POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

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*)

1. OBJETIVO

Essa Política de Segurança da Informação ("Política") tem por objetivo estabelecer princípios e diretrizes norteadores da Segurança da Informação da CSD CENTRAL DE SERVIÇOS DE REGISTRO E DEPÓSITO AOS MERCADOS FINANCEIRO E DE CAPITAIS S.A. ("CSD BR" ou "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 e sigilo 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. RESPONSÁVEIS

Todas as ações e diretivas relacionadas neste documento foram definidas pela Diretoria da CSD BR, que é responsável pela manutenção, execução e cumprimento desta Política e o Conselho de Administração é responsável por sua aprovação.

Qualquer situação de violação ou conflito envolvendo essa Política configura um incidente, e deve ser tratado conforme o estabelecido na Política de Gestão de Continuidade de Negócios.

3. APLICABILIDADE

Esta Política se aplica a 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, nos termos estabelecidos em normativos e na legislação específica.

Esta Política se aplica aos colaboradores, administradores, Participantes, prestadores de serviços, e terceiros da CSD BR, bem como a todos os processos ligados às suas atividades.

Os terceiros e os prestadores de serviços contratados, considerando a criticidade dos serviços a serem prestados, devem, a exclusivo critério da CSD BR, aderir formalmente a um termo comprometendo-se a cumprir e agir de acordo com as regras de segurança da informação da CSD BR, assegurando a confidencialidade das informações de acordo

com esta Política.

4. PRINCÍPIOS GERAIS

Esta Política considera os seguintes princípios gerais:

- Possuir dispositivos e práticas para proteção de dados pessoais e sigilo bancário de modo a evitar a divulgação indevida de informações e a perda de dados;
- Assegurar a confidencialidade, integridade e disponibilidade das informações;
  Garantir a proteção adequada dos dados pessoais, das informações, dos documentos e dos sistemas contra acesso, modificação, destruição e divulgação não autorizados;
- Disseminar o conhecimento desta Política entre seus colaboradores por meio de treinamentos e conscientização para a correta observação da segurança da informação; e
- Garantir o cumprimento desta Política e demais procedimentos internos que visam a segurança da informação.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

A comunicação veiculada dentro da rede corporativa da Companhia segue uma classificação de acordo com a sua respectiva confidencialidade, que pode ser: (i) uso interno, e/ou (ii) uso externo. Ainda, a estrutura de documentos recebe a seguinte classificação:

Informação Pública - Constituem dados que não necessitam de proteção sofisticada, que podem ser disponibilizados e acessados por qualquer pessoa. No entanto, devem ser observados sua integridade e disponibilidade.

Informação de Uso Interno - Baixo nível de confidencialidade. Trata-se de informações que não podem ser divulgadas para pessoas de fora da Companhia, mas que, caso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

Informação Restrita - Nível médio de confidencialidade. Trata-se de informações estratégicas que devem estar disponíveis apenas para grupos restritos de pessoas. Podem ser protegidas, por exemplo, restringindo o acesso a uma pasta ou diretório da rede.

Informação Confidencial - É o nível mais alto de segurança. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer prejuízos à Companhia. Podem ser protegidas por meio de criptografia, por exemplo. Excetua-se ao ora previsto o envio de informação confidencial às pessoas, físicas e jurídicas, que mantenham condições de confidencialidade em NDA e/ou em instrumento contratual com a Companhia, e aos órgãos reguladores.

6. ESTRUTURA FÍSICA

6.1 Gestão de acesso físico

O acesso ao ambiente físico da CSD BR é controlado por meio de senha, pessoal e intransferível, e disponibilizado apenas às pessoas autorizadas.

A Plataforma está hospedada em provedor de serviços em nuvem (*cloud computing*). Os dados no Ambiente de Produção trafegam e são armazenados em território brasileiro.

6.2 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, como sistemas, computadores, e-mail, telefones, dentre outros, devem ser manuseados, armazenados, protegidos e utilizados para a finalidade única e exclusiva de atender aos interesses da Companhia.

6.3 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 drivers é proibido e bloqueado. Não é permitida a utilização de dispositivos de gravação e armazenamento de dados externos e sua conexão às estações de trabalho.

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.

Caberá ao Comitê de Riscos da Companhia a avaliação de eventuais exceções com base em solicitação formal efetuada ao Departamento de Produção e Segurança da

Informação (“DPSI”).

Os equipamentos utilizados devem estar configurados de acordo com as regras de segurança da informação, com softwares padronizados, antivírus instalado com update da última atualização vigente.

Essas diretrizes são válidas e aplicáveis a todos os colaboradores, administradores, Participantes, prestadores de serviços, e terceiros da CSD BR, que utilizem dispositivos ou sistemas da CSD BR, independentemente da forma de acesso (presencial, remota ou teletrabalho).

