacional e Controle Interno (PROCI).

Art. 3º - A gestão dos riscos de segurança da informação e cibernéticos, entre outros aspectos, deve observar:

I - os processos internos;

II - os requisitos legais;

III - os objetivos e controles da PCSI;

IV - os objetivos e controles da PROCI;

V - os objetivos e controles da Política Corporativa de Gestão de Continuidade de Negócios (PGCN); e

VI - a Organização Interna Básica do Sistema BNDES.

Art. 4º - A análise de riscos cibernéticos tem como escopo principal os serviços de Tecnologia da Informação classificados como relevantes de acordo com os critérios da PCSI.

Art. 5º - A análise de riscos à segurança da informação e cibernéticos deve ser realizada, preferencialmente, no âmbito da análise de riscos operacionais, de acordo com uma metodologia definida pela UAP gestora da Segurança da Informação e dos riscos operacionais.

Parágrafo Único - A metodologia deve prever, entre outros requisitos estabelecidos à luz dos melhores guias de práticas para gestão de riscos de segurança da informação e da regulamentação em vigor, a elaboração do plano para gestão de riscos de segurança da informação e cibernéticos e dos relatórios para identificação, análise, avaliação e tratamento de riscos de segurança da informação e cibernéticos, bem como sua revisão periódica.

Art. 6º - Os gestores de sistemas e de processos cujos riscos foram avaliados devem deliberar sobre o tratamento dos riscos identificados e sobre a aplicabilidade dos controles sugeridos no mapeamento.

§ 1º - O tratamento dos riscos e a aplicabilidade dos controles sugeridos devem, no que couber, observar:

I - a eficácia das ações de segurança da informação;

II - as restrições técnicas;

III - as restrições físicas estruturais;

IV - as restrições operacionais;

V - as restrições organizacionais;

VI - os requisitos legais; e

VII - a relação custo-benefício dos controles.

§ 2º - Os planos de ação definidos para tratamento de riscos identificados devem ser acompanhados pela unidade gestora dos riscos operacionais e pelos gestores de processos e de sistemas envolvidos, observado que esses gestores devem estabelecer os prazos e recursos necessários para a implementação dos controles propostos.

CAPÍTULO III - MAPEAMENTO DE INFORMAÇÕES SENSÍVEIS

Art. 7º - Periodicamente, no máximo em ciclos bienais, deve ser realizado o mapeamento de ativos de informações sensíveis, com vistas a subsidiar, de forma complementar, os processos de gestão de riscos operacionais (em especial os riscos de segurança da informação), de gestão de continuidade de negócios e de gestão de mudanças.

§ 1º - O processo para o mapeamento de ativos de informação sensíveis deve ser formalmente documentado e, para definição do escopo, no mínimo, considerar:

I - os objetivos estratégicos das Empresas do Sistema BNDES;

II - os processos internos;

III - os requisitos legais; e

IV - a estrutura organizacional.

§ 2º - O registro resultante do mapeamento de ativos de informação sensíveis deve permitir identificar:

I - a referência aos processos envolvidos com o tratamento do ativo de informação sensível mapeado;

II - informações básicas sobre os requisitos de segurança de cada ativo; e

III - os principais contêineres de cada ativo de informação sensível, em especial os ativos de tecnologia da informação envolvidos;

CAPÍTULO IV - GESTÃO DE VULNERABILIDADES

Art. 8º - O levantamento de vulnerabilidades em ativos de TI deve ser atividade realizada, no mínimo, trimestralmente pela unidade gestora de Segurança da Informação.

Art. 9º - O teste de invasão em ativos ou serviços de TI expostos por meio da Internet deve ser realizado, no mínimo, anualmente.

Art. 10 - A execução de levantamentos de vulnerabilidades e testes de invasão deve ser comunicada à UF gestora de TI, por conta do risco decorrente da execução dos procedimentos inerentes a ambas as atividades.

Art. 11 - Cada vulnerabilidade encontrada deve receber uma pontuação que indique sua gravidade de acordo com critérios definidos no sistema CVSS (*Common Vulnerabilities Score System*).

Art. 12 - As vulnerabilidades com pontuação superior a 7 (sete) na escala do sistema CVSS, nos termos do Art. 11 -, e não corrigidas tempestivamente, devem ser notificadas pela unidade gestora de Segurança da Informação para posterior correção pela UF gestora de TI.

§ 1º - A critério técnico da unidade gestora de Segurança da Informação, podem ser notificadas vulnerabilidades com pontuação inferior à definida no *caput*.

§ 2º - A UF gestora de Tecnologia da Informação deve notificar vulnerabilidades identificadas em sistemas cujos gestores são externos à UF gestora de Tecnologia da Informação aos respectivos gestores, com vistas a promover a sua correção.

Art. 13 - Sempre que possível, a UF gestora de TI deve indicar uma estimativa de esforço para a correção e o prazo para resolução da vulnerabilidade.

Art. 14 - A unidade gestora de Segurança da Informação deve acompanhar a correção de vulnerabilidades cadastradas.

CAPÍTULO V - GESTÃO DE INCIDENTES

Art. 15 - A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação em Redes das Empresas do Sistema BNDES – ETIR BNDES deve ter sua composição, atribuições e serviços definidos no Plano de Resposta a Incidentes de Segurança da Informação das Empresas do Sistema BNDES (PRISI).

Art. 16 - O Plano de Resposta a Incidentes de Segurança da Informação das Empresas do Sistema BNDES deve definir a metodologia que será utilizada para o tratamento de incidentes de Segurança da Informação e deve contemplar, no mínimo, as etapas de preparação, identificação, resposta e lições aprendidas.

Art. 17 - A ETIR-BNDES deve disponibilizar canais oficiais para envio e recebimento de notificações referentes a incidentes de Segurança da Informação.

Art. 18 - Os incidentes de Segurança da Informação devem ser registrados, classificados de acordo com a sua relevância e priorizados pela equipe responsável por seu tratamento (ETIR-BNDES).

Art. 19 - Os resultados do tratamento de incidentes relevantes de Segurança da Informação, bem como todas as evidências e artefatos associados, devem ser armazenados com vistas a permitir quantificação e tipificação desses incidentes.

Art. 20 - A ETIR-BNDES deve comunicar a ocorrência de incidentes relevantes de Segurança da Informação no âmbito das Empresas do Sistema BNDES aos órgãos competentes, de acordo com os requisitos e prazos legais aplicáveis.

Art. 21 - A ETIR-BNDES pode compartilhar com outros órgãos da APF e com outras instituições financeiras informações ostensivas envolvidas em incidentes de segurança relevantes que possam contribuir para preservação da segurança da sociedade.

Art. 22 - Para fins de tratamento de incidentes de Segurança da Informação, a ETIR-BNDES deve buscar a confirmação da autenticidade das partes, bem como zelar pela preservação da integridade e da confidencialidade das informações enviadas e recebidas.

Parágrafo Único - A ETIR-BNDES é responsável por promover a divulgação para entidades externas das chaves criptográficas e certificados digitais que tenham sido

revogados ou que não sejam mais confiáveis e que tenham sido criados para proteger a comunicação com entidades externas ou permitir a verificação da autenticidade das partes.

CAPÍTULO VI - COLETA DE EVIDÊNCIAS E ARTEFATOS

Art. 23 - A coleta de evidências e artefatos associados a incidentes de Segurança da Informação deve ser realizada exclusivamente pela ETIR BNDES ou por profissionais da UF gestora de Tecnologia da Informação devidamente orientados pela referida equipe.

Art. 24 - Evidências e artefatos coletados durante o tratamento de incidentes relevantes de Segurança da Informação devem ser devidamente identificados e armazenados de forma a preservar sua integridade e prevenir acessos não autorizados.

Parágrafo Único - Devem ser observados os procedimentos previstos em normas do Gabinete de Segurança Institucional da Presidência da República (GSIPR) para coleta e preservação das evidências.

Art. 25 - A análise de evidências e artefatos deve ser realizada em ambiente isolado daquele onde tenha ocorrido o incidente de Segurança da Informação.

CAPÍTULO VII - INTERVENÇÕES EM ATIVOS DE TI

Art. 26 - A execução de procedimentos para conter imediatamente ataques em andamento, evitar sua extensão ou coletar evidências deve ser priorizada pela UF gestora de Tecnologia da Informação.

Art. 27 - Nenhuma ação corretiva no sentido de sanar vulnerabilidades que potencialmente tenham sido exploradas ou de restabelecer ativos de TI comprometidos deve ser empreendida sem o conhecimento da ETIR-BNDES.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Uso da *Internet*

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem o objetivo de estabelecer a conduta adequada para uso da *Internet* nas Empresas do Sistema BNDES.

Art. 2º - A presente norma se aplica a todos os colaboradores que utilizam a *Internet* por meio da infraestrutura fornecida pelas Empresas do Sistema BNDES.

CAPÍTULO II - USO ACEITÁVEL DA *INTERNET*

Art. 3º - A *Internet* deve ser utilizada para exercício de atividades profissionais voltadas aos interesses corporativos das Empresas do Sistema BNDES e em consonância com as atribuições de cada colaborador.

Art. 4º - A utilização da *Internet* deve ser realizada exclusivamente através da infraestrutura disponibilizada e autorizada pela UF gestora de Tecnologia da Informação.

Art. 5º - Durante a utilização da *Internet*, em particular em redes sociais e fóruns, os colaboradores devem adotar linguagem e postura em consonância com o Código de Ética do Sistema BNDES e do Guia de Comportamento On-line.

Art. 6º - A utilização de serviços de computação em nuvem disponibilizados através da *Internet* deverá atender aos termos da Norma de Uso de Serviços de Computação em Nuvem.

Art. 7º - Não é permitido o uso de recursos em *softwares* para videoconferência ou apresentações que possibilitem o controle remoto do ativo de TI interno a partir da *Internet* e a transferência de arquivos.

Parágrafo Único - O acesso remoto é permitido nos termos da Norma de Segurança da Informação para Acesso Remoto a Ativos de TI.

