BB TECNOLOGIA E SERVIÇOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

POL600 v.15

1. ÁREA(S) RESPONSÁVEL(IS)

1.1. Governança da I&T: Gerência de Governança Digital - Dites/Geati/Govit
1.2. Segurança da Informação: Gerência de Serviços e de Segurança Cibernética e Produtos Digitais – Dites/Gesec

2. ABRANGÊNCIA

2.1 Esta política orienta o comportamento da BB Tecnologia e Serviços, considerando as necessidades específicas e os aspectos legais e regulamentares a que a BBTS está sujeita.

3. OBJETIVO

3.1. Esta política tem por objetivo estabelecer princípios e diretrizes a serem observados no tratamento e proteção de informações corporativas e do ambiente cibernético da companhia.
3.2. Fornecer insumos para a elaboração de Normas Internas, Procedimentos, Processos e demais documentos para a otimização do uso de recursos, aprimorar a qualidade dos serviços e permitir a condução exitosa de respostas a incidentes de segurança da informação e cibernéticos, bem como a recuperação em casos de desastres.

4. REGULAMENTAÇÃO

4.1. Resolução CGPAR nº 41, de 4 de agosto de 2022.
4.2. Lei Nº13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD).

5. PERIODICIDADE DE REVISÃO

5.1. A Política de Segurança da Informação deve ser revisada no prazo mínimo de 01 ano ou, extraordinariamente, a qualquer tempo.

6. CONCEITOS

6.1. Para a construção desta política foram utilizadas as seguintes referências:

6.1.1. Resolução CGPAR nº 41, de 4 de agosto de 2022

6.1.2. ABNT NBR ISO/IEC 27001:2022 – Sistemas de gestão da segurança da informação – Requisitos.

6.1.3. ABNT NBR ISO/IEC 27002:2022 – Código de prática para controles de segurança da informação.

6.1.4. Norma complementar 03/IN01/DSIC/GSIPR (Gabinete de Segurança Institucional da Presidência da República) – Diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

6.1.5. Decreto Nº 9.637, de 26 de dezembro de 2018 - Política Nacional de Segurança da Informação.

6.1.6. Lei Nº13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD).

6.1.7. Decreto N° 10.222, de 5 de FEVEREIRO de 2020 - Estratégia Nacional de Segurança Cibernética – E- Cyber.

6.1.8. Resolução CMN 4.893/21 – 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, as quais a BBTS não faz parte. Sendo assim, seu uso como referência da concepção desta política tem a finalidade de reconhecer sua importância e aprimorar nossa segurança da informação e cibernética.

6.1.9. Decreto 11.586/23 Política Nacional de Segurança Cibernética

6.2. **Atributos da informação:** são os pilares que sustentam a segurança da informação, sendo estes a confidencialidade, integridade, disponibilidade e autenticidade;

6.2.1. Autenticidade: assegura que os dados permaneçam precisos, completos e não sejam alterados indevidamente.

6.2.2. Confidencialidade: assegura que os dados permaneçam precisos, completos e não sejam alterados indevidamente.

6.2.3. Disponibilidade: assegura que os dados permaneçam precisos, completos e não sejam alterados indevidamente.

6.2.4. Integridade: assegura que os dados permaneçam precisos, completos e não sejam alterados indevidamente.

6.3. **Dado Pessoal:** é qualquer informação relacionada a pessoa natural identificada ou identificável;

6.4. **Privacidade:** Se refere a vida privada, intimidade e o direito de manter reservadas as informações pessoais;

6.5. **Segurança Cibernética:** conjunto de ações que trata de aspectos da operacionalização de recursos para a segurança da informação para a proteção contra-ataques cibernéticos;

6.6. **Zero Trust:** é uma estratégia a ser perseguida pela segurança da informação, seus princípios são direcionados a garantir que a rede não será acessada por nenhuma pessoa ou dispositivo sem que seja considerado e validado como confiável. Também considera que toda tentativa de acesso é considerada uma ameaça, até ser identificada e validada.

7. ENUNCIADO

7.1. Tratamos a informação, na gestão empresarial, como ativo e, portanto, deve ser amplamente protegida, a partir de práticas e políticas que garantam a sua autenticidade, confidencialidade, integridade e disponibilidade;

7.2. Alinhamos a gestão da segurança da informação e da segurança cibernética aos objetivos da empresa, colaborando para um ambiente seguro, estável e confiável para a realização de negócios;

7.3. Sem prejuízo das condições contratuais e das condutas de boas práticas esperadas, entendemos que todos os dados fornecidos, tratados e armazenados de nossos clientes, fornecedores e parceiros, sejam pautados sobre a ética e que sua confidencialidade seja preservada durante todo ciclo de vida da informação;

7.4. Entendemos que nossos clientes, fornecedores e parceiros, devam estabelecer em suas organizações ações direcionadas a garantia da confidencialidade, integridade, disponibilidade e ética, sobre todas as informações por eles tratadas.