6.4 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 sobre gravados com segurança. Para tanto, a CSD BR utilizará aplicativos que proporcionem a deleção segura dos arquivos e, conforme prévia avaliação, empresas especializadas para o descarte de equipamentos.

7. ESTRUTURA LÓGICA

7.1 Gestão de Acesso Lógico

Todo acesso ao ambiente da CSD BR é restringido por meio da adoção de tecnologias com criptografia e segmentação de níveis de segurança. O acesso ao Ambiente de Homologação e Ambiente de Produção apenas é concedido pelo DPSI, mediante prévia autorização dos gestores das áreas, para as pessoas que efetivamente necessitarem.

Os acessos aos sistemas são pessoais e intransferíveis e todos os usuários têm o dever e a responsabilidade de proteger, não divulgar ou emprestar, e utilizar única e exclusivamente com a finalidade para a qual foi autorizada.

O compartilhamento de senhas constitui infração do Código de Conduta Ética da Companhia, sem prejuízo da aplicação das sanções nele dispostas.

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

7.2 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, de acordo com as respectivas regras e permissões.

Para mitigar eventuais problemas de segurança com relação à definição de senhas, a CSD BR adota o seguinte conjunto mínimo de exigências:

- Quantidade mínima de caracteres;
- Obrigatoriedade de composição por uma combinação de caracteres com nível de complexidade mínima; e
- A troca pode ser realizada diretamente pelo próprio usuário.

Adicionalmente, dentro de condições técnicas, cada sistema deve ser conectado ao sistema centralizado de autenticação da Companhia.

A senha é sigilosa, pessoal e intransferível, não podendo ser compartilhada ou divulgada entre os colaboradores e terceiros. Todos os colaboradores possuem ciência sobre essa diretiva e restrição uma vez que concordaram e assinaram o termo de adesão ao Código de Conduta Ética da CSD BR.

7.3 Ferramentas de Comunicação

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

O telefone, o endereço de e-mail e demais ferramentas de comunicação corporativos disponibilizados aos colaboradores são de propriedade da CSD BR e devem ser utilizados exclusivamente para atividades relacionadas ao trabalho a ser desempenhado. A CSD BR realiza o monitoramento e o *backup* e poderá realizar a gravação das comunicações realizadas por meio das ferramentas corporativas.

É proibido, em regime de trabalho presencial ou de teletrabalho, o acesso e utilização de e-mail pessoal de conta *gmail*. A referida proibição se aplica aos colaboradores e administradores, bem como aos prestadores de serviços e terceiros quando prestarem serviços alocados na Companhia, caracterizando o acesso e utilização, infração ao Código de Conduta Ética da Companhia, sem prejuízo das penalidades nele previstas.

7.4 Utilização de equipamentos em regime de teletrabalho

Aos colaboradores que atuam em regime de teletrabalho, há a possibilidade de utilização dos equipamentos da CSD BR ou equipamentos pessoais, conforme solicitação.

Para os colaboradores que utilizam equipamentos pessoais, o acesso às informações e ao sistema da CSD BR só deve ser realizado mediante configuração e uso de VPN.

O equipamento da CSD BR, por meio do qual o acesso é realizado, seja diretamente ou por meio de acesso à VPN, deve conter um antivírus atualizado e em caso de qualquer incidente de segurança o usuário deverá acionar imediatamente o DPSI e reportar o incidente, por meio da abertura de chamado, com a criticidade alta.

7.5 Segregação de acesso aos ambientes - “Desenvolvimento Seguro”

A CSD BR possui quatro ambientes segregados para sua Plataforma: produção, homologação de Participantes, homologação interna (“QA”) e desenvolvimento. 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 informações fictícias para testes ou simulações.
  - Externo: acesso liberado aos Participantes homologados ou em processo de homologação, às 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 informações fictícias 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 informações fictícias.
  - Externo: não liberado.
  - Interno: acesso liberado aos colaboradores da CSD -BR com funções específicas envolvendo os processos de desenvolvimento e testes do sistema.

7.6 Segurança dos Ambientes Operacionais

Visando garantir alta disponibilidade de seus equipamentos e serviços, a CSD BR realiza manutenções periódicas, preferencialmente aos sábados. 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 a equipe do DPSI mantém contato direto com os fabricantes dos equipamentos a fim de antecipar eventuais pontos de impacto ou melhorias ao ambiente da CSD BR.

É expressamente proibido armazenar, guardar arquivos corporativos nos *drives* locais dos *desktops* e *notebooks*, sendo imprescindível seu armazenamento nos *drives* corporativos, em ambiente seguro e salvaguardados por sistema de *backup* diário e incrementais.