CAPÍTULO III - CONTROLE

Art. 8º - A UF gestora de TI deve empregar recursos na sua infraestrutura e adotar as medidas necessárias para controlar o acesso à *Internet* com vistas à proteção dos ativos de informação.

Parágrafo Único - A unidade gestora de Segurança da Informação deve deliberar sobre as diretrizes que determinarão a implementação dos controles de acesso à Internet.

Art. 9º - O acesso dos colaboradores à Internet pode ser suspenso nos casos de ameaça iminente a ativos de informação ou de desrespeito à Política Corporativa de Segurança da Informação.

Art. 10º - O acesso a conteúdo que represente ameaça à segurança de ativos de informação pode ser bloqueado sem aviso prévio.

Art. 11º - A UF gestora de TI pode impor limites à utilização da Internet, com vistas a preservar a disponibilidade do acesso.

Art. 12º - O acesso à Internet por profissionais terceirizados prestadores de serviços nas Empresas do Sistema BNDES somente pode ser concedido mediante avaliação da UF gestora de Tecnologia da Informação, após solicitação formal do gestor do contrato.

CAPÍTULO IV - MONITORAÇÃO

Art. 13º - Todos os acessos à Internet devem ser registrados com vistas à formação de trilhas de auditoria e, a critério das Empresas do Sistema BNDES e observada a legislação vigente, poderá haver a monitoração dos dados transmitidos ou recebidos.

§ 1º Os registros de auditoria devem ser armazenados em conformidade com os termos da Norma para Uso e Administração de Ativos de TI.

§ 2º Os registros devem ser armazenados pelo período mínimo de um ano.

Art. 14º - A UF gestora de TI do BNDES poderá inspecionar o conteúdo trafegado por canais criptografados para aplicação de controles de segurança e monitoração dos usuários.

Parágrafo Único - A unidade gestora de Segurança da Informação deve definir os critérios de monitoração e dar publicidade interna acerca das categorias de *sites* cujos acessos por canais criptografados serão inspecionados.

Art. 15º - Os registros de acesso à Internet devem ser regularmente analisados com o objetivo de identificar ameaças iminentes a ativos de informação e evidências de desrespeito à Política Corporativa de Segurança da Informação.

CAPÍTULO V - CONTEÚDO MALICIOSO

Art. 16º - Os colaboradores devem repassar à unidade gestora de Segurança da Informação qualquer conteúdo na Internet que seja suspeito quanto à possibilidade de representar ameaça a ativos de informação, de acordo com as orientações do Plano de Resposta a Incidentes de Segurança da Informação (PRISI) do BNDES.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Uso de Ativos de Tecnologia da Informação

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem o objetivo de estabelecer as responsabilidades e condições que devem ser observadas para uso de ativos de Tecnologia da Informação das Empresas do Sistema BNDES e aplica-se a todos os colaboradores.

Art. 2º - Todos são responsáveis por zelar pela segurança dos ativos de Tecnologia da Informação e devem utilizá-los para o exercício das atividades profissionais voltadas aos interesses corporativos e em consonância com suas atribuições.

Art. 3º - As Empresas do Sistema BNDES podem, a seu critério e observada a legislação vigente, monitorar os dados transmitidos, recebidos ou armazenados por meio de seus ativos de Tecnologia da Informação.

Art. 4º - A aquisição e o desenvolvimento de ativos de Tecnologia da Informação devem respeitar os padrões definidos pela UF gestora de Tecnologia da Informação.

Art. 5º - Devem ser observadas as orientações da UF gestora de Tecnologia da Informação e as recomendações do fabricante para proteger os ativos de tecnologia da informação de propriedade das Empresas do Sistema BNDES, especialmente os dispositivos móveis corporativos.

CAPÍTULO II - REGRAS GERAIS

Art. 6º - A utilização de dispositivos móveis corporativos das Empresas do Sistema BNDES deve ser precedida de recebimento, ciência e aceite formal dos termos de responsabilidade e uso pertinentes.

Art. 7º - A utilização de ativos de Tecnologia da Informação deve ser realizada através da infraestrutura disponibilizada e autorizada pela UF gestora de Tecnologia da Informação.

§ 1º É permitido o uso de dispositivos móveis corporativos em infraestrutura de TI externa à disponibilizada pelas Empresas do Sistema BNDES, desde que mantidos os mecanismos de proteção contra ameaças digitais existentes no equipamento.

§ 2º É permitido o uso de dispositivos pessoais em infraestrutura de TI externa à disponibilizada pelas Empresas do Sistema BNDES para acesso, com restrições, a serviços de computação em nuvem contratados pelas Empresas do Sistema BNDES que sejam autorizados pela UF gestora de Tecnologia da Informação, de acordo com as diretrizes da Norma de Segurança da Informação Para Uso de Dispositivos Pessoais.

Art. 8º - Não é permitido adicionar, remover ou manipular os componentes físicos internos (*hardware*) de ativos de Tecnologia da Informação sem o consentimento da UAP gestora de Infraestrutura de Tecnologia da Informação.

Art. 9º - É proibido desenvolver, manter, utilizar ou distribuir sistemas ou dispositivos não autorizados pela UF gestora de Tecnologia da Informação ou que possam capturar ou corromper informações armazenadas ou em trânsito, bem como danificar ativos de Tecnologia da Informação.

Art. 10 - Não é permitida a instalação de programas (*software*), independente do regime de licenciamento, sem o consentimento da UF gestora de Tecnologia da Informação.

§ 1º A instalação de programas nas estações de trabalho é condicionada à anuência do gestor da unidade do colaborador demandante.

§ 2º É dispensada a aprovação do gestor indicado no parágrafo anterior para instalação de *softwares* que componham um catálogo específico mantido pela UF gestora de Tecnologia da Informação.

§ 3º A inclusão de *softwares* no catálogo deve ser precedida da validação da sua segurança pela UF gestora de tecnologia da informação.

Art. 11 - A execução de *software* deve ser condicionada à validação da sua segurança, o que pode ser feito de forma automatizada e com base em critérios definidos pela UF gestora de tecnologia da informação e pela unidade gestora de Segurança da Informação.

Art. 12 - A utilização de repositórios de armazenamento de dados disponibilizados para colaboradores e unidades organizacionais das Empresas do Sistema BNDES deve respeitar os limites determinados pela UF gestora de Tecnologia da Informação com vistas a preservar a disponibilidade desses recursos.

Art. 13 - O uso, por visitantes, dos ativos de TI das Empresas do Sistema BNDES através de serviços de rede, com ou sem fio, somente deve ser permitido a pessoas cujo acesso físico às dependências das Empresas do Sistema BNDES tenha sido autorizado por um empregado das Empresas do Sistema BNDES ou permitido no âmbito de eventos internos organizados pelo Banco.

§ 1º A autenticação do visitante deve ser feita com uso de credenciais:

I - fornecidas por um colaborador autorizado a conceder acessos à rede sem fio para visitantes;

II - automaticamente geradas a partir das informações pessoais fornecidas para acesso físico às dependências das Empresas do Sistema BNDES; ou

III - criadas pelo próprio usuário através de funcionalidades de autosserviço da infraestrutura da rede sem fio, por meio do qual o próprio visitante fornece informações pessoais e de contato validadas por meio de SMS, serviços do governo de identificação e redes sociais.

Art. 14 - O cadastro de credencias para acesso às redes sem fio das Empresas do Sistema BNDES deve ser realizado de tal forma que se permita a identificação da pessoa responsável pelo cadastro e pelo uso das credenciais de acesso.

Art. 15 - A critério das Empresas do Sistema BNDES e em prol da preservação da segurança das informações, o serviço de rede sem fio pode ser interrompido a qualquer tempo.

CAPÍTULO III - TERCEIROS

Art. 16 - O uso da infraestrutura de TI das Empresas do Sistema BNDES a partir de equipamentos de profissionais externos somente pode ser permitido mediante avaliação da UF gestora de Tecnologia da Informação, após solicitação formal do gestor do contrato ou profissional das Empresas do Sistema BNDES responsável por acompanhar o profissional externo.

Parágrafo Único - Os aspectos de segurança da informação associados ao acesso devem ser avaliados pela unidade gestora de Segurança da Informação.

CAPÍTULO IV - DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEIS

Art. 17 - A gravação de informações em dispositivos de armazenamento removíveis a partir da infraestrutura de TI, inclusive de dispositivos móveis corporativos das Empresas do Sistema BNDES, deve ser restrita a colaboradores autorizados.

§ 1º A autorização deve ser feita pelo superintendente da UF de lotação do colaborador, ou por outro colaborador delegado pelo superintendente.

§ 2º A restrição pode ser excetuada pela unidade gestora de segurança da informação mediante a adoção de controles alternativos e eficazes para mitigar suficientemente riscos de vazamento de informações envolvendo a escrita em dispositivos de armazenamento removíveis.

Art. 18 - A unidade gestora de segurança da informação deve estabelecer os critérios e controles técnicos a serem aplicados para utilização de dispositivos de armazenamento removíveis com vistas à proteção dos ativos de TI e das informações corporativas.

Parágrafo Único - Os critérios e controles devem ser estabelecidos considerando o grau de sigilo das informações.

Art. 19 - Sempre que possível, arquivos com informações sigilosas gravados em dispositivos de armazenamento removíeis devem ser protegidos por mecanismo de criptografia.

Art. 20 - O uso de dispositivos de armazenamento removíveis, para leitura ou gravação de informações, deve ser registrado apropriadamente para permitir a formação de trilhas de auditoria, de acordo com a Norma de Segurança da Informação para Administração de Ativos de TI.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Administração de Ativos de Tecnologia da Informação

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem o objetivo de estabelecer as responsabilidades e condições que devem ser observadas para administração de ativos de Tecnologia da Informação das Empresas do Sistema BNDES e aplica-se a todos os colaboradores.

