PSI – Política de Segurança da Informação

Diretrizes e Normas Administrativas

Santos Bevilaqua Advogados

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

SUMÁRIO

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar

CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro

Rua Lauro Muller, 116, sala 1903

CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

1. INTRODUÇÃO

1.1 Apresentação

A finalidade da Política de Segurança da Informação (PSI) do Santos Bevilaqua Advogados, e definir diretrizes, controles e princípios claros para proteger seus ativos informacionais. priorizando minimizar os riscos e aprimorar continuamente o Sistema de Gestão de Segurança da Informação (SGSI). Deve, portanto, ser cumprida e aplicada em todas as áreas do escritório.

1.2 Objetivo

A presente Política de Segurança da Informação (PSI) visa assegurar a confidencialidade, integridade e disponibilidade das informações, ou seja, impedir o acesso por pessoas não autorizadas, assegurar que os dados não sejam alterados ou corrompidos, e garantir que as informações estejam sempre acessíveis quando necessário.

- ⇒ **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- ⇒ **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- ⇒ **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

1.2.1 Aplicação/Abrangência

A aplicação é válida para todos os usuários que têm acesso às informações do Santos Bevilaqua Advogados, sem distinção de vínculo com o escritório. Para proteger as informações do

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

escritório, cada colaborador (sócios, associados, diretores, gestores, celetista, e prestadores de serviços.) precisa:

⇒ Garantir a segurança das informações sob sua responsabilidade;

⇒ Conhecer e seguir a PSI e as normas internas;

⇒ Em caso de dúvidas, procurar a gestão ou a Gerência para obter ajuda.

2. Referências e Normativas

Esta Política de Segurança foi desenvolvida segundo os seguintes enunciados normativos:

⇒ Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD): Dispõe sobre o tratamento de dados pessoais, incluindo as regras para coleta, uso, armazenamento, compartilhamento e eliminação de dados.

⇒ Decreto nº 8.771/2016: Regulamenta o Marco Civil da Internet e estabelece diretrizes para a segurança das redes de comunicação e o tratamento de dados.

⇒ Resolução nº 5.956/2021 da Anatel: Dispõe sobre os requisitos de segurança cibernética para as redes de telecomunicações.

⇒ Normas técnicas da ABNT: Conjunto de normas que estabelecem padrões e requisitos para diversos aspectos da segurança da informação, como a NBR ISO/IEC 27002:2022, que trata do sistema de gestão de segurança da informação.

⇒ Regulamento Europeu – GDPR: O Regulamento Geral sobre a Proteção de Dados 2016/679 é uma legislação europeia que aborda questões relacionadas à privacidade e proteção de dados pessoais. Criado em 2018, este regulamento é aplicável a todas as pessoas na União Europeia e Espaço Econômico Europeu. Além disso, ele estabelece diretrizes para a transferência de dados pessoais para fora dessas regiões.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

É importante ressaltar que esta Política de Segurança está em constante atualização para se adequar às novas legislações e melhores práticas de segurança da informação. Para mais informações sobre os enunciados normativos citados, consulte os seguintes links:

⇒ Lei nº 13.709/2018 (LGPD): https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

⇒ Decreto nº 8.771/2016: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm

⇒ Resolução nº 5.956/2021 da Anatel: https://www.anatel.gov.br/legislacao/resolucoes/2021/1435-resolucao-no-5956

⇒ Normas técnicas da ABNT: https://www.abnt.org.br/

⇒ General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

3. DIRETRIZES GERAIS

O Santos Bevilaqua Advogados estabelece claramente que todos os dados gerados, processados, transmitidos ou armazenados por seus colaboradores são ativos de propriedade intelectual do escritório.

A forma como essa informação é apresentada, seja física, eletrônica, escrita ou falada, e o modo como é compartilhada, armazenada ou transmitida não alteram seu propósito fundamental: a informação deve ser usada exclusivamente para os fins autorizados. O escritório implementa e mantém esforços contínuos de segurança da informação para proteger os dados sob sua gestão.

As diretrizes de segurança são rigorosamente seguidas e monitoradas para garantir uma proteção adequada e eficaz. O Santos Bevilaqua Advogados reserva-se o direito de monitorar, auditar, bloquear ou fazer cópias de segurança de quaisquer dados ou

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

informações em sua posse, que trafeguem em sua rede, ou qualquer tipo de acesso físico ou lógico aos seus sistemas e ambientes.

Fica ainda estabelecido que equipamentos de informática, comunicação, sistemas e informações do escritório devem ser utilizados pelos colaboradores somente durante o exercício de suas atividades profissionais. A Gestão do escritório pode implementar medidas de monitoramento do uso de sistemas e serviços para assegurar a segurança das informações utilizadas.

4. COMITÊ DE SEGURANÇA DA INFORMAÇÃO – (CSI)

O comitê tem a finalidade de definir, coordenar e tomar decisões pertinentes, bem como deliberar sobre os principais aspectos de segurança da informação, assegurando que os projetos e iniciativas sejam compreendidos, avaliados e priorizados.

