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

1. OBJETIVO

Essa Política de Segurança da Informação ("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" 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, 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. APLICABILIDADE

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.

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.

3. RESPONSABILIDADES

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, responsável por sua aprovação.

Os colaboradores, administradores, Participantes, prestadores de serviços, e terceiros da CSD BR devem cumprir todas as obrigações previstas nesta Política, no que lhes for aplicável, bem como observar os mais altos padrões de conduta profissional ao conduzir suas atividades.

Toda e qualquer inconsistência ou irregularidade relativas aos procedimentos e práticas ora estabelecidos, deverão ser reportados ao superior imediato do Colaborador, ou à Diretoria de Governança, Riscos e Controles Internos, conforme aplicável, ou através do Canal de Atendimento da CSD BR indicado no site da Companhia.

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 e dados pessoais;
- 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 treinamento 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. DIRETRIZES

5.1 Classificação da Informação

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

Pública – Informação que pode ser disponibilizada e acessada por qualquer pessoa. Devem ser observadas a sua integridade (consistência e confiabilidade das informações) e disponibilidade (tempo e acessibilidade que se tem das informações, ou seja, se podem ser consultadas a qualquer momento).

Uso Interno – Informações que não podem ser divulgadas para pessoas de fora da Companhia, mas que, caso aconteça, não causarão grandes prejuízos. Deve ser considerada a integridade da informação (consistência e confiabilidade).

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 para trazer prejuízos à Companhia, com exceção do envio de informações aos órgãos reguladores, e às pessoas físicas ou jurídicas quem mantenham obrigações de confidencialidade com a Companhia.

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

5.2 Gestão de Acesso Físico

O acesso ao ambiente físico da CSD BR para colaboradores, visitantes e prestadores de serviços é controlado e concedido apenas à 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 em nuvem (*cloud computing*). Os dados no Ambiente de Produção trafegam e são armazenados em território brasileiro, de forma criptografada.

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.

5.3 Gestão de Acesso Lógico

Todos os acessos ao ambiente da CSD BR são restritos às pessoas autorizadas para cada atividade específica, por meio da adoção de tecnologias com criptografia e segmentação de níveis de segurança.

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.

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

5.3.1 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 essa Política.

A senha de acesso aos sistemas e ambientes da CSD BR é sigilosa, pessoal e intransferível, não podendo ser compartilhada ou divulgada entre os colaboradores e terceiros. Todos os acessos aos sistemas são pessoais e intransferíveis e todos os usuários têm o dever e a responsabilidade de proteger, não divulgar ou emprestar, utilizar única e exclusivamente com a finalidade para a qual foi autorizada e realizar a sua troca a cada 90 dias.

5.4 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.

5.4.1 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.

5.4.2 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 área solicitante deve encaminhar solicitação ao DPSI, que procederá às análises de viabilidade e autorizações necessárias.

Toda instalação de software deve ser realizada pela equipe técnica da CSD BR, que deve considerar os requisitos de segurança e as necessidades do negócio, além de manter 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.

5.4.3 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 drivers é proibido e bloqueado.

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 equipe de Segurança da Informação e Comitê de Riscos quando aplicável.

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).

5.4.4 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 sobre gravados com segurança.

Em caso de descarte de equipamentos e quando necessário, a CSD BR utiliza software específico de deleção segura dos arquivos (Ferramenta de Wipe - Padrão DoD 5220.22-M), que permite a destruição de todos os dados em discos (HD), excluindo qualquer possibilidade de recuperação de arquivos e pastas excluídas. Este software gera certificado com a formalização de que os dados foram apagados.

5.5 Ferramentas de Comunicação Corporativa

5.5.1 Uso da Internet, E-mail, Telefonia e Aplicativo de Mensagens

O uso das 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 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 informativas de produtos e serviços da CSD BR.

Quando o usuário se afastar de sua estação de trabalho, deverá bloquear ou encerrar a sessão.

5.6 Uso da Rede Interna

O acesso à rede 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.

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.

