BB TECNOLOGIA E SERVIÇOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

POL600 v.13

1. ÁREA RESPONSÁVEL

1.1. Gerência de Segurança Digital e Governança da Informação e Tecnologia – Geseg.

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 11, de 10 de maio de 2016.

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

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

4.4. 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.

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

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

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

4.8. 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.

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. **Atributos da informação:** Confidencialidade, Integridade, Disponibilidade e Autenticidade.

6.2. **Autenticidade:** Característica, particularidade ou estado do que é autêntico. Natureza daquilo que é real ou verdadeiro.

6.3. **Confidencialidade:** assegurar que a informação será acessível somente por quem tem autorização de acesso.

6.4. **Disponibilidade:** assegurar que usuários autorizados tenham acesso às informações e aos recursos associados, quando requeridos.

6.5. **Integridade:** assegurar que a informação não foi alterada durante seu processo de transporte e armazenamento.

6.6. **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável.

6.7. **Privacidade:** Vida privada, intimidade, direito à reserva de informações pessoais e da própria vida privada.

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

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 integridade, confidencialidade 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. Preservamos nossos requisitos de segurança da informação e de segurança cibernética na aquisição de produtos, contratação de serviços ou pessoas e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários e demais pessoas físicas ou jurídicas que tenham relacionamento com a empresa.

7.4. 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.

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 as informações quanto à 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, as ameaças e os riscos que envolvem os ativos de informação e os 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. Adotamos ações, mecanismos ou medidas voltadas à comunicação de ataques cibernéticos e de ações maliciosas de acordo com o Plano de Resposta a Incidentes.

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 e estagiários e demais pessoas físicas ou jurídicas que tenham 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.

8. APROVAÇÃO

8.1. Mediante Nota Técnica 2023/0319, esta política foi apreciada pela Diretoria Executiva em 22/06/2023 e aprovada pelo Conselho de Administração (Conad) da BBTS na data de 30/06/2023.