Os arquivos armazenados fora dos *drives* corporativos não serão itens de *backup* e, por conseguinte, não terão garantia de sua integridade e segurança, sendo o usuário responsável por qualquer impacto nos ambientes corporativos.

7.7 Atualizações periódicas de segurança

As atualizações de segurança dos sistemas são realizadas periodicamente, em datas previamente determinadas. Para casos específicos, atualizações de segurança extraordinárias podem ser realizadas de acordo com uma avaliação prévia de sua criticidade pelo DPSI.

Tendo em vista que a Plataforma fica indisponível aos finais de semana, a Companhia realiza, conforme necessidade, as atualizações ordinárias nesse período.

7.8 Monitoramento de Eventos e Incidentes de TI

O monitoramento de todo o ambiente da CSD BR é fundamentado na utilização de sistemas de alertas e envio de notificações para as áreas responsáveis, com níveis de criticidade definidos. Este monitoramento engloba indicadores específicos do status de funcionamento e utilização dos equipamentos físicos, disponibilidade da estrutura de comunicação, ambiente de processamento da Plataforma, com todos seus módulos acessórios, além do controle de acesso e operação dos Participantes.

Neste monitoramento são utilizadas ferramentas específicas que realizam a coleta ativa de medidas e logs através de agentes configurados nos sistemas, consolidados em bancos de dados específicos e acompanhados continuamente através de *dashboards*, que disparam alertas quando qualquer indicador ultrapassa os limites previamente definidos.

7.9 Prevenção e Monitoramento – Incidentes de Segurança

Todos os pontos de interface de comunicação com a CSD BR são controlados por sistemas específicos e framework NIST, 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 *firewalls* para controlar as permissões de acesso, sistemas de IDS ("*Intrusion Detection System"*) para detectar acessos indevidos dentro da rede da CSD BR e sistema de IPS ("*Intrusion Prevention System"*) para monitorar atividades suspeitas na rede, tais como ameaças de segurança ou violações de políticas.

7.10 Gestão de Vulnerabilidades

Os acessos e comportamentos do ambiente de sistemas da CSD BR são monitorados continuamente para garantir a disponibilidade e segurança dos serviços, utilizamos o framework NIST de cibersegurança, para atuar contra todas as ameaças cibernéticas. A equipe de cibersegurança 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.

Todos os acessos são restritos às pessoas autorizadas para cada atividade especifica. Havendo necessidade de realização de serviço de terceiros, estes acessos serão

liberados somente durante o tempo necessário para a realização da atividade específica, conforme avaliação do Comitê de Riscos.

Uma estrutura de permissões segmentadas é utilizada para garantir essa política de acesso, além do monitoramento de tudo o que é feito no ambiente através de um sistema de logs e relatórios de auditoria.

A CSD BR possui mecanismos para realização periódica de testes que avaliam a aderência das configurações dos ambientes da sua Plataforma em relação às boas práticas de segurança da informação e resiliência cibernética.

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

7.11 Criptografia

A CSD BR conta com chaves criptográficas que visam garantir a segurança dos usuários nos ambientes disponibilizados pela Companhia, contando com uma política sobre o uso, proteção e tempo de vida das chaves criptográficas em todo o seu ciclo de vida.

A infraestrutura da Plataforma é baseada em alta disponibilidade, em que o tráfego das informações é realizado de forma segura, também através de criptografia.

7.12 Contingência e Continuidade de Negócios

Com o objetivo de obter maior performance, segurança, confiabilidade e escalabilidade, a Plataforma está hospedada em provedor de serviços em nuvem (*cloud computing*) localizado em território brasileiro, sendo que foi desenhada de forma a garantir a continuidade da operação, 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.

8. 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 do sigilo bancário, que estejam em sua posse ou que por qualquer forma sejam do conhecimento direto ou indireto de seus colaboradores, sejam tratados nos termos dos normativos e legislação em vigor, no que lhe for aplicável, com todas as suas particularidades e desdobramentos.

8.1 Vazamento de Dados Sigilosos

Na eventualidade de ocorrer o 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 que, de acordo com a análise prévia da criticidade ou gravidade do evento, comunicará ao Banco Central do Brasil, Comissão de Valores Mobiliários, Superintendência de Seguros Privados e ao Conselho de Administração da CSD BR. Além de adotar todas as medidas necessárias para evitar que novas informações sigilosas sejam divulgadas, a Diretoria também determinará a instauração imediata de uma sindicância interna e demais medidas necessárias para apuração das causas, responsabilização e adoção de eventuais medidas punitivas.

9. CONTROLE DO DOCUMENTO

9.1 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.

9.2 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.

9.3 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.