4.1 Organização do Comitê de Segurança da Informação – (CSI)

O Comitê de Segurança da Informação (CSI) é formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano. Os encontros do Comitê de Segurança da Informação (CSI) serão a cada semestre, no mínimo. Além disso, o (CSI) se reunirá em outras ocasiões sempre que houver necessidade de discutir incidentes sérios ou tomar decisões importantes para o escritório Santos Bevilaqua Advogados. O (CSI) utilizará especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

- ⇒ publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo próprio CSI.
- ⇒ propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos;
- ⇒ propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
- ⇒ avaliar os incidentes de segurança e propor ações corretivas;

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

⇒ definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares;

⇒ manter a segurança dos sistemas e da infraestrutura de TI realizando monitoramento contínuo e auditorias periódicas

4.2 Diretrizes para Notificação de Incidentes

O Santos Bevilaqua Advogados adota diretrizes para se preparar e responder a incidentes de segurança de forma rápida, organizada e eficiente, minimizando as consequências para todos os envolvidos. O nível de resposta dependerá da quantidade de dados e da complexidade do tratamento aplicado.

O que é um Incidente de Segurança?

Um incidente de segurança é uma situação inesperada que altera a ordem normal. No contexto da proteção de dados, isso significa uma ocorrência que coloca em risco os dados pessoais de indivíduos que se relacionam com o escritório. O National Institute of Standards and Technology (NIST) classifica um incidente de segurança como uma violação ou ameaça de violação de políticas de segurança computacional, políticas de uso aceitável ou padrões de prática de segurança.

A Lei Geral de Proteção de Dados (LGPD), em seu Artigo 46, exige que os agentes de tratamento de dados implementem medidas de segurança (técnicas e administrativas) para proteger os dados pessoais. O objetivo é evitar acessos não autorizados e situações acidentais ou ilícitas, como destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Além disso, o Artigo 48 da LGPD determina que o controlador deve comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados qualquer incidente de segurança que possa causar risco ou dano relevante. Essa comunicação deve ser feita em um prazo razoável e deve incluir, no mínimo:

⇒ Descrição da natureza dos dados pessoais afetados.

⇒ Informações sobre os titulares dos dados envolvidos.

⇒ Indicação das medidas técnicas e de segurança usadas para proteger os dados, resguardando segredos comercial e industrial.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

⇒ Riscos relacionados ao incidente.

⇒ Motivos da demora, caso a comunicação não tenha sido imediata.

⇒ Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Em resumo, as diretrizes do escritório estabelecem um protocolo claro e eficaz para a gestão de incidentes de segurança, garantindo a proteção dos dados pessoais e a conformidade com a LGPD

5. SEGURANÇA EM RECURSOS HUMANOS

Para a uniformidade da informação, a PSI será comunicada a todos os colaboradores do Santos Bevilaqua Advogados, a fim de que a política seja cumprida dentro e fora do escritório.

A inclusão do Termo de Confidencialidade ou da Cláusula de Confidencialidade é uma condição indispensável em todos os contratos do Santos Bevilaqua Advogados. Somente com essa garantia de confidencialidade será permitido o acesso aos ativos de informação disponíveis pelo escritório.

A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores. Todos deverão orientados sobre os procedimentos de segurança e o uso adequado dos ativos, a fim de minimizar possíveis riscos. Além disso, devem assinar um termo de responsabilidade.

Os ambientes de produção são segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação, quando pertinente.

Criar e instituir controles apropriados, trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que considerar relevantes. Isso abrange áreas como estações de trabalho, notebooks, acesso à internet, correio eletrônico e sistemas comerciais e financeiros, desenvolvidos internamente ou externamente.

O Santos Bevilaqua Advogados exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

A manutenção dos principais sistemas e serviços são testados periodicamente, visando reduzir os riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.
A PSI será executada no Santos Bevilaqua Advogados por meio de procedimentos específicos, obrigatórios para todos os colaboradores, sem distinção de nível hierárquico ou função na organização, bem como de vínculo empregatício ou prestação de serviços.
O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas do escritório e sujeitará o usuário às medidas administrativas e legais cabíveis.

5.1 Responsabilidades Específicas

5.1.1 Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física - sócios, associados, diretores, gestores, celetista, advogados, prestadores de serviços por intermédio de pessoa jurídica ou não - que exerça alguma atividade dentro ou fora do escritório.
Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao Santos Bevilaqua Advogados e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

5.1.2 Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação (CSI).
A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.1.3 Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de estágio, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do Santos Bevilaqua Advogados. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do Santos Bevilaqua Advogados.

Antes de conceder acesso às informações do escritório, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Em virtude dos privilégios inerentes às suas funções, administradores e operadores de sistemas computacionais possuem a capacidade de acessar arquivos e dados de outros
usuários. No entanto, tal acesso é restrito a situações em que se faz necessário para o desempenho de atividades operacionais sob sua responsabilidade, a exemplo da
manutenção de computadores, realização de cópias de segurança, auditorias ou testes no ambiente.

A fim de garantir a integridade dos registros de auditoria e evitar fraudes, segregar as funções administrativas e operacionais. Tais medida, visa restringir ao mínimo necessário os poderes de cada indivíduo, eliminando, ou ao menos reduzindo, a existência de pessoas que possam excluir os logs e trilhas de auditoria de suas próprias ações.