CAPÍTULO II - REGRAS GERAIS

Art. 2º - Devem ser configurados protetores de tela que resultem no bloqueio de ativos de TI após período pré-definido de inatividade e que só permitam o desbloqueio mediante nova autenticação do usuário.

§ 1º A configuração de bloqueios em estações utilizadas para monitoramento pode ser dispensada, mediante justificativa da unidade interessada no monitoramento.

§ 2º No caso previsto no parágrafo anterior, outros mecanismos de controle devem ser aplicados à estação de monitoramento ou à credencial de acesso utilizada, especialmente para restringir o *login* da credencial na estação de monitoração, para restringir o acesso à *Internet* e a compartilhamentos de rede, de acordo com o princípio do privilégio mínimo.

Art. 3º - O acesso com privilégio administrativo às estações de trabalho deve ser restrito a profissionais designados pela UF gestora de Tecnologia da Informação e deverá ocorrer utilizando-se preferencialmente credenciais de acessos pessoais. Caso seja necessária a utilização de credenciais administrativas locais, deverão ser utilizadas senhas temporárias.

CAPÍTULO III - ADMINISTRAÇÃO DE ATIVOS DE TECNOLOGIA DE INFORMAÇÃO

Art. 4º - A administração de ativos de Tecnologia da Informação deve ser realizada por meio de credenciais de acesso pessoais utilizadas exclusivamente para esse fim ou de mecanismos que exijam autenticação para uso temporário dos privilégios estritamente necessários.

Parágrafo Único - A utilização de privilégios administrativos deve ser realizada somente quando indispensável para a execução de atividade necessária à sustentação de ativos de Tecnologia da Informação ou para o cumprimento de tarefa específica formalmente atribuída.

Art. 5º - Toda informação sigilosa obtida durante a utilização de privilégios administrativos, seja pessoal ou corporativa, deve ser devidamente tratada de acordo com o seu grau de sigilo.

Art. 6º - Toda implantação ou mudança não emergencial que envolva ativos de Tecnologia da Informação em regime de produção deve ser precedida de homologação, sempre que existir ambiente de TI disponível para esse fim.

Art. 7º - Os sistemas desenvolvidos no BNDES para operação em regime de produção no seu ambiente de TI devem utilizar bibliotecas e pacotes de softwares desenvolvidos ou homologados pela UF gestora de Tecnologia da Informação e disponibilizados nos seus repositórios institucionais ou em repositórios oficiais de fornecedores homologados.

Art. 8º - A implantação de pacotes de *software* de mercado ou *open source*, para operação no ambiente de TI do BNDES, deve ser precedida de avaliação da sua segurança pela unidade gestora de Tecnologia da Informação que contemple, ao menos, os seguintes aspectos:

I - a adoção da versão estável mais atual do *software*;

II - a disponibilidade e periodicidade da publicação de atualizações;

III - existência de alerta emitido pelo fabricante do software ou publicado em fóruns e grupos dedicados à sua manutenção, que indique a existência, na versão do software a ser utilizada, de vulnerabilidade que possa representar risco de segurança da informação;

Art. 9º - Os sistemas operacionais de ativos de Tecnologia da Informação que suportem serviços de TI relevantes devem seguir uma *baseline* de segurança definida pela unidade gestora de Segurança da Informação.

Art. 10 - Deve ser priorizada a homologação e a subsequente aplicação de atualizações necessárias para corrigir vulnerabilidades em ativos de Tecnologia da Informação que suportem serviços de TI relevantes.

Art. 11 - Deve haver um programa de manutenção para assegurar a disponibilidade e a integridade dos ativos de Tecnologia da Informação.

Art. 12 - Os ativos de Tecnologia da Informação que possuam requisitos especiais quanto à disponibilidade devem ser protegidos contra falhas no fornecimento de energia elétrica e de quaisquer outros recursos necessários ao seu funcionamento.

Art. 13 - As condições de temperatura e umidade dos ambientes onde há ativos de Tecnologia da Informação que suportem serviços de TI relevantes devem, sempre que possível, ser monitoradas com vistas a detectar situações que possam causar problemas de funcionamento ou redução de sua vida útil.

Art. 14 - As estações de trabalho e *notebooks* corporativos devem possuir mecanismos de proteção, devidamente atualizados, que impeçam a execução de código malicioso.

Art. 15 - Os ativos de Tecnologia da Informação devem manter, sempre que possível, seu relógio interno sincronizado com uma fonte confiável que tenha como referência a "Hora Legal Brasileira (HLB)".

Art. 16 - Os ativos de Tecnologia da Informação devem manter registros para formação de trilhas de auditoria.

§ 1º Sempre que possível, os registros devem ser transmitidos para servidores remotos de propriedade das Empresas do Sistema BNDES e logo após a ocorrência dos eventos, preferencialmente por meio do uso do padrão *syslog*.

§ 2º Os registros de auditoria devem permitir, por meio do exame de uma sequência de eventos, a identificação de circunstâncias, objetos e agentes envolvidos em ocorrências que podem comprometer a segurança das informações, e devem conter minimamente:

I - a data, o horário e o fuso horário ("quando") em que ocorreu o evento associado, observando o previsto no Art. 15 -;

II - informações sobre a natureza do evento associado ("o que"), como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc;

III - identificação inequívoca do usuário ("quem") que realizou o acesso;

IV - informações como a identificação do ativo de informação, o seu endereço IP, sua coordenada geográfica, se disponível, ou outras informações que permitam identificar a origem ("de onde") do acesso.

§ 3º Os ativos de TI utilizados para publicar serviços *Web* na *Internet* devem incluir nos registros de auditoria o número da porta de origem da conexão.

§ 4º A unidade gestora de Tecnologia da Informação deve assegurar que os registros sejam armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos.

Art. 17 - Os registros de auditoria relevantes para segurança da informação devem, desde que não exista impedimento técnico, ser replicados para infraestrutura mantida pela unidade gestora de Segurança da Informação.

§ 1º São considerados relevantes para segurança da informação os registros de auditoria relacionados, ao menos, aos seguintes tipos de eventos:

I - tentativas malsucedidas e bem-sucedidas de autenticação em ativos de TI;

II - uso de credenciais privilegiadas em ativos de TI;

III - concessão e revogação de acessos;

IV - alteração de senha;

V - criação e acesso a arquivos para leitura, modificação ou exclusão;

VI - *restart* de sistemas operacionais;

VII - associados ao uso da *Internet*;

VIII - gerados por elementos de controle da infraestrutura de TI, especialmente os alertas de segurança e de alteração de configurações e de políticas de controle de acesso;

IX - troca de mensagens de correio eletrônico;

X - instalação de *softwares* em estações de trabalho;

XI - execução de *softwares* e processos no sistema operacional das estações de trabalho;

§ 2º A unidade gestora de Tecnologia da Informação deve promover, na concepção e implantação de novos ativos de TI, como sistemas, pacotes de software ou soluções de infraestrutura, a implementação das devidas configurações com vistas a assegurar a replicação dos registros de auditoria prevista no caput.

§ 3º A unidade gestora de segurança da informação é responsável pela gestão das informações associadas aos registros de trilhas de auditoria que recebe e deve assegurar o seu uso adequado e o devido controle de acesso, devendo utilizá-los exclusivamente para execução dos processos de segurança da informação, especialmente para fins de tratamento de incidente e para o monitoramento de eventos de segurança.

Art. 18 - Os ativos de Tecnologia da Informação devem, sempre que viável tecnicamente, realizar de forma periódica cópias de segurança de forma a garantir sua recuperação em caso de incidentes.

§ 1º Os procedimentos para a realização das cópias de segurança devem ser definidos pela UF gestora da Tecnologia da Informação em normativo específico.

§ 2º As cópias devem ser armazenadas criptografadas, salvo quando houver restrição técnica justificada para aplicação desse controle.

Art. 19 - A alienação ou descarte de ativos de Tecnologia da Informação deve contemplar a realização de procedimento que assegure a eliminação prévia e definitiva de todo e qualquer dado porventura armazenado.

CAPÍTULO IV - REDE CORPORATIVA

Art. 20 - A rede corporativa deve ser segregada em sub-redes por meio de dispositivo de filtragem de tráfego de rede.

Art. 21 - A comunicação entre sub-redes contendo ativos de TI em regime de produção deve obedecer ao conceito de privilégio mínimo.

Art. 22 - Os acessos à rede corporativa realizados a partir da *Internet* devem ser inspecionados por meio de dispositivo de prevenção e detecção de intrusão.

Art. 23 - Ativos de TI acessíveis diretamente a partir de redes externas devem ser ligados a sub-redes segregadas da rede interna por intermédio de dispositivos de filtragem de tráfego de rede.

Art. 24 - Os acessos a servidores *Web* realizados a partir da *Internet* devem ser inspecionados por meio de filtros de aplicação *Web*.

Art. 25 - O acesso à rede corporativa deve ser restrito a pessoas autorizadas e precedido, preferencialmente, de autenticação do usuário e do equipamento com base nas credenciais de acesso à rede interna das Empresas do Sistema BNDES.

Parágrafo Único - A conexão à rede corporativa de equipamentos que não disponham de recursos para autenticação, como impressoras etc, deve ser controlada e autorizada pela unidade gestora de tecnologia da informação.

Art. 26 - O acesso a partir de equipamentos não gerenciados pelas Empresas do Sistema BNDES deve ocorrer a partir de sub-rede segregada das demais estações de trabalho por meio de dispositivo de filtragem de tráfego de rede.

Art. 27 - A comunicação dos ativos de TI acessíveis diretamente a partir de redes externas com ativos de TI de uso exclusivamente interno deve, sempre que tecnicamente possível, partir dos ativos de uso exclusivamente interno.

CAPÍTULO V - REDE SEM FIO CORPORATIVA

Art. 28 - O acesso de colaboradores à rede sem fio deve ser precedido da autenticação do usuário com base nas credenciais de acesso à rede interna das Empresas do Sistema BNDES.