5.6.1 Segurança na Utilização de Rede Wifi / Wireless

O acesso remoto à rede interna é disponibilizado somente aos colaboradores da CSD BR por meio de VPN, controlada e monitorada pela Companhia. Para utilização da rede é necessário que o usuário solicite o cadastro do equipamento junto à equipe de Segurança da Informação da CSD BR.

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

5.7 Impressão de Documentos

Todos os colaboradores devem recolher o material impresso de imediato, de modo a evitar que informações sensíveis ou confidenciais fiquem expostas. 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, à área de Segurança da Informação ou à GRC, que tem autonomia para destruir o que foi encontrado e não retirado da impressora.

5.8 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 ao deixar a estação de trabalho, ainda que momentaneamente e não deverá deixar informações sensíveis ou confidenciais disponíveis.

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.

5.9 Utilização de equipamentos em regime de teletrabalho

Em caso de regime de teletrabalho, o acesso às informações e ao sistema da CSD BR, só deve ser realizado mediante a utilização de equipamentos próprios da CSD BR, 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.

5.10 Criptografia

A CSD BR utiliza criptografia para garantir a segurança no acesso aos ambientes disponibilizados pela Companhia.

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

5.11 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.

Havendo dúvidas, não forneça a informação e contate o GRC ou a área de DPSI para a devida orientação.

5.12 Conscientização

A CSD BR atua na disseminação da cultura de Segurança da Informação e Segurança Cibernética por meio de treinamentos e ações específicas de conscientização focados em garantir a segurança, confidencialidade, integridade e disponibilidade das informações.

5.13 Desenvolvimento e Manutenção Segura do Ambiente

5.13.1 Segregação de acesso aos ambientes da Plataforma

A CSD BR possui quatro ambientes segregados para sua Plataforma: produção ("PROD"), 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 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.

5.13.2 Desenvolvimento e Mudança da Plataforma

Os requisitos de segurança da informação devem ser considerados e incluídos no desenvolvimento e mudança da Plataforma.

As versões da Plataforma e funcionalidades passam por testes e aprovações nos ambientes de “teste” e “Homologação” antes de entrarem em “Produção”.

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

5.13.3 Acesso e Utilização do Código Fonte

O acesso ao Código Fonte da Plataforma, quando e se necessário, é concedido pela CSD BR apenas à pessoas autorizadas, sendo o referido acesso pessoal e intransferível, de modo que cada usuário é responsável pelo seu acesso, 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.

5.14 Manutenção dos Ambientes Operacionais

Visando garantir alta disponibilidade de seus equipamentos e serviços, a CSD BR realiza manutenções periódicas, preferencialmente aos finais de semana ou em casos extraordinários, 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 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.

5.15 Monitoramento de Eventos e Vulnerabilidades

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.

5.16 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, através 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. A implementação dessas diretrizes é realizada através de ferramenta específica, para garantir o registro e o gerenciamento do ciclo de vida dos incidentes, possibilitando o rápido atendimento de forma a minimizar o impacto e a normalização da prestação de serviço.

Os incidentes são categorizados e em caso o incidente seja classificado como “Crítico”, deve-se observar o estabelecido no Processo de Gestão de Crises. Em caso de interrupção da operação, deve-se observar e seguir o Plano de Continuidade de Negócio, considerando o tempo estimado de recuperação (RTO).

6. 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 um possível risco;

(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; e (v) envolvimento da alta liderança para a tomada de decisões e construção de planos de ação.

7. SEGURANÇA CIBERNÉTICA

7.1 Prevenção e Monitoramento de Incidentes de Segurança

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.

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.

7.2 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 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.

8. CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Com o objetivo de obter maior performance, segurança, confiabilidade e escalabilidade,a Plataforma da CSD BR está hospedada em provedor de serviços em nuvem (*cloud computing*) localizado em território brasileiro, sendo que o Módulo Operações SUSEP poderá estar em território brasileiro ou fora dele, neste caso, nos Estados Unidos da América.

A arquitetura da Plataforma 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. As diretrizes relacionadas a assunto, estão contidas na Política de Gestão de Continuidade de Negócios.

9. 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.

9.1 Monitoramento

A CSD BR tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de 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 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 passa a ser gravada.

