POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

SUMÁRIO

CONTROLE DE VERSÃO

Data da Versão	Autores	Número da Versão	Descrição
07/12/2018	Diretoria Executiva	1.0	Elaboração inicial do documento
17/07/2020	Diretoria Executiva	1.1	Revalidação da Política
30/11/2020	Diretoria Executiva	2.0	Inclusão da execução anual dos testes de intrusão (*pentests*), Inclusão sobre previsão de lei geral de proteção de dados; Revisão geral
30/03/2021	Diretoria Executiva, Departamento de Produção e Segurança da Informação	3.0	Revisão Geral
16/07/2021	Diretoria	4.0	Adequação relativa à alteração da infraestrutura da Plataforma para computação em nuvem (*cloud computing*)
20/12/2021	Diretoria de Governança. Riscos e Controles Internos; Departamento de Produção e Segurança da Informação	5.0	Atualização geral do documento Inclusão de previsões sobre: uso da rede interna, impressão de documentos, ambiente de trabalho – mesa e tela limpa, conscientização, gestão de riscos, segurança cibernética
24/01/2022	Diretoria de Governança. Riscos e Controles Internos; Departamento de Produção e Segurança da Informação	6.0	Possibilidade de hospedar a infraestrutura da Plataforma de seguros para a *cloud computing* fora do território brasileiro
18/07/2023	Diretoria de Governança. Riscos e Controles Internos; Departamento de Produção e Segurança da Informação	7.0	Adequação relativa à RCVM 135; Revisão geral
18/07/2024	Diretoria de Governança. Riscos e Controles Internos; Departamento de Produção e Segurança da Informação	7.1	Revalidação da Política
19/12/2024	Diretoria de Governança. Riscos e Controles Internos; Departamento de Produção e Segurança da Informação	8.0	Atualizações considerando a inclusão das atividades de Depósito Centralizado e de Compensação e Liquidação de Ativos; Padronização e atualização do capítulo com as referências normativas; Revisão geral; Documento aprovado pelo Conselho de Administração em 19/12/2024

Data da Versão	Autores	Número da Versão	Descrição
18/12/2025	Diretoria de Governança. Riscos e Controles Internos; Departamento de Produção e Segurança da Informação	9.0	Atualização para novo *leiaute* de documentos; Inclusão de capítulo de Definições, de Responsabilidades, de Controles de Rastreabilidade da Informação Sensível e de Gestão de Vulnerabilidades; Ajustes textuais para melhor contemplar os processos internos; Documento aprovado pelo Conselho de Administração em 18/12/2025

1. OBJETIVO

Essa Política de Segurança da Informação e Segurança Cibernética ("Política") tem por objetivo estabelecer princípios e diretrizes norteadores da Segurança da Informação e Segurança Cibernética da CSD CENTRAL DE SERVIÇOS DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. ("CSD BR", "CSDBr" ou "Companhia"), visando garantir mecanismos de prevenção, detecção, redução de vulnerabilidades, resposta e recuperação de incidentes cibernéticos para proteger a confidencialidade, integridade e disponibilidade das informações, mitigar riscos e assegurar a continuidade dos serviços essenciais da Companhia.

Por meio de princípios e diretrizes estabelecidos nesta Política, a CSD BR assegura aos Participantes, aos órgãos reguladores e ao mercado de forma geral, o controle, fluxo, guarda, sigilo e a segurança de toda informação de posse da CSD BR.

Os termos e expressões aqui iniciados em maiúsculas, tanto no singular quanto no plural, têm o significado a eles atribuído no Glossário da CSD BR disponível em www.csdbr.com.

2. REFERÊNCIAS REGULATÓRIAS E NORMATIVAS

Este documento utiliza como referências regulatórias e normativas:

- Resolução CMN nº 4.893, de 26 de fevereiro de 2021 ("Resolução CVM 4.893/2021");
- Resolução CVM nº 135, de 10 de junho de 2022 ("RCVM 135/2022");
- Resolução BCB n° 304 de 20 de março de 2023 ("RBCB 304/2023");
- Resolução BCB nº 287, de 24 de janeiro de 2023 ("Resolução BCB 287/2023");
- Circular SUSEP nº 619, de 04 de dezembro de 2020 ("Circular SUSEP 619/2020");
- ABNT NBR ISO 31.000:2009;
- ABNT NBR ISO 31.010:2012;
- ABNT NBR ISO 27.001: 2022;
- *Committee of Sponsoring Organizations of the Tradeway Commission* ("COSO");
- *Control Objectives for Information and Related Technologies* ("COBIT");
- *National Institute of Standards and Technology* ("NIST");
- *Principles for Financial Market Infrastructures*, de 15 de abril de 2012;
- Documento da Companhia de Autoavaliação da Observância aos Princípios para Infraestruturas do Mercado Financeiro ("Autoavaliação PFMI").

Qualquer referência a qualquer lei ou normativo aplicável será considerada também como uma referência a todas as suas atualizações e regulamentações promulgadas ao abrigo dele, salvo disposição em contrário.