A segurança de sistemas com acesso público deve ser tratada com atenção especial, implementando medidas de proteção robustas e garantindo a guarda de evidências que permitam a rastreabilidade das ações para fins de auditoria ou investigação, caso seja necessário.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.1.4 Encarregado de Dados Pessoais (DPO)

O Santos Bevilaqua Advogados, nomeou um Encarregado de Dados Pessoais, também conhecido como Data Protection Officer (DPO), para desempenhar um papel importante no processo de proteção de dados, principalmente na resposta a incidentes de segurança da informação. Esse colaborador será o elo de comunicação entre o escritório, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), garantindo a conformidade com a LGPD.

Suas principais responsabilidades relacionadas incluem:

Facilitar a comunicação: Atuando como um facilitador entre a equipe técnica de resposta a incidentes e os gestores. Isso garante que o plano seja seguido corretamente e que todas as ações estejam em conformidade com as exigências da LGPD.

O DPO assegura que os titulares de dados sejam informados de forma clara e transparente sobre quaisquer incidentes que possam afetar seus dados pessoais.

5.2 Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI o Santos Bevilaqua Advogados poderá:

⇒ Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

⇒ Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação da gerência ou comitê de sócios do escritório ou por determinação do Comitê de Segurança da Informação;

⇒ Realizar, a qualquer tempo, inspeção nas máquinas de sua propriedade;

⇒ Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.3 Conscientização e Treinamentos

Promover treinamentos e conscientizações periódicas, com foco em Segurança de informação, para todos os seus colaboradores, terceiros e prestadores de serviço.
Mais informações podem ser encontradas na "*Treinamento de Conscientização de Segurança da Informação*".

5.4 Uso do correio eletrônico

O objetivo desta norma é informar aos colaboradores do Santos Bevilaqua Advogados quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do Santos Bevilaqua Advogados é para fins corporativos e relacionados às atividades do colaborador usuário dentro do escritório. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o Escritório e que não cause impacto no tráfego da rede.
O Santos Bevilaqua Advogados se reserva o direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas via e-mail corporativo.
Fica proibido aos colaboradores o uso do correio eletrônico do Santos Bevilaqua Advogados para/ou que:

- ⇒ Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do Escritório;
- ⇒ Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o escritório ou suas unidades vulneráveis a ações civis ou criminais;
- ⇒ Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

- ⇒ Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- ⇒ Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do escritório estiver sujeita a algum tipo de investigação;
- ⇒ Produzir, transmitir ou divulgar mensagem que: contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Santos Bevilaqua advogados;
- ⇒ Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- ⇒ Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg,.dll, .inf) ou qualquer outra extensão que represente risco à segurança;
- ⇒ Vise obter acesso não autorizado a outro computador, servidor ou rede;
- ⇒ Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- ⇒ Vise burlar qualquer sistema de segurança;
- ⇒ Vise vigiar secretamente ou assediar outro usuário;
- ⇒ Vise acessar informações confidenciais sem explícita autorização dos sócios;
- ⇒ Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- ⇒ Inclua imagens criptografadas ou de qualquer forma mascaradas;
- ⇒ Contenha anexo(s) superior(es) a 30 MB para envio (interno e internet) e 30 MB para recebimento (internet);
- ⇒ Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- ⇒ Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico etc.;
- ⇒ Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- ⇒ Tenha fins políticos locais ou do país (propaganda política);
- ⇒ Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

⇒ Nome do colaborador
⇒ Logo do escritório
⇒ Endereço da unidade
⇒ Telefone(s)
⇒ Link do site do Escritório

5.5 Uso de internet

O Santos Bevilaqua Advogados estabeleceu um conjunto de regras para promover o uso ético e profissional da internet por seus colaboradores. Embora a conexão à rede corporativa ofereça grandes benefícios, ela também apresenta riscos significativos para os ativos de informação do escritório

5.5.1 Monitoramento e Propriedade

Qualquer informação acessada, transmitida, recebida ou produzida na internet por meio da rede do escritório está sujeita a divulgação e auditoria. Por isso, o Santos Bevilaqua Advogados, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.
Os equipamentos, tecnologia e serviços que dão acesso à internet são propriedade do escritório. Isso significa que o escritório pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicativo armazenado na rede ou internet (seja em disco local, na estação de trabalho ou em áreas privadas da rede) para assegurar o cumprimento de sua Política de Segurança da Informação.

5.5.2 Segurança da Informação e Responsabilidades

O monitoramento da rede interna visa garantir a integridade dos dados e programas. Qualquer tentativa de alterar os parâmetros de segurança sem a devida credencial e autorização será

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

considerada inadequada, e os riscos envolvidos serão comunicados ao colaborador e ao seu gestor. O uso de recursos para atividades ilícitas pode resultar em ações administrativas e penalidades civis e criminais, com o escritório cooperando ativamente com as autoridades competentes.

5.5.3 Uso Pessoal da Internet

A internet disponibilizada pelo escritório pode ser utilizada para fins pessoais, desde que:

- ⇒ Não prejudique o andamento dos trabalhos nas unidades.
- ⇒ Não comprometa a banda da rede em horários comerciais.
- ⇒ Não perturbe o bom andamento das atividades.
- ⇒ Não implique conflitos de interesse com os objetivos de negócio do escritório.

Isso significa que o uso de sites de notícias ou serviços, por exemplo, é aceitável, pois o Santos Bevilaqua Advogados tem interesse que seus colaboradores estejam bem-informados.