Parágrafo Único - Em representações, escritórios ou instalações temporárias cuja infraestrutura de rede sem fio não permita o controle individual de acesso, é permitido o uso de chave de acesso compartilhada para acesso à rede sem fio corporativa, desde que observados os requisitos adicionais enumerados a seguir:

I - o acesso a recursos da rede interna deve ser feito através de conexão VPN ponto a ponto com um concentrador na rede local;

II - o acesso a recursos da rede local dispensa a conexão VPN, mas devem observar os termos da norma para controle de acesso à informação.

Art. 29 - A rede sem fio deve dispor de mecanismos para prover categorias de acessos diferenciadas que considerem o usuário e o dispositivo utilizados para o acesso.

§ 1º As restrições e requisitos de cada categoria de acesso devem estar em consonância com as definições da unidade gestora de Segurança da Informação.

§ 2º Devem ser realizadas validações dos requisitos de acesso, que considerem o usuário e o dispositivo utilizados, para o enquadramento na categoria de acesso adequada.

Art. 30 - O acesso pleno à rede interna através da rede sem fio deve ser restrito aos colaboradores com credenciais de acesso à rede interna das Empresas do Sistema BNDES, a partir de dispositivos administrados pelas Empresas do Sistema BNDES.

§ 1º Os dispositivos que não estiverem em conformidade com os controles de segurança exigidos devem ter o acesso restrito a uma rede de quarentena para adequação aos requisitos de acesso.

§ 2º Os controles de segurança exigidos para este acesso devem ser definidos pela unidade gestora de Segurança da Informação.

Art. 31 - Os acessos à rede interna por meio da rede sem fio realizados a partir de dispositivos não administrados pelas Empresas do Sistema BNDES, devem ser restritos aos serviços definidos pela unidade gestora de Segurança de Informação.

§ 1º O acesso de dispositivos que possuem autorização para conexão em segmentos segregados da rede cabeada, por exemplo, uma rede de terceiros (consultoria), podem ser os mesmos permitidos aos equipamentos conectados naquele segmento de rede.

Art. 32 - A rede sem fio corporativa deve ser segregada das demais redes de acesso sem fio.

Art. 33 - O tráfego de dados na rede sem fio corporativa deve ser protegido contra a sua captura indevida por meio do uso de protocolo de criptografia seguro.

Art. 34 - O serviço de rede sem fio deve dispor de mecanismos que busquem garantir sua disponibilidade.

Art. 35 - Os acessos realizados através das redes sem fio devem ser devidamente registrados e, a critério do BNDES, os dados transmitidos ou recebidos podem ser monitorados.

Art. 36 - Os dispositivos disponibilizados pelas Empresas do Sistema BNDES, quando fazem uso de rede sem fio, devem utilizar exclusivamente a rede sem fio corporativa quando esta estiver disponível, salvo quando houver restrição técnica justificada para aplicação desse controle.

Art. 37 - A rede sem fio deve ter sua cobertura gerenciada de forma a minimizar o vazamento de sinal para áreas externas às dependências do BNDES.

CAPÍTULO VI - INVENTÁRIO DE ATIVOS DE TECNOLOGIA DE INFORMAÇÃO

Art. 38 - Os ativos de TI devem ser inventariados periodicamente e ter seus gestores e custodiantes identificados.

Art. 39 - Os ativos de TI devem ter seu valor, de forma quantitativa ou qualitativa, identificado pelos gestores. O valor dos ativos deve refletir sua importância e criticidade para os objetivos estratégicos do BNDES.

Art. 40 - Os ativos de TI devem ter seus requisitos de segurança da informação classificados pelos gestores por meios de critérios que considerem a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações que contém.

Art. 41 - Os ativos físicos de Tecnologia da Informação devem, sempre que possível, ser etiquetados com identificadores que exibam, no mínimo, alguma identificação das Empresas do Sistema BNDES e um número de patrimônio que referencie o ativo inequivocamente.

CAPÍTULO VII - INVENTÁRIO DE LICENÇAS DE *SOFTWARE*

Art. 42 - A unidade administrativa responsável pela futura gestão das licenças de *software* será definida no instrumento administrativo (ex. Informação Padronizada - IP) que propõe a aquisição das licenças de uso de *software*.

§ 1º Nos casos em que não houver uma unidade definida, a unidade administrativa responsável pelas licenças será a unidade administrativa do respectivo gestor do contrato.

§ 2º Nos casos em que não houver instrumento administrativo ou contrato, a unidade administrativa responsável pelas licenças será aquela que solicitar a implantação do *software* à ATI.

§ 3º Enquanto o *software* continuar em uso no BNDES, mesmo após o término do contrato, a unidade administrativa permanece como responsável pelas licenças de *software* até que o uso do *software* seja descontinuado.

Art. 43 - O executivo principal da unidade administrativa responsável pela licença do *software* é designado Gestor de Licença do *Software*.

Parágrafo Único - O executivo principal pode delegar o papel de Gestor de Licença do *Software* para outro executivo lotado na mesma unidade administrativa.

Art. 44 - Os colaboradores do BNDES devem trabalhar em conformidade com a licença e os direitos de uso do *software*, as regras definidas pelo Gestor da Licença do *Software* e o respectivo contrato de aquisição do *software* quando aplicável.

Art. 45 - Na ausência de dispositivo contratual, prevalecerá a documentação da EULA (*End-user License Agreement*) ou outro modelo de licenciamento definido pelo fabricante na data de solicitação das licenças de *software* pelo BNDES.

Parágrafo Único - Caberá ao Gestor da Licença de *Software* guardar a EULA na data de emissão das licenças.

Art. 46 - Pelo menos uma vez por ano, o Gestor da Licença de *Software* deve inventariar as licenças em uso para verificar se o BNDES dispõe do número suficiente de licenças.

§ 1º Caso necessário, a UF gestora de Tecnologia da Informação apoiará no referido inventário.

§ 2º Em caso de constatação de qualquer inconformidade nas licenças do *software*, o Gestor de Licença do *Software* deve coordenar as ações para regularização.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Uso do Correio Eletrônico

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem o objetivo de estabelecer a conduta adequada dos colaboradores das Empresas do Sistema BNDES na utilização do correio eletrônico corporativo.

Art. 2º - A presente norma se aplica a todos os colaboradores que utilizam o correio eletrônico corporativo das Empresas do Sistema BNDES.

CAPÍTULO II - RESPONSABILIDADES E USO ACEITÁVEL

Art. 3º - O endereço de correio eletrônico corporativo de cada colaborador é para uso individual e de responsabilidade intransferível.

§ 1º. Todo colaborador é integralmente responsável pelo teor das mensagens enviadas a partir da sua caixa postal, ainda que tenha concedido acesso à sua caixa de correio eletrônico individual para terceiros.

§ 2º. O acesso a caixas postais de correio eletrônico individuais pode ser conferido a terceiros pelo colaborador responsável pela caixa mediante a configuração de acesso, mas jamais com o compartilhamento de credenciais.

Art. 4º - Os colaboradores das empresas do Sistema BNDES devem utilizar exclusivamente os endereços de correio eletrônico corporativo do BNDES para envio, recebimento e armazenamento de informações sigilosas.

Parágrafo Único - É vedado o encaminhamento automático de mensagens de correio eletrônico recebidas no e-mail corporativo para endereços de e-mail em domínios externos ao BNDES.

Art. 5º - Os endereços de correio eletrônico institucionais de uso compartilhado (por exemplo, de unidades organizacionais, de grupos de trabalho, etc) devem ser utilizados apenas por colaboradores autorizados pelos gestores destas caixas postais.

Art. 6º - O correio eletrônico corporativo deve ser utilizado para o exercício das atividades de interesse das Empresas do Sistema BNDES e em consonância com as atribuições de cada colaborador.

Art. 7º - Durante a utilização do correio eletrônico corporativo, devem ser adotadas linguagem e postura de acordo com o Código de Ética do Sistema BNDES.

CAPÍTULO III - GESTÃO DE ENDEREÇOS

Art. 8º - A criação de novos endereços de correio eletrônico individuais deve privilegiar composição formada pelo primeiro nome e por um sobrenome do colaborador, separados por um ponto.

Art. 9º - A criação de novos endereços de correio eletrônico concedidos a prestadores de serviços ao BNDES deve privilegiar composição formada pelo primeiro nome seguido por um sobrenome do prestador, separados por um ponto, e acrescidos do sufixo "_prest".

Art. 10 - A divulgação externa de listas ou catálogos de endereços corporativos de correio eletrônico do BNDES não é permitida sem autorização expressa da UF gestora de Recursos Humanos e ciência da unidade gestora de Segurança da Informação.

Art. 11 - Os endereços de correio eletrônico de colaboradores devem ser bloqueados em casos de desligamento ou aposentadoria.

Parágrafo Único - Justificadamente, por prazo definido e mediante autorização de um Superintendente, de um Diretor, ou do Presidente, o bloqueio do endereço eletrônico pode ser adiado.

Art. 12 - Os endereços de correio eletrônico concedidos a prestadores de serviços às Empresas do Sistema BNDES devem ser bloqueados em casos de encerramento, cancelamento ou suspensão da prestação do serviço.

Parágrafo Único - É responsabilidade do gestor do contrato de prestação do serviço solicitar o bloqueio dos endereços de correio eletrônico à UF gestora de Tecnologia da Informação nos casos previstos no *caput*.

CAPÍTULO IV - COMUNICAÇÃO EXTERNA

Art. 13 - Mensagens enviadas para endereços externos devem ser assinadas com certificado digital, de modo a permitir verificação da autenticidade da origem.

Art. 14 - Mensagens enviadas para endereços externos devem incluir, ao final de seu corpo, aviso padrão sobre a sua confidencialidade e sobre a exclusividade de utilização de seu conteúdo pelos destinatários legítimos.

Art. 15 - O privilégio de envio de mensagens para endereços externos pode ser concedido para profissionais externos responsáveis pela prestação de serviços às Empresas do Sistema BNDES somente mediante autorização formal do gestor do contrato.