3. DEFINIÇÕES

As definições a seguir servem como base para a interpretação deste documento e de todos os documentos da Companhia aqui mencionados, no que couber:

i. Atividade: ações específicas realizadas para a composição de um processo ou conjunto de processos executados pela Companhia (ou em seu nome) que produzam ou suportam um ou mais serviços;

ii. Ativo: qualquer recurso essencial utilizado pela Companhia para a execução de atividades, processos ou serviços;

iii. Autenticação: validação da identidade de usuários, sistemas ou dispositivos, por meio de credenciais, senhas, certificados ou outros mecanismos reconhecidos;

iv. Backup: cópia de segurança dos dados e informações para garantir a recuperação em caso de perda, indisponibilidade ou incidente;

v. Confidencialidade: princípio de segurança da informação que garante que a informação seja acessada apenas por pessoas autorizadas, protegendo contra divulgação não autorizada e uso indevido;

vi. Criptografia: processo de proteção das informações por meio de algoritmos que tornam os dados ilegíveis para pessoas não autorizadas;

vii. Disponibilidade: princípio de segurança da informação que garante que as informações estejam acessíveis sempre que necessário, para pessoas autorizadas;

viii. Integridade: princípio de segurança da informação que assegura que as informações permaneçam corretas, completas e não sejam alteradas de forma não autorizada;

ix. *Malware*: *software* malicioso projetado para causar danos, comprometer ou obter acesso não autorizado a sistemas e informações;

x. Processo: conjunto estruturado de atividades interligadas que, quando executadas em sequência, garantem a entrega de um produto ou serviço;

xi. Rastreabilidade: capacidade de registrar, monitorar e auditar acessos, alterações e movimentações de informações, garantindo transparência e responsabilização.

xii. *Recovery Point Objective* (“RPO”) ou Ponto de Recuperação de Dados: tempo máximo permitido de perda de dados em caso de uma interrupção. Ele define o ponto até o qual as informações devem ser recuperadas, determinando a frequência necessária de backups para minimizar perdas;

xiii. *Recovery Time Objective* (“RTO”) ou Tempo de Recuperação: é o tempo máximo aceitável para que uma atividade, processo ou serviço interrompido seja retomado após um incidente. Ele serve como um parâmetro essencial para planejar os esforços de recuperação;

xiv. Ruptura Operacional: indisponibilidade da Plataforma ocasionada em decorrência da indisponibilidade simultânea de 2 (duas) zonas de disponibilidade da AWS;

xv. Serviço crítico: serviço cuja interrupção ou degradação pode causar impacto significativo na Companhia. Esses serviços são essenciais para o cumprimento da missão institucional e para a entrega de valor aos Participantes;

xvi. Teste de Intrusão (*Pentest*): avaliação técnica realizada para identificar vulnerabilidades exploráveis em sistemas, aplicações ou infraestrutura, por meio de simulação de ataques controlados; e

xvii. Vazamento de Informação: divulgação, acesso ou exposição não autorizada de dados ou informações sensíveis, podendo causar prejuízos à Companhia ou aos titulares das informações.

4. APLICABILIDADE

Esta Política se aplica aos colaboradores, administradores, Participantes, prestadores de serviços e terceiros, que utilizem dispositivos ou sistemas da Companhia, independentemente da forma de acesso (presencial, remota ou teletrabalho), bem como a todos os processos ligados às suas atividades.

Esta Política abrange toda e qualquer informação que estiver em posse, for enviada, gerada e acessada, de forma direta ou indireta, principalmente informações que estejam sob a proteção de dados pessoais e sigilo bancário, conforme regulamentação e Políticas da CSD BR vigentes.

Esta Política estabelece os critérios e fundamentos que orientam o Programa de Segurança Cibernética e o Plano Diretor de Segurança da Informação da Companhia.

5. RESPONSABILIDADES

- Conselho de Administração: responsável pela aprovação desta Política, observados os papéis e responsabilidades nela definidos.
- Diretoria Estatutária: responsável por apoiar e fornecer recursos para o cumprimento e melhoria contínua desta Política e demais processos relacionados à segurança da informação.
- Departamento de Produção e Segurança da Informação (DPSI), responsável por:
    - elaborar, analisar e revisar esta Política, em conjunto com os departamentos competentes, conforme aplicável;
    - implementar e monitorar os controles de segurança da informação e cibernética;
    - Gerenciar os processos que suportam a implementação desta Política.
- Diretoria de Governança, Riscos e Controles Internos (GRC), responsável por:
    - submeter esta Política e demais documentos correlatos aos órgãos de governança aplicáveis;
    - comunicar aos órgãos reguladores alterações relevantes que impactem a segurança da informação;
    - gerenciar os riscos relacionados à segurança da informação e cibernética, promovendo a melhoria contínua dos controles.
- Gestores de departamento, responsáveis por:
    - garantir a participação das equipes sob sua gestão em treinamentos, testes e processos de segurança;
    - assegurar o cumprimento das diretrizes de segurança em seus departamentos.
- Colaboradores, responsáveis por:
    - cumprir as obrigações previstas nesta Política, observando os mais altos padrões de conduta profissional;
    - participar dos treinamentos e ações de conscientização promovidos pela Companhia;
    - zelar pela confidencialidade, integridade e disponibilidade das informações sob sua guarda;
    - reportar inconsistências ou irregularidades relativas aos processos de segurança ao superior imediato ou aos canais indicados pela Companhia.