5.5.4 Diretrizes Específicas de Uso

Imagens e Direitos Autorais: Apenas colaboradores autorizados podem copiar, capturar, imprimir ou enviar imagens da tela para terceiros, devendo seguir a norma interna de uso de imagens, a Lei de Direitos Autorais, a proteção da imagem garantida pela Constituição Federal e demais leis aplicáveis.

Informações Confidenciais: É proibida a divulgação ou compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo, comunicadores instantâneos ou qualquer outra tecnologia correlata na internet.

Downloads: Colaboradores com acesso à internet só podem fazer download de programas diretamente ligados às suas atividades no escritório e devem providenciar a regularização da licença e o registro desses programas, mediante autorização da Gestão.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Softwares Não Autorizados/Pirateados: A instalação, cópia ou distribuição não autorizada de softwares com direitos autorais, marca registrada ou patente na internet são expressamente proibidas. Softwares não autorizados baixados serão excluídos pela Gerência de Sistemas. Em hipótese alguma, os recursos do escritório podem ser usados para download ou distribuição de software ou dados pirateados, o que é considerado crime.

Conteúdo Sensível: Materiais de cunho sexual não podem ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja estritamente necessário para um perfil de usuário especial, grupos de segurança específicos deverão ser criados e seus integrantes definidos pelos gestores.

Upload de Dados do Escritório: Colaboradores com acesso à internet não podem fazer upload de softwares licenciados ao Santos Bevilaqua Advogados ou de dados de sua propriedade para parceiros e clientes sem autorização expressa do responsável.

Vírus e Ameaças: É proibido utilizar os recursos do escritório para propagar deliberadamente qualquer tipo de vírus, *worm*, *cavalo de troia*, *spam*, assédio, perturbação ou programas de controle de outros computadores.

5.5.5 Aplicações Específicas

Não é permitido:

- ⇒ Acesso a softwares *peer-to-peer* (como Kazaa, BitTorrent e similares).
- ⇒ o acesso a sites de *proxy*

Serviços de *streaming* (rádios online, canais de *broadcast* e similares) serão permitidos apenas para grupos específicos.

Serviços de comunicação instantânea (Microsoft Teams, WhatsApp e similares) serão inicialmente disponibilizados, mas podem ser bloqueados caso o gestor requisite formalmente ao comitê de sócios.

Essas diretrizes asseguram que o ambiente digital do Santos Bevilaqua Advogados seja utilizado de forma segura, ética e legal, protegendo tanto os ativos do escritório quanto os dados de seus clientes.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.6 Uso das mídias sociais

Todas as questões relativas à comunicação externa e mídias sociais são centralizadas nas áreas de marketing, comunicação ou outras áreas formalmente autorizadas. Consequentemente, nenhum colaborador, terceiro, prestador de serviços e/ou parceiro está autorizado a publicar, comentar ou adotar comportamentos similares em nome do Santos Bevilaqua Advogados, seja por meio de comunicação, mídias sociais ou sites externos, sem a devida autorização.

5.7 Uso de software de mensageria

O Santos Bevilaqua Advogados autoriza o uso da ferramenta Microsoft Teams para a comunicação interna de seus colaboradores, sendo proibida a transferência ou compartilhamento de arquivos ou quaisquer informações confidenciais para fora da rede corporativa.

5.8 Uso dos Computadores e Recursos Tecnológicos

As diretrizes para o uso de equipamentos e recursos de TI no Santos Bevilaqua Advogados visam garantir a segurança, a integridade dos dados e a utilização adequada dos ativos do escritório. Os colaboradores devem manusear os equipamentos corretamente e seguir os procedimentos operacionais.

5.8.1 Manutenção e Atualizações

Qualquer procedimento de manutenção, instalação, desinstalação, configuração ou modificação em equipamentos e sistemas é de responsabilidade exclusiva do departamento de Suporte de TI. Atualizações e correções de segurança só podem ser aplicadas após validação em ambiente de homologação e disponibilização pelo fabricante.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.8.2 Antivírus e Reporte de Incidentes

Todos os sistemas e computadores devem ter antivírus instalado, ativado e permanentemente atualizado. Em caso de suspeita de vírus ou problemas de funcionalidade, o usuário deve acionar o departamento técnico abrindo um chamado no service desk.

5.8.3 Transferência e Armazenamento de Dados

Transferência de Software: A transferência ou divulgação de qualquer software ou programa para terceiros só pode ser feita com a devida identificação do solicitante, após verificação positiva, de acordo com a classificação da informação e a real necessidade do destinatário.
Arquivos Pessoais**:** Arquivos pessoais (fotos, músicas, vídeos etc.) não devem ser copiados para os drives de rede para evitar sobrecarga dos servidores. Caso identificados, esses arquivos poderão ser excluídos definitivamente, após comunicação prévia ao usuário.
Documentos Essenciais: Documentos cruciais para as atividades do escritório devem ser salvos nos drives de rede. Arquivos salvos apenas localmente (ex: "drive C:") não terão garantia de backup e podem ser perdidos em caso de falha no computador, sendo responsabilidade do próprio usuário.

5.8.4 Uso da Rede e Segurança

Colaboradores, especialmente os com contas privilegiadas, não devem executar comandos ou programas que sobrecarreguem a rede corporativa sem prévia autorização da Gerência de Sistemas. Todos os incidentes corporativos, como vulnerabilidades, vírus ou ataques digitais, devem ser imediatamente reportados à segurança da informação pelo e-mail suporte@santosbevilaqua.com.br .