Art. 16 - A UF gestora de Tecnologia da Informação deve assegurar a existência de controles que busquem registrar e quando possível evitar o envio de informações sigilosas para destinatários externos às Empresas do Sistema BNDES de forma indevida por meio do correio eletrônico corporativo.

CAPÍTULO V - ARQUIVOS ANEXOS

Art. 17 - Arquivos executáveis, mesmo compactados, não devem ser transmitidos em anexos de mensagens de correio eletrônico.

Art. 18 - Apenas imagens e documentos, nos formatos utilizados internamente, mesmo compactados, devem ser anexados a mensagens de correio eletrônico.

Art. 19 - Arquivos anexados em mensagens recebidas somente devem ser abertos se forem imagens ou documentos, nos formatos utilizados internamente, compactados ou não.

Art. 20 - A UF gestora de Tecnologia da Informação deve assegurar a existência de controles que busquem evitar a disseminação de arquivos de conteúdo malicioso na infraestrutura de TI do BNDES por meio do correio eletrônico corporativo.

CAPÍTULO VI - CONTROLE

Art. 21 - O acesso dos colaboradores ao correio eletrônico pode ser revogado temporária ou permanentemente nos casos de desrespeito recorrente à Política Corporativa de Segurança da Informação ou ameaça a ativos de informação.

Art. 22 - A transmissão ou a recepção, no correio eletrônico, de conteúdo dissonante dos interesses corporativos ou potencialmente danoso à segurança dos ativos de informação podem ser bloqueadas a critério do BNDES.

Art. 23 - Limites à utilização do correio eletrônico podem ser impostos, a critério do BNDES, com vistas a preservar a disponibilidade do ambiente de Tecnologia da Informação.

Art. 24 - O envio de mensagens para endereços específicos e o recebimento de mensagens oriundas de endereços específicos podem ser bloqueados, a critério do BNDES.

Art. 25 - A UF gestora de Tecnologia da Informação deve oferecer os meios e as orientações suficientes para garantir, dentro de limites previamente estabelecidos em normativo que discipline a execução de cópias de segurança (*backup*), o adequado armazenamento e arquivamento permanente das informações corporativas mantidas no correio eletrônico, bem como sua recuperação.

CAPÍTULO VII - MONITORAÇÃO

Art. 26 - Todas as transmissões e recepções de mensagens através do correio eletrônico corporativo devem ser registradas.

Art. 27 - Todo e qualquer dado transmitido ou recebido através do correio eletrônico corporativo pode ser monitorado, a critério do BNDES.

Art. 28 - O acesso ao conteúdo de correio eletrônico corporativo individual, ressalvadas as hipóteses constantes do art. 18 do Anexo Único à Resolução CA nº 10/2020-BNDES, que trata do Regulamento da Auditoria Interna (AT), e na Resolução CA Nº 21/2019-BNDES, que Regulamenta o Sistema de Correição Interna do Sistema BNDES, poderá ser autorizado, conjuntamente, pelo Diretor responsável pela Área de Integridades e Compliance e pelo Diretor responsável pela Área Jurídica do BNDES.

§ 1º. As solicitações para acesso ao conteúdo de correio eletrônico corporativo individual devem ser formalmente realizadas e adequadamente registradas juntamente com as justificativas apresentadas e o registro da autorização.

§ 2º. Caso a solicitação de acesso envolva o correio eletrônico corporativo individual dos Diretores referidos no *caput*, havendo alguma negativa por parte deles, o acesso pode ser autorizado por decisão da Diretoria.

§ 3º. A autorização para acesso ao conteúdo do correio eletrônico corporativo individual ou de uso compartilhado (Assessoria, Gerências, Departamentos, Superintendência, etc) utilizada por empregados lotados na AT, ou por empregados que

nela já atuaram durante algum período, deve ser autorizada também pelo Comitê de Auditoria do BNDES, por conta do sigilo das informações obtidas no exercício das atividades de Auditoria Interna eventualmente armazenadas nessas caixas postais.

§ 4º. O acesso ao conteúdo do correio eletrônico corporativo (individual ou de uso compartilhado) sujeita o solicitante e todos que vierem a ter acesso às informações sigilosas armazenadas nessas caixas postais aos deveres de confidencialidade e guarda, com destaque especial às informações originariamente custodiadas pela AT.

§ 5º. Fica dispensada de qualquer autorização formal a concessão de acesso necessária para o atendimento de ordem judicial devidamente repassadas pelo Presidente, pelo Diretor responsável pela Área de Integridade e *Compliance*, pelo Diretor responsável pelas Áreas Jurídicas das Empresas do Sistema BNDES ou pela Auditoria Interna.

Art. 29 - Colegiados ou grupos de trabalho que atuem no âmbito de uma sindicância podem ter acesso às trilhas de auditoria (registro de *logs*) do sistema de correio eletrônico, que resumidamente permitem identificar a data e hora da troca de mensagens, bem como o remetente, o destinatário, o assunto e o nome de arquivos anexados.

Parágrafo Único - As solicitações para acesso com as justificativas devem ser formalmente realizadas e adequadamente registradas.

CAPÍTULO VIII - CONTEÚDO MALICIOSO

Art. 30 - Os colaboradores devem repassar à unidade gestora de Segurança da Informação as mensagens que possam representar ameaça a ativos de informação.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Uso de Dispositivos Pessoais

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem o objetivo de estabelecer as responsabilidades e condições para uso de dispositivos pessoais, ou seja, de propriedade de colaboradores ou visitantes das Empresas do Sistema BNDES, conectados à infraestrutura de Tecnologia da Informação (TI) do Banco.

Art. 2º - O Manual de Conceitos (Anexo I da Política Corporativa de Segurança da Informação) define os termos apresentados nesta norma.

Art. 3º - A conexão de dispositivos pessoais na infraestrutura de TI das Empresas do Sistema BNDES está condicionada à ciência e aceite dos termos dessa norma.

Parágrafo Único - O aceite dos termos dessa norma implica o reconhecimento e autorização às Empresas do Sistema BNDES pelo usuário e/ou proprietário do dispositivo pessoal para que se possa, eventualmente, proceder quaisquer modificações necessárias neste dispositivo pessoal indicado, quando conectado à infraestrutura de TI das Empresas do Sistema BNDES, de forma a configurar, monitorar, validar e verificar a aderência ao que estiver determinado nessa norma.

CAPÍTULO II - USO DE DISPOSITIVOS PESSOAIS

Art. 4º - Os dispositivos pessoais de colaboradores podem ter acesso, com restrições, à rede interna, e à *Internet* a partir da infraestrutura de TI das Empresas do Sistema BNDES, desde que precedido de autenticação do usuário e que a rede disponha de controle de acesso ao meio.

Parágrafo Único - O acesso referido no caput é vedado a partir da rede com fio (rede cabeada) sem autorização da unidade gestora de infraestrutura de Tecnologia da Informação.

Art. 5º - Os dispositivos pessoais de visitantes podem ter acesso somente à *Internet* e com restrições.

Art. 6º - As restrições de acesso a partir de dispositivos pessoais por meio da infraestrutura de TI das Empresas do Sistema BNDES devem ser definidas pela unidade gestora de Segurança da Informação.

Art. 7º - Enquanto conectado a qualquer rede das Empresas do Sistema BNDES, o dispositivo pessoal não pode ser conectado a nenhuma outra rede de dados externa.

Art. 8º - Os dispositivos pessoais de colaboradores podem ter acesso a serviços de computação em nuvem contratados pelas Empresas do Sistema BNDES desde que precedido de autenticação por pelo menos dois fatores distintos e de acordo com os demais controles aplicados pela Unidade Gestora de Tecnologia da Informação.

CAPÍTULO III - GERENCIAMENTO E CONTROLE

Art. 9º - O acesso por colaborador a recursos da rede interna das Empresas do Sistema BNDES a partir de dispositivos pessoais, desde que de acordo com os demais termos dessa norma, está condicionado à aplicação, no dispositivo, de configurações para proteção de aplicativos corporativos, de forma que seja possível às Empresas do Sistema BNDES:

I - ter controle sobre as informações corporativas acessadas e armazenadas por meio dos aplicativos gerenciados;

II - estabelecer e validar requisitos mínimos de controles de segurança implementados no dispositivo para conexão à sua infraestrutura de TI.

§ 1º Quando não for possível a aplicação de configurações para proteção de aplicativos no dispositivo pessoal do colaborador, o acesso à rede interna deve sofrer restrições adicionais definidas pela unidade gestora de Segurança da Informação.

§ 2º Informações sigilosas de propriedade ou sob custódia das Empresas do Sistema BNDES armazenadas em dispositivos pessoais devem estar protegidas por criptografia.

§ 3º A exclusão de informações sigilosas de propriedade ou sob custódia das Empresas do Sistema BNDES desses dispositivos deve ser feita de forma que não seja possível a sua recuperação.

§ 4º Ao utilizar os recursos disponibilizados pelas Empresas do Sistema BNDES o colaborador consente que, em caso de perda, furto, roubo ou suspeita de comprometimento do

dispositivo, as Empresas do Sistema BNDES podem remover todas as informações corporativas armazenadas no dispositivo.

Parágrafo Único - Caso não seja possível a remoção apenas das informações corporativas armazenadas, mediante o conhecimento do empregado e da viabilidade técnica, a unidade gestora de tecnologia da informação pode remover todo conteúdo e resetar o dispositivo para os padrões de fábrica, com vistas a garantir o sigilo dos dados das Empresas do Sistema BNDES.

CAPÍTULO IV - MONITORAÇÃO

Art. 10º - Os acessos realizados através de dispositivos pessoais por meio da infraestrutura de TI das Empresas do Sistema BNDES devem ser registrados e, a seu critério e observada a legislação vigente, os dados transmitidos e recebidos poderão ser monitorados.

CAPÍTULO V - RESPONSABILIDADES

Art. 10 - As Empresas do Sistema BNDES não se responsabilizam por problemas ou por mau funcionamento de dispositivos pessoais utilizados no seu ambiente de TI, tampouco arcará com qualquer despesa decorrente de qualquer dano a estes dispositivos.

