



CSD_{BR}
registradora

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



SUMÁRIO

CONTROLE DE VERSÃO	3
1. OBJETIVO	4
2. DESCRIÇÃO	4
3. RESPONSÁVEIS	4
4. APLICABILIDADE	5
5. PRINCÍPIOS GERAIS	5
6. EQUIPAMENTOS.....	5
6.1 Acesso físico aos Datacenters	6
6.2 Monitoramento e Vigilância Física.....	6
6.3 Ataque Cibernético.....	6
6.4 Dispositivos Móveis.....	7
6.5 Ferramentas de Comunicação	7
7. ESTRUTURA LÓGICA.....	7
7.1 Política de Senhas	7
7.2 Atualizações periódicas de Segurança.....	8
7.3 Segregação de Acesso aos Ambientes.....	8
7.4 Prevenção de incidentes	9
7.5 Plano de monitoramento	9
7.6 Controle de Vulnerabilidades	10
7.7 Testes	10
8. PROTEÇÃO DE DADOS PESSOAIS E SIGILO BANCÁRIO	10
8.1 Identificação.....	11
8.2 Vazamento de Dados Sigilosos.....	11
9. CONTROLE DO DOCUMENTO	11
9.1 Revisão.....	11
9.2 Direitos Autorais e Distribuição	11



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 (<i>pentests</i>), Inclusão sobre previsão de lei geral de proteção de dados; Revisão geral



1. OBJETIVO

O objetivo deste documento é descrever a Política de 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 de sua plataforma eletrônica (“Participantes”), reguladores e ao mercado financeiro de forma geral, o controle, fluxo, guarda e sigilo de toda informação de posse da CSD BR.

2. DESCRIÇÃO

Esta Política de Segurança da Informação (“Política”) é aplicada a toda e qualquer informação que estiver em posse, for enviada, gerada ou que qualquer colaborador da CSD BR tenha acesso de forma direta ou indireta, principalmente informações que estejam sob a proteção de dados pessoais, política de sigilo bancário de acordo com a legislação específica.

3. RESPONSÁVEIS

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

Para qualquer situação de violação ou conflito envolvendo essa Política, relacionamos a seguir a estrutura de responsabilidade e comando definida pela CSD BR.

O 1º Nível sempre deve ser acionado prioritariamente e, na sua ausência ou inaccessibilidade, os próximos níveis serão acionados, conforme informação de contato disponível em www.csdb.com, obedecendo a seguinte ordem de prioridade:

- 1º Nível: Diretor Operações e Tecnologia
- 2º Nível: Diretor Presidente
- 3º Nível: Diretor de Fiscalização e Supervisão

Exclusivamente para a Filial de São Carlos, nos casos de ocorrência de alguma situação que necessite resposta imediata e a comunicação com a estrutura de comando acima



não seja possível em tempo hábil, a estrutura de responsabilidade e comando substituta responsável localmente pela Filial será:

- 1º Nível Substituto: Coordenador de Atendimento ao Cliente
- 2º Nível Substituto: Coordenador de Pesquisa & Desenvolvimento

4. APLICABILIDADE

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

Os contratos e terceiros contratados pela CSD BR devem aderir formalmente a um termo específico, comprometendo-se a cumprir e agir de acordo com esta Política.

Todos os contratos da CSD BR devem assegurar a confidencialidade das informações de acordo com esta Política.

5. PRINCÍPIOS GERAIS

A Política de Segurança da Informação da CSD BR 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.

6. EQUIPAMENTOS

Todos os equipamentos e serviços da CSD BR estão localizados em três Datacenters



contratados pela CSD BR, geograficamente dispostos na região que engloba a Grande São Paulo.

6.1 Acesso físico aos Datacenters

A fim de garantir a segurança física da informação, somente pessoas da Equipe de Administração de Sistemas e a Diretoria Executiva da CSD BR possuem acesso físico aos racks dos três Datacenters onde estão localizados os equipamentos. Para o acesso físico a qualquer Datacenter é necessário cadastro prévio e identificação da pessoa perante o Portal do Datacenter.

Ainda, objetivando garantir o total controle do ambiente e segurança dos dados, informações e equipamentos, as pessoas autorizadas obrigatoriamente precisam cumprir os requisitos abaixo para conseguir acesso físico aos equipamentos, conforme segue:

- Cadastro prévio da visita no Portal do Datacenter, com a identificação completa do colaborador;
- Liberação da visita técnica da pessoa de acordo com os cadastros de autorização do Datacenter; e
- Checagem dos dados pessoais e documentação da pessoa pela equipe de segurança local do Datacenter.

As manutenções agendadas ou emergenciais em qualquer Datacenter somente serão realizadas por essas pessoas autorizadas pela CSD BR.

6.2 Monitoramento e Vigilância Física

Todos os equipamentos alocados nos Datacenters possuem vigilância 24x7 com gravação de imagens, restrição de acesso físico e ambiente altamente seguro com testes periódicos contra incêndios e quedas de energia. Todos os racks são fechados com controle de chaves.