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.8.5 Diretrizes de Uso de Computadores e Equipamentos

As principais diretrizes para o uso adequado de computadores e recursos de informática são:

Senhas: Todos os computadores individuais devem ter senha para restringir acesso não autorizado. As senhas são definidas pela Gerência do escritório, que terá acesso para fins de manutenção.

Dispositivos Estranhos: Colaboradores devem informar ao suporte@santosbevilaqua.com.br sobre qualquer dispositivo estranho conectado ao computador.

Manuseio e Reparo: É proibido abrir ou manusear computadores ou outros equipamentos para reparos não realizados por um técnico da Gerência do escritório ou por terceiros contratados.

Os dispositivos USB são bloqueados; impedindo transferência de dados, e assim protegendo o ambiente de programas ou vírus indesejados. Em situações excepcionais, o desbloqueio dos dispositivos USB pode ser permitido como contingência, condicionado a autorização expressa dos gestores das áreas envolvidas, e ciência da equipe de informática.

Alimentação e Fumo: É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

Configuração e Segurança: O colaborador deve manter a configuração do equipamento fornecido pelo escritório, seguindo as políticas de segurança da informação e as normas específicas, assumindo a responsabilidade como custodiante das informações.

Bloqueio de Terminais: Terminais de computador e impressoras devem ser protegidos por senha (bloqueados) quando não estiverem em uso, conforme a Norma de Autenticação.

Senhas Padrão: Senhas padrão (default) de recursos tecnológicos adquiridos pelo escritório devem ser alteradas imediatamente.

Registros de Eventos: Os equipamentos devem preservar de forma segura os registros de eventos, incluindo identificação dos colaboradores, datas e horários de acesso.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

5.8.6 Usos Proibidos de Computadores e Recursos Tecnológicos

É proibido o uso dos recursos do Santos Bevilaqua Advogados para as seguintes situações:

- ⇒ Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- ⇒ Burlar sistemas de segurança.
- ⇒ Acessar informações confidenciais sem autorização explícita dos sócios.
- ⇒ Vigiar secretamente outras pessoas por dispositivos eletrônicos ou softwares (ex: *sniffers*).
- ⇒ Interromper serviços, servidores ou redes por métodos ilícitos/não autorizados.
- ⇒ Usar recursos tecnológicos para cometer ou ser cúmplice de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem autorização legal.
- ⇒ Hospedar pornografia, material racista ou qualquer outro que viole a legislação, moral, bons costumes e ordem pública.
- ⇒ Utilizar software pirata, o que é considerado crime pela legislação nacional.

5.8.7 Utilização da Rede Corporativa

O Santos Bevilaqua Advogados detém a propriedade exclusiva de todos os bens materiais e digitais, incluindo softwares, documentos, designs e outros, criados por seus colaboradores, terceiros, prestadores de serviço e parceiros, desde que utilizados recursos tecnológicos do escritório, independentemente do horário de criação. A título de exemplificação, informações, documentos (sejam estes em formato físico ou lógico), criações, inventos, desenvolvimentos, aperfeiçoamentos ou quaisquer outras melhorias que sejam feitas, armazenadas, produzidas ou transformadas, podem ser considerados bens materiais e intelectuais.

Todos os usuários possuem a responsabilidade de preservar a propriedade intelectual da organização, bem como de observar e respeitar a propriedade intelectual de terceiros, em conformidade com a legislação vigente. Em casos de omissão, dolo ou culpa, os usuários poderão ser responsabilizados.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Todas as informações pertencentes ao escritório, ou por ele disponibilizadas, são de uso exclusivo para fins corporativos, sendo vedada a sua utilização para fins particulares, bem como o seu repasse a terceiros, independentemente da forma como tenham sido obtidas, inferidas ou desenvolvidas pelo colaborador em seu ambiente de trabalho.

6. Segurança de Acessos (Lógico E Físico)

A responsabilidade por todas as ações realizadas com as credenciais de acesso (físicas ou lógicas) é do colaborador, incluindo as ações em sua estação de trabalho durante o período de login. As credenciais são pessoais e intransferíveis.

6.1 Gestão de Acessos Físicos

Controle de acesso: O acesso ao Datacenter somente deverá ser feito por pessoas autorizadas. O acesso de visitantes ou terceiros somente poderá ser realizado com prévia autorização da gerência e/ou diretoria do escritório e acompanhamento de um colaborador autorizado.

Vigilância: câmeras de segurança do condomínio monitoram as instalações. Deverão existir duas cópias de chave da porta do Datacenter. Uma das cópias ficará de posse do responsável pelo acesso ao ambiente e a outra de posse da gerência do escritório.

Proteção contra incêndios: Implementação de sistemas de detecção e combate a incêndios para proteger os bens materiais.

Controle ambiental: O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizada com a colaboração do Departamento de Serviços Gerais. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto inflamável.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

6.2 Gestão de identidade, acessos lógicos e configuração de senhas

A proteção de identidade e senhas é fundamental no Santos Bevilaqua Advogados para prevenir fraudes e garantir a segurança das informações. O controle de acesso é rigoroso, seguindo o princípio do menor privilégio, onde cada colaborador acessa apenas o essencial para suas funções.

