POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

Título	Código	Área de Emissão	Data da Emissão	Versão
Política de Segurança da Informação Cibernética	POL-SI-001	Tecnologia da Informação	02/10/2025	4.0

Título	Código	Área de Emissão	Data de Emissão	Versão
Política de Segurança da Informação Cibernética	POL-SI-001	Tecnologia da Informação	02/10/2025	4.0

SUMÁRIO

1.INTRODUÇÃO **5**

2.OBJETIVO **5**

3.DOCUMENTOS DE REFERÊNCIA **5**

5. DEFINIÇÕES **6**

6.PAPÉIS E RESPONSABILIDADES **7**

6.1. Diretoria **7**

6.2. Tecnologia da Informação **7**

6.3.Controles Internos **7**

7. ESCOPO7

7.1. Arquitetura da Segurança **7**

7.1.1. Política de Segurança da Informação **7**

7.1.2. Controles de Segurança de Informações **8**

7.1.3. Padrões, Diretrizes e Procedimentos de Segurança de Informações **8**

7.2. Terminologia e Conceitos de Segurança da Informação **8**

7.3. Procedimento de Exceções à Política **9**

8. DIRETRIZES **9**

8.1. Diretrizes Gerais **9**

8.2. Organização **10**

8.2.1. Gestão da Segurança da Informação **10**

8.2.2. Cooperação com Terceiros (Parcerias, Joint Ventures, Fornecedores, Contratados) **10**

8.2.3. Outsourcing de Atividades da B&T para Terceiros **11**

8.2.4. Níveis de Segurança **11**

8.2.5. Criação de serviço **11**

8.2.6. Contratos **12**

8.3. Classificação **12**

8.3.1. Propriedade **12**

8.3.2. Classificação da Informação 12

8.3.3. Salvaguarda de Registros da Sociedade 13

8.4. Segurança dos Colaboradores 14

8.4.1. Segurança no Trabalho – Definição e Recursos 14

8.4.1.1. Triagem de Colaboradores 14

8.4.1.2. Termos e Condições de Emprego 14

8.4.1.3. Acordos de Confidencialidade 14

8.4.1.4. Segurança nas Descrições dos Cargos 15

8.4.1.5. Código de Conduta 15

8.4.1.6. Encerramento de Contrato de Emprego 15

8.4.1.7. Segregação de Funções 15

8.4.1.8. Nível de Autorização de cargo 15

8.4.2. Educação, Treinamento e Conscientização 16

8.4.3. Notificando Incidentes de Segurança 16

8.4.3.1. Notificando Fragilidades na Segurança 16

8.5. Segurança Física e do Ambiente 16

8.6. Segurança de rede 17

8.6.1. As Redes da B&T 17

8.6.2. Conexões com Internet Pública 18

8.6.3. Conexões de Terceiro 18

8.6.4. Acesso remoto 19

8.7. Segurança do Host / Sistema 20

8.7.1 Medidas Gerais de Segurança 20

8.7.2. Identificação e Autenticação 20

8.7.3. Autorização 21

8.7.4. Administração de Segurança 21

8.7.5. Gestão de Sistema 21

8.7.6. Registrando, Monitorando, Relatando e Auditando 22

8.7.7. Backup e Recuperação 23

8.7.8. Proteção antivírus 23

8.7.9. Computação Móvel e Teletrabalho 25

8.7.10. Confiabilidade de Estações de Trabalho 26

8.8. Segurança de Aplicativos e Dados 27

8.8.1. Aplicativos de Negócios da B&T 27

8.8.2. Aplicativos de Clientes 28

8.8.2.1. Requisitos de Segurança em Aplicativos de Clientes 28

8.8.2.2. Ambientes de Teste e de Produção 28

8.9. Serviços Genéricos da B&T 28

8.9.1. Correio Eletrônico 28

8.9.2. Intranet da B&T 29

8.9.3. Web Externa da B&T 30

8.10. Gestão de Continuidade do Negócio 30

8.11. Segurança em Cloud Computing (Nuvem) 30

8.11.1. Acordos de Níveis de Serviço (SLA) 31

8.11.2. Proteção de Dados Pessoais 31

8.11.3. Documentações de Manuais de Procedimentos 31

8.11.4. Garantir a Conformidade em Nuvem 31

8.12. Conformidade 32

8.12.1. Conformidade com a Política de Segurança 32

8.12.2. Conformidade com Requisitos Legais 32

8.12.3. Verificação de Conformidade 33

9. DISPOSIÇÕES FINAIS 33

10. HISTÓRICO DE VERSÕES 34

1.INTRODUÇÃO

Em atendimento à exigência estipulada pelo Conselho Monetário Nacional o Banco Central do Brasil através da Resolução nº 4.893 estabeleceu que as Instituições Financeiras e demais Instituições autorizadas a funcionar pelo Banco Central do Brasil devem implementar política de segurança cibernética estabelecendo diretrizes de forma a assegurar a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informações utilizados. Em janeiro de 2024, a mencionada Resolução passou a não mais se aplicar a corretoras de câmbio, e a Resolução nº 85 foi alterada para incluí-las.

A presente Política de Segurança da Informação estabelece as diretrizes da **B&T CORRETORA** e **B&T CÂMBIO** (**B&T**) para segurança das informações de sua propriedade e/ou sob sua guarda. Esta política considera o porte, o perfil de risco e o modelo de negócios, uma vez que a B&T está enquadrada como segmento **S5** junto ao órgão regulador desde julho de 2024, tem seu risco institucional definido na Avaliação Interna de Risco e seu modelo de negócio atualmente é voltado majoritariamente para intermediação de negócios e sem correspondentes cambiais enquadrados no inciso i) da Circular CMN 4.935/2021.

2.OBJETIVO

O objetivo deste documento é estabelecer os padrões e regras necessárias para a elaboração dos controles e dos documentos referentes a Segurança da Informação da **B&T**, assegurar a continuidade do negócio e minimizar danos causados pelo impacto de incidentes de segurança, além de proteger os ativos de Informação da **B&T** e seus respectivos clientes, conforme firmado em contrato, contra todas as ameaças, sejam elas internas ou externas, propositais ou acidentais.

3.DOCUMENTOS DE REFERÊNCIA

- Resolução nº **85,** de 08 de abril de 2021, do Banco Central do Brasil;
- ISO 27001
- ISO 27002
- Normativos internos

4. APLICABILIDADE

A observância e cumprimento desta Política e suas respectivas Normas é aplicável a todos os empregados, estagiários, menor aprendizes, sócios e diretores, prestadores de serviços, auditores, terceirizados, fornecedores, parceiros de negócios, correspondentes cambiais, consultores e todos os demais responsável pela Segurança de Informações dentro da instituição, os quais, para efeito desta Política serão denominados como “Usuários”.

Política ou Norma	Localização
PSI 001 - Política de Segurança da Informação	Engage Treinamentos
PSI 002 - Política de Classificação da Informação	Engage Treinamentos
NSI 002 - Norma de Segurança em Recursos Humanos	Engage Treinamentos
NSI 003 - Norma de Segurança Física e do Ambiente	Engage Treinamentos
NSI 004 - Norma de Gestão das Operações e Comunicações	Engage Treinamentos
NSI 007 - Norma de Tratamento de Incidentes em Segurança da Informação	Engage Treinamentos
NSI 009 - Norma de Conformidade em Segurança	Engage Treinamentos
NSI 010 - Norma de Segurança no Acesso de Usuários	Engage Treinamentos
NSI 011 - Norma de Segurança de Rede	Engage Treinamentos
NSI 013 - Norma de Segurança da Internet	Engage Treinamentos
NSI 015 – Norma de Segurança de Acesso Físico	Engage Treinamentos
NSI 016 – Norma de Tratamento de Dados	Engage Treinamentos

5. DEFINIÇÕES

Nesta Política todas as entidades de negócio dentro da **B&T** são chamadas de ‘departamento’ e os gestores que são responsáveis por elas são chamados de ‘gestão de linha’ (ou ‘gerentes de linha’).

6.PAPÉIS E RESPONSABILIDADES

6.1. Diretoria

A Diretoria da **B&T** é responsável pela aprovação da Política de Segurança da Informação Cibernética.

6.2. Tecnologia da Informação

É responsável pela gerência dos aspectos de segurança da informação e conta com a ajuda de organizações operacionais e de todos os colaboradores da **B&T**.

6.3 Controles Internos

É responsável por garantir a segurança e a organização de segurança dentro da **B&T** e por manter a Política de Segurança atualizada e em conformidade com as normas de regulatórias e as boas práticas de mercado.

7. ESCOPO

Esta política é mandatória para a segurança dos processos de negócio interno e externos (relacionados com o cliente) da **B&T**.