Art. 11 - Os controles implantados para proteger a infraestrutura de TI das Empresas do Sistema BNDES e os dispositivos pessoais não devem ser burlados e qualquer falha de segurança eventualmente descoberta deve ser imediatamente notificada para a unidade gestora da Segurança da Informação através do e-mail *csirt@bndes.gov.br*.

Art. 12 - É responsabilidade do usuário e/ou proprietário do dispositivo pessoal efetuar cópia de segurança dos seus dados e informações particulares, armazenados no dispositivo.

CAPÍTULO VI - SUPORTE

Art. 13 - As Empresas do Sistema BNDES não oferecerão suporte técnico para dispositivos pessoais.

Parágrafo Único - A instalação de *softwares* necessários para acesso à infraestrutura das Empresas do Sistema BNDES a partir de dispositivos pessoais, bem como a sua configuração, são de responsabilidade do seu proprietário.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para Uso de Serviços de Processamento, Armazenamento e Transmissão de Dados e de Computação em Nuvem

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Art. 1º - Esta norma de segurança tem por objetivo disciplinar os procedimentos e requisitos para o uso de serviços prestados por terceiros que contemplem o tratamento de informações corporativas fora do ambiente de Tecnologia da Informação (TI) do BNDES.

Art. 2º - No âmbito dessa norma, o termo "computação em nuvem" define os serviços de TI hospedados em infraestrutura de terceiros baseados em um modelo computacional que permite acesso por demanda e independentemente da localização do provedor, a um conjunto compartilhado de recursos configuráveis de computação e comunicação, tais como: rede de computadores, servidores, armazenamento, aplicativos e serviços; provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.

§ 1º. A presente norma não tem por objetivo disciplinar o uso de serviços de computação em nuvem própria do BNDES e de serviços geridos pela UF gestora de Tecnologia da Informação em Centro de Processamento de Dados próprio ou de contingência.

§ 2º. Também não se inclui no contexto dessa norma a utilização de serviços publicados por meio da Internet ordinariamente utilizados em integrações a partir de sistemas corporativos desenvolvidos, serviços publicados via Internet para consulta a informações (bases de dados de informação, site de jornais, blogs etc), sistemas de Internet banking, serviços do governo publicados via Internet e serviços cujo objeto envolva apenas a troca esporádica e não sistematizada de informações corporativas.

Art. 3º - A presente norma disciplina o uso de computação em nuvem das seguintes categorias de serviços:

I - *SaaS – Software as a Service* (*Software* como Serviço) – modelo no qual o provedor de serviços disponibiliza sua solução de *software* para uso normalmente através da *Internet*. Nesse modelo, o usuário possui acesso exclusivamente ao *software* contratado, pois a responsabilidade pela administração e manutenção de toda infraestrutura de TI é do provedor. Normalmente, utilizam essa modalidade de serviço os usuários finais.

II - *IaaS – Infrastructure as a Service* (Infraestrutura como Serviço) – modelo no qual o provedor de serviços disponibiliza, normalmente por meio da *Internet*, uma infraestrutura básica de tecnologia da informação que permite ao usuário do serviço a instanciação de servidores,

computadores, elementos para configuração e controle de redes remotas privadas etc. Os usuários dessa modalidade são tipicamente analistas de infraestrutura de TI.

III - *PaaS – Plataform as a Service* (Plataforma como Serviço) – nesta modalidade, o cliente tem a possibilidade de ter sua capacidade computacional atendida por uma infraestrutura customizada na nuvem, possibilitando o uso de aplicações adquiridas ou desenvolvidas utilizando-se de ferramentas, bibliotecas, serviços ou linguagens de programação suportadas pelo provedor de serviço. O cliente tem ingerência sobre os aplicativos implementados e hospedados na nuvem, e sobre as configurações do ambiente. Trata-se de uma modalidade intermediária entre a modalidade *SaaS* e a modalidade *IaaS* na qual o provedor de serviço é responsável por garantir a infraestrutura para execução dos serviços, mas que permite ao usuário, normalmente equipes de TI que dão suporte a aplicações desenvolvidas, a administração de serviços oferecidos pela plataforma.

Art. 4º - Quanto à arquitetura, os serviços de computação em nuvem podem ser classificados da seguinte forma:

I - Nuvem própria: a infraestrutura da nuvem pertence apenas à própria organização que a utiliza;

II - Nuvem pública: a infraestrutura da nuvem está disponível para a sociedade ou para um grupo de organizações e é administrada por um provedor os serviços;

III - Nuvem comunitária: a infraestrutura da nuvem é compartilhada entre a própria organização e outras que possuem necessidades comuns;

IV - Nuvem híbrida: é a composição de dois ou mais modelos de nuvem interligados por padrões ou tecnologias proprietárias que proporcionam a interoperabilidade entre elas, possibilitando a portabilidade de aplicações e dados;

V - Nuvem privada virtual: quando um provedor de serviços utiliza recursos de nuvem pública para criar e fornecer nuvens privadas, o resultado é uma nuvem privada virtual, ou seja, uma nuvem pública sem compartilhamento de recursos, onde os recursos são acessados por uma conexão de rede privativa virtual.

Art. 5º - Para os efeitos da presente norma, considera-se:

I - Tratamento da informação: o conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

II - Informação sigilosa: aquela submetida à restrição de acesso segundo critérios e procedimentos estabelecidos em normativo interno que disponha sobre o assunto.

CAPÍTULO II - RESTRIÇÕES PARA O USO E ANÁLISE PRELIMINAR DE RISCOS

Art. 6º - Não é permitido o uso de serviços de computação em nuvem:

I - para tratamento de informações sigilosas classificadas como reservada ou secreta; e

II - para o tratamento de documento preparatório que possa originar informação classificada como reservada ou secreta.

Art. 7º - É permitido o uso de serviços prestados por terceiros, desde que os dados, metadados, informações e conhecimento, produzidos ou custodiados pelas empresas do Sistema BNDES sejam mantidos exclusivamente em território nacional, para sistemas que tratem:

I - informações sigilosas classificadas como controlada ou confidencial;

II - informações pessoais relativas à intimidade, vida privada e imagem; e

III - documentos preparatórios das informações a que se referem os incisos I e II deste artigo.

Art. 8º - É permitido o uso de serviços prestados por terceiros no exterior desde que uma cópia dos dados e seus *backups* sejam mantidos em território nacional, para sistemas que tratem informações classificadas como ostensivas.

§ 1º. Caso os serviços sejam prestados no exterior, a prestadora deve informar em quais países e regiões em cada país os serviços podem ser prestados e os dados armazenados, processados e gerenciados.

§ 2º. Caso não exista convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços podem ser prestados, o Banco Central do Brasil deve autorizar a contratação previamente.

Art. 9º - O uso de serviços prestados por terceiros deve ser precedido de uma avaliação que indique sua vantagem comparativamente ao modelo de computação suportado pela UF gestora de Tecnologia da Informação.

§ 1º. A avaliação deve ser realizada pelo executivo da unidade administrativa demandante do serviço, doravante denominado gestor do serviço prestado por terceiros no âmbito dessa norma.

§ 2º. A avaliação de serviços prestados por terceiros deve observar a seguinte ordem de priorização:

I - Serviços oferecidos em arquitetura de nuvem comunitária com outras entidades da Administração Pública Federal;

II - Serviços oferecidos pela Administração Pública Federal;

III - Serviços oferecidos exclusivamente em *datacenter* no Brasil;

IV - Serviços oferecidos em *datacenter* no Brasil;

Art. 10 - Na contratação de serviços prestados por terceiros deve-se garantir que a legislação brasileira prevaleça sobre qualquer outra, de modo a ter todas as garantias legais enquanto tomadora do serviço e proprietária das informações.

Art. 11 - O uso de serviços de computação em nuvem do tipo *SaaS* deve ser comunicado à UF gestora de Tecnologia da Informação.

Parágrafo Único - Quando houver necessidade de integração com sistemas internos, o uso do serviço de computação em nuvem deve ser precedido de autorização da UF gestora de Tecnologia da Informação e da UF/UAP gestora do sistema.

Art. 12 - O uso de serviços de computação em nuvem dos demais tipos definidos nessa norma deve ser precedido da aprovação da UF gestora de Tecnologia da Informação.

Art. 13 - O uso de serviços para tratamento de informações corporativas deve ser precedido de uma análise de riscos preliminar realizada pelo gestor do serviço em conjunto com o gestor da informação que será tratada.

§ 1º. Para serviços do tipo *SaaS* que tratem exclusivamente informações ostensivas cuja disponibilidade não seja relevante para processos do BNDES, a análise de riscos preliminar poderá ser dispensada pela unidade gestora de Segurança da Informação.

§ 2º. A análise de riscos preliminar deve observar as diretrizes da UAP gestora dos Riscos Operacionais e da unidade gestora de Segurança da Informação.

§ 3º. O cenário de uso do serviço e o escopo de informações que serão abarcadas devem estar explícitos em documento que irá compor a análise preliminar de riscos.

§ 4º. A análise de riscos preliminar deve considerar o impacto decorrente de ameaças à confidencialidade, integridade, disponibilidade e autenticidade das informações corporativas da seguinte forma:

I - Durante a análise, o gestor da informação deve considerar a importância, interesse por terceiros, sensibilidade e valor da informação que será tratada no serviço.

II - A seguinte gradação qualitativa deve ser atribuída à medida de tal impacto:

a) Muito Alto;

b) Alto;

c) Moderado;

d) Baixo;

e) Muito Baixo.

III - A análise de risco preliminar deve considerar, no mínimo, os seguintes aspectos para estimativa do impacto:

a) A criticidade dos processos de negócio e as perdas decorrentes de sua interrupção;

b) O tempo de indisponibilidade aceitável;

c) O impacto de eventual degradação ou lentidão no acesso;

d) A classificação quanto à proteção das informações;

e) O impacto financeiro decorrente da exposição das informações a terceiros não autorizados, bem como a amplitude dessa exposição e o risco jurídico associado;

f) O impacto à imagem do Banco ou do Estado;

g) O impacto na execução ou no resultado de planos estratégicos do Banco ou do Estado.