6.2.1 Responsabilidade e Uso de Dispositivos de Identificação

O uso de dispositivos ou senhas de terceiros é crime (Art. 307 do Código Penal). Todos os dispositivos de identificação no escritório – como crachás, acessos a sistemas, certificados digitais e dados biométricos – devem estar associados a uma única pessoa física e seus documentos oficiais. O usuário é o único responsável pelo uso correto desses dispositivos, tanto perante o escritório quanto a lei.

6.2.2 Compartilhamento de Login e Senhas

É proibido compartilhar qualquer dispositivo de identificação pessoal. Se um login for de uso compartilhado, a responsabilidade legal recai sobre os usuários que o utilizarem, exceto se o gestor tiver conhecimento ou solicitado o compartilhamento. O compartilhamento de login para funções de administração de sistemas é estritamente proibido.

6.2.3 Requisitos e Gerenciamento de Senhas

O acesso aos sistemas é protegido por autenticação forte, incluindo senhas seguras e autenticação multifator (MFA).
Senhas de usuários sem perfil de administrador: Mínimo de 8 caracteres alfanuméricos, com caracteres especiais (@ # $ %) e variação de letras maiúsculas e minúsculas.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Senhas de administradores ou com acesso privilegiado: Mínimo de 12 caracteres alfanuméricos, com caracteres especiais (@ # $ %) e variação de letras maiúsculas e minúsculas, obrigatoriamente.

As senhas não devem ser:

⇒ Anotadas ou armazenadas em arquivos eletrônicos não criptografados.

⇒ Baseadas em informações pessoais (nome, data de nascimento etc.).

⇒ Combinações óbvias de teclado (ex: "abcdefgh").

⇒ A troca de senhas deve ocorrer a cada 60 dias, sem repetição das últimas 24 senhas. Para sistemas críticos e logins privilegiados, a troca é a cada 30 dias. Os sistemas devem forçar essa troca dentro dos prazos estabelecidos.

6.2.4 Bloqueio de Acessos e Recuperação de Senha

Todos os acessos são bloqueados imediatamente quando se tornam desnecessários. Em caso de desligamento de um colaborador, o Departamento Pessoal deve comunicar imediatamente o Departamento de TI para o bloqueio do acesso. Essa regra também se aplica a contratos encerrados ou usuários de testes.

Se um colaborador esquecer sua senha, deve solicitar formalmente uma nova ao administrador do ambiente, via e-mail suporte@santosbevilaqua.com.br

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

6.2.5 Processo de Revogação de Acesso

Desligamento	Desfavorável	Boas condições
Momento da Revogação	Imediato/abrupto na comunicação do desligamento.	Geralmente no último dia de trabalho, ou gradualmente.
Nível de Risco	Alto	Baixo a moderado
Abrangência	Total e completa. Nenhum acesso residual.	Pode haver manutenção temporária de acessos específicos para transição.
Monitoramento	Potencial para monitoramento.	Geralmente sem monitoramento intensivo pós-aviso.
Acompanhamento	Com foco na mitigação de ameaças.	Com foco na transição suave.

7. SEGURANÇA DE DADOS

Todas as informações do Santos Bevilaqua Advogados são classificadas, através de atribuição de um nível adequado de proteção, consoante o seu valor, nível de sigilo, sensibilidade e criticidade para o negócio **(privilégio mínimo).** Os dados do Santos Bevilaqua Advogados são manipulados e armazenados em computadores corporativos e/ou nuvem privada oficiais.

Não é permitido manusear, armazenar e transferir dados, sem autorização, para dispositivos ou meios de armazenamento externos, como ambientes de armazenamento em nuvens que não sejam da organização (Dropbox, OneDrive, iCloud, Google Drive, dentre outros).

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.1 Classificação da informação de dados

Para garantir a segurança e a confidencialidade das informações, o Santos Bevilaqua Advogados restringe o acesso ao que é essencial para as atividades de cada colaborador.

7.1.1 Classificação da Informação e Responsabilidades

As informações do Santos Bevilaqua, de terceiros ou de suas subsidiárias, são classificadas conforme seu grau de sensibilidade. Essa classificação define a prioridade e o nível de proteção adequados. A responsabilidade pela classificação é dos gestores de cada área ou de colaboradores por eles designados. Mesmo que a tarefa seja delegada, a responsabilidade final recai sobre o gestor. O escritório designou agentes de mudança/transformação para ajudar a implementar a cultura de classificação da informação. No entanto, é responsabilidade de todos os colaboradores tratar as informações de acordo com seu nível de classificação e as diretrizes estabelecidas.

7.1.2 Monitoramento e Reclassificação

Periodicamente, o processo de classificação e tratamento da informação poderá ser monitorado e medido para verificar a aderência, obter métricas, sugerir melhorias e criar planos de ação.
A classificação exige uma análise cuidadosa de fatores como:

- ⇒ Valor intrínseco da informação.
- ⇒ Obrigações legais.
- ⇒ Nível de sensibilidade e criticidade.
- ⇒ Prazo de validade.
- ⇒ Necessidades de compartilhamento e restrição.
- ⇒ Riscos envolvidos.
- ⇒ Impacto potencial nos negócios e na reputação do escritório.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

O responsável pela classificação deve realizar análises críticas periódicas para garantir que o nível de proteção esteja sempre adequado à realidade, já que a classificação pode mudar ao longo do tempo. Uma informação pode ser reclassificada quando:

⇒ For identificada uma classificação incorreta.
⇒ Ocorrerem mudanças no contexto de sensibilidade da informação durante seu ciclo de vida.
⇒ Houver necessidade de atender a um requisito legal ou a mudanças em processos internos do Santos Bevilaqua.