A política também é destinada a todas as formas intelectuais e físicas de ativos da informação tanto próprios, como usados ou mantidos em custódia pela **B&T**. Estas formas incluem *hardware*, redes, *software* e dados, tanto armazenados e processados em computadores, transmitidos através de redes, impressos ou escritos, enviados por fax, armazenados em mídias removíveis (por ex.: fitas, dispositivos de armazenamento conectados em interface USB) ou falados em conversas e ligações telefônicas ou postadas na Internet, como por exemplo em redes sociais, chats, *wikis* ou assemelhados.

7.1. Arquitetura da Segurança

Para permitir uma abordagem estruturada para a Segurança de Informações foi definida uma arquitetura em camadas. A estrutura consiste nos seguintes elementos:

7.1.1. Política de Segurança da Informação

Nesta política os objetivos globais de Segurança da Informação da **B&T** são definidos através de um conjunto de normas de segurança. A política demonstra o compromisso da

B&T com a Segurança de Informações. Deve ser vista como uma referência a todas as decisões relacionadas à segurança.

7.1.2. Controles de Segurança de Informações

Os controles de segurança consistem em um conjunto amplo de medidas de segurança, compreendendo práticas de segurança comuns, e são necessários para implementar a política de segurança da **B&T**. Os controles de segurança são baseados na norma de segurança aceita internacionalmente (ISO 27000, ISO 27001, ISO 27002, entre demais referências normativas e boas práticas de mercado).

7.1.3. Padrões, Diretrizes e Procedimentos de Segurança de Informações

Esta camada consiste em um conjunto de normas técnicas, procedimentos e diretrizes detalhadas para apoio adicional na implementação da política de segurança. Por exemplo: em uma plataforma específica ou em um serviço específico são descritos os passos para gestão de uma ferramenta de segurança.

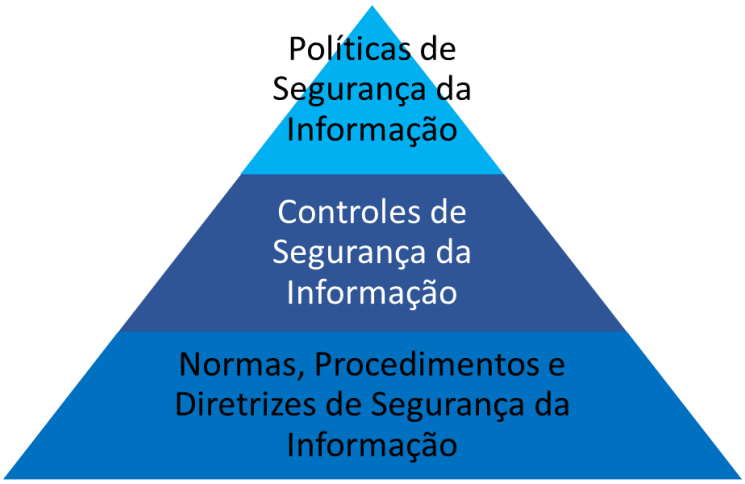


*Figura 1 - Arquitetura de Segurança da **B&T***

7.2. Terminologia e Conceitos de Segurança da Informação

A Segurança de Informações salvaguarda a confidencialidade, integridade, disponibilidade, autenticidade, legalidade e não-repúdio da informação e sistemas da informação. Estes aspectos têm o seguinte significado:

- **Confidencialidade**: A Informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados.

- **Integridade**: É compreendida por duas categorias:
  - Integridade de dados: Dados não são alterados ou destruídos de forma não autorizada.
  - Integridade de Sistemas: O sistema executa a sua função da maneira prevista, sem que haja manipulações deliberadas ou acidentais não autorizadas.
- **Disponibilidade**: Ativos que são acessíveis a partes autorizadas nos momentos apropriados.
- **Autenticidade:** É um processo que se estabelece a validade.
- **Legalidade:** A informação é armazenada, transmitida, acessada e retida de acordo com os termos legais existentes.
- **Não-repúdio:** São as partes envolvidas em uma transação que são capazes de provar, posteriormente, o que aconteceu.

7.3. Procedimento de Exceções à Política

Todos os itens descritos como "**deve**", "**devem**", "**deverão**" ou "**deverá**" são mandatórios e estão relacionados principalmente a requisitos estatutários ou mínimos. Itens rotulados como "**recomendável**" são vistos como boas práticas e normalmente **devem** ser cumpridos. Exceções não **devem** colocar em risco outras partes da **B&T,** seus clientes, fornecedores ou parceiros de negócio, e **devem** ser formalmente aprovadas conforme alçadas de risco.

8. DIRETRIZES

8.1. Diretrizes Gerais

A presente Política estabelece assegurar que:

- As informações serão protegidas contra acesso não-autorizado;
- A confidencialidade das informações será assegurada;
- A Integridade das informações será mantida;
- Requisitos do negócio quanto à disponibilidade da informação e sistemas serão atendidos;
- A Gestão de Risco será executada para identificar e avaliar riscos de segurança para que medidas apropriadas possam ser adotadas;
- A classificação de ativos de informação será aplicada;
- Requisitos legais e regulatórios do país, bem como requisitos contratuais de segurança, serão atendidos;
- Treinamento em Segurança de Informações é mandatório para todos os colaboradores;

- Padrões, procedimentos e diretrizes adicionais deverão ser elaborados localmente para apoiar a implementação da política global de acordo com a legislação local. Estas regras definem o nível mínimo de conformidade para todos os funcionários sobre Segurança da Informação;
- Todos os gestores são diretamente responsáveis pela Implementação da Política dentro de suas áreas de negócio e pela adesão a mesma pelas suas equipes;
- É responsabilidade de cada funcionário aderir à Política de Segurança da Informação e aos padrões, procedimentos e diretrizes relacionados. Violações podem resultar em ações disciplinares, até e inclusive demissão;
- Todos os colaboradores **devem** reportar violações de Segurança de Informações, reais ou potenciais, ao seu gestor ou ao gestor da área de Tecnologia da Informação. No caso de um incidente de segurança ações imediatas devem ser tomadas para reduzir os riscos e impactos de danos para a **B&T** e nossos clientes;
- Exceções a esta Política de Segurança da Informação requerem aprovação da área de Tecnologia da Informação;
- Nesse contexto, os domínios de segurança lógica e segurança física (pessoas e sites) contribuem para reforçar a proteção das informações.

8.2. Organização

8.2.1. Gestão da Segurança da Informação

Uma estrutura de gestão deve ser estabelecida para iniciar e controlar a implementação de Segurança de Informações dentro da **B&T**. A Diretoria da **B&T** deve aprovar e apoiar os desenvolvimentos da política de segurança, avaliações de normas de segurança e implementação de segurança dentro da Sociedade.

Uma organização de gestão de segurança corporativa foi estabelecida com a tarefa de promover boas práticas de Segurança de Informações e é responsável por ajudar gestores, usuários e colaboradores de TI e outros a cumprir suas responsabilidades de Segurança de Informações.

Os Gestores da **B&T** são responsáveis pela conformidade das diretrizes de Segurança da Informação e medidas devem ser tomadas para coordenar a atividade de Segurança de Informações dentro de sua área de negócios.

8.2.2. Cooperação com Terceiros (Parcerias, Joint Ventures, Fornecedores, Contratados)

Sempre que a **B&T** entrar em parcerias, *joint ventures*, *insourcing* ou outros acordos com terceiros, é recomendável realizar uma análise de risco com relação a questões de

segurança. Esta análise de risco fornecerá os controles e procedimentos de segurança, que devem ser acordados e definidos em um contrato seguindo os controles de negócio normais deste tipo de acordo.

Nos contratos da **B&T** firmados com fornecedores para prestação de serviços é necessário a assinatura do **Termo de Confidencialidade** de modo a assegurar que seus funcionários estarão em conformidade com a política, padrões e procedimentos de segurança.

8.2.3. Outsourcing de Atividades da B&T para Terceiros

Outsourcing de sistemas de informação ou processos de negócios necessitam de uma análise de risco. Esta análise indicará os controles e procedimentos a serem implementados no contrato.

8.2.4. Níveis de Segurança

É meta a **B&T** entregar aos seus clientes serviços de alta qualidade. Assim um nível de segurança básico **deve** ser incorporado aos serviços entregues pela **B&T**. É recomendável que este nível de segurança básico seja consistente com "controles de segurança geralmente aceitos" para serviços de TI. É recomendável que o "nível de segurança básico" de um serviço seja definido e documentado nas Descrições de Serviço da **B&T** mantidas pela organização, países ou departamentos de entrega de serviço.

Quando a infraestrutura, instalações e recursos de TI da **B&T**, são compartilhados entre clientes múltiplos, o nível de segurança básico será o nível mínimo. Este nível não pode ser reduzido, porque isto pode comprometer o nível de segurança de outros clientes.