§ 5º. No mínimo, as seguintes ameaças devem ser consideradas na análise de riscos preliminar:

I - Indisponibilidade do serviço ou da infraestrutura de TI necessária para utilizá-lo;

II - Violação do sigilo dos dados, seja por falha no controle de acesso ao serviço, seja por acesso indevido realizado por terceiros inclusive a partir do ambiente do próprio provedor;

III - Alterações não controladas na infraestrutura oferecida pelo provedor de serviços;

IV - Impossibilidade de obter acesso às trilhas de auditoria do serviço ou informações incompletas nessas trilhas;

V - A perpetração de fraudes.

§ 6º. Os eventos de risco operacional acompanhados pela UAP gestora dos Riscos Operacionais e aplicáveis ao cenário de uso do serviço devem ser considerados na análise de riscos preliminar.

§ 7º. A unidade gestora de Segurança da Informação deve publicar orientações e um material de apoio para orientar a execução da análise de riscos preliminar.

§ 8º. O gestor do serviço deve avaliar os termos de uso e a política de privacidade do serviço analisado.

Art. 14 - O uso de serviços prestados por terceiros e a análise de riscos preliminar devem ser aprovados pelos executivos da unidade gestora do serviço e da unidade gestora da informação.

Art. 15 - O resultado da análise preliminar de riscos deve ser informado à unidade gestora de Segurança da Informação.

Parágrafo Único - Caso necessário, as unidades informadas sobre a análise preliminar de riscos podem solicitar a avaliação do impacto decorrente de outras ameaças aplicáveis ao caso específico.

Art. 16 - A maior medida de impacto identificada na análise preliminar de riscos definirá o nível exigido de proteção para o serviço de computação em nuvem de acordo com a seguinte escala:

I - Impacto Muito Alto – o nível 4 de proteção deve ser exigido;

II - Impacto Alto – o nível 3 de proteção deve ser exigido;

III - Impacto Médio – o nível 2 de proteção deve ser exigido;

IV - Impacto Baixo e Muito baixo – o nível 1 de proteção deve ser exigido.

§ 1º. Os controles exigidos para o uso do serviço devem ser definidos com base no nível exigido de proteção.

§ 2º. Os controles exigidos para o serviço de computação em nuvem em função de um determinado nível de proteção devem ser também exigidos para níveis de proteção superiores.

§ 3º. Todos os controles adotados, definidos ou não nesta norma, devem compor o documento da análise preliminar de riscos aprovada.

§ 4º. Os serviços prestados por terceiros que se enquadrem nos critérios de serviço relevante devem ser classificados como tendo impacto muito alto.

§ 5º. A contratação ou alteração contratual de um serviço prestado por terceiros classificado nos critérios de serviço relevante deve ser comunicada ao Banco Central do Brasil em até 10 dias após a contratação ou alteração contratual, nos termos do Art. 15 da Resolução CMN 4.893 publicada pelo Banco Central do Brasil em 26 de fevereiro de 2021.

CAPÍTULO III - AUTENTICAÇÃO, PROVISIONAMENTO E AUTORIZAÇÃO

Art. 17 - O acesso para tratamento de informações corporativas em serviços prestados por terceiros deve ser precedido de autenticação.

§ 1º. O serviço contratado deve implementar controles de acesso que permitam a segregação dos dados de propriedade do BNDES daqueles de propriedade de seus demais clientes.

§ 2º. Devem-se priorizar serviços que permitam a integração da autenticação com sistemas do BNDES por meio do uso de protocolos abertos, por exemplo, o protocolo SAML para troca de informações sobre credenciais e privilégios de acesso.

§ 3º. Quando a autenticação não for integrada, o serviço deve dispor de mecanismo para troca e reinício da senha de acesso. A senha deve ser armazenada criptografada e deve obedecer aos critérios de formação definidos na Norma para Controle de Acesso à Informação.

§ 4º. Os colaboradores não devem utilizar as mesmas senhas para acesso a sistemas internos.

§ 5º. Para serviços com nível 2 de proteção exigido, o provedor de serviço deve implementar mecanismo para mitigar ataques para quebra de senha, por exemplo, por meio do uso de técnicas por força bruta.

§ 6º. Para serviços com nível 3 de proteção exigida, a autenticação deve ser realizada mediante a apresentação de um segundo fator distinto, por exemplo, com a apresentação de um certificado digital ou de um *token* do tipo OTP (*One Time Password*).

Art. 18 - O provedor de serviços deve oferecer mecanismos para revogação de acessos, exclusão de usuários e bloqueio de credenciais.

§ 1º. Para serviços que tratem informações com nível 3 de proteção exigido, deve ser possível extrair de forma estruturada e automatizada a lista de usuários com acesso.

§ 2º. O gestor do serviço deve revisar periodicamente os acessos aos sistemas e promover a revogação de acordo com a Norma de Segurança para Controle de Acesso à Informação.

Art. 19 - Sempre que possível, os privilégios de acesso a recursos do serviço devem ser atribuídos com base em papéis, especialmente para separar os usuários com privilégios administrativos dos demais usuários regulares do serviço.

CAPÍTULO IV - AUDITORIA E TRATAMENTO DE INCIDENTES DE SEGURANÇA

Art. 20 - O provedor do serviço deve prever, em seus procedimentos operacionais internos, os registros dos acessos para auditoria, com vistas ao adequado tratamento de incidentes de segurança.

Art. 21 - Deve-se priorizar a contratação de serviços que permitam acesso tempestivo às trilhas de auditoria do ativo ou serviço disponibilizado para uso do BNDES ou serviços que permitam a exportação dessas trilhas de auditoria geradas a qualquer tempo.

§ 1º. As trilhas de auditoria devem conter minimamente as informações exigidas na Norma para Uso e Administração de Ativos de TI.

§ 2º. Quando exigido nível de proteção 3, além do estabelecido no parágrafo anterior, as trilhas devem permitir a identificação de ações críticas realizadas.

§ 3º. Os ativos de Tecnologia da Informação utilizados pelo provedor de serviço devem manter seu relógio interno sincronizado com uma fonte confiável única de referência.

§ 4º. O gestor da informação deve avaliar se o conteúdo, a disponibilidade e o período de guarda das trilhas de auditoria definido pelo provedor do serviço são suficientes, por exemplo, para o cumprimento de obrigações legais.

§ 5º. Quando exigido nível 3 de proteção, os registros de auditoria devem ser disponibilizados de forma estruturada acessível via internet para o BNDES, se possível por meio de uma API.

Art. 22 - Para *PaaS* e *IaaS*, quando exigido nível 3 de proteção, os registros de auditoria de acessos aos servidores hospedeiros de máquinas virtuais (*hypervisor*) ou aos servidores físicos que suportam o serviço devem ser disponibilizados ao BNDES.

Art. 23 - O provedor de serviço deve realizar a monitoração permanente de sua infraestrutura e do seu sistema, com vistas a garantir a disponibilidade e desempenho esperados bem como a ocorrência de incidentes que possam afetar a confidencialidade, integridade e autenticidade dos dados armazenados.

Parágrafo Único - O gestor do serviço deve estabelecer Níveis Mínimos Aceitáveis para o serviço e acompanhar periodicamente o cumprimento de tal acordo, como ocorre ordinariamente em contratações administrativas de serviços de TI, devendo o prestador de serviço fornecer todas as informações que se façam necessárias para esse acompanhamento.

Art. 24 - O provedor de serviços deve dispor de procedimentos para:

I - Tratamento de incidentes de segurança da informação;

II - *Backup* e recuperação de dados; e

III - Bloqueio de acessos.

§ 1º. Para informações com nível de proteção 3, o provedor deve dispor de procedimentos para:

I - Destruição de informação;

II - Planos de contingência para garantir a continuidade do serviço em caso de incidentes; e

III - Execução de testes de penetração ou levantamento de vulnerabilidades na sua infraestrutura de TI.

§ 2º. Para informações com nível de proteção 4, o provedor deve dispor de procedimentos para a realização de testes de segurança dos *softwares* em seu processo de Gestão de Mudanças, de forma a evitar os efeitos de eventuais vulnerabilidades na liberação de novas versões de *software*.

Art. 25 - Em caso de notificações pelo BNDES acerca de vulnerabilidades críticas de segurança que afetem o serviço, o provedor deve corrigir ou remediar a fragilidade apontada.

Parágrafo Único - Quando exigido o nível 3 de proteção, o gestor do serviço deve estabelecer, na contratação, o prazo máximo para correção ou remediação das vulnerabilidades apontadas.

Art. 26 - O provedor do serviço deve disponibilizar procedimentos e os contatos (telefones e e-mails) para acionamento em caso de incidentes de segurança, bem como de indisponibilidade total ou parcial do serviço por tempo superior ao definido como Nível Mínimo de Serviço.

Parágrafo Único - Tais contatos devem ser informados à unidade gestora de segurança da informação e periodicamente atualizados.

Art. 27 - O provedor de serviços deve observar as boas práticas de segurança, o que poderá ser confirmado com a apresentação de uma política corporativa de segurança aprovada e implantada, com a publicação de seus termos de uso aceitáveis (*Acceptable Use Policy*) ou por meio da certificação por entidades reconhecidas.

§ 1º. Quando exigido nível 4 de proteção a comprovação dos controles de segurança implementados pelo provedor de serviço deve ser evidenciada com a apresentação de relatório elaborado por empresa de auditoria especializada independente.

CAPÍTULO V - CONTINUIDADE DO SERVIÇO

Art. 28 - Devem ser priorizados serviços cuja gestão possa ser realizada de forma institucional, ou seja, o serviço deve oferecer meios para que o BNDES possa realizar a troca da credencial de administração do serviço.