7.2 Responsáveis pela Demanda de Classificação

⇒ Todos os usuários são responsáveis por comunicar ao gestor da informação a inexistência ou inconsistência na devida classificação da informação;
⇒ A responsabilidade da reclassificação ou não, cabe ao gestor;
⇒ Informações de origem externa que participam dos processos do Santos Bevilaqua, tais como relatórios de terceiros, informações e documentos de clientes e fornecedores, são tratados de acordo com o nível de criticidade e sensibilidade definido pelo responsável externo;
⇒ Deve-se procurar estabelecer um acordo com terceiros, no qual se faz troca de informações, para que se tenha a devida identificação, classificação e tratamento das informações entre as organizações, visando o compartilhamento seguro das informações;
⇒ O responsável por receber e/ou compartilhar informações proveniente de agente externo, deve ter uma atenção especial na interpretação dos rótulos de classificação sobre os documentos, pois podem ter definições diferentes para rótulos iguais, ou semelhantes aos aqui usados;

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.3 Responsáveis pela Demanda de Reclassificação

Todos os usuários são responsáveis por comunicar ao gestor da informação a inexistência ou inconsistência na devida classificação da informação. A responsabilidade da reclassificação ou não, cabe ao gestor.

7.4 Níveis de classificação.

Abaixo os níveis de classificação que são utilizados no Santos Bevilaqua Advogados.

Níveis de Classificação	Características
Pública	As informações que podem ou serão divulgadas publicamente são aquelas cuja divulgação não acarreta prejuízo ao Santos Bevilaqua Advogados, seus clientes ou parceiros. Essas informações podem ser compartilhadas livremente com o público em geral, desde que sua integridade seja preservada. A Santos Bevilaqua Advogados reserva-se o direito de designar um responsável ou setor para realizar tais divulgações. A classificação dessas informações permanece sob a responsabilidade do gestor.
Interna	As informações internas do escritório são acessíveis a todos os colaboradores e prestadores de serviços, desde que estes assumam o compromisso de manter a confidencialidade das informações às quais têm acesso.
Reservada	Informações confidenciais são aquelas cujo acesso é restrito a um grupo específico de indivíduos, áreas ou cargos dentro do Santos Bevilaqua Advogados. O acesso a tais informações é restrito àqueles que necessitam delas para o desempenho de suas funções profissionais. Exemplos de informações confidenciais incluem projetos, relatórios, indicadores e outros documentos similares.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Secreta/Confidencial	Informações classificadas como Secretas/Confidenciais exigem tratamento especial, visto que sua divulgação não autorizada ou acesso indevido podem acarretar prejuízos de natureza financeira, legal, normativa, contratual, ou ainda, danos à reputação, imagem ou estratégia do Santos Bevilaqua Advogados. São exemplos de informações Secretas/Confidenciais dados pessoais de indivíduos, informações de fornecedores e informações estratégicas do escritório.

7.5 Rotulação da Informação

Todas as informações do Santos Bevilaqua Advogados são identificadas com, no mínimo, o nível de classificação atribuído, o grupo de acesso permitido e a data de criação. A identificação da informação deve deixar claro o nível de classificação e o grupo de acesso.
Exemplos de materiais que são rotulados:

- ⇒ Documentos
- ⇒ Pastas
- ⇒ Envelopes
- ⇒ Arquivos físicos
- ⇒ Arquivos eletrônicos
- ⇒ Mídias eletrônicas
- ⇒ Conversas
- ⇒ Palestras

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.5.1 Rotulagem de Documentos e Mídias

Relatórios (em tela, arquivo, impressos), telas de sistemas, mensagens eletrônicas e transferências de arquivos devem apresentar rótulos apropriados da classificação da informação. Esses rótulos devem estar claramente visíveis, no mínimo, na capa de documentos, pastas ou arquivos de armazenamento. É fortemente recomendado rotular todas as páginas dos documentos, adicionando cabeçalhos ou rodapés.

O responsável pela rotulagem é o mesmo que realizou o processo de classificação. Se um documento contiver diferentes níveis de classificação, ele deve ser classificado e rotulado de acordo com o nível mais alto/restritivo presente no arquivo.

7.5.2 Transmissão Verbal de Informações

Em situações como reuniões ou apresentações, quem for transmitir informações verbalmente deve divulgar a classificação da informação e os cuidados necessários, tanto no início quanto no fim do evento.

7.5.3 Armazenamento Digital

Informações armazenadas em servidores de arquivos e outros dispositivos de armazenamento devem ter um rótulo claro de grupo de acesso. Se for uma pasta compartilhada, ela deve possuir bloqueio para acesso não autorizado. Documentos em meios digitais devem conter cabeçalhos ou rodapés informando a categoria da informação.