Se uma organização tem *outsourcing* ou recursos conjuntos de seus serviços de TI para com a **B&T**, o nível de segurança de recursos compartilhados **deve** ser levado até pelo menos ao "nível básico de segurança" da **B&T**.

Para atender os requisitos dos clientes, níveis adicionais de segurança podem ser selecionados para prover serviços de segurança estendidos aos clientes, com um custo adicional.

É recomendável que o nível de segurança de serviços globais entregues pela **B&T** tenha um padrão mínimo acordado em cada grupo local de entrega.

8.2.5. Criação de serviço

Quando a **B&T** estiver desenvolvendo novos serviços, uma análise dos riscos e requisitos de segurança deve ser realizada. Como parte do processo de criação, é recomendável que os níveis de segurança básicos da **B&T** e possivelmente de níveis estendidos para este novo serviço, sejam declarados nas descrições de serviços da **B&T.**

8.2.6. Contratos

Boas práticas de segurança são frequentemente o resultado da cooperação entre a **B&T**, seus clientes e outros fornecedores. Portanto, as responsabilidades de todas as partes para o nível de segurança acordado devem ser descritas em propostas iniciais, contratos resultantes e Acordos de Nível de Serviço.

Se, a pedido de um cliente, o nível de segurança a ser implementado para um serviço em particular for inferior ao nível básico de segurança da **B&T**, o nível de segurança acordado e as tarefas e responsabilidades da **B&T** e do cliente devem ser explicitamente declarados no contrato ou acordo de nível de serviço. Também será adicionado que os riscos correspondentes são de inteira responsabilidade do Cliente e que a **B&T** é dispensada de qualquer responsabilidade resultante dessa implementação. Como resultado, a **B&T** será formalmente dispensada de suas obrigações de fornecer um nível básico de segurança para estes serviços.

Reduzir o nível de segurança para um cliente nunca pode levar risco a outros clientes e, portanto, pode exigir algumas medidas adicionais.

Quando a **B&T** adquire novos contratos de *outsourcing* ou de recursos conjuntos, o nível de segurança do ambiente do cliente **deve** ser analisado criticamente e avaliado como parte do *due diligence*. Os níveis de riscos de segurança **devem** ser claramente documentados antes dos contratos serem formalizados.

8.3. Classificação

8.3.1. Propriedade

Para manter a proteção adequada de ativos, todos os ativos mais importantes devem ser inventariados (*hardware e software*) e ter um proprietário nomeado (*hardware, software* e informação). Colaboradores específicos, envolvidos na operação dos processos de negócio da Sociedade, que possuem habilidades específicas, conhecimento e experiência de difícil substituição, também pode ser considerado como um dos ativos importantes e devem ser identificados em um plano de sucessão.

8.3.2. Classificação da Informação

Para assegurar que a informação recebe um nível adequado de proteção, é recomendável que seja classificada de acordo com o padrão de classificação da **B&T**, para ocorrer o nível adequado de proteção.

Na criação da informação, o criador dela é responsável por sua classificação imediata. O proprietário da informação é responsável pela correta classificação e é recomendável que analise criticamente a classificação de acordo com procedimentos de controle de

documentos da **B&T**. Maiores informações disponíveis no documento PSI 002 - Política de Classificação da Informação.

O Colaborador ou Terceiro deverá consultar o Departamento de Controles Internos caso haja qualquer dúvida a respeito da classificação de uma informação pela sua sensibilidade.

8.3.3. Salvaguarda de Registros da Sociedade

Registros importantes da Sociedade devem ser protegidos contra perda, destruição e falsificação. Alguns registros podem necessitar de retenção segura para atender a requisitos estatutários ou regulamentares, bem como apoiar atividades essenciais de negócios.

Exemplos disso são registros que podem ser exigidos como evidência de que uma empresa opera dentro de regras estatutárias ou regulamentares, ou para assegurar defesa adequada contra ação criminal ou civil potencial, ou para confirmar o status financeiro de uma Sociedade com relação a acionistas, sócios e auditores. A lei ou regulamentação nacional pode definir o período e conteúdo de dados para retenção de informações. Quando são escolhidos meios eletrônicos de armazenagem, procedimentos para assegurar a capacidade para acessar dados (tanto a legibilidade da mídia quanto do formato) por todo o período de retenção, para salvaguardar contra perda devido à mudança futura de tecnologia.

O sistema de armazenagem e manuseio de registros deve assegurar a clara identificação de registros e de seu período de retenção estatutário ou regulamentar.

Deve permitir a destruição apropriada dos registros após esse período se a **B&T** ou seus Clientes não mais necessitarem deles.

Para atender estas obrigações, os seguintes passos devem ser considerados por e/ou departamento:

a. É recomendável emitir diretrizes sobre a retenção, renovação, armazenagem, manuseio e descarte de registros e informações de negócios;

b. É recomendável esboçar um programa de retenção identificando tipos essenciais de registro de negócios e o período que eles **devem** ser retidos;

c. É recomendável manter um inventário de fontes de informações de negócios-chave; e

d. É recomendável programar controles adequados para proteger registros e informações de negócios essenciais contra perda, destruição, acesso não autorizado e falsificação.

8.4. Segurança dos Colaboradores

8.4.1. Segurança no Trabalho – Definição e Recursos

8.4.1.1. Triagem de Colaboradores

O recrutamento de colaboradores para cargos sensíveis pode exigir triagem adicional de seus empregos anteriores e referências, de acordo com a natureza da posição a ser preenchida. Isto será conduzido de acordo com a legislação vigente no país. A triagem é responsabilidade da Gerência de Recursos Humanos e aplica-se a todos os colaboradores, **B&T**, contratados e outros funcionários temporários. Maiores informações disponíveis no documento **NSI 002 - Norma de Segurança em Recursos Humanos**.

8.4.1.2. Termos e Condições de Emprego

Os termos e condições de emprego da **B&T devem** incluir uma cláusula com a qual os colaboradores estão familiarizados e concordam com a **Política de Segurança** da Informação da **B&T,** ou assinarem um Termo de Adesão. No caso de uma violação da Política de Segurança por parte de um colaborador, poderá ser aplicada medida disciplinar. Essa ação pode variar de uma advertência escrita ou verbal (com ou sem observação no arquivo pessoal) e demissão. A gravidade do incidente **deve** orientar a severidade da ação a ser tomada.

É recomendável que os termos e condições para fornecedores, colaboradores, contratados e funcionários temporários trabalhando para a **B&T** sejam definidos em contratos formais, que especifiquem as condições de segurança necessárias para assegurar a conformidade com a Declaração de Política de Segurança da **B&T**. O contrato **deve** ser estabelecido previamente ao seu acesso às instalações, recursos e/ou informações da **B&T**.

8.4.1.3. Acordos de Confidencialidade

Os colaboradores da **B&T devem** assinar Termo de Confidencialidade que será parte integrante de seus termos e condições de trabalho.

Fornecedores, colaboradores, contratados e outros funcionários temporários, se não estiverem cobertos por um contrato entre empresas já existente contendo uma declaração

de confidencialidade, **devem** assinar o Termo de Confidencialidade, antes do início das atividades e acessos aos sistemas dentro ou fora das instalações da **B&T**.

É recomendável que os Termos de Confidencialidade sejam analisados criticamente quando houver alterações nos termos e condições de emprego, particularmente quando funcionários estão em vias de deixar a organização, ou os contratos em vias de expirar.

8.4.1.4. Segurança nas Descrições dos Cargos

É recomendável que as tarefas e responsabilidades de segurança sejam aprovadas pela gestão e, incluídas nas descrições de cargo adequadamente. Assim como as tarefas e responsabilidades relacionadas à segurança consistente com as Políticas de Segurança da **B&T** sejam conhecidas por aqueles envolvidos em gestão de segurança ou na entrega de serviços de segurança e outras partes interessadas.

8.4.1.5. Código de Conduta

O Código de Conduta e ética da **B&T** descrito nos documentos **Código de Ética e Conduta** define regras para conduta pessoal, que cada membro da equipe é recomendado a seguir e **deve** incluir segurança e questões relacionadas.

8.4.1.6. Encerramento de Contrato de Emprego

Quando um membro da equipe deixa a **B&T**, o gestor da área e o Recursos Humanos são responsáveis por assegurar que o usuário devolva tudo o que é de propriedade da **B&T** e que todos os privilégios de acesso sejam imediatamente solicitados e removidos.

8.4.1.7. Segregação de Funções

Quando apropriado, a gestão **deve** separar os cargos, tarefas e responsabilidades para evitar que um indivíduo subverta um processo crítico da **B&T** ou de cliente.