- Terceiros e prestadores de serviços, responsáveis por:
    - manter padrões mínimos de segurança da informação e cibernética, compatíveis com os requisitos da CSD BR e com a legislação aplicável;
    - cumprir as cláusulas contratuais relacionadas à segurança, incluindo requisitos técnicos, operacionais e regulatórios.
- Participantes: devem observar as disposições dos regulamentos da CSD BR que lhes sejam aplicáveis para o uso seguro dos produtos e serviços da Plataforma. Os regulamentos estabelecem obrigações, responsabilidades e recomendações de segurança visando garantir a disseminação de práticas seguras e a proteção dos dados e operações realizadas na Plataforma.

6. PRINCÍPIOS GERAIS

Esta Política considera os seguintes princípios gerais:

i. **Compromisso institucional:** a segurança da informação é tratada como valor estratégico e essencial para a Companhia;
ii. **Confidencialidade:** as informações são protegidas contra acessos não autorizados, garantindo sigilo e privacidade;
iii. **Integridade:** os ativos de informação são preservados contra alterações indevidas, assegurando exatidão e confiabilidade;
iv. **Disponibilidade:** os sistemas e dados permanecem acessíveis conforme as necessidades do negócio, mesmo diante de incidentes;
v. **Prevenção e resiliência:** são adotadas medidas para evitar incidentes e promover a pronta recuperação das operações;
vi. **Melhoria contínua:** os controles e processos de segurança são revisados e aprimorados regularmente;
vii. **Cultura de segurança:** a Companhia incentiva a conscientização e o engajamento dos colaboradores e terceiros;
viii. **Conformidade e ética:** as ações de segurança observam rigorosamente os requisitos legais, normativos e padrões éticos.
ix. **Responsabilidade compartilhada:** todos os colaboradores da Companhia contribuem para a proteção das informações.

7. DIRETRIZES

7.1. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação da CSD BR considera a relevância e o impacto potencial em caso de divulgação ou perda, garantindo que os controles aplicados sejam proporcionais ao risco.

Para prevenir o vazamento de informações, devem ser adotadas medidas técnicas e administrativas adequadas à categoria de classificação, incluindo ferramentas de prevenção de perda de dados, restrição de acesso, monitoramento, proteção contra ameaças e capacitação dos colaboradores.

A Companhia adota as seguintes categorias para efeitos de classificação da informação:

- **Pública –** Informação que pode ser disponibilizada e acessada por qualquer pessoa, dentro ou fora da Companhia;
- **Uso Interno –** Informações que não podem ser divulgadas para pessoas de fora da Companhia, mas que, caso aconteça, não causarão grandes impactos;
- **Restrita –** Consiste em informações estratégicas, que devem estar disponíveis apenas para um grupo restrito de pessoas, nas interações internas ou externas;
- **Confidencial –** Informações que, se divulgadas interna ou externamente, tem potencial de causar impactos relevantes à Companhia, devendo ser compartilhadas apenas com as pessoas estritamente necessárias e com quem mantenham obrigações apropriadas de confidencialidade, além de órgãos reguladores e autoridades incumbidas de receber tal informação.

Todo colaborador deve zelar pela manutenção dos níveis de confidencialidade das informações, avaliando, classificando e manuseando-as de maneira adequada e de acordo com a sua confidencialidade.

7.2. GESTÃO DE ACESSO FÍSICO

O acesso ao ambiente físico da CSD BR para colaboradores, visitantes e prestadores de serviços é controlado e concedido apenas às pessoas autorizadas e mediante identificação e controles físicos de acesso.

A CSD BR não possui servidores físicos, de modo que sua Plataforma está hospedada em provedor de serviços de computação em nuvem (*cloud computing*). O provedor de serviços contratado é responsável por proteger a infraestrutura que executa todos os

serviços oferecidos em nuvem. Esta infraestrutura é composta por *hardware*, *software*, redes e instalações que executam estes serviços.

7.3. GESTÃO DE ACESSO LÓGICO

Todos os acessos aos ambientes, sistemas e informações da Companhia são realizados conforme diretrizes desta Política e do Processo de Gestão de Acessos. Esses acessos são restritos às pessoas autorizadas para cada atividade específica, por meio da adoção de autenticação, tecnologias com criptografia e segmentação de níveis de segurança.

Para fins de auditoria e rastreabilidade a CSD BR gera logs dos acessos realizados e ações relevantes.

Havendo necessidade de realização de serviço de terceiros, os acessos são liberados somente durante o tempo necessário para a realização da atividade específica, utilizando os princípios de privilégio mínimo, conforme avaliação da Segurança da Informação e Compliance, se necessário.