7.5. Controlamos e identificamos o acesso às informações por meio da individualização da autorização de acesso para cada usuário, tornando este o responsável pela segurança, confidencialidade e privacidade das informações que estejam sob sua custódia, ou que venha a conhecer, e por todos os atos executados com suas identificações;

7.6. Autorizamos e concedemos aos solicitantes o acesso e uso, somente das informações necessárias ao desempenho de suas funções e atribuições ou por determinação legal;

7.7. Tratamos as informações geradas, adquiridas e/ou custodiadas pela BB Tecnologia e Serviços de modo a garantir que os atributos de confidencialidade, integridade e disponibilidade estejam presentes em todo o seu ciclo de vida: coleta, produção, manuseio, reprodução (cópia), compartilhamento, transporte, transmissão, armazenamento, descarte ou restauração;

7.8. Classificamos e rotulamos as informações, garantindo a confidencialidade, integridade e disponibilidade, aplicando proteção de forma compatível com sua criticidade para as atividades e alcançando todos os processos, inclusive aqueles que tratam dados pessoais, informatizados ou não;

7.9. Estabelecemos Gestão de Riscos de Segurança da Informação, Segurança Cibernética e Continuidade dos Negócios, identificando e corrigindo as vulnerabilidades, ameaças e os riscos que possam envolver nossos ativos de informação e ambientes tecnológicos, inclusive na rede de comunicação de dados e computação em Nuvem *(Cloud Computing);*

7.10. Temos o compromisso de manter o parque tecnológico preservado e protegido, dentro das melhores práticas de segurança física e tecnológica. Os acessos aos ambientes físicos da Empresa, são controlados e concedidos somente a pessoas autorizadas, com especial atenção para aos ambientes onde ocorre o tratamento de informações;

7.11. Mantemos um plano de comunicação e tratamento de incidentes cibernéticos, de modo que reflitam as ações estritamente necessárias a resposta de um incidente cibernético identificado;

7.12. Disseminamos a cultura de segurança da informação e Cibernética, por meio de programa permanente de sensibilização, conscientização e capacitação voltado aos empregados, colaboradores, fornecedores, terceiros, parceiros, contratados, estagiários e qualquer pessoa física ou jurídica que tenha relacionamento com a empresa;

7.13. Analisamos as ocorrências de tratamento indevido de informações corporativas, sob os aspectos legal e disciplinar vigentes, imputando responsabilização. Sob o aspecto técnico, utilizamos ferramentas de proteção contra ameaças cibernéticas;

7.14. Investimos em mecanismos de proteção, monitoração, resposta e recuperação de riscos cibernéticos;

7.15. Nos preocupamos com a resiliência cibernética para que haja as devidas tratativas, na ocorrência de um incidente cibernético ou potencial ameaça cibernética;

7.16. Prezamos pelo uso consciente da inteligência de ameaças, recebendo e transmitindo informações relacionadas a vulnerabilidades e ameaças não identificadas anteriormente;

7.17. Entendemos que o uso da IA deve ser responsável, pautado na ética e com governabilidade, de modo que haja proteção ao sigilo da informação, assim como a manutenção da conformidade interna e externa;

7.18. Fortalecemos e melhoramos nossos controles de segurança da informação e cibernética, através do conhecimento adquirido no reconhecimento e na resposta aos incidentes registrados;

7.19. Mantemos nossos ambientes físicos controlados, monitorados e protegidos;

7.20. Encorajamos nossos colaboradores a adotarem a política da mesa limpa, de modo que dados importantes não sejam expostos;

7.21. Compreendemos a importância da gestão de risco cibernético na cadeia de suprimentos, para tanto empenhamos esforços para adotar as melhores práticas, direcionadas a aprimorar a resiliência cibernética.
7.22. Direcionamos nossas ações para conquistarmos o *zero trust*, investindo em tecnologia e acompanhando as tendências de mercado;
7.23. Buscamos desenvolver nossas soluções de maneira segura, durante todo ciclo de vida desta;
7.24. Realizamos o tratamento das informações de modo ético e responsável, aplicando a elas as normas, políticas, legislações vigentes e as boas práticas reconhecidas por entidades de controle interno e externos;

8. APROVAÇÃO

8.1. Mediante Nota Técnica 2025/0380, esta política foi apreciada pela Diretoria Executiva em 21/07/2025, aprovada pelo Conselho de Administração (Conad) da BBTS na data de 31/07/2025 e pelo Conselho Fiscal (Cofis) da BBTS na data de 12/08/2025.