8.4.1.8. Nível de Autorização de cargo

A gestão **deve** certificar-se que os colaboradores desempenham somente aquelas funções exigidas para seu cargo dentro da Sociedade. Eles também são responsáveis por verificar se os funcionários somente possuem as autorizações necessárias para desempenhar esse cargo.

8.4.2. Educação, Treinamento e Conscientização

É obrigatória a implementação de programas de capacitação e de avaliação periódica pessoal de maneira que colaboradores recebam treinamento e educação em bases regulares para assegurar que estão conscientes da política e padrões de segurança da **B&T**, equipados para apoiar a implementação das normas no transcorrer de seu trabalho normal.

8.4.3. Notificando Incidentes de Segurança

Incidentes de segurança devem ser notificados à gestão responsável o mais rápido possível. Gestores são responsáveis por tomar ações para resolver incidentes em suas áreas. É recomendável que todos os membros de sua equipe estejam conscientes dos procedimentos para notificar incidentes de segurança conforme definido na organização local. Maiores informações disponíveis no documento **NSI 007 - Norma de Tratamento de Incidente em Segurança da Informação**.

8.4.3.1. Notificando Fragilidades na Segurança

É recomendável que fragilidades na segurança sejam notificadas à gestão responsável. Os gestores são responsáveis por avaliar o risco de segurança, elaborar plano de ação em suas áreas de responsabilidade quando exigido, e **devem** estar conscientes dos procedimentos para notificar incidentes de segurança, conforme definido na organização local. Tais fragilidades **não devem** ser testadas sem o acordo escrito de um nível adequado de gestão.

8.5. Segurança Física e do Ambiente

As áreas de computação e rede da **B&T** (por ex. centros de computação, sites de servidores e outras instalações de TI, como por exemplo e centros de publicação) devem ser operadas como instalações fechadas com acesso controlado, permitido somente a pessoal autorizado. É recomendável que o acesso seja limitado somente aos colaboradores da **B&T** que tenha um requisito de negócio válido para acesso.

No ambiente do servidor, local que contém os dados sensíveis da **B&T**, é **PROIBIDO** qualquer tipo de gravação de áudios e vídeos, a não ser em um local designado (mediante a liberação do gestor de TI) especificamente para essa finalidade. Essa regra é aplicada para todos os usuários, sem qualquer exceção.

É recomendável que procedimentos especiais sejam aplicados para visitantes e a pessoa responsável pela segurança física da área analise criticamente autorizações de acesso pelo menos uma vez por ano. Assim como os sistemas da **B&T,** localizados em sites de clientes, sejam instalados em uma área ou sala controlada pela **B&T**. É recomendável que as áreas

de entrega especial e de carga sejam controladas e, se possível, isoladas das áreas de computação da **B&T**. Maiores informações disponíveis no documento **NSI 003 - Norma de Segurança Física e do Ambiente** e **NSI 015 - Norma de Segurança de Acesso Físico**.

É recomendável que as áreas de computação e rede da **B&T** sejam fisicamente protegidas contra ameaças à segurança e que os equipamentos estejam localizados de forma a reduzir os riscos de ameaças ambientais e perigos, tais como incêndio e dano por fumaça, inundação, falha de energia, problemas de umidade, iluminação, mau-funcionamento técnico, sabotagem e roubo. É recomendável que o equipamento seja mantido de acordo com os procedimentos documentados de fornecedores, para assegurar sua disponibilidade contínua. Assim como os controles adequados sejam determinados com base em uma avaliação de risco.

A gestão de linha **deve** autorizar de maneira auditável o uso de equipamento para processamento de informação fora das instalações da **B&T** e é recomendável que esse equipamento receba proteção adequada. Isto também se aplica a computadores laptop usados fora das instalações da **B&T**.

É recomendável que o acesso à informação em mídia removível ou papel seja protegido por controles adequados. Assim como uma informação não seja deixada onde possa ser acessada, lida, copiada ou levada por pessoal não autorizado a fazê-lo.

É recomendável que estações de trabalho e servidores sejam protegidos contra acesso não autorizado (bloqueio do computador) quando não estão sendo usadas. Isto também se aplica a equipamento eletrônico portátil (por ex. notebooks, *smartphones* e *tablets*).

Quando equipamento e mídia que contêm informações são descartados, é recomendável que o processo assegure que as informações não podem ser recuperadas posteriormente.

8.6. Segurança de rede

8.6.1. As Redes da B&T

As redes da **B&T devem** ser separadas de redes externas.

As redes privadas são as sub-redes, contendo todos os colaboradores e os recursos internos da **B&T** para apoiar os processos de negócios. Elas são acessíveis somente aos colaboradores e subcontratados da **B&T**.

As redes de serviço são as sub-redes que a **B&T** utiliza para entregar serviços a clientes. É recomendável que apoiem tanto a gestão de serviço quanto as atividades de entregas de serviços.

É recomendável que o acesso a dados transportados pela rede seja restrito somente às pessoas autorizadas, para proteger sua integridade e confidencialidade. Normalmente, dados transportados pela rede não são criptografados, a menos que seja solicitado pela **B&T**, cliente, por lei ou regulamentação do país.

Não é permitido aos colaboradores da **B&T** tentar qualquer tipo de acesso ou uso não-autorizado aos sistemas ou redes internas da **B&T**, clientes ou terceiros usando recursos de computadores da **B&T**, seus próprios ou do cliente. Maiores informações disponíveis no documento **NSI 011 - Norma de Segurança de Rede**.

Somente softwares e ferramentas padrão aprovados da **B&T** (ou do cliente) são permitidos em computadores e redes da **B&T**. *Software* ou ferramentas extras necessárias além desses **devem** ser formalmente autorizados de maneira auditável pelo seu gestor (e/ou cliente).

Não é permitido aos colaboradores da **B&T** instalar qualquer ferramenta de categoria "*hacking*" na rede da **B&T** ou de clientes e/ou em estações de trabalho (computadores desktop ou notebooks), incluindo, mas não se limitado a, produtos como crackers de senha, *war dialers*, *port scanners*, ferramentas *peer-to-peer*, ferramentas de compartilhamento de arquivos, *packet sniffers*, etc. a menos que explicitamente autorizado pela gestão, de acordo com diretrizes de segurança; estas ferramentas **devem** ser autorizadas em bases individuais e não podem ser compartilhadas com ninguém mais. Qualquer um que tenha estas ferramentas tem que removê-las imediatamente, ou solicitar seu uso à gerência com uma justificativa de negócios.

Todas as práticas intencionais que coloquem em perigo a segurança da rede da **B&T** são proibidas e as consequências de fazê-las são descritas na seção referente a processos disciplinares.

8.6.2. Conexões com Internet Pública

Todas as conexões entre as redes da **B&T** (**REDES DE SERVIÇO** e **REDES PRIVADAS**) e a **Internet** (ou qualquer outra rede pública) para acessar serviços de rede **devem** incluir arquitetura de 'firewall' para filtrar tráfego e bloquear acesso não-autorizado. Todo tráfego entrando e saindo **deve** passar pelo "firewall".

Somente será permitida passagem através do firewall de serviços de rede para os quais existe uma necessidade do negócio. Todos os firewalls **devem** ser configurados e gerenciados para atender aos requisitos de segurança.

O estabelecimento de uma conexão direta entre os sistemas de computação da **B&T** e sistemas de computador em organizações externas via Internet ou outra rede

pública **devem** ser apoiadas por uma autenticação forte e criptografia de tráfego, dependendo da classificação de informação.

8.6.3. Conexões de Terceiro

Redes de terceiros **não devem** ser conectadas diretamente às redes da **B&T** (REDES DE SERVIÇO e REDES PRIVADAS). Todas as conexões entre as redes da **B&T**, redes de terceiros **devem** passar através de um 'gateway' seguro para filtrar tráfego / protocolos e bloquear acesso não-autorizado. Todo o tráfego entre as redes da **B&T** e a rede de terceiros

(entrando e saindo) **deve** passar por este gateway. Conexões entre a REDES DE SERVIÇO e redes de terceiros exigem uma análise de risco.

É recomendável que os requisitos de segurança da **B&T** sejam incorporados a contratos, que definem as responsabilidades da **B&T** e da empresa terceira.

8.6.4. Acesso remoto

Acesso remoto às redes da **B&T** serão disponibilizados aos colaboradores da **B&T** com base na "necessidade do negócio", a critério de seu gestor. Acesso remoto **deve** ser restrito a membros autorizados.

Somente será permitido acesso remoto usando soluções padrão da **B&T**.

Quando a Internet ou uma conexão dedicada de terceiro é usada para acessar as redes da **B&T**, **deve** ser usada autenticação forte, juntamente com criptografia.