7.3.1. POLÍTICA DE SENHAS

Para obter acesso a qualquer equipamento ou serviço das instalações da CSD BR é obrigatória a identificação e a autenticação dos usuários.

Para mitigar eventuais problemas de segurança relacionados à definição de senhas, a CSD BR adota uma regra de senhas para os seus ambientes, que deve ser observada por todas as pessoas abrangidas por esta Política.

A senha de acesso aos sistemas e ambientes da CSD BR é estritamente sigilosa, pessoal e intransferível, não podendo ser compartilhada ou divulgada entre os colaboradores e terceiros. Cada usuário é responsável por proteger sua credencial, por não divulgá-la ou emprestá-la, e utilizá-la única e exclusivamente com a finalidade para a qual foi autorizada. O compartilhamento dessas credenciais constitui infração ao Código de Conduta Ética da Companhia, sem prejuízo da aplicação das sanções nele dispostas.

7.4. GESTÃO DOS ATIVOS

Considerando que a informação é o principal ativo da CSD BR, o uso e o controle dos ativos e dos recursos de processamento da informação e dados devem ser realizados com atenção e zelo de forma a garantir a segurança das informações tratadas.

A gestão dos ativos de informação, incluindo identificação, classificação, controle, manutenção e descarte, segue as diretrizes desta Política e é operacionalizada conforme o Processo de Gestão de Ativos.

7.4.1. GERENCIAMENTO DE ATIVOS DE HARDWARE

O Gerenciamento de Ativos de Hardware consiste no controle do ciclo de vida e na centralização das informações relacionadas a esses ativos. Para este processo são considerados os seguintes aspectos: planejamento, aquisição, implantação, gerenciamento, manutenção e descarte.

Todas as modificações e atualizações de hardwares devem ser analisadas de acordo com as necessidades do negócio, controladas e documentadas.

7.4.2. GERENCIAMENTO DE ATIVOS DE SOFTWARES

É permitido apenas o uso ou instalação de softwares adquiridos e homologados pela CSD BR. Havendo a necessidade de aquisição ou desenvolvimento de um software não homologado, o usuário ou departamento solicitante deve encaminhar solicitação ao Departamento de Produção e Segurança da Informação (“DPSI”), que procederá às análises de viabilidade e autorizações necessárias.

Toda instalação de software deve ser disponibilizada pela equipe técnica da CSD BR, que deve considerar os requisitos de segurança e as necessidades do negócio, além de manterem seus sistemas atualizados.

Os equipamentos utilizados devem estar configurados de acordo com as regras de segurança da informação, com softwares homologados, especialmente soluções de *endpoint*, que deverão ser configurados para monitoramento ativo em tempo real, atualização recorrente e periodicidade de execução de *scan* contra vírus.

7.4.3. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS E DE GRAVAÇÃO

Com o objetivo de evitar o compartilhamento e a cópia indevida de informações, nas estações de trabalho de todos os colaboradores o acesso às portas USB e outros tipos de *driver* é proibido e bloqueado para transferência de informações.

Para os colaboradores que tenham permissão de acesso ao Ambiente de Produção, não é permitida a utilização de aparelhos celulares, tablets ou equivalentes, que disponham de mecanismos de comunicação e gravação de dados e imagens para a extração de

informações, dados ou imagens da Companhia, caracterizando infração ao Código de Conduta Ética da Companhia, sem prejuízo da aplicação das penalidades nele previstas.

As exceções devem ser direcionadas e avaliadas pela instância de governança designada pela Companhia.

7.4.4. DESCARTE, REUTILIZAÇÃO OU DOAÇÃO DE EQUIPAMENTOS

Em caso de descarte, reutilização ou doação, todos os equipamentos que contenham mídias de armazenamento de dados devem ser previamente examinados de modo a assegurar que todos os dados, sensíveis ou não, e todos os softwares licenciados tenham sido removidos ou sobrescritos com segurança.

Em caso de descarte de equipamentos e quando necessário, a CSD BR utiliza software específico de deleção segura dos arquivos, como por exemplo, ferramenta de Wipe - Padrão DoD 5220.22-M, que permite a destruição dos dados em discos.

7.5. FERRAMENTAS DE COMUNICAÇÃO CORPORATIVA

7.5.1. USO DA INTERNET, E-MAIL, TELEFONIA E APLICATIVO DE MENSAGENS

As ferramentas de comunicação corporativas disponibilizadas aos colaboradores são de propriedade ou licenciadas pela CSD BR e devem ser utilizadas exclusivamente para atividades relacionadas ao trabalho a ser desempenhado.

A CSD BR efetua o monitoramento e o *backup* das informações e poderá realizar a gravação das comunicações realizadas por meio das ferramentas corporativas.

O acesso a sites de internet é monitorado e pode ser bloqueado conforme política da Companhia.

Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes ter certeza de sua procedência e da existência de prévia expectativa do recebimento da mensagem.