9.2 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 que, de acordo com a análise prévia da criticidade ou gravidade do evento, comunicará à Associação Nacional de Proteção de Dados (ANPD), ao Banco Central do Brasil, à Comissão de Valores Mobiliários, à 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.

10. REFERÊNCIAS

10.1 Referências Regulatórias (conforme alteradas)

Resolução CMN 4.968, de 25 de novembro de 2021

Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Link para Acesso: https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.968-de-25-de-novembro-de-2021-362739343

Resolução CMN nº 3.380, de 29 de junho de 2006

Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional.

Link para Acesso:

https://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_L.pdf

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.

Link para Acesso:

https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973

Resolução CMN nº 4.745, de 29 de agosto de 2019 (altera a Resolução 4.557)

Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

Link para Acesso:

https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50827/Res_4745_v1_O.pdf

Resolução CMN nº 4.595, de 28 de agosto de 2017

Dispõe sobre a política de conformidade (compliance) das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50427/Res_4595_v1_O.pdf

Resolução CVM 135, de 10 de junho de 2022

Dispõe sobre o funcionamento dos mercados regulamentados de valores mobiliários; a constituição, organização, funcionamento e extinção das entidades administradoras de mercado organizado.

Link para Acesso:

https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/100/resol135.pdf

Circular Susep 249/2004

Dispõe sobre a implantação e implementação de sistema de controles internos nas sociedades seguradoras, nas sociedades de capitalização e nas entidades abertas de previdência complementar.

Link para Acesso:

https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/4141

Resolução CNSP 416, de 20 de julho de 2021

Dispõe sobre o sistema de Controles Internos, a Estrutura de Gestão de Riscos e a atividade de Auditoria Interna.

Link para Acesso:

https://www.in.gov.br/en/web/dou/-/resolucao-cnsp-n-416-de-20-de-julho-de-2021-333252056

Circular Susep 638, de 27 de julho de 2021

Dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais.

Link para Acesso:

https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/25121

Circular SUSEP nº 619, de 04 de dezembro de 2020

Dispõe sobre a política de segurança e sigilo de dados e informações das entidades registradoras credenciadas a prestarem o serviço de registro de operações de seguros, previdência complementar aberta, capitalização e resseguro (“Circular SUSEP 619”).

Link para Acesso:

https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/23958

10.2 Framewoks de Mercado

Committee of Sponsoring Organizations of the Tradeway Commission (“COSO”)

Referência: COSO ERM. Gerenciamento de Riscos Corporativos - Estrutura Integrada, 2004. / COSO. Gerenciamento de Riscos Corporativos – Estrutura Integrada. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e Pricewaterhouse Coopers Governance, Risk and Compliance, Estados Unidos da América, 2007.

ABNT NBR ISO 31.000:2009

Referência: ABNT, Associação Brasileira de Normas Técnicas, ABNT NBR ISO 31000: Gestão de Riscos - Princípios e Diretrizes, 2018.

ABNT NBR ISO 31010:2012

.Referência: ABNT, Associação Brasileira de Normas Técnicas, ABNT NBR ISO IEC 31010: Técnicas para o processo de avaliação de riscos, 2012.

Principles for Financial Market Infrastructures - PFMI

Referência: https://www.bis.org/cpmi/publ/d101a.pdf

***Control Objectives for Information and Related Technologies* (“*COBIT*”)**

Referência: https://www.isaca.org/resources/cobit

National Institute of Standards and Technology (“NIST”)

Link para Acesso: https://www.nist.gov/cyberframework

ABNT NBR ISO 27.001: 2005 / ABNT NBR ISO 27.002:2013

Link para Acesso: https://www.normas.com.br/visualizar/abnt-nbr-nm/25074/abnt-nbriso-iec27001-tecnologia-da-informacao-tecnicas-de-seguranca-sistemas-de-gestao-da-seguranca-da-informacao-requisitos

10.3 Outras

RESOLUÇÃO BCB Nº 287, DE 24 DE JANEIRO DE 2023

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

Link para Acesso:

https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=287

11. CONTROLE DO DOCUMENTO

11.1 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.

11.2 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.

11.3 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.