O acesso aos recursos de computação efetuados por um colaborador e/ou terceiro que se encontre fora das dependências da **B&T**, **deve** ser concedido em conformidade com o procedimento, **TERMO DE RESPONSABILIDADE POR EMPRÉSTIMO**. O mesmo **deverá** ser realizado de maneira segura, garantido que ocorra a comunicação criptografada entre os recursos de computação da **B&T** e o equipamento utilizado pelo colaborador e/ou terceiro.

É recomendável que os colaboradores da **B&T** que utilizem facilidades de acesso remoto, protejam adequadamente suas estações de trabalho para evitar acesso não-autorizado à rede da **B&T** ou de clientes. Eles são pessoalmente responsáveis pela proteção de sua estação de trabalho e uso correto das facilidades de acesso remoto da **B&T**.

É recomendável que o acesso remoto seja realizado através de uma VPN e seja respectivamente configurado, de tal forma que todo o tráfego seja roteado, apenas, pela VPN, prevenindo a conexão simultânea a qualquer outra rede.

Quando facilidades de acesso remoto forem oferecidas, a estação de trabalho (computadores desktop ou notebooks) usada **deve** estar rodando a última versão de ferramenta antivírus juntamente com os arquivos de vacina atualizados e **deve** estar continuamente habilitada, monitorando constantemente por vírus e suas atividades.

O acesso direto a redes de cliente, por colaboradores da **B&T**, através de qualquer tipo de instalação de acesso remoto não é permitido, a menos que explicitamente acordado pelo cliente e mencionado no Acordo de Nível de Serviço; neste caso, o cliente **deverá** dispensar a **B&T** de qualquer responsabilidade sobre danos potenciais resultantes de tais acessos.

8.7. Segurança do Host / Sistema

8.7.1 Medidas Gerais de Segurança

Os colaboradores da **B&T** são responsáveis pela proteção de suas estações de trabalho (computadores *desktop* ou *notebooks*) em todo o tempo. A fim de reduzir o risco de acesso não autorizado aos computadores desktop ou notebooks, é recomendável bloqueá-los e utilizar uma proteção de tela protegida por senha quando abandonadas.

É recomendável atribuir senhas de BIOS para oferecer maior proteção de dados em caso de perda ou extravio deste equipamento.

Todos os computadores desktop ou notebooks da **B&T devem** estar equipados com *firewall* pessoal e/ou aplicativo de proteção/detecção de intrusão do equipamento e ainda as medidas de segurança, padrão da **B&T**, para *anti-spyware* e outros *malwares*.

Atualização dos sistemas e aplicações com patches de segurança são obrigatórios.

8.7.2. Identificação e Autenticação

A **autenticação** de usuários nos sistemas da **B&T** é efetuada **mediante senha**; os usuários **devem** manter a sua senha em segredo, modificá-la regularmente, **não devem** armazená-las em seus computadores sem usar arquivos criptografados, e **não devem** tentar descobrir senhas pertencentes a outras pessoas. Devido à responsabilidade pessoal, o uso de credenciais de acesso funcionais ou compartilhadas não é permitido. Exceções podem ser concedidas desde que procedimentos adequados para o acesso controlado as credenciais de acesso funcionais ou compartilhados sejam aplicados.

A gestão de sistemas **deve** estabelecer um procedimento para redefinir senhas, que inclua disposições para identificação positiva do solicitante. É recomendável que o usuário altere imediatamente estas senhas iniciais.

É recomendável que medidas adicionais e mais fortes de identificação e autorização sejam implementadas para usuários e clientes da **B&T** quando necessário. Para um perfil com privilégios especiais, é recomendável considerar o uso de técnicas mais rígidas de autenticação, tais como *tokens* ou pergunta/resposta. Identificação e autenticação são realizadas por um sistema de autenticação dependente de plataforma. É recomendável que este procedimento de acesso autenticado ofereça informações mínimas sobre o sistema para evitar fornecer a um usuário não-autorizado, assistência desnecessária. Ao realizar uma tentativa de autenticação em um sistema, se qualquer parte do processo estiver incorreto, é recomendável não fornecer ao usuário *feedback* específico indicando a fonte do problema. Caso contrário, é recomendável simplesmente informar ao usuário que o processo de autenticação está incorreto. Maiores informações disponíveis no documento **NSI 005 - Norma de Controle de Acesso Lógico**.

Onde a identificação do usuário não for possível, por ex. acesso via rede pública ou comunicação entre aplicativos, é recomendável tomar medidas adicionais. Estas medidas incluem roteamento forçado a serviços predefinidos, aplicativo via gateways de rede ou aplicativos de confiança.

É recomendável considerar, para certos usuários, restrições em horários de conexão para sistemas críticos ou sensíveis. Também é recomendável considerar um sistema de usuário com um log-off automático, ativado automaticamente após um período de inatividade.

8.7.3. Autorização

Controle de acesso é exigido para sistemas e dados compartilhados com outros. O proprietário da informação em um sistema compartilhado é responsável por decidir quem poderá acessar e que autoridades serão concedidas.

Deve existir um processo formal de autorização para assegurar acesso aos sistemas. É recomendável que o acesso ao sistema seja alocado com base na "necessidade de uso". O uso de "privilégios de sistema" ou utilidades de sistema **deve** ser restrito aos responsáveis pela gestão de sistema. Como responsáveis pela custódia destes sistemas, a gestão de sistema **deve** ter um processo estabelecido para implementar o acesso de usuário a qualquer sistema sob seu controle.

8.7.4. Administração de Segurança

É recomendável haver um procedimento de registro de usuário para entrada de novos usuários em um sistema. Somente pedidos aprovados pelo proprietário da informação em um sistema, podem ser implementados. Um registro de todos os usuários registrados para usar o sistema deve estar disponível.

É responsabilidade da organização usuária notificar a administração de segurança quando um usuário deixar uma Sociedade. É recomendável existir um processo estabelecido para bloquear ou excluir credenciais de acesso mediante notificação. Assim como bloquear uma credencial de acesso se não for utilizada por 3 meses e, em seguida, excluída se não for usada por 6 meses. É recomendável existir um processo estabelecido para analisar criticamente direitos de acesso de usuários pelo menos trimestralmente.

8.7.5. Gestão de Sistema

É recomendável que todas as credenciais de acesso ao Sistema ou Contas padrão que não são necessárias sejam removidas do sistema. Quando uma conta padrão de Sistema é necessária, a senha entregue pelo fornecedor deve ser alterada.

Instalações de teste e desenvolvimento **devem** ser segregadas de sistemas de produção ou operacionais. Maiores informações disponíveis no documento **NSI 006 - Norma de Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação.**

É recomendável que os procedimentos operacionais documentados estejam disponíveis para todos os sistemas de produção, para garantir sua correta operação. Assim como as mudanças nos sistemas sejam estritamente controladas pelo uso de procedimentos documentados de controle de alteração.

É recomendável que requisitos e projeções de capacidade sejam monitorados e feitas para assegurar que processamento adequado e capacidade de armazenagem estão disponíveis quando necessário.

Gestores de Sistema devem assegurar que instalações apropriadas de retorno à situação anterior estejam estabelecidas para todas as alterações de sistema, de acordo com sua criticidade para o negócio, especialmente nos casos de sistemas *outsourcing*.

8.7.6. Registrando, Monitorando, Relatando e Auditando

É recomendável que eventos e atividades relacionados com segurança sejam registrados conforme ocorrerem. Todos os eventos e atividades devem ser rastreáveis até o usuário individual. É recomendável que gestores e administradores de sistema analisem criticamente, de forma regular, os registros de incidentes, os quais são recomendáveis serem arquivadas por doze meses, para auxiliar em futuras análises críticas de auditoria.

É recomendável registrar pelo menos as seguintes atividades:

- Tentativas de autenticação de acesso malsucedidas;
- Usuários adicionados ou excluídos de um sistema;
- A atribuição e uso de privilégios especiais de sistema e utilidades de sistema;
- O uso de credenciais de Usuário ou Contas privilegiadas; e
- O uso de recursos sensíveis ou críticos (por ex. diretórios, arquivos).
- É recomendável que as seguintes atividades sejam ativamente monitoradas:
- Tentativas malsucedidas de autenticação de acesso;
- O uso de credenciais ou Contas privilegiadas; e
- O uso de recursos críticos ou sensíveis (p.ex. diretórios, arquivos, programas autorizados).

É recomendável que indicações de possíveis invasões ou violações de acesso sejam investigadas e relatadas ao gestor de linha responsável. Ações corretivas imediatas devem ser tomadas para minimizar os riscos. É recomendável que clientes sejam informados

conforme acordado no contrato com o cliente. Incidentes de segurança devem ser relatados usando processos padronizados.