Não devem ser transmitidas mensagens não-solicitadas, conhecidas como *spam* ou *junk mail*, correntes, *chain letters* ou distribuição em massa de mensagens, salvo mensagens de interesse da Companhia.

7.5.2. USO DA REDE INTERNA

O acesso à rede interna é para uso exclusivo das atividades da CSD BR. Todos os arquivos corporativos devem ser armazenados somente nos drives corporativos, em ambiente seguro e salvaguardados por sistema de backup diário e incrementais.

7.5.3. SEGURANÇA NA UTILIZAÇÃO DE VPN E REDE WI-FI

O acesso remoto à rede interna é disponibilizado somente aos colaboradores e prestadores de serviço autorizados da CSD BR, por meio de VPN, controlada e monitorada pela Companhia. Para utilização da rede é necessário que o usuário utilize equipamentos configurados e autorizados pelo Departamento de Produção e Segurança da Informação da CSD BR.

O acesso à rede *Wi-Fi* nos escritórios, quando disponível, deve ser segregado da rede local da Companhia, sendo também controlado e monitorado.

7.5.4. IMPRESSÃO DE DOCUMENTOS

Todos os colaboradores devem recolher o material impresso de imediato, de modo a evitar que informações sensíveis ou confidenciais fiquem expostas a pessoas não autorizadas. Os logs de impressão são monitorados pela CSD BR.

Todo o colaborador que constatar irregularidades na utilização da impressora deve comunicar o fato ao seu gestor, ao Departamento de Produção e Segurança da Informação ou à GRC, que têm autonomia para destruir o que foi encontrado e não retirado da impressora.

7.6. AMBIENTE DE TRABALHO – MESA E TELA LIMPA

A CSD BR possui práticas orientadas aos colaboradores e prestadores de serviço para que não deixem informações à mostra e as descartem sempre que necessário.

O colaborador deverá sempre bloquear seu computador ou suspender a sessão ativa ao deixar a estação de trabalho, ainda que momentaneamente, e não deverá deixar informações sensíveis ou confidenciais disponíveis. Os dispositivos dos usuários também devem possuir medidas de segurança para bloquear a tela automaticamente após determinado período de inatividade; e processo de bloqueio temporário de acesso do colaborador após limite de tentativas incorretas de autenticação.

Informações confidenciais e de uso restrito devem ser impressas ou anotadas em papel apenas em caso de necessidade, devendo ser guardadas em local seguro, como armários e gavetas com chave e nunca deixados sem supervisão sobre a mesa.

7.7. UTILIZAÇÃO DE EQUIPAMENTOS EM REGIME DE TELETRABALHO

Em regime de teletrabalho, o acesso às informações e aos sistemas da CSD BR devem ser realizados mediante a utilização de equipamentos corporativos fornecidos pela Companhia, devidamente configurados e conectados via *Virtual Private Network* ("VPN").

Todos os dispositivos utilizados para essa finalidade devem possuir antivírus atualizado para proteção contra *softwares* maliciosos e demais controles de proteção e detecção de intrusão.

Em caso de incidente de segurança, o usuário deverá acionar imediatamente o Departamento de Produção e Segurança da Informação, conforme os procedimentos de comunicação definidos no Processo de Gestão de Incidentes Cibernéticos.

7.8. CRIPTOGRAFIA

A CSD BR utiliza criptografia por meio de algoritmo seguro para garantir a segurança no acesso aos ambientes disponibilizados pela Companhia.

Para garantir a segurança e a confidencialidade dos dados armazenados em sistemas e dispositivos, são adotadas medidas de criptografia de disco em dispositivos de colaboradores, assegurando que os dados permaneçam ilegíveis para qualquer pessoa não autorizada em caso de perda ou roubo de dispositivos.

A comunicação com a infraestrutura da Plataforma é estruturada para que o tráfego das informações seja realizado de forma segura através de criptografia em trânsito durante sua transmissão, e armazenado de maneira segura com criptografia em repouso.

7.9. COMUNICAÇÃO

A comunicação e o fornecimento de informações aos Participantes, prestadores de serviços, fornecedores, parceiros, colaboradores e quaisquer outros interessados, devem obedecer à classificação de confidencialidade.

O fornecimento de informações da CSD BR a terceiros, quando necessário, deve ser realizado com extremo cuidado, sempre buscando assegurar que a pessoa que está

recebendo a informação seja o destinatário correto e que esta informação não traga prejuízos à Companhia.

No contexto de incidentes relevantes, a Companhia estabelece mecanismos para o compartilhamento de informações com outras instituições do segmento, realizado por canais seguros, respeitando os princípios de confidencialidade, integridade e divulgação responsável. A comunicação aos Participantes, órgãos reguladores e demais partes interessadas é realizada conforme Plano de Comunicação de Crise, assegurando que todos sejam informados de forma tempestiva, precisa e segura.

Havendo dúvidas, a recomendação é que não seja fornecida a informação e que seja realizado o contato com o Departamento de Produção e Segurança da Informação para a devida orientação.