7.6 Tratamento da Informação

O tratamento adequado da informação é essencial para assegurar sua confidencialidade, integridade e disponibilidade, garantindo maior controle e proteção. Todas as informações recebem o mesmo cuidado, independentemente da pessoa, cargo ou área.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

7.6.1 Manuseio de Documentos Físicos

Documentos classificados como confidenciais ou secretos em formato físico devem ser guardados em gavetas ou armários trancados, impedindo o acesso de pessoas não autorizadas. Quando o local de trabalho estiver desocupado, esses documentos devem ser removidos de mesas e outras áreas visíveis. Informações internas, confidenciais ou secretas não devem ser deixadas expostas em quadros, lousas ou similares, para evitar que pessoas não autorizadas as vejam.

7.6.2 Cenários Não Previstos

As diretrizes para o tratamento de informações, considerando os diferentes cenários e níveis de classificação, estão detalhadas em uma tabela específica. Se um cenário não estiver previsto, o gestor imediato deve ser acionado para que a norma seja atualizada.

Nível de Classificação				
Cenário	**Público**	**Interno**	**Reservado**	**Secreto**
Acesso Lógico ou Físico	Sem Restrições	Somente para colaboradores do Santos Bevilaqua	Somente pessoas do grupo de acesso	Somente pessoas do grupo de acesso
Armazenamento em mídia impressa (papéis, cartazes etc.)	Sem Restrições	Somente para colaboradores do Santos Bevilaqua Advogados	Somente pessoas do grupo de acesso	Somente em áreas com acesso físico controlado ao grupo de acesso, em locais com restrição de acesso (armários/gavetas com chaves).
Armazenamento em arquivos digitais (rede)	Sem Restrições	Somente dentro das áreas do Santos Bevilaqua Advogados	Somente em áreas com acesso físico controlado ao grupo de acesso.	Somente nos servidores de arquivos na rede do Santos Bevilaqua Advogados e com controle de acesso. Preferencialmente com mais um nível de acesso (ex. criptografia).

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Armazenamento em mídia digital (DVD, CD, Pen drive etc.)	Sem Restrições	Somente nos servidores de arquivos na rede do Santos Bevilaqua Advogados	Somente nos servidores de arquivos na rede do Santos Bevilaqua Advogados e com controle de acesso.	Somente com autorização do sócio ou gestor da área e tendo senha ou criptografia forte. Preferencialmente a mídia deve ser armazenada dentro das dependências do Santos Bevilaqua Advogados, em armário ou gaveta com chave e em locais com acesso físico controlado ao grupo de acesso.
Reprodução (impressa ou digital)	Sem Restrições	Mídias são armazenadas dentro das dependências do Santos Bevilaqua Advogados	Somente com autorização do sócio ou gestor da área. Preferencialmente a mídia deve ser armazenada dentro das dependências do Santos Bevilaqua Advogados, em armário ou gaveta com chave e em locais com acesso físico controlado ao grupo de acesso.	Somente com a autorização do gestor responsável.
Reprodução (impressão)	Sem Restrições	Somente para os colaboradores do Santos Bevilaqua Advogados	Somente quando o usuário acompanhar a impressão e garantir que ninguém terá acesso ao documento impresso. Usar senha para liberar impressão, quando a impressora possuir este recurso.	Somente com autorização do gestor responsável e o usuário deve acompanhar a impressão e garantir que ninguém terá acesso ao documento impresso. Usar senha para liberar impressão, quando a impressora possuir estes recursos.
Transporte físico	Sem Restrições	Sem restrições dentro dependências do Santos Bevilaqua Advogados Transporte para fora do Santos Bevilaqua Advogados, deve haver autorização do gestor responsável	Somente com utilização de lacres, caso o transporte não seja realizado, por alguém do grupo de acesso. Necessário autorização do gestor responsável se for para fora das dependências do Santos Bevilaqua Advogados, no qual se deve armazenar as informações em um local protegido durante a viagem.	Somente com utilização de lacre. Caso o transporte não seja realizado por alguém do grupo de acesso, usar serviço de entrega em mãos. Transporte para fora das dependências do Santos Bevilaqua Advogados, necessita de autorização do gestor responsável. Armazenar a informação em um local protegido preferencialmente com chave ou em um cofre, durante a viagem.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Transmissão por e-mail	Sem Restrições	Interno, sem restrições. Para fora do Santos Bevilaqua Advogados, é necessário a autorização do gestor responsável.	Somente para o grupo de acesso. Para fora do grupo de acesso, é necessária a autorização do sócio da informação.	Somente para o grupo de acesso. Para fora do grupo de acesso, é necessária a autorização do sócio da informação. Adicionalmente são consideradas técnicas de proteção, como, senha e criptografia.
Transmissão digital externa (FTP, link, internet etc.)	Sem Restrições	Somente com autorização do gestor responsável.	Somente com autorização do gestor responsável e através dos equipamentos do Santos Bevilaqua Advogados	Somente com autorização do gestor responsável e através dos equipamentos do Santos Bevilaqua Advogados e de forma criptografada.
Transmissão de vídeo/voz	Sem Restrições	Somente para os colaboradores do Santos Bevilaqua Advogados	Somente para o grupo de acesso.	Somente para o grupo de acesso e através dos equipamentos do Santos Bevilaqua Advogados
Transmissão em apresentações	Sem Restrições	Somente para os colaboradores do Santos Bevilaqua Advogados	Somente para o