É recomendável que auditorias regulares sejam realizadas por gestores e administradores de Sistema, para assegurar que a Confidencialidade, Integridade, Disponibilidade, Autenticidade, Legalidade e Não Repúdio do Sistema estão mantidas.

8.7.7. Backup e Recuperação

Instalações adequadas de backup, de acordo com a importância e valor do sistema e dos dados, devem ser fornecidas para assegurar que software de sistemas, software de aplicativo e dados possam ser recuperados após uma falha de mídia ou de sistema.

É recomendável que arquivos de backup sejam armazenados em local remoto, a distância suficiente do local principal e, providos com o nível adequado de proteção física, consistente com a segurança física do local principal. É recomendável que o processo de backup e restauração seja testado regularmente.

8.7.8. Proteção antivírus

Todas as estações de trabalho da **B&T** (computadores, desktop ou notebooks) capazes de executar o conjunto de ferramentas antivírus padrão da **B&T**, devem estar protegidas contra vírus1 usando este conjunto de ferramentas. Todos os servidores conectados com estações de trabalho (computadores, desktop ou notebooks) ou conectados a um ambiente não-protegido devem executar o conjunto de ferramentas antivírus. Os arquivos de assinatura de vírus devem ser atualizados pelo menos uma vez por semana. É recomendável que o software de proteção antivírus seja mantido atualizado e continuamente habilitado, monitorando permanentemente quanto aos vírus e suas atividades.

Devem ser implementados em todas as máquinas no âmbito interno da **B&T** o recurso Device Control, que é um serviço que permite controlar o acesso aos dispositivos removíveis. A partir da configuração, devem ser bloqueados os dispositivos USB (Universal Serial Bus): todos os drivers de mídia, modens, dispositivos de fita, *smart card*, adaptadores de rede externo, *bluetooth*, câmeras, scanners entre outros dispositivos. Caso comprovada a necessidade de tal utilização, o dispositivo poderá ser homologado e liberado mediante aprovação do Gestor do usuário. Este acesso será aplicado a todos os usuários, exceto colaboradores de TI, dependendo da aprovação de um gestor de TI.

[1] Um vírus de computador é um programa não-autorizado que se autorreplica inclusive para outras redes, sistemas e ou mídias de armazenamento de dados. Outros exemplos de *softwares* maliciosos são os vermes, "*spyware*" e Cavalos de Tróia. Esta política se aplica a todos os softwares maliciosos.

Os usuários que utilizam recursos de internet devem ser submetidos a regras de *Web Control*, que é um serviço que permite controlar o acesso aos recursos da Internet em vários níveis (usuários, grupos, sites etc.). As seguintes regras devem ser consideradas:

I. **Bloqueio Padrão**: Configurado uma regra, com sites que não são permitidos dentro da **B&T**, geralmente sites mal-intencionados. Aplicado a todos usuários, exceto aos colaboradores de TI, em função de análise e investigação de riscos.

II. **Liberar Sites** - Vídeos/Imagens Treinamento: Configurado uma regra, com sites específicos que disponibilizam vídeos com fins instrutivos. Limitado a usuários específicos, após a provação do gestor da área de negócio ou diretor. No entanto, é pré-requisito a liberação técnica da TI, em função da avaliação de impacto no link de dados.

III. **Liberar Padrão** - Por Conteúdo/Endereço: Configurado uma regra, com sites específicos que são permitidos dentro da **B&T**, geralmente sites governamentais, Intranet etc. Permitido o acesso a todos os usuários que têm uma credencial de acesso na rede.

IV. **Liberar Gestores - Por Conteúdo/Todos os Endereços:** Configurado uma regra, permitindo acesso a qualquer site, sem nenhuma restrição, exceto as apontadas na regra de "Bloqueio Padrão". Acesso restrito a alguns grupos de usuários, tais como gestores e consultores externos. Porém, dependendo da aprovação de um gestor de TI ou diretor.

V. **Liberar Sites de Proxy -** Por Conteúdo/Endereço: Configurado uma regra, permitindo acesso a sites de proxy específicos. Acesso restrito ao grupo de usuários, gestores de TI. Porém, depende da aprovação final de um gestor de TI ou diretor.

VI. **Bloquear Sites de Stream -** Por Conteúdo/Endereço: Configurado uma regra, com sites de stream que não são permitidos dentro da **B&T**, geralmente sites que disponibilizam vídeos de diversas fontes. Acesso aplicado a todos os usuários, exceto aos gestores e colaboradores da TI. Porém, depende da aprovação de um gestor da TI.

VII. **Bloquear Sites Por Conteúdo/Categoria/Tipos de Arquivo:** Configurado uma regra, com categorias de conteúdo e tipos de arquivos que não são permitidos dentro da **B&T**, geralmente sites que disponibilizam conteúdo adulto, violência etc. Acesso aplicado a todos os usuários, exceto aos gestores e colaboradores da TI. Porém, depende da aprovação de um gestor da TI.

VIII. **Bloquear Sites Por Conteúdo/Endereço:** Configurado uma regra, com sites específicos não permitidos dentro da **B&T**, geralmente sites de webmail, proxies, vídeos. Acesso aplicado a todos os usuários, exceto aos gestores e colaboradores da TI. Porém, depende da aprovação de um gestor da TI.

É recomendável que todos os arquivos em estações de trabalho da **B&T**, sistemas servidores conforme identificados acima, passem por uma varredura quanto a vírus pelo menos uma vez por semana.

Todos os novos softwares e arquivos de dados, especialmente se estes arquivos vêm de uma fonte desconhecida ou não-confiável (como a Internet), dispositivos desprotegidos como mídias de armazenamento USB ou drives de discos externos, devem passar por varredura quanto a vírus antes de seu uso. Antes da distribuição de qualquer software ou arquivo de dados a um terceiro, os arquivos devem passar por varredura quanto a vírus.

Se um vírus for detectado e não puder ser automaticamente excluído, pelo software de proteção antivírus, a organização local de suporte deve ser imediatamente informada.

Os colaboradores da **B&T** não devem nunca intencionalmente escrever, gerar, propagar, executar ou tentar introduzir qualquer vírus ou outra forma de código malicioso na **B&T**, ambiente de seu cliente ou na Internet.

Os colaboradores da **B&T** usando seus dispositivos pessoais por justificativas de negócio deve estar protegido contra vírus usando software de proteção antivírus aprovado pela **B&T** (antivírus, desktop firewall entre demais outros mecanismos de proteção). É recomendável que eles façam varredura de seus arquivos de dados antes de usar estes arquivos dentro do ambiente da **B&T** e não devem se conectar simultaneamente a um Terceiro Provedor de Serviço Internet. Maiores informações, estão disponíveis no documento NSI 013 - Norma de Segurança da Internet.

8.7.9. Computação Móvel e Teletrabalho

Os colaboradores da **B&T** são responsáveis pela proteção de seus *notebooks*, *tablets* e *smartphones* durante viagens e nos dias de home office. É recomendável que os notebooks, tablets e smartphones não sejam deixados em locais públicos. É recomendável que todos os dados de informações sensíveis da **B&T** e de seus clientes sejam criptografados nestes dispositivos. Para reduzir o risco de roubo, é recomendável que sejam utilizados cadeados de segurança sempre que os dispositivos forem “abandonados”, tanto na **B&T** quanto nas instalações de clientes, salas de reunião, hotéis ou até mesmo em residências.

É recomendável que também sejam implementados *bitlockers* (criptografia de disco), quando possível, para oferecer alguma proteção aos dados no caso de perda da máquina.

Os colaboradores da **B&T** trabalhando em atividades de negócio dentro ou distantes do escritório da **B&T** (por exemplo: em casa, hotel, site do cliente ou demais outras localidades) é responsável pela proteção de ativos da **B&T** (hardware, software e informações), incluindo todos os dispositivos móveis, como notebooks, tablets e smartphones. É recomendável que tomem todas as precauções razoáveis para proteger ativos da **B&T** em conformidade com a política de segurança da **B&T** incluindo senhas de proteção dos dispositivos móveis e criptografia de informações confidenciais.

8.7.10. Confiabilidade de Estações de Trabalho

Somente as estações de trabalho da **B&T** pertencentes aos ativos da **B&T** são vistas como estações de trabalho confiáveis e podem ser usadas para qualquer tipo de atividade autorizada nas redes da **B&T** enquanto manipulam qualquer tipo de dados classificados.

Visitantes externos da **B&T** só **devem** ter acesso de modo restrito a redes da **B&T**, quando absolutamente necessário. Cada funcionário ao receber visitantes, **deve** contatar o administrador de rede local para verificar procedimentos relativos à liberação de acesso *Guest* (Visitante).