7.10. CONSCIENTIZAÇÃO

A CSD BR mantém um programa de conscientização e treinamento de segurança da informação para integrar a segurança da informação aos valores corporativos, bem como, realizar a capacitação e avaliação dos colaboradores, por meio de treinamentos e ações específicas de conscientização focados em garantir a confidencialidade, integridade e disponibilidade das informações. Como parte dessas ações, também são realizados envios de *newsletters* de segurança e simulações de *phishing* para avaliar a postura de segurança.

A Companhia orienta os Participantes sobre as precauções necessárias para o uso seguro dos produtos e serviços da Plataforma por meio dos seus regulamentos, que estabelecem obrigações, responsabilidades e recomendações de segurança visando garantir a disseminação de práticas seguras e a proteção dos dados e operações realizadas na Plataforma.

7.11. DESENVOLVIMENTO E MANUTENÇÃO SEGURA DO AMBIENTE

7.11.1. SEGREGAÇÃO DE ACESSO AOS AMBIENTES DA PLATAFORMA

A CSD BR possui quatro ambientes segregados para sua Plataforma: Produção (“PRD”), Homologação de Participantes (“HML”), Homologação Interna (“QA”) e Desenvolvimento

("DEV"). Para cada ambiente são aplicados níveis de acesso diferenciados, com permissões específicas:

- **Produção:** contém os dados reais de todos os Participantes.
  - **Externo**: acesso liberado somente aos Participantes homologados.
  - **Interno**: acesso liberado somente aos colaboradores da CSD BR com funções específicas envolvendo o Ambiente de Produção e permissão de visualização de dados reais dos Participantes.
- **Homologação de Participantes:** deve ser utilizado com dados fictícios para testes ou simulações.
  - **Externo**: acesso liberado aos Participantes, às Instituições Elegíveis, Instituições Candidatas e aos *Vendors*, nos termos dos normativos da Companhia.
  - **Interno**: acesso liberado aos colaboradores da CSD BR com funções específicas envolvendo o Ambiente de Homologação.
- **Homologação Interna:** utilizado somente com dados fictícios para homologação de novas versões e pacotes corretivos do sistema.
  - **Externo**: não liberado.
  - **Interno**: acesso liberado aos colaboradores da CSD BR com funções específicas envolvendo os processos internos de testes e homologação do sistema.
- **Desenvolvimento:** utilizado para o desenvolvimento de novas versões e pacotes corretivos do sistema, somente com dados fictícios.
  - **Externo**: não liberado.
  - **Interno**: acesso liberado aos colaboradores da CSD BR com funções específicas envolvendo os processos de desenvolvimento e testes do sistema.

7.11.2. DESENVOLVIMENTO E MUDANÇA DA PLATAFORMA

Os requisitos de segurança da informação devem ser considerados e incluídos na adoção de novas tecnologias e nos processos de Gestão de Desenvolvimento da Plataforma e de Gestão de Mudança na Plataforma.

As versões da Plataforma e suas funcionalidades passam por testes e aprovações nos ambientes de Desenvolvimento e Homologação Interna antes de entrarem em Homologação de Participante e Produção.

O controle de versões da Plataforma deve garantir que todas as mudanças sejam feitas de modo ordenado e que esteja disponível a versão anterior para recuperação em caso de problemas.

7.11.3. ACESSO E UTILIZAÇÃO DO CÓDIGO FONTE

O acesso ao código fonte da Plataforma, quando e se necessário, é concedido pela CSD BR apenas às pessoas autorizadas, sendo o referido acesso pessoal e intransferível, de modo que cada usuário é responsável pelo seu acesso e por todas as ações realizadas por meio dele. Ainda, o usuário deve manter o acesso seguro e protegido, sob pena de responsabilização nos termos do Código de Conduta Ética da Companhia.

7.12. MANUTENÇÃO DOS AMBIENTES OPERACIONAIS

Visando garantir alta disponibilidade de seus serviços, a CSD BR realiza manutenções periódicas, preferencialmente em datas pré-determinadas, de acordo com a avaliação prévia de sua criticidade pela equipe técnica responsável. Além das atualizações periódicas de segurança, quando necessário também são realizadas atualizações de hardware, drivers ou firmwares, visando garantir a integridade do funcionamento de todos os equipamentos. Para isso o Departamento de Produção e Segurança da Informação mantém contato com os fabricantes dos equipamentos a fim de antecipar eventuais pontos de impacto ou melhorias ao ambiente tecnológico da CSD BR.

7.13. MONITORAMENTO DE EVENTOS

O monitoramento do ambiente tecnológico da CSD BR é fundamentado na utilização de sistemas de monitoramento e alertas por meio do envio de notificações para os departamentos responsáveis, com o objetivo de identificar situações que possam indicar anormalidades, riscos ou impactos à operação.

Esse monitoramento engloba indicadores específicos do status de funcionamento e utilização dos equipamentos físicos, da disponibilidade da estrutura de comunicação e do processamento de dados, incluindo os módulos acessórios.