Art. 29 - Devem ser priorizados serviços cuja administração possa ser realizada por mais de um colaborador.

Art. 30 - No cadastro de credenciais de acesso ao serviço devem-se utilizar o *e-mail* e telefones institucionais.

Art. 31 - Os serviços utilizados devem dispor de meios para a exportação dos dados do BNDES, com vistas a promover a continuidade dos processos de negócio do Banco em caso de interrupção do serviço.

§ 1º. Quando exigido nível 2 de proteção, o serviço deve permitir a exportação dos dados em formatos estruturados de padrão aberto, por exemplo, em linguagem XML, JSON ou no formato CSV, com vistas a facilitar a migração das informações para outro provedor de serviços, se necessário.

§ 2º. Não obstante a realização de cópias de segurança (*backup*) pelo provedor, o gestor do serviço deve avaliar a necessidade de realizar a exportação periódica dos dados para guarda no ambiente interno do BNDES, com vistas a permitir a realização de cópias de segurança pela UF gestora de Tecnologia da Informação.

§ 3º. Para serviços do tipo *IaaS*, deve-se utilizar provedores que realizem a exportação da máquina virtual em formato que possa ser utilizado na infraestrutura do BNDES ou no formato OVF, com vistas a promover a recuperação da máquina virtual no ambiente do Banco, se necessário.

Art. 32 - A contratação de serviços prestados por terceiros deve considerar o seu uso a partir do ambiente de contingência do BNDES.

CAPÍTULO VI - PROTEÇÃO DOS DADOS E DA COMUNICAÇÃO

Art. 33 - O acesso ao serviço deve ser realizado por meio de canais de comunicação seguros, protegido por criptografia, preferencialmente por meio do protocolo HTTPS.

Art. 34 - Quando exigido o nível 3 de proteção, todas as informações sigilosas armazenadas devem ser protegidas com uso de algoritmos públicos de criptografia, preferencialmente com a adoção de chaves criptográficas assimétricas.

Parágrafo Único - O gestor do serviço deve zelar pela adequada administração de tais chaves de criptografia.

Art. 35 - Quando exigido o nível 4 de proteção, o serviço deve permitir a exclusão segura das informações sigilosas armazenadas mediante solicitação do BNDES.

CAPÍTULO VII - OBRIGAÇÕES CONTRATUAIS

Art. 36 - Os contratos de prestação de serviços com nível 4 de proteção devem prever, dentre os demais requisitos previstos na legislação:

I- A obrigação de o provedor de serviços notificar a instituição contratante sobre a subcontratação de serviços relevantes durante a prestação do contrato;

II- A permissão de acesso do Banco Central do Brasil e da Comissão de Valores Mobiliários aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

III- A obrigação do provedor de serviços de manter o BNDES permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

IV- A obrigação do provedor de serviços de adotar medidas em decorrência de determinação do Banco Central do Brasil.

Art. 37 - Para o caso da decretação de regime de resolução do BNDES pelo Banco Central do Brasil, os contratos de prestação de serviços com nível 4 de proteção devem prever:

I - A obrigação de o provedor de serviços conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em seu poder; e

II - A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção do provedor de serviços de computação em nuvem interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) O provedor de serviços deve obrigar-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

b) A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência do BNDES.

CAPÍTULO VIII - DISPOSIÇÕES FINAIS

Art. 38 - A exceção de controles previstos nessa norma dependerá de uma avaliação da unidade gestora de Segurança da Informação que poderá detalhar a análise de riscos preliminar com informações técnicas sobre vulnerabilidades existentes no serviço, probabilidades de ocorrência e outros controles possíveis de serem aplicados no caso específico.

Art. 39 - O gestor do serviço é responsável, a luz das indicações da unidade gestora de Segurança da Informação, pelo tratamento dos riscos residuais decorrentes da exceção de controles previstos nessa norma.

Art. 40 - Caso necessária, a análise de riscos detalhada deverá ser apresentada pela unidade gestora de Segurança da Informação ao Comitê de Gestão de Risco Operacional, Controle Interno e Integridade e aprovada pelo executivo da Unidade Administrativa Principal demandante do serviço.

Política Corporativa de Segurança da Informação
Norma de Segurança da Informação para

Uso Institucional de Mídias Sociais

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º - Esta norma tem o objetivo de estabelecer a conduta adequada para uso e gestão de perfis institucionais das Empresas do Sistema BNDES mantidos em mídias sociais.

Art. 2º - A presente norma se aplica a todos os colaboradores das Empresas do Sistema BNDES.

CAPÍTULO II - RESPONSABILIDADES

Art. 3º - A Unidade Fundamental responsável pela comunicação institucional deve definir uma equipe de administração e de gestão de perfis institucionais, bem como estabelecer critérios e procedimentos para:

I - criação e encerramento de contas institucionais em mídias sociais, que considerem aspectos de conveniência, oportunidade e segurança da informação;

II - realização de postagens em mídias sociais em nome das Empresas do Sistema BNDES;

III - gestão de perfis institucionais em mídias sociais;

Art. 4º - Quanto aos aspectos relacionados ao uso institucional seguro de mídias sociais nas atividades de gestão de perfis, de criação e manutenção de contas e de gestão e publicação de conteúdos, os critérios e procedimentos de que trata o Art. 3º devem estar pautados em processos que garantam:

I - a observância dos objetivos de uso da conta;

II - a verificação de conteúdo antes e após a postagem;

III - a adoção de elementos visuais que estejam de acordo com os padrões normatizados;

IV - a adoção, por parte da empresa provedora do serviço ou aplicativo de mídia social, de políticas e procedimentos que busquem preservar a segurança da informação e a privacidade;

V - meios de prevenção e correção de caso de postagem que esteja em desacordo com os normativos internos ou padrões e critérios estabelecidos para a comunicação institucional;

Art. 5º - O colaborador autorizado a gerenciar perfis institucionais ou realizar postagens em mídias sociais em nome das Empresas do Sistema BNDES deve zelar pela preservação da segurança das informações corporativas.

Art. 6º - Os colaboradores devem alertar a equipe de administração e gestão de perfis institucionais no caso de suspeita ou constatação do comprometimento ou uso não autorizado do perfil institucional em mídias sociais.

Parágrafo Único - A equipe de administração e gestão de perfis institucionais do sistema BNDES deve comunicar o fato à unidade Gestora de Segurança da Informação e tomar as medidas necessárias junto ao provedor da mídia social afetada com vistas a cessar o mau uso do perfil, bem como conter e sanar os danos decorrentes.

Art. 7º - Os colaboradores devem comunicar à unidade gestora de segurança da informação caso de suspeita ou constatação de violação da segurança das informações institucionais em conteúdos publicados em mídias sociais.

§ 1º Sendo confirmada a violação, a unidade gestora de segurança da informação deve acionar a equipe de administração e gestão de perfis institucionais.

§ 2º A equipe de administração e gestão de perfis institucionais deve tomar as medidas necessárias para corrigir ou excluir a informação cuja segurança foi violada, bem como conter e sanar os danos decorrentes.

Art. 8º - O uso de perfil institucional em mídia social que implique ameaça à imagem ou à reputação do Sistema BNDES decorrente de evento de comprometimento da segurança das informações deve ser tempestivamente comunicado ao Coordenador do Comitê de Crise de Imagem e Reputação do Sistema BNDES, de acordo com o Plano de Gerenciamento de Crise de Imagem e Reputação do Sistema BNDES – PGCIR, e à unidade gestora de segurança da informação.

CAPÍTULO III - USO INSTITUCIONAL DE MÍDIAS SOCIAIS

Art. 9º - A postagem em mídias sociais em nome das Empresas do Sistema BNDES deve ser realizada exclusivamente pela equipe de administração e gestão de perfis institucionais ou mediante sua aprovação.

Art. 10 - A criação de perfil institucional só poderá ser feita pela equipe de administração e gestão de perfis institucionais do sistema BNDES ou mediante sua aprovação e da Unidade Fundamental responsável pela comunicação institucional.

Art. 11 - A comunicação institucional por meio de mídias sociais deve observar o disposto no Código de Ética do Sistema BNDES e demais políticas e normativos que regulamentam a comunicação institucional.

Parágrafo Único - A observância de conteúdo publicado em perfil institucional das Empresas do Sistema BNDES em mídias sociais que estejam em desacordo com o estabelecido no caput deve ser comunicada à equipe de administração e gestão de perfis institucionais.

Art. 12 - Somente informações classificadas como ostensivas, quanto ao seu grau de sigilo, estão sujeitas à publicação em mídias sociais, observados os demais termos desta norma e do normativo interno que dispõe sobre a classificação e tratamento de informações.

§ 1º A reclassificação de informação já publicada deve ser informada à equipe de administração e gestão de perfis institucionais.

§ 2º A publicação de dados pessoais em mídias sociais deve observar as diretrizes e regras estabelecidas na Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD).

CAPÍTULO IV - CONTROLE

Art. 13 - A publicação de conteúdo e gestão do perfil institucional em mídias sociais devem ser realizadas, sempre que possível tecnicamente, por meio do uso de contas individuais.

Parágrafo Único - A equipe de administração e gestão de perfis institucionais do sistema BNDES é responsável pela gestão das contas autorizadas a publicar, gerenciar o perfil institucional em mídias sociais, ou realizar outras ações de acordo com a política

de permissão das redes, como responder comentários ou gerar relatórios de análise, garantindo a revogação tempestiva das contas não mais autorizadas.

Art. 14 - Deve ser gerado relatório mensal sobre a utilização dos perfis institucionais em mídias sociais, que contenha, no mínimo:

I - o total de contas criadas e excluídas;

II - o total de seguidores registrados; e

III - a quantidade de postagens realizadas e removidas.

Art. 15 - Deve ser gerado relatório que contenha a descrição dos incidentes de segurança ocorridos em perfis institucionais em mídias sociais e as medidas de correção adotadas.

Art. 16 - Esta norma entra em vigor após decorridos 180 dias de sua publicação.