6.3 Ataque Cibernético

Todos os pontos de interface de comunicação com a CSD BR são controlados 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 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.

6.4 Dispositivos Móveis

Com o objetivo de evitar a cópia indevida de informações, nas estações de trabalho de todo colaborador o acesso às portas USB e outros tipos de drivers é proibido e bloqueado. Não é permitida a utilização de dispositivos de 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.

A utilização de aparelhos celulares, tablets ou equivalentes é vedada dentro das instalações físicas da CSD BR, onde dados sigilosos são acessados ou consultados.

6.5 Ferramentas de Comunicação

O acesso aos sites de e-mails pessoais, mídias sociais e assemelhados é proibido para todos os colaboradores que tenham permissão de acesso ao ambiente de Produção e estão bloqueados por ferramentas específicas. Esses colaboradores somente poderão acessar em suas estações de trabalho as ferramentas e sites autorizados.

O telefone, e-mail e 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, o backup e gravação de toda a comunicação realizada através destas ferramentas corporativas.

7. ESTRUTURA LÓGICA

Todo acesso ao ambiente da CSD BR é restringido através da adoção de tecnologias com Criptografia e segmentação de níveis de segurança. O acesso apenas é liberado para as pessoas que efetivamente necessitam de acesso ao ambiente dos Datacenters, durante o menor período possível.

7.1 Política de Senhas

Para obter acesso a qualquer equipamento ou serviço das instalações da CSD BR é



obrigatória a identificação e autenticação dos usuários, de acordo com as respectivas permissões.

Para mitigar eventuais problemas de segurança com relação a definição de senhas, adotamos o seguinte conjunto mínimo de exigências:

- Quantidade mínima de caracteres;
- Composição, obrigatoriamente, por uma combinação de caracteres com nível de complexibilidade mínima;
- Impossibilidade de ser repetida ou baseada em informações pessoais, como próprio nome, login;
- Todas as restrições são garantidas pelo próprio sistema centralizado de autenticação; e
- Sua troca pode ser realizada diretamente pelo próprio usuário.

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.

7.2 Atualizações periódicas de Segurança

As atualizações de segurança dos sistemas são realizadas mensalmente, em datas previamente determinadas. Para casos específicos, atualizações de segurança extraordinárias podem ser realizadas de acordo com uma avaliação prévia de sua criticidade pela Equipe de Administração de Sistemas.

As atualizações ordinárias ocorrem preferencialmente aos sábados, com a informação de previsão do período de eventual restrição de serviços previamente enviada aos Participantes.

7.3 Segregação de Acesso aos Ambientes

A CSD BR possui quatro níveis de ambientes segregados para sua Plataforma de Sistemas: Produção, Homologação de Participantes, Homologação Interna e Desenvolvimento. Para cada tipo de ambiente são aplicados níveis de acesso diferenciados, com permissões específicas:

- **Produção:** contém as informações 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:** pode ser utilizado com informações fictícias para testes ou simulações dos Participantes.
 - Externo: acesso liberado aos Participantes homologados ou em processo de homologação.
 - Interno: acesso liberado aos colaboradores da CSD BR com funções específicas envolvendo o ambiente de Homologação de Participantes.
- **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.

7.4 Prevenção de incidentes

A CSD BR realiza manutenções periódicas visando garantir alta disponibilidade de seus equipamentos e serviços. 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 equipamentos. Para isso a Equipe de Administração de Sistemas mantém contato direto com os fabricantes de equipamentos a fim de antecipar eventuais pontos de impacto ou melhoria ao ambiente da CSD BR.

7.5 Plano de monitoramento

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 do sistema de registro de títulos 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 definidos.

7.6 Controle de Vulnerabilidades

Os acessos e comportamentos do ambiente de sistemas da CSD BR são monitorados continuamente para garantir a disponibilidade e segurança dos serviços. Todos os acessos são restritos exclusivamente às pessoas autorizadas para cada atividade específica, liberados somente durante o tempo necessário para a realização da atividade específica.

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

7.7 Testes

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.

8. PROTEÇÃO DE DADOS PESSOAIS E SIGILO BANCÁRIO

A CSD BR adota todas as regras e os controles pertinentes 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 Identificação

A fim de mitigar a exposição indevida de informações advindas dos Participantes, na eventualidade de uma ocorrência de vazamento de dados pessoais e/ou quaisquer informações, a CSD BR definiu em sua arquitetura de sistema que as informações dos titulares de Ativos serão armazenadas de forma criptografada. Essa diretiva cria um segundo nível de proteção, tendo em vista que a identificação do titular de um Ativo na Plataforma da CSD BR nunca está disponível de forma aberta, mas sim criptografada.

8.2 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 Executiva que, de acordo com a análise prévia da criticidade ou gravidade do evento, comunicará ao Banco Central do Brasil 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 Executiva 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 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.

9.2 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.