Neste monitoramento são utilizadas ferramentas específicas que realizam a coleta ativa de informações, consolidadas em bancos de dados específicos e acompanhadas

continuamente através de *dashboards*, que disparam alertas quando qualquer indicador ultrapassa os limites previamente definidos.

7.13.1. CONTROLES DE RASTREABILIDADE DA INFORMAÇÃO SENSÍVEL

A Companhia adota controles específicos para garantir a rastreabilidade e a segurança das informações sensíveis, incluindo a implementação de trilhas de auditoria nos ambientes de TI, registros de acessos e alterações. Esses registros são armazenados de maneira segura e imutável, interligados com ferramentas de correlação de eventos e retidos conforme as legislações vigentes.

7.14. GESTÃO DE VULNERABILIDADES

A Companhia mantém um processo estruturado de gestão de vulnerabilidades, com o objetivo de identificar, analisar, priorizar e tratar vulnerabilidades que possam causar riscos à segurança da informação da Companhia. Este processo contempla:

- Monitoramento contínuo dos ambientes tecnológicos, utilizando ferramentas automatizadas, varreduras periódicas, execução de testes de intrusão (“*pentests*“) ou outros métodos de detecção para encontrar vulnerabilidades em sistemas, aplicações e dispositivos;
- Classificação e priorização das vulnerabilidades identificadas, considerando o contexto operacional;
- Tratamento das vulnerabilidades por meio de estratégia específica, conforme metodologia definida no Processo de Gestão de Vulnerabilidades;
- Monitoramento e reporte dos resultados visando a melhoria contínua e a redução da exposição frente a incidentes cibernéticos.

As vulnerabilidades identificadas são documentadas em ferramenta específica, permitindo o acompanhamento e a revisão periódica das vulnerabilidades eventualmente aceitas, assegurando a efetividade do ciclo de gestão de vulnerabilidades.

7.15. GESTÃO DE INCIDENTES DE TI

A Gestão de Incidentes de TI da CSD BR visa promover de forma célere a restauração e a qualidade do serviço prestado, por meio da rápida identificação e eficiência das

tratativas dos incidentes, de forma a garantir a redução do impacto ao negócio e garantir a qualidade dos serviços prestados.

Para este processo, são consideradas as seguintes diretrizes: prevenção, identificação, tratamento, reporte e lições aprendidas, abrangendo tanto as informações da CSD BR quanto aquelas recebidas de Prestadores de Serviços Críticos. A implementação dessas diretrizes é realizada por meio do Processo de Gestão de Incidentes de TI, utilizando ferramentas específicas para garantir o registro, a análise da causa e o impacto do incidente, incluindo o controle dos efeitos para as atividades da Companhia, além de todo o gerenciamento de seu ciclo de vida, possibilitando o rápido atendimento de forma a minimizar o impacto e garantir a normalização da prestação de serviço.

Os incidentes são categorizados e na avaliação de sua relevância devem ser considerados os seguintes critérios: impacto financeiro, criticidade dos sistemas afetados, extensão da interrupção dos serviços e potencial repercussão para a imagem da Companhia, conforme metodologia estabelecida no Processo de Gestão de Incidentes de TI. Caso o incidente seja classificado como “Crítico”, deve-se observar o estabelecido no Plano de Gestão de Crises. Em caso de interrupção da operação, deve-se observar e seguir o Plano de Continuidade de Negócio e Recuperação de Desastres, considerando o *Recovery Time Objective* (“RTO”) definido no *Business Impact Analysis* (“BIA”).

8. GESTÃO DE RISCOS

A Gestão de Riscos da CSD BR visa identificar, avaliar e atuar sobre riscos ao negócio, proativamente com o objetivo de mantê-los dentro de parâmetros adequados à continuidade da operação, as melhores práticas e a regulamentação vigente, conforme Política de Riscos e Controles Internos da Companhia.

A CSD BR está em constante ação, fazendo que seus processos sejam sustentáveis e que estejam de acordo com o estabelecido em suas políticas, manuais e procedimentos, visando: (i) a coleta de informações necessárias para a verificação de possíveis riscos; (ii) a identificação e a quantificação do risco; (iii) o desenvolvimento da estratégia para mitigar o possível risco; (iv) a comunicação e o engajamento dos *stakeholders* na busca da melhor solução em caso de materialização de um risco; (v) envolvimento da alta liderança para a tomada de decisões e construção de planos de ação; e (vi) a garantia de que os prestadores de serviços contratados possuam procedimentos e controles de

segurança para prevenção e tratamento de incidentes equivalentes aos controles da Companhia, de acordo com o serviço a ser prestado.

9. SEGURANÇA CIBERNÉTICA

9.1. PREVENÇÃO E MONITORAMENTO DE INCIDENTES DE SEGURANÇA

Todos os pontos de interface de comunicação com a CSD BR são controlados e monitorados por sistemas específicos, visando a prevenção e detecção de possíveis ataques cibernéticos e acessos indevidos ou não autorizados. Nesse sentido, toda comunicação externa obrigatoriamente passa por uma estrutura de controle de permissões de acesso, detecção de acessos indevidos e monitoramento de atividades suspeitas.