Quando em viagem e em *home office* (fora do escritório da **B&T)** os colaboradores da **B&T** são fortemente aconselhados a usar unicamente estações de trabalho de ativos da **B&T**, para manipulação de dados sob a responsabilidade da **B&T** e para conexão às redes da **B&T**. Entretanto, circunstâncias específicas podem impedir o uso de estações de trabalho pertencentes aos ativos da **B&T** quando for este o caso, as seguintes restrições devem ser aplicadas:

EQUIPAMENTO / AÇÕES	PC de propriedade **B&T**	PC doméstico de propriedade do funcionário[2,3]	PC do cliente alocado permanentemente ao funcionário [5,4]	PC de propriedade de terceiro [5,4]
Conectam-se a redes **B&T**	Sim	Não	Parcialmente	Não
Armazenagem local de dados classificados da **B&T** ou dados do Cliente	Sim	Não	Somente dados do cliente[5]	Não
Acesso à Internet	Sim	Sim	Sim	Sim [6]
Acesso a e-mail Web	Sim	Sim	Sim	Somente ler e-mails

Tabela 1 – Descrição de Restrições

[2] **Deve** estar de acordo com as regras de segurança para estações de trabalho: Antivírus, firewall de micro, atualizações de software etc.
[3] A referência a este tipo de uso não implica que seja prestado suporte a ele; favor consultar seu acordo de nível de serviço.
[4] **Deve** estar de acordo com as regras de segurança ou com as Regras de Segurança do Cliente.
[5] Isto exclui qualquer aplicativo de e-mail de cliente para o gerenciamento de um endereço de caixa postal.
[6] A diferença é apenas a rede utilizada (B&T Corporativa, Diretoria e Visitantes).

8.8. Segurança de Aplicativos e Dados

8.8.1. Aplicativos de Negócios da B&T

É recomendável que todo aplicativo de negócio crítico tenha um proprietário nomeado (um departamento ou área específica da empresa), os requisitos de segurança sejam determinados e documentados em um plano de segurança antes que um aplicativo seja projetado, desenvolvido ou adquirido. Assim como requisitos de segurança, com relação à confidencialidade, integridade, disponibilidade, autenticidade e não repudio sejam acordados com o proprietário. É remendável que as especificações técnicas estejam documentadas.

Todos os aplicativos **devem** ser testados e aceitos antes de serem levados à produção. Durante o teste de aceitação de aplicativos recém-desenvolvidos ou adquiridos é recomendável verificar se os requisitos de segurança são preenchidos. O **Departamento de Tecnologia da Informação deverá** assegurar que as aplicações de uso da **B&T** sejam instaladas corretamente no ambiente de produção, informando aos envolvidos sobre as regras e responsabilidades inerentes. Além disto, garantirá que os documentos e/ou procedimentos relacionados sejam sempre mantidos atualizados. Também quando aplicativos são subsequentemente corrigidos, os requisitos de segurança **devem** ser verificados. É recomendável que os aplicativos não sejam testados com dados de produção reais.

É recomendável controle estrito de acesso de todos os ambientes. As aplicações desenvolvidas pela **B&T**, **deverão** ter o acesso ao código-fonte restrito aos integrantes do projeto. Quando operacional, é recomendável que todas as medidas de segurança necessárias, manuais e automatizadas sejam cumpridas.

É recomendável que alterações afetando aplicativos sejam estritamente controladas pelo uso de procedimentos documentados de controle de alterações.

Qualquer vulnerabilidade ou evento de quebra de Segurança da Informação observado por colaboradores e terceiros **deve** ser relatado na forma de Registro de Incidente e enviado pela área de Tecnologia da Informação para o e-mail: **controlesinternos@btcorretora.com.br.**

É recomendável serem considerados controles especiais, para aplicativos que iniciam processos de negócio críticos envolvendo o manuseio ou intercâmbio de informações sensíveis.

8.8.2. Aplicativos de Clientes

8.8.2.1. Requisitos de Segurança em Aplicativos de Clientes

É recomendável que os clientes sejam fortemente aconselhados a considerar com cuidado os requisitos de segurança, antes de um aplicativo ser desenvolvido, alterado ou selecionado.

É prudente que os clientes sejam fortemente aconselhados a verificar cuidadosamente se seus requisitos de segurança são preenchidos, quando novos aplicativos são colocados em produção e alterados.

A **B&T** assegurará que fragilidades e eventos de Segurança da Informação associados com sistemas da informação, sejam comunicados ao **Departamento de Tecnologia da informação** permitindo a tomada de ação corretiva em tempo hábil.

8.8.2.2. Ambientes de Teste e de Produção

É boa prática de segurança e requerimento normativo, criar diferentes ambientes para atividades durante o ciclo de vida de um aplicativo, i.e., teste e produção. **Deve** haver segregação entre estes ambientes para evitar que dados de ambientes de teste e desenvolvimento sejam usados no ambiente de produção. Dados reais de produção podem ser usados, desde que de forma controlada para garantir a segurança da informação. Segregação de ambientes de produção e teste é fortemente aconselhado. É recomendável controle de acesso a todos os ambientes.

8.9. Serviços Genéricos da B&T

8.9.1. Correio Eletrônico

É recomendável que os colaboradores da **B&T** estejam cientes de que mensagens eletrônicas podem ser encaminhadas, interceptadas, impressas e armazenadas por outras pessoas. A menos que a mensagem seja criptografada, os colaboradores **devem** evitar enviar informações sensíveis via *e-mail.* Em casos extraordinários devem utilizar corretamente os rótulos de confidencialidade.

O emissor de uma mensagem eletrônica é considerado pessoalmente responsável por seu conteúdo. É recomendável que os colaboradores da **B&T** estejam cientes de que todas as mensagens originadas de usuários da **B&T** levam o nome da **B&T** em seu endereço de origem. É recomendável que toda mensagem seja preparada e enviada de maneira profissional seguindo todas as regras de decoro social. Da mesma forma, os colaboradores da **B&T devem** evitar enviar mensagens que podem ser consideradas inflamatórias, discriminatórias, injuriosas ou de outra forma ofensivas ou ilegais.

É recomendável que os colaboradores da **B&T** exerçam com cuidado o encaminhamento de mensagens, reconhecendo que certas informações são dirigidas a indivíduos específicos e podem não ser adequadas para distribuição geral em comunicações eletrônicas. Assim como as informações sensíveis não sejam encaminhadas a qualquer parte fora da **B&T** sem a aprovação prévia do proprietário da informação. Não é permitido encaminhamento automático de mensagens a partes fora da **B&T**.

E-mails indesejados ou "*spam"* são considerados ofensivos e e-mail contendo material ilegal, ofensivo ou malicioso é considerado intolerável.

É recomendável que ao visitar *websites* e tendo que preencher informações, os colaboradores tomem cuidado antes de usar o endereço de e-mail da Sociedade da **B&T.** Isto pode resultar em e-mail comercial indesejado e não solicitado. É recomendável que os funcionários evitem deixar seus endereços de *e-mail* da **B&T** se a política de privacidade do *website* é inexistente ou declarar que aquela informação será vendida ou compartilhada.

A **B&T** respeitará a privacidade de seus usuários de e-mail. Normalmente usuários de e-mail podem presumir que somente o destinatário lê sua correspondência eletrônica.

Entretanto, o acesso a caixas de correio eletrônico de usuários pode ser solicitado no caso de qualquer urgência comercial, incluindo atividades de investigação. Também pode ser necessário para o suporte técnico revisar o conteúdo das comunicações de membros individuais dos colaboradores durante a resolução de problema. Todos estes acessos precisam estar de acordo com a legislação local de privacidade, políticas corporativas com as devidas aprovações em alçada executiva (Recursos Humanos, Diretor da Área de Negócio e Jurídico). Maiores informações disponíveis no documento **NSI 012 - Norma de Segurança em Correio Eletrônico**.

8.9.2. Intranet da B&T

A Intranet da **B&T**, é um recurso do negócio particular e é recomendável que seja usada somente para fins de negócio. Somente os colaboradores da **B&T deverão** ter acesso autorizado.

Informações na Intranet destinam-se apenas a uso interno. É recomendável que as informações na Intranet não sejam compartilhadas com Terceiros. Os requisitos do Padrão de Classificação de Informação aplicam-se a todas as informações na Intranet. Informações classificadas como "Confidenciais" ou "Sensíveis" **deverão** ser armazenadas com controles eficientes de acesso e criptografia. Nenhum controle adicional é exigido ao armazenar informações "Públicas" ou "Internas".

Não é permitido uso inadequado do sistema Intranet. Uso inadequado inclui, porém não se limita a:

- Tentativas não autorizadas de acessar informações protegidas;

- Atividades que prejudiquem o desempenho da Intranet; e
- Qualquer atividade ilegal, antiética ou qualquer outra atividade que possa afetar adversamente a Sociedade.

8.9.3. Web Externa da B&T

É recomendável haver um processo de autorização formal antes de informações serem disponibilizadas publicamente na Internet. A integridade destas informações **deve** ser protegida de modificações não autorizadas a cargo da área de Marketing e de Comunicação Interna.

8.10. Gestão de Continuidade do Negócio

A **B&T deve** avaliar os riscos para sua continuidade no negócio de um desastre potencial nas suas atividades críticas de negócio. É recomendável que sejam desenvolvidos planos de continuidade de negócio para oferecer proteção contra a perda de ativos (*hardware*, *software* e informações) ou indisponibilidade de serviços.

A **B&T** deve, no mínimo, manter o macroprocesso de gestão dos incidentes disruptivos registrado e disponível para consulta pela área de Tecnologia da Informação e de Controles Internos.

Para assegurar que a infraestrutura da **B&T** continue a entregar serviços, gestores responsáveis por componentes da infraestrutura **devem** manter um plano de continuidade de negócio para implementação se um desastre impedir o funcionamento normal dos serviços.

Planos de continuidade de negócios **devem** ser capazes de entregar os requisitos de disponibilidade contratados aos clientes e **devem** ser testados e auditados, pelo menos, uma vez por ano.

É recomendável que o planejamento de continuidade de negócios seja discutido com clientes e descrito nos contratos e Acordos de Nível de Serviço. Maiores informações disponíveis no documento **NSI 008 - Norma de Continuidade de Negócios**.

8.11. Segurança em Cloud Computing (Nuvem)

Atualmente a **B&T** mantém grande parte de seus serviços em nuvem, entre eles, máquinas virtuais, servidores, bancos de dados, entre outras tecnologias. Portanto, as seguintes práticas são seguidas toda vez que novos serviços de nuvem são contratados.

8.11.1. Acordos de Níveis de Serviço (SLA)

É necessário verificar as questões atreladas aos SLA's (*Service Level Agreement*), que **devem** contemplar medidas de contingência, por exemplo, em casos de potenciais incidentes em segurança da informação, que visam assegurar a disponibilidade dos serviços da **B&T**. Tais documentos/acordos **devem** ser revisados periodicamente, em intervalos regulares, visando identificar potenciais incompatibilidades em relação ao atendimento do serviço contratado.

É recomendável que essa revisão contemple os seguintes aspectos:

- Qual tempo necessário para o reestabelecimento do serviço em casos de falhas;
- Qual plano de recuperação (*backup*) em caso de falha;
- Qual o tempo máximo aceitável para o negócio da **B&T** e quais as medidas **devem** ser tomadas pelo provedor para respeitar esse tempo;

8.11.2. Proteção de Dados Pessoais

O provedor de serviço em nuvem **deve** assegurar os cuidados necessários em relação a privacidade e segurança dos dados dos clientes, por exemplo, estar em conformidade com a Lei Geral de Proteção de dados Pessoais (LGPD). A Lei Federal 13.709 de 14 de agosto de 2018 tem como objetivo dispor sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O encarregado de dados da **B&T** deve ter seu nome e contato de email profissional divulgado no site da empresa. Este profissional tem o conhecimento sobre a lei, tecnologia e procedimentos utilizados no negócio da empresa.

Maiores informações disponíveis no **documento Política de Privacidade de Dados da B&T.**

8.11.3. Documentações de Manuais de Procedimentos

Procedimentos operacionais **devem** ser documentados e atualizados, uma vez que os sistemas/tecnologias sofrem atualizações de tempos em tempos. Essa medida tem por objetivo garantir a correta operacionalização das tecnologias mantidas em nuvem, além de assegurar que os profissionais estarão treinados para operar as máquinas virtuais, servidores, bancos de dados, entre outras tecnologias mantidas em nuvem.

8.11.4. Garantir a Conformidade em Nuvem

A **B&T deve** assegurar que todos os serviços contratados de provedores em nuvem, estão em conformidade com as leis e regulamentos de conformidade aplicáveis. Portanto, em

intervalos regulares, relatórios de auditoria **devem** ser solicitados ao provedor do serviço, visando identificar potenciais aspectos de não conformidade em armazenamento, processamento e transmissão de informações.

8.12. Conformidade

8.12.1. Conformidade com a Política de Segurança

O desenho, operação e uso de cada instalação, rede, sistema, aplicativo e suas informações **devem** estar em conformidade com a Política de Segurança da Informação da **B&T**, acordos contratuais, leis relevantes e outros requisitos normativos. Maiores informações disponíveis no documento **NSI 009 – Norma de Conformidade em Segurança**.

8.12.2. Conformidade com Requisitos Legais

A **B&T** é uma instituição financeira regulada pelo Banco Central do Brasil, dessa forma, está sujeita às regulamentações emitidas pelo BACEN. Além disso, a B&T segue o modelo de Três Linhas previsto em sua Política de Conformidade e Controles Internos, segundo o qual, as áreas que lidam diretamente com o negócio são as primeiras responsáveis por manter controles efetivos para a mitigação de riscos e conformidade com acordos nacionais, leis e regulamentos.

A **B&T** poderá promover as medidas que julgar necessárias, inclusive judiciais, para garantir que o uso dos Recursos de Computação seja feito conforme previsto neste documento. Para qualquer solicitação de serviços de competência da Assessoria Jurídica da **B&T** conforme descrito no procedimento **Solicitação de Serviços Jurídicos**.

Aplica-se a este documento toda a legislação nacional, em especial as normas abaixo, cujo conteúdo pode ser obtido integral e gratuitamente no sítio da Presidência da República, em http://www.planalto.gov.br:

- A Constituição da República Federativa do Brasil de 1988;
- O Decreto-Lei nº. 2.848/40 (Código Penal);
- O Decreto-Lei nº. 5.452/43 (Consolidação das Leis do Trabalho – CLT);
- A Lei Federal nº. 9.279/96 (Código de Propriedade Industrial);
- A Lei Federal nº. 9.609/98 (Lei do Programa de Computador);
- A Lei Federal nº. 9.610/98 (Lei de Direitos Autorais);
- A Lei Federal nº. 10.406/02 (Novo Código Civil).

8.12.3. Verificação de Conformidade

A conformidade com esta política e subsequentes padrões e procedimentos de segurança dentro de uma organização será revisada sob a responsabilidade **Departamento de Tecnologia da Informação**. Não conformidades serão relatadas à gestão responsável.

Gestores **devem** assegurar que ações serão tomadas oportuna e adequadamente, de forma auditável, para resolver não conformidades.

9. DISPOSIÇÕES FINAIS

Serão responsabilizados pelos seus atos e omissões não aderentes a esta política aqueles que criarem, modificarem, armazenarem e transmitirem qualquer informação pertencente a **B&T**, sejam estes colaboradores, terceiros ou clientes, por período estabelecido em contrato junto ao Departamento de Recursos Humanos.

A utilização inadequada da informação pode resultar em sanções contratuais, além de penalidades previstas por lei.

Esta Política deve ser revisada anualmente, ou em períodos mais curtos, de acordo com as necessidades da B&T.

Estas instruções reguladoras têm por finalidade definir as condições de uso dos recursos oferecidos pela B&T, com base nos padrões e normas da família ISO 27000 e Legislação Brasileira, incluindo a lei nº 13.709, de 14 de agosto de 2018 (LGPD), além das exigências nos aspectos de segurança da B&T.

Quaisquer observações a esta política de segurança ou sugestões para sua melhoria devem ser encaminhadas para o Departamento de Controles Internos através do correio eletrônico: **controlesinternos@btcorretora.com.br**

10. HISTÓRICO DE VERSÕES

Versão	Data	Responsável (CI)	Validador (Gestor)	Aprovador (Diretor)
1.0	08/01/2020	Natalia Amador Controles Internos	N/A	Pablo Acylino Tecnologia da Informação
1.1	07/12/2021	Ana Vieira Controles Internos	Felipe Nicácio Segurança da Informação	Pablo Acylino Tecnologia da Informação
2.0	06/12/2022	Marcela Souza Controles Internos	Felipe Nicácio Segurança da Informação	Pablo Acylino Tecnologia da Informação

Título	Código	Área de Emissão	Data de Emissão	Versão
Política de Segurança da Informação Cibernética	POL-SI-001	Tecnologia da Informação	02/10/2025	4.0

2.1	08/08/2023	Ana Elisa Controles Internos	Felipe Nicácio Segurança da Informação	Pablo Acylino Tecnologia da Informação
3.0	16/07/2024	Ana Elisa Controles Internos		Pablo Acylino Tecnologia da Informação
4.0	02/10/2025	Ana Elisa Controles Internos	Alexandre Oliveira Infraestrutura	Ramon Coimbra Finanças e Tecnologia