

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Classificação da Informação	Interno
------------------------------------	---------

Responsável pelo Documento	Área
Elaboração	Tecnologia e Segurança da Informação
Revisão	Diretor de Tecnologia e Segurança da Informação
Aprovação	Diretoria Executiva

Registro de Alterações:

Versão	Item Modificado	Data de Aprovação
01	Aprovação da versão inicial	04/01/2021
02	Revisão integral, incluindo atualização normativa e de razão social	26/08/2022
03	Revisão integral, incluindo itens para atender Proteção de Dados	23/11/2023
04	Revisão integral com unificação das DTVM's	10/06/2025
05	Inclusão das diretrizes previstas na Resolução BCB nº 538	27/07/2026

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICAVersão:
05Código de Acesso
TEC.002

1	OBJETIVO	3
2	ABRANGÊNCIA	3
3	VIGÊNCIA.....	3
4	DIRETRIZES.....	3
5	PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	3
6	USO DE EQUIPAMENTOS, MESA E TELA LIMPA	4
7	COMPUTAÇÃO MÓVEL	4
8	USO DE INTERNET, E-MAIL, MENSAGERIA ELETRÔNICA E TELEFONIA.....	5
9	ESTRUTURAS DE COMPUTAÇÃO EM MODALIDADE NUVEM	5
10	CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS E PRESTADORES DE SERVIÇOS	6
11	DISSEMINAÇÃO	6
12	GESTÃO DE ATIVOS	6
13	GESTÃO DE RISCOS	7
14	IDENTIFICAÇÃO DOS RISCOS	7
15	SISTEMAS DE PROTEÇÃO DE DADOS	7
16	GESTÃO DE ACESSOS	8
17	ACESSO REMOTO	9
18	GERENCIAMENTO DE INCIDENTES E DE SEGURANÇA DA INFORMAÇÃO	9
19	GERENCIAMENTO DE MUDANÇAS	10
20	DESENVOLVIMENTO E MANUTENÇÕES DE SISTEMAS	10
21	CÓPIA DE SEGURANÇA DE DADOS E SISTEMAS (BACKUP)	10
22	GESTÃO DE CONTINUIDADE	11
23	CONTROLES SOBRE SOFTWARES E COMPUTADORES	11
24	GERENCIAMENTO DE FIREWALL E VULNERABILIDADES	12
25	GESTÃO DE CERTIFICADOS DIGITAIS	12
26	LICENCIAMENTO DE SOFTWARE E MANUTENÇÃO DE INVENTÁRIO	13
27	MONITORAMENTO DE AMBIENTES	13
28	SEGURANÇA DE INFRAESTRUTURAS DO SFN	13
29	PROTEÇÃO DE DADOS PESSOAIS	14
30	AUDITORIA E CONFORMIDADE.....	14
31	GESTÃO DE CONSEQUÊNCIAS	14
32	PAPÉIS E RESPONSABILIDADES.....	14

	TRUSTEE E BANVOX DTVM LTDA	Página 3 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

1 OBJETIVO

Estabelecer as diretrizes que permitam aos colaboradores, clientes e prestadores de serviços seguirem os padrões de comportamento relacionados à segurança da informação e cibernética adequados às necessidades de negócio da Trustee Distribuidora de Títulos e Valores Mobiliários Ltda. e da Banvox Distribuidora de Títulos e Valores Mobiliários Ltda. (“Distribuidoras”) de acordo com a Resolução BCB nº 85, Resolução BCB nº 538, Resolução CVM nº 21, Resolução CMN nº 5.274 e Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.

2 ABRANGÊNCIA

Esta Política aplica-se a todos os níveis hierárquicos das Distribuidoras, além de terceiros e prestadores de serviços que acessam ou processam dados em nome da Distribuidoras.

3 VIGÊNCIA

Esta Política entra em vigor na data da aprovação pela Diretoria Executiva e possui vigência anual. Eventuais alterações relevantes nos processos operacionais serão realizadas pelo time de Compliance antes do vencimento da vigência.

4 DIRETRIZES

- Prevenir, identificar e reduzir vulnerabilidades presentes no ambiente cibernético e tratar tempestivamente incidentes ocorridos de forma a não gerar impactos negativos em suas operações.
- Assegurar que a informação não será conhecida por pessoas que não estejam autorizadas para tal (confidencialidade).
- Garantir que a informação armazenada ou transferida está correta e é apresentada corretamente para quem a consulta (integridade).
- Manter as informações que possam ser obtidas sempre que for necessário, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções (disponibilidade).
- Proteger a privacidade dos dados pessoais, em conformidade com as leis aplicáveis e as melhores práticas de mercado.
- Eventuais exceções as diretrizes desta Política devem ser aprovadas pelo Diretor de Tecnologia e Segurança da Informação.

5 PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A seguir estão relacionados os principais controles e procedimentos utilizados para proteger as informações, atender às necessidades da segurança cibernética e diminuir a vulnerabilidade a incidentes. Tais controles e procedimentos devem ser observados por todos os Colaboradores, como primeira linha de defesa.

O responsável pela segurança da informação é o Superintendente de Tecnologia.

	TRUSTEE E BANVOX DTVM LTDA	Página 4 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

6 USO DE EQUIPAMENTOS, MESA E TELA LIMPA

É de responsabilidade de todos os Colaboradores zelar pelos equipamentos fornecidos, garantindo sua segurança e utilização adequada. No exercício de suas funções, os Colaboradores devem observar as seguintes práticas em relação à organização de suas mesas e telas de computadores:

- Tratar com cuidado especial os documentos e mídias eletrônicas que contenham dados pessoais e confidenciais, armazenando-os adequadamente e garantindo que não sejam deixados sobre as mesas na ausência do Colaborador ou após o horário de expediente; e
- Manter as telas de seus computadores livres de informações de negócios quando desassistidos e garantir que estejam protegidas por mecanismos de autenticação controlados por senha ou outro mecanismo similar, além de serem desligados quando não estiverem em uso por longos períodos.

Adicionalmente, os Colaboradores devem observar as seguintes considerações sobre uso de impressoras corporativas:

- As impressoras são utilizadas por qualquer usuário que possua acesso à rede;
- A impressão de documentos é feita em função da estrita necessidade dos serviços;
- O usuário zelar pelos documentos impressos, não sendo permitido deixá-los na impressora; e
- A TI é responsável por configurar a impressora padrão do usuário de acordo com o seu local de trabalho.

Essas práticas visam assegurar a confidencialidade, integridade e disponibilidade das informações, bem como a proteção de dados pessoais de colaboradores, clientes e prestadores.

Todos os Colaboradores são responsáveis por cumprir essas medidas de segurança e devem relatar quaisquer incidentes de segurança de informações ou outras preocupações de segurança imediatamente.

7 COMPUTAÇÃO MÓVEL

Para a utilização de computação móvel (notebooks) são observados as regras e os controles abaixo:

- Será permitida a entrada de notebooks de fornecedores nas dependências das Distribuidoras, desde que não acessem rede de TI corporativa utilizada pelos colaboradores;
- Quando disponível, os fornecedores e visitantes, utilizam rede específica para acesso à internet (rede de visitantes) provida pela área de TI; e
- Quando disponível, será permitido o acesso e utilização de rede sem fio (*Wireless*), tanto por usuários autenticados na rede sem fio corporativa, como por fornecedores e visitantes identificados na rede sem fio de visitantes. Sendo a utilização e navegação nestas redes sujeita à monitoração e controle.

Reserva-se o direito de monitorar a utilização de notebooks e redes sem fio, podendo, a seu critério, bloquear o acesso a tais recursos caso seja identificado o uso inadequado ou não autorizado.

É responsabilidade dos usuários de computação móvel adotar medidas de segurança para garantir a proteção das informações e dados a que têm acesso, incluindo o uso de senhas robustas e a criptografia de arquivos sensíveis.

Os usuários de notebooks também devem garantir a segurança física dos equipamentos, evitando deixá-los desacompanhados ou sem supervisão em locais públicos ou de acesso não autorizado.

	TRUSTEE E BANVOX DTVM LTDA	Página 5 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

8 USO DE INTERNET, E-MAIL, MENSAGERIA ELETRÔNICA E TELEFONIA

• Internet

- O acesso à internet destina-se **exclusivamente** para tarefas relativas ao trabalho. O uso para outros fins deve ser autorizado pelo gestor responsável; e
- O acesso a conteúdo impróprios, pornografia, jogos, bate-papo, conteúdo para hackers, apostas, músicas, são terminantemente proibidos e bloqueados.

Vale ressaltar que o Responsável pela Segurança da Informação, bem como o Compliance e a Diretoria Executiva possuem permissão para monitorar toda e qualquer conexão.

• E-mail corporativo

As seguintes considerações são observadas na utilização e-mail corporativo:

- O uso do e-mail corporativo é exclusivo para tarefas relacionadas ao trabalho de cada colaborador;
- É proibida a troca de mensagens que possam comprometer a confidencialidade de informações; e
- Caso receba mensagens suspeita de que o conteúdo seja impróprio, contrário às regras estabelecidas, o departamento de Tecnologia da Informação será notificado, para correção do problema e aplicação de medidas adequadas a bloquear futuras repetições da ocorrência.

• Mensageria eletrônica

A gravação das conversas por mensageria eletrônica é feita no banco de dados da aplicação e são armazenadas por cinco anos, onde pode ser consultada.

• Telefonia corporativa

A administração do sistema de gravações telefônicas e manutenção é de responsabilidade do respectivo fornecedor e as ligações podem ser ouvidas a qualquer momento pela área de Controles Internos, que possui acesso total as gravações. Todos os colaboradores devem cumprir rigorosamente as regras e considerações acima. O não cumprimento pode resultar em medidas disciplinares. As Distribuidoras se reservam ao direito de realizar auditorias e inspeções para assegurar o cumprimento das políticas e procedimentos estabelecidos.

9 ESTRUTURAS DE COMPUTAÇÃO EM MODALIDADE NUVEM

Sobre o uso de estruturas de computação em nuvem, as seguintes diretrizes devem ser seguidas:

- Existirá um controle efetivo e proativo sobre o consumo dos recursos e da capacidade de processamento da estrutura de nuvem;
- Os dados, indicadores e relatórios dos recursos e configurações de segurança do ambiente em estrutura de nuvem são reportados e monitorados pelo Responsável pela Segurança da Informação;
- Serão definidas, na contratação do fornecedor, em conjunto com os provedores de serviços de nuvem, as responsabilidades de cada parte envolvida na segurança dos dados armazenados na nuvem, de forma a garantir que todas as partes estejam cientes de suas obrigações e responsabilidades. Além disso, na seleção de provedores de serviços em nuvem serão considerados critérios de maturidade do fornecedor em segurança da informação e privacidade. Os provedores de serviços de nuvem serão avaliados quanto à segurança de suas estruturas e processos, bem como quanto à conformidade com as regulamentações;
- Serão estabelecidos perfis de acesso, que definirão o nível de acesso de cada usuário aos dados armazenados na nuvem. Serão utilizados mecanismos de autenticação de usuários, para garantir que apenas pessoas autorizadas tenham acesso aos dados armazenados na nuvem; e
- Será implementado um sistema de monitoramento constante dos dados armazenados na nuvem, a fim de detectar e prevenir qualquer violação de segurança que possa ocorrer. Serão utilizadas ferramentas de monitoramento de segurança, que permitirão a detecção de qualquer tentativa de acesso não autorizado aos dados armazenados na nuvem. Serão definidos procedimentos para a investigação e tratamento de eventuais incidentes de segurança. Será realizado um relatório periódico das atividades de monitoramento, para garantir a efetividade das medidas de segurança implementadas.

	TRUSTEE E BANVOX DTVM LTDA	Página 6 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

10 CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS E PRESTADORES DE SERVIÇOS

A contratação de serviços de terceiros e prestadores de serviço na área de tecnologia considerados relevantes, seguirá as diretrizes estabelecidas na Política de Contratação e Monitoramento dos Prestadores de Serviços. Adicionalmente, antes da assinatura de contratos será realizada pela área de TI, e após reportado aos controles internos, uma avaliação das empresas contratadas sob a ótica de Segurança da Informação e Cibersegurança de forma a identificar possíveis riscos. A avaliação de empresas contratadas sob a ótica de privacidade e proteção de dados será conduzida pelo DPO.

Serão incluídas cláusulas contratuais específicas nos contratos firmados com os prestadores de serviços, que garantam o cumprimento das obrigações de segurança da informação, proteção de dados pessoais e cibersegurança por parte dos prestadores de serviços.

11 DISSEMINAÇÃO

Para fortalecer a cultura de Segurança da Informação, a Política de Segurança da Informação será amplamente divulgada para todos os colaboradores, tanto durante o processo de admissão quanto em treinamentos de segurança da informação. Além disso, a política será disponibilizada em um local de fácil acesso a todos os colaboradores, sendo notificados à medida que as regras e conceitos contidos nesta Política sejam atualizados.

Para o conhecimento explícito será disponibilizado um treinamento em plataforma EAD sobre Segurança da Informação, que será obrigatório para todos os colaboradores. O treinamento abordará as regras e conceitos contidos na Política de Segurança da Informação, ministrado em plataforma EAD.

Será realizada uma comunicação constante com os colaboradores, para reforçar a importância da segurança da informação e a necessidade de cumprir as regras estabelecidas na Política de Segurança da Informação. A comunicação poderá ser realizada por meio de campanhas de conscientização, murais, informativos ou outros meios.

12 GESTÃO DE ATIVOS

Os ativos de informação são identificados de forma individual, inventariados e protegidos fisicamente e logicamente. Para controle dos ativos é necessário:

- Identificar os seus proprietários e custodiantes;
- Mapear as suas ameaças e vulnerabilidades;
- Estabelecer controles para entrada/saída nas dependências autorizadas e registradas por autoridade competente;
- Condicionar o acesso aos ativos de informação e sua utilização, quando autorizado, ao aceite do termo de sigilo e responsabilidade; e
- Serem utilizados estritamente dentro do seu propósito, sendo vedado o uso para entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Além disso, deve-se implementar medidas adicionais para proteger os dados pessoais que estão sendo tratados em seus ativos de informação, incluindo:

- Identificação dos dados pessoais:** todos os ativos de informação devem ser avaliados para identificar quais dados pessoais estão sendo armazenados em cada um deles. Isso permitirá que saber quais informações estão sendo protegidas e aplique as medidas de segurança adequadas.
- Registros de tratamento de dados pessoais:** deve manter um registro de todas as atividades de tratamento de dados pessoais realizadas em cada ativo de informação. Isso inclui informações sobre a finalidade do tratamento, a base legal para o tratamento, os tipos de dados pessoais tratados, os destinatários dos dados, e quaisquer transferências internacionais de dados. Esses registros ajudarão a garantir que as Distribuidoras estejam em conformidade com a LGPD e possa rastrear o tratamento de dados pessoais, caso necessário.
- Avaliação de risco:** deve realizar avaliações de risco periódicas para identificar ameaças e vulnerabilidades que possam afetar a segurança dos dados pessoais tratados em seus ativos de informação. Com base nessa avaliação, deve implementar medidas de segurança apropriadas para proteger os dados pessoais.

Deve-se garantir que os seus ativos de informação sejam utilizados exclusivamente para o propósito estabelecido e que o seu uso para entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins seja vedado.

	TRUSTEE E BANVOX DTVM LTDA	Página 7 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

13 GESTÃO DE RISCOS

Os riscos são identificados durante o processo de auditoria e/ou avaliação de riscos de segurança da informação.

A cada avaliação de riscos de segurança da informação é elaborado um escopo claramente definido e identificando as relações com as avaliações de riscos em outras áreas, quando apropriado. Este escopo pode ser para toda a organização, parte dela, um sistema individual, componentes específicos ou determinado serviço.

As avaliações de riscos são identificadas, quantificadas e priorizadas de acordo com os objetivos da organização. Os resultados são guiados e determinados para ações e prioridades da gestão de segurança da informação e para implementar controles selecionados para proteção contra estes riscos.

A avaliação de riscos será revisada anualmente para adereçar mudanças nos ativos, ameaças, vulnerabilidades ou impactos. O tratamento de um risco envolve aplicar controles preventivos, detectivos e corretivos adequados, porém outros tratamentos podem ser mais apropriados em alguns casos como evitar um risco, transferência de riscos ou a aceitação do risco.

Para estes riscos onde a decisão é aplicar controles de segurança da informação, controles adequados são selecionados e implementados para satisfazer os requisitos identificados. Os controles reduzirão os riscos a um nível aceitável levando em conta:

- Qualquer requisito ou restrições legais ou regulamentárias;
- Políticas e objetivos;
- Requisitos e restrições operacionais;
- O custo da concepção, implementação, operação, gerenciamento e manutenção de controles em relação aos riscos sendo reduzidos, mantendo-se proporcional aos requisitos e restrições da organização; e
- A necessidade de balancear o investimento em segurança da informação contra os prejuízos recorrentes de falhas de segurança e contra investimentos potenciais que podem gerar um retorno melhor.

14 IDENTIFICAÇÃO DOS RISCOS

- Malware – softwares desenvolvidos para corromper computadores e redes (tais como vírus, cavalo de tróia, spyware e ransomware);
- Engenharia Social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing e Acesso Pessoal);
- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

15 SISTEMAS DE PROTEÇÃO DE DADOS

- Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e das Distribuidoras, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações por meio eletrônico são devidamente arquivadas e registradas em backup.
- Governança da Gestão de Risco:** a eficácia da gestão de risco quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.
- As informações são classificadas de acordo com a confidencialidade e as proteções necessárias para os seguintes níveis: Confidencial, Restrita, Uso Interno e Pública.
- A detecção, classificação, orientação tempestivamente e pró ativamente aos usuários, parceiros e clientes em resposta a incidentes e quaisquer fraudes de segurança que envolvam dados pessoais, financeiros e produtos em plano de resposta a incidentes de Segurança, Segurança em Dados Pessoais e sistemas.
- Deverá ser fomentada a conscientização de todos os funcionários e parceiros comerciais sobre a importância da proteção de dados pessoais, cabendo ao Encarregado pela proteção de dados pessoais a realização dos treinamentos e informativos relacionados ao Programa de Governança em Privacidade, o que deve ser feito sempre observando as necessidades do referido Programa.
- Tratamento de dados pessoais:** trata os dados pessoais com base em das hipóteses legais previstas na LGPD.
- Gestão de incidentes de segurança de dados:** possui um processo para a gestão de incidentes de segurança de dados, com um plano de resposta a incidentes.

	TRUSTEE E BANVOX DTVM LTDA	Página 8 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

16 GESTÃO DE ACESSOS

Garante que nenhuma ação poderá comprometer a segurança e obter acesso não autorizado aos dados.

- **Acesso físico ao CPD (Centro de Processamento de Dados)**

Com o objetivo de preservar a segurança e sigilo das informações é feito um controle de acessos via crachá de acesso, no caso de colaboradores, e através da planilha de Acesso para fornecedores externos às salas de Servidores e Telecom.

Na prestação dos serviços por terceiros concernentes a assistência técnica de servidores e equipamentos, auditorias e outros, os terceiros contratados são sempre acompanhados de pessoa(s) autorizada(s). Sempre que possível e para evitar transtornos, a solicitação para que o prestador terceiro tenha acesso ao CPD será feita com antecedência suficiente para programação da TI.

- **Acesso físico as dependências das Distribuidoras**

A responsabilidade por controlar a liberação e bloqueio do acesso físico é do RH, onde todo acesso as dependências da empresa é rastreável.

- **Acesso Lógico**

As Distribuidoras mantêm controle de monitoramento de acesso a pastas e arquivos eletrônicos de acordo com as funções e cargos de cada profissional, conforme autorizado pelo gestor da respectiva área, sendo o acesso a rede de tais pastas com base em senha e login disponibilizados.

- **Manutenção de Senhas**

- Dificultar a identificação da senha evitando datas, nomes de parentes, números de documentos, telefones e outros de fácil identificação.
- As senhas devem ser atualizadas periodicamente, de acordo com a frequência estabelecida pela política de segurança da informação.
- As senhas não devem ser compartilhadas com terceiros e não devem ser reutilizadas em diferentes sistemas.
- As senhas são alteradas sempre que houver a suspeita de que foi identificada por outra pessoa.
- A senha não será anotada em papéis, tampouco deixada em local visível a outras pessoas.

A autenticação multifator (MFA) é adotada para todos os acessos aos sistemas e aplicações, sendo implementada como controle padrão de verificação de identidade. Para acessos privilegiados (administradores de sistemas, contas de serviço com elevação, consoles de nuvem e ambientes de produção), o MFA deve utilizar fatores de autenticação robustos (token físico, FIDO2 ou aplicativo autenticador com push notification), vedado o uso exclusivo de SMS como segundo fator, em conformidade com a Resolução BCB nº 538.

A parametrização de senha de rede e principais sistemas utilizados estão consonantes com as especificações mínimas:

Parâmetros	Requisitos Mínimos Vigentes
Tamanho mínimo	8 caracteres
Tempo máximo de expiração	90 (noventa) dias
Quantidade máxima de tentativas antes do bloqueio	3
Duração do desbloqueio	desbloqueio pelo administrador
Histórico mínimo de senhas utilizadas:	10
Complexidade	Ativada
Armazenamento das senhas criptografadas	Ativada

	TRUSTEE E BANVOX DTVM LTDA	Página 9 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

17 ACESSO REMOTO

Estabelece como diretriz a adoção de autenticação multifator (MFA) para todos os acessos remotos à rede corporativa, independentemente do método de conexão (VPN, RDP, SSH, console de nuvem). Todas as sessões de acesso remoto são registradas com trilha de auditoria completa, incluindo identificação do usuário, horário, origem da conexão e duração da sessão. Os controles serão documentados e mantidos à disposição do Compliance e do Banco Central do Brasil, em conformidade com a Resolução BCB nº 538.

- Acesso remoto para informações de negócio e recursos será concedido somente caso seja necessário, pelos departamentos de TI;
- A conexão de rede interna da empresa será feita utilizando uma autenticação de usuário diferente da autenticação utilizada na rede interna. Os métodos de autenticação incluem chaves dinâmicas de *software*, *tokens* (*smart cards*), e outras tecnologias aprovadas pela Diretora de Controles Internos;
- O processo de autenticação será totalmente encriptado. Nenhum processo de autenticação poderá ser feito através de uma conexão não segura;
- As conexões remotas são feitas através de *softwares* de conexão remota supervisionada, VPNs *clients*, bem como por acesso remoto supervisionado utilizando ferramentas específicas e validadas para esta atividade. Os registros de VPNs são mantidos com a área de TI e são rastreáveis.

18 GERENCIAMENTO DE INCIDENTES E DE SEGURANÇA DA INFORMAÇÃO

Os procedimentos operacionais de detecção, resposta, contenção, erradicação e comunicação de incidentes (incluindo os prazos regulatórios perante o BACEN e a ANPD) estão detalhados no Plano de Resposta a Incidentes (PRI), que é parte integrante do arcabouço normativo de Segurança da Informação.

- São considerados incidentes de segurança da informação e segurança cibernética todas as situações de ataques e de violação ou descumprimento dos controles de proteção de informações que coloquem em risco os dados, incluindo os dados pessoais, sistemas e equipamentos de TI fazendo-os ficar indisponíveis, ou funcionarem de maneira incorreta ou imprecisa ou possibilitando que sejam acessados por pessoas não autorizadas.
- Na ocasião da ocorrência de qualquer incidente, seja de segurança da informação ou cibernética, deverão ser imediatamente contatados e informados a Diretora de Controles Internos, a área de TI e o DPO.
- Os incidentes de Segurança da Informação ou Cibernética, são registrados na ferramenta utilizada para registro dos Incidentes de TI e direcionados ao Responsável pela Segurança da Informação e ao DPO.
- Será realizada análise de causa e impacto de todos os incidentes para as operações das Distribuidoras, conforme parâmetros disponíveis na documentação do processo. Serão realizadas melhorias contínuas no plano de gerenciamento de incidentes para garantir que ele esteja atualizado e eficaz.
- Os Incidentes de Segurança da Informação relacionados à segurança Cibernética são monitorados e registrados pela estrutura de SOC (Security Operations Center) mantida pelo Responsável pela Segurança da Informação. O SOC é responsável por monitorar, identificar anomalias e ataques e realizar o registro e acionamento do Responsável pela Segurança da Informação e Suporte de TI.
- Os incidentes de Segurança da Informação e Cibernéticos críticos são reportados à Diretoria.
- Os Incidentes de Segurança da Informação que expuserem dados dos clientes e ou do sistema financeiro nacional brasileiro, são direcionados para estrutura de Compliance e ao DPO. Deve ser estabelecido um fluxo de comunicação interna e externa para informar as áreas envolvidas, os dados afetados e as medidas de solução. A comunicação com clientes e autoridades competentes será realizada conforme exigido pela LGPD e demais normas aplicáveis.
- Empresas prestadoras de serviços considerados relevantes terão processos estabelecidos para gerenciamento de incidentes de Segurança da Informação e Cibernética. As Distribuidoras serão comunicadas e envolvidas no processo de resolução caso ocorram incidentes que impactem direta ou indiretamente suas informações ou de seus clientes.

	TRUSTEE E BANVOX DTVM LTDA	Página 10 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

19 GERENCIAMENTO DE MUDANÇAS

A fim de minimizar os riscos de indisponibilidade dos sistemas de informação desenvolvidos internamente ou através de terceiros, será observado o rígido controle para implementações de mudanças no ambiente de produção das Distribuidoras, devendo ser respeitado, para tanto, os seguintes controles, sem prejuízo de outros a serem aplicados.

- Antes da implementação de qualquer mudança que possa afetar dados pessoais, será realizada uma avaliação de impacto de proteção de dados (DPIA).
- O acesso ao ambiente de produção para instalação de *softwares* e implantação de mudanças está restrito a profissionais de infraestrutura e banco de dados.
- Registros de todas as mudanças implementadas serão mantidos e arquivados por um período adequado.
- Toda mudança será executada pela infraestrutura de TI seguindo estritamente o necessário para a manutenção da segurança e usabilidade idêntica a prévia mudança.

20 DESENVOLVIMENTO E MANUTENÇÕES DE SISTEMAS

- Os ambientes tecnológicos de desenvolvimento, homologação, e produção, bem como todos seus acessos, são segregados lógica e fisicamente.
- Não será permitido aos desenvolvedores acessarem os ambientes de produção, de forma que, apenas através do processo de gerência de mudanças, os programas desenvolvidos ou mantidos podem ser colocados em produção.
- A abertura e alteração dos programas fontes das aplicações apenas ocorrem nos ambientes de desenvolvimento e os programas fonte são sempre armazenados em bibliotecas controladas por versão.
- Em casos de desenvolvimento de *software* por terceiros, será elaborado um documento especificando os controles e requisitos mínimos aceitáveis de segurança e qualidade que o sistema irá conter, incluindo cláusulas de proteção de dados pessoais, propriedade dos direitos autorais e do código fonte.
- As Bases de dados que possuam dados de clientes e transações financeiras não podem ser armazenadas ou processadas em ambientes de nuvem que não sejam de acesso exclusivo a área de TI.
- Sistemas que possuam dados pessoais deverão ser analisados pelo DPO, para garantir que esses sistemas estejam em conformidade com a LGPD e com as políticas internas de proteção de dados pessoais.

No desenvolvimento e manutenção de sistemas, todas as bibliotecas e dependências de terceiros (incluindo componentes open-source) utilizadas nos projetos das Distribuidoras deverão passar por análise de segurança antes de sua incorporação ao código. A análise incluirá:

- Verificação de vulnerabilidades conhecidas em bases públicas (CVE/NVD);
- Avaliação da maturidade e suporte ativo do projeto open-source;
- Validação de licenciamento compatível; e
- Monitoramento contínuo de novas vulnerabilidades após a adoção. As APIs de parceiros integradas aos sistemas críticos também entram no escopo de revisão periódica de segurança, devendo ser submetidas a testes de segurança antes da integração e reavaliadas a cada atualização relevante, em conformidade com a Resolução BCB nº 538/2025.

21 CÓPIA DE SEGURANÇA DE DADOS E SISTEMAS (BACKUP)

- Todas as mídias e meios de backup são permanecidas em ambiente seguro, evitando o acesso indevido, a destruição ou o extravio físico ou lógico destes dados, inviabilizando a recuperação deles.
- O prazo máximo de retenção das cópias de segurança será definido em política específica, que estabelecerá procedimentos para a destruição física ou a exclusão segura dos dados, objetivando ainda a minimização da coleta e do armazenamento excessivo de dados.
- As mídias e meios de backup serão adequadamente identificados e o acesso e utilização do conteúdo destas mídias será aprovado pela infraestrutura de TI.
- A recuperação de informações (quaisquer que sejam: módulos de sistemas, tabelas de parâmetros, scripts, bancos de dados, arquivos da rede etc.) baseadas em cópias de segurança backup somente pode ser executada pela infraestrutura de TI.
- As informações serão objeto de backup diário com o uso de computação na nuvem.

	TRUSTEE E BANVOX DTVM LTDA	Página 11 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

22 GESTÃO DE CONTINUIDADE

As diretrizes estratégicas, a estrutura do Comitê de Gestão de Crises (CGC) e os procedimentos de contingência para garantir a resiliência operacional estão documentados no Plano de Continuidade de Negócios (PCN) e no Plano de Recuperação de Desastres (PRD).

As Distribuidoras manterão um Plano de Continuidade de Negócios (PCN) abrangente, atual, viável, que atenda minimamente aos seguintes controles:

- a) No Plano de Continuidade de Negócios serão endereçadas medidas para tratar da maior parte dos incidentes e desastres que possuírem alta probabilidade e alto impacto sobre as operações de negócio da empresa, incluindo incidentes de segurança da informação e cibernéticos;
- b) O PCN deverá contemplar a salvaguarda e recuperação tempestiva dos principais equipamentos, serviços, sistemas, *softwares*, dados, instalações, recursos e informações utilizados nas operações de negócio, assegurando a apropriada integridade e disponibilidade destes recursos;
- c) A Infraestrutura de TI em conjunto com o responsável pela Segurança da Informação planejará, implementará e manterá operando todas as estruturas e recursos de contingência necessários para continuar e recuperar as operações de negócio, conforme definido no PCN, em situações de desastres, sejam estes decorrentes de causas naturais, sociais, ambientais, tecnológicas, cibernéticas ou de outras naturezas; e
- d) Medidas de segurança de dados pessoais serão tomadas para garantir a proteção de dados pessoais durante a recuperação de desastres e incidentes, incluindo o backup de dados e mecanismos de criptografia.

23 CONTROLES SOBRE SOFTWARES E COMPUTADORES

- a) Todo colaborador possuirá uma identificação de usuário (login) e uma senha para acesso aos equipamentos, *softwares* e sistemas que utiliza.
- b) Por padrão todos os computadores contêm *softwares* de proteção contra ameaças cibernéticas (ex: antivírus) sendo que estes são atualizados automaticamente e não são desabilitados pelos usuários.
- c) Os *softwares* e sistemas utilizados devem ser legítimos e licenciados, evitando riscos de segurança, penalizações legais e danos à imagem da empresa.
- d) Caso necessário, para a instalação de programas adicionais aos *softwares* padrão, será registrado uma solicitação específica para o TI realizar a análise da necessidade, após a prévia autorização do superior direto do colaborador, o Responsável pela Segurança da Informação analisar os riscos e os efeitos dos *softwares* e sistemas novos.
- e) Todos os equipamentos estão configurados para garantir que no máximo após 3 minutos sem utilização sejam ativados mecanismos automáticos de bloqueio da estação de trabalho (*screen saver/ lock workstation*), sendo exigida nova autenticação na rede para desbloqueio.
- f) Todas as unidades de disquetes, conexões de pen-drive e HD externo em portas USB, gravadores de CD/DVD são desabilitadas nos equipamentos, de forma a impedir que usuários utilizem dispositivos de armazenamento externo que possam trazer vírus ou scripts maliciosos para dentro da intranet da empresa ou mesmo serem utilizados para transportar arquivos de dados para fora da empresa, os pedidos de liberação das portas dos equipamentos são autorizadas e aprovadas pelo Responsável pela Segurança da Informação e pelo Diretor do Colaborador.
- g) Nenhum tipo de arquivo, base de dados ou sistema será armazenado ou permanecer nos discos locais dos equipamentos de TI disponibilizados aos usuários.
- h) A Infraestrutura de TI é responsável por manter e disponibilizar na rede da empresa, locais para armazenamento de arquivos. O objetivo é garantir o armazenamento dos documentos adequados nas respectivas unidades de rede e não no disco local das estações de trabalho dos usuários.

	TRUSTEE E BANVOX DTVM LTDA	Página 12 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

24 GERENCIAMENTO DE FIREWALL E VULNERABILIDADES

- a) As regras e configurações de *firewall* são direcionadas para negar por padrão (*default deny*) o acesso externo a qualquer rede ou subrede da empresa. Com essa estratégia, os protocolos que podem passar pelo *firewall* e os *hosts* que podem transmitir dados será previamente especificado e aprovado pelo Responsável pela Segurança da Informação e Infraestrutura de TI.
- b) São criados segmentos de rede separados e com acesso restrito chamados de *DMZ*, para servidores e equipamentos que necessitem ser acessados externamente do ambiente de TI da empresa.
- c) É de responsabilidade da Infraestrutura de TI, quando identificar a necessidade de nova regra ou alguma alteração em regra existente nos equipamentos de segurança de TI, efetuar o registro e seguir o processo de gerenciamento de mudança definido.
- d) Devem ser realizadas periodicamente a varredura e a análise das vulnerabilidades do ambiente de TI incluindo as configurações dos equipamentos de segurança de perímetro reportando as vulnerabilidades que existirem, para que sejam corrigidas pela infraestrutura de TI.
- e) Será realizado, no mínimo uma vez por ano, teste de intrusão (pentest) conduzido por empresa ou profissional independente, com escopo abrangendo a infraestrutura de rede, aplicações web, APIs expostas e ambientes de nuvem. Os resultados do pentest, incluindo vulnerabilidades identificadas, classificação de risco (CVSS) e planos de ação para mitigação, serão formalmente documentados e apresentados à Diretoria e ao Compliance. As evidências do teste, os relatórios e os registros de remediação serão retidos por, no mínimo, 5 (cinco) anos à disposição do Banco Central do Brasil, em conformidade com a Resolução BCB nº 538/2025.
- f) Apenas servidores e equipamentos protegidos por soluções de *firewall* e de segurança são apontados ou com endereço IP publicados na Internet.
- g) Os ambientes de computação em nuvem utilizados devem possuir recursos de *Firewall* para proteção, monitoração e restrição do acesso.
- h) Os logs de Firewalls, IDS, IPS e outros equipamentos de segurança de TI e proteção do perímetro de TI são configurados e ativados para serem coletados, conforme as definições e recomendações de Segurança da Informação e de Infraestrutura de TI. Estes arquivos de LOG são armazenados em locais externos aos equipamentos, são retidos por um mínimo de 90 dias para fins operacionais. Adicionalmente, as evidências de testes de intrusão, planos de ação de remediação de vulnerabilidades, relatórios de Threat Intelligence e registros de incidentes cibernéticos serão retidos por, no mínimo, 5 (cinco) anos à disposição do Banco Central do Brasil, conforme Resolução BCB nº 538/2025 e qualquer acesso a estes arquivos são autorizados pelo Responsável pela Segurança da Informação.
- i) Estabelecer como diretriz a manutenção de processo de Inteligência Cibernética (Threat Intelligence), contemplando o monitoramento proativo de ameaças em ambientes como a deep web e a dark web, fóruns de cibercriminosos e feeds de indicadores de comprometimento (IoC). O processo será conduzido pelo Responsável pela Segurança da Informação, com apoio da estrutura de SOC, e contemplará: (i) coleta e correlação de IoCs relevantes ao setor financeiro; (ii) alertas sobre campanhas de ataque direcionadas a DTVMs; (iii) atualização das regras de bloqueio em firewalls e endpoints; e (iv) reporte periódico de ameaças à Diretoria. Os controles e evidências relacionados a este processo serão documentados e mantidos à disposição do Compliance e do Banco Central do Brasil, em conformidade com a Resolução BCB nº 538/2025.

25 GESTÃO DE CERTIFICADOS DIGITAIS

As Distribuidoras manterão processo formal de gestão do ciclo de vida de certificados digitais, abrangendo todos os certificados utilizados em comunicações seguras (TLS/SSL), assinatura digital de documentos, autenticação de servidores e integração com infraestruturas do mercado financeiro (B3, RTM, BACEN). O processo incluirá:

- a) Inventário centralizado de todos os certificados digitais em uso, com registro de emissor (CA), data de emissão, data de expiração, sistema/serviço associado e responsável técnico;
- b) Alertas automáticos de renovação com antecedência mínima de 60 dias antes do vencimento, evitando interrupções de serviço por certificados expirados;
- c) Procedimento de revogação imediata em caso de comprometimento de chave privada, com comunicação ao Gerente de Segurança da Informação e registro no PRI;
- d) Armazenamento seguro das chaves privadas em módulos de segurança de hardware (HSM) ou cofres de chaves gerenciados (AWS KMS), com acesso restrito e auditável;
- e) Revisão semestral do inventário de certificados pelo Gerente de Infraestrutura, com relatório ao Compliance; e
- f) Este controle atende ao requisito mínimo de gestão de certificados digitais estabelecido pela Resolução BCB nº 538/2025.

	TRUSTEE E BANVOX DTVM LTDA	Página 13 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

26 LICENCIAMENTO DE SOFTWARE E MANUTENÇÃO DE INVENTÁRIO

- É propriedade das Distribuidoras todo programa de computador ou *software* desenvolvido ou mantido por funcionários, terceiros ou prestadores de serviço contratados, aplicando-se integralmente os termos da lei 9.609 – Lei de *Software*.
- Todo programa de computador, banco de dados, sistema operacional ou utilitários só pode ser instalado ou removido pelo suporte técnico de TI ou por pessoas autorizadas.
- Somente podem ser instalados nas estações de trabalho *softwares* homologados pela TI.
- A Infraestrutura de TI garante que todos os *softwares* instalados nos computadores estejam devidamente licenciados, sendo proibida a prática de pirataria.
- Não é permitida a instalação de *softwares* que degradem a performance ou comprometam a integridade dos equipamentos.
- Os sistemas operacionais e os aplicativos instalados nos computadores estão com as correções e atualizações dos fabricantes (*service pack ou service release*) instalados e atualizados, após homologados e aprovados em produção em conformidade com o procedimento de atualização de *patch* vigente.
- A área de TI mantém um inventário de *hardware* e *software* atualizado e mantém o registro de atualizações deste inventário para verificação, quando solicitado pelo Responsável pela Segurança da Informação.

27 MONITORAMENTO DE AMBIENTES

As Distribuidoras possuem mecanismos para monitorar servidores críticos e sua infraestrutura de rede. Caso seja detectado algum alerta de desempenho ou falha na capacidade e disponibilidade do ambiente, a equipe de infraestrutura da TI e o grupo de resposta a incidente analisa as causas e toma as devidas providências para solucionar ou minimizar tais problemas.

Ademais, a equipe de infraestrutura de TI deve manter registros atualizados de todas as atividades de monitoramento realizadas, incluindo os alertas identificados, as análises de causas e as providências adotadas para solucionar os problemas detectados. Esses registros devem ser disponibilizados para consulta do Responsável pela Segurança da Informação, sempre que solicitado.

28 SEGURANÇA DE INFRAESTRUTURAS DO SFN

Caso as Distribuidoras mantenham conectividade direta ou indireta com a Rede do Sistema Financeiro Nacional (RSFN), o Sistema de Transferência de Reservas (STR), o Sistema de Pagamentos Instantâneos (Pix) ou outros sistemas operados pelo Banco Central do Brasil, os seguintes controles adicionais serão observados:

- Isolamento lógico e físico dos ambientes que processam transações RSFN/STR/Pix em relação à rede corporativa geral, com segmentação de rede dedicada e firewalls específicos;
- Monitoramento contínuo e em tempo real das credenciais de acesso às infraestruturas do SFN, com alertas automáticos para tentativas de acesso não autorizado;
- Vedação expressa de acesso de terceiros (incluindo prestadores de serviço de TI) às chaves privadas utilizadas para autenticação e assinatura de mensagens nas infraestruturas do SFN, exceto em situações de manutenção emergencial com dupla custódia e registro formal;
- Armazenamento das chaves criptográficas em HSM (Hardware Security Module) certificado, com controle de acesso por dupla custódia e logs de auditoria imutáveis; e
- Testes periódicos de contingência da conectividade RSFN/STR, em conformidade com os calendários de testes estabelecidos pelo Banco Central do Brasil.

Caso não possua conectividade direta com RSFN/Pix/STR, este item será registrado como 'não aplicável' na próxima revisão anual, com justificativa formal aprovada pela Diretoria.

Estes controles atendem aos requisitos de segurança para participantes do SFN estabelecidos pela Resolução BCB nº 538/2025 e pelas normas operacionais do BACEN.

	TRUSTEE E BANVOX DTVM LTDA	Página 14 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

29 PROTEÇÃO DE DADOS PESSOAIS

A categorização das informações e os controles específicos aplicáveis aos dados sensíveis estão definidos na Política de Classificação de Dados. A governança e o atendimento aos direitos dos titulares são apoiados pelo Encarregado de Proteção de Dados Pessoais (DPO).

As Distribuidoras se comprometem a proteger os dados pessoais de seus colaboradores, clientes e terceiros em conformidade com as leis e regulamentações aplicáveis. Os dados pessoais incluem qualquer informação que possa ser utilizada para identificar uma pessoa.

Para proteger os dados pessoais, será implementado as seguintes medidas:

- a) Cumprir os princípios de proteção de dados pessoais, incluindo o tratamento de dados de forma lícita, justa e transparente, a limitação da finalidade do processamento, a garantia da exatidão dos dados e a manutenção da segurança dos dados;
- b) Implementar controles de acesso aos dados pessoais, garantindo que somente os colaboradores autorizados tenham acesso aos dados pessoais. Esses controles incluem a utilização de senhas fortes, autenticação de dois fatores e permissões de acesso baseadas em funções;
- c) Monitorar e detectar possíveis incidentes de segurança que possam afetar os dados pessoais. Caso um incidente seja detectado, segue os procedimentos de resposta a incidentes para mitigar os efeitos do incidente e notificar as partes afetadas;
- d) Fornecer treinamento e conscientização aos colaboradores sobre a proteção de dados pessoais; e
- e) Avaliar seus fornecedores e parceiros em relação às práticas de privacidade de dados antes de compartilhar dados pessoais com eles. Os fornecedores e parceiros são obrigados a seguir as mesmas políticas de segurança da informação e proteção de dados pessoais.

As Distribuidoras estão comprometidas em proteger os dados pessoais de seus colaboradores, clientes e terceiros e continuará a revisar e atualizar suas práticas de segurança da informação para atender aos padrões de privacidade de dados em constante evolução.

30 AUDITORIA E CONFORMIDADE

A efetividade da Política é verificada por meio de avaliações periódicas de auditoria, onde é abordado aspectos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade na segurança física e lógica.

31 GESTÃO DE CONSEQUÊNCIAS

O Colaborador que violar as regras desta Política ou dos controles relacionados a ela, comete um Incidente de Segurança da Informação podendo ser advertido formalmente e, eventualmente, penalizado.

32 PAPÉIS E RESPONSABILIDADES

• COMITÊ DA DIRETORIA EXECUTIVA

- a) Aprovar a Política e prover recursos necessários para execução das diretrizes previstas.
- b) Disseminar a cultura de segurança da informação e cibernética entre os colaboradores e terceiros, conforme aplicável, inclusive por meio da adoção de programas periódicos de capacitação.
- c) Comprometer-se a melhorar continuamente os controles e procedimentos relacionados à segurança cibernética descritos nesta Política.

	TRUSTEE E BANVOX DTVM LTDA	Página 15 / 15
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA		Versão: 05 Código de Acesso TEC.002

- **TECNOLOGIA DA INFORMAÇÃO**

- Implementar e configurar sistemas de acordo com os padrões de segurança aprovados.
- Testar e implementar as modificações técnicas aos sistemas da rede.
- Manter documentação de GMUDs (gerenciamento de mudanças), de configuração e implementações aos sistemas ou serviços na rede.
- Gerenciar pedidos de acesso de concessão, término ou mudança de direitos de acesso a rede e recursos da rede.
- Relatar qualquer evento descoberto que possa comprometer a segurança da informação ao Compliance.

- **SEGURANÇA DA INFORMAÇÃO**

- A administração do *Compliance* e TI é organizada sob diferentes níveis hierárquicos de gerenciamento;
- Não existirá um único administrador para qualquer sistema ou aplicação. No mínimo, controle duplo ou, tratando-se de sistemas operacionais, administradores primários e backup são estabelecidos; e
- Para manter a correta separação de interesses, *Compliance* não terá responsabilidade operacional nos sistemas operacionais (ex: atualização de um sistema, mudanças de configuração, aplicação de atualizações etc.). Qualquer parte, tanto interna como externa, que gerencia ou mantém um sistema, não pode ser responsável por auditar o mesmo sistema.

- **COMPLIANCE**

- Definir e manter as políticas corporativas de segurança da informação, seus procedimentos e padrões.
- Supervisionar a implementação das políticas corporativas de segurança da informação, procedimentos e padrões previstos na presente Política.
- Monitorar e relatar a Diretoria, periodicamente, aderência às políticas, procedimentos e padrões da Política.
- Monitorar periodicamente a aderência às regulamentações dos órgãos reguladores.
- Avaliar periodicamente os processos de concessão, término ou mudança de direitos de acesso à rede e aplicações críticas, garantindo que as autorizações sejam realizadas pelos respectivos Gestores das Áreas (Data Owners).
- Monitorar a conformidade regulatória dos processos de desenvolvimento, manutenção e testes do Plano de Continuidade de Negócios (PCN).

- **COLABORADORES**

- Cumprir integralmente com as diretrizes dispostas nesta Política.