Adicionalmente, para atestar a segurança da infraestrutura da Plataforma, bem como, identificar possíveis vulnerabilidades, e objetivando manter seu ambiente seguro e resiliente, a Companhia executa *pentests* semestrais, por meio da contratação de empresa externa especializada.

9.2. GESTÃO DE INCIDENTES DE SEGURANÇA

Os acessos e comportamentos do ambiente de sistemas da CSD BR são monitorados continuamente para garantir a disponibilidade e segurança dos serviços. A equipe do DPSI é notificada sobre qualquer incidente de segurança através de alarmes para atuar na detecção, resposta, contenção, erradicação e recuperação do ambiente em caso de incidentes de segurança da informação.

10. CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Com o objetivo de obter maior performance, segurança, confiabilidade e escalabilidade, os serviços críticos da Companhia são suportados por ativos hospedados em provedor de serviços de computação em nuvem (“*Cloud Service Provider*”). Esses serviços estão previstos no BIA da Companhia.

A arquitetura dos ativos que suportam esses serviços críticos foi desenhada de forma a garantir a continuidade das operações, com a utilização de mais de uma zona de disponibilidade e com os serviços e o armazenamento dos dados configurados para

redundância ativa em todas as zonas, garantindo a continuidade do funcionamento e integridade dos dados, mesmo em caso de falha em alguma das zonas de disponibilidade.

A estratégia de continuidade de negócios da Companhia contempla a definição e execução de testes periódicos que validem a resiliência dos serviços críticos. Esses testes devem incluir cenários de incidentes abrangendo riscos de indisponibilidade causados por meio de ruptura operacional, definidos conforme metodologia do Plano de Continuidade de Negócios e Recuperação de Desastres (“PCN-RD”).

11. PROTEÇÃO DE DADOS PESSOAIS E SIGILO BANCÁRIO

A CSD BR adota regras e controles para que as informações e os dados pessoais protegidos pela Lei Geral de Proteção de Dados e legislação específica de Sigilo Bancário sejam tratados nos termos dos normativos e legislações em vigor, no que for aplicável.

11.1. MONITORAMENTO

A CSD BR tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos, incluindo rede ou nuvem, como também acesso às ligações telefônicas, e-mails e outros canais de comunicação internos. Dessa forma, a CSD BR se reserva no direito de monitorar e armazenar registros de informações, de ligações e conversas de texto, bem como consultá-las sem prévio aviso ao colaborador, uma vez que devem ser utilizadas para fins profissionais.

A CSD BR zela pelo sigilo de qualquer informação, incluindo as de caráter pessoal, que eventualmente se depare nos processos de monitoramento.

As reuniões virtuais só podem ser gravadas com o consentimento dos integrantes. Ao iniciar a reunião, quando houver a necessidade de gravação, é realizada a solicitação de consentimento de forma verbal. Estando todos os integrantes de acordo, a reunião poderá ser gravada.

11.2. VAZAMENTO DE DADOS SIGILOSOS

Na eventualidade de ocorrer vazamento de dados pessoais e/ou quaisquer outras informações de caráter sigiloso, originado por: (i) ataques cibernéticos externos; (ii) divulgação indevida por colaboradores internos; ou (iii) qualquer outra forma não permitida; o fato deve ser comunicado imediatamente à Diretoria Estatutária que, de

acordo com a análise prévia da criticidade ou gravidade do evento, comunicará à Autoridade Nacional de Proteção de Dados (“ANPD”), ao Banco Central do Brasil (“BCB”), à Comissão de Valores Mobiliários (“CVM”), à Superintendência de Seguros Privados (“SUSEP”) e/ou ao Conselho de Administração da CSD BR.

Além de adotar todas as medidas necessárias para evitar que novas informações sigilosas sejam divulgadas, a Diretoria Estatutária também determinará a instauração imediata de uma sindicância interna e demais medidas necessárias para apuração das causas, responsabilização e adoção de eventuais medidas punitivas.

12. CONTROLE DO DOCUMENTO

12.1. VIGÊNCIA E DIVULGAÇÃO

Este documento deverá ser divulgado no site da Companhia após a sua aprovação pelo Conselho de Administração, entrando em vigor na data mais recente do quadro no item “CONTROLE DE VERSÃO”, acima, cancelando e substituindo o documento vigente desde a data imediatamente anterior.

12.2. REVISÃO

Este documento deverá ser revisado, no mínimo, anualmente, considerando a data de publicação mais recente (quadro no item “CONTROLE DE VERSÃO”, acima), podendo ser atualizado a qualquer tempo para incorporar melhorias, corrigir erros ou atender normativos.

12.3. DIREITOS AUTORAIS E DISTRIBUIÇÃO

A Companhia possui sobre esse documento todos os direitos de elaboração, alteração, reprodução e distribuição. Este documento substitui todas as versões anteriores. A Companhia não se responsabiliza por versões desatualizadas, modificadas, ou por quaisquer versões provenientes de outras fontes que não a fonte oficial designada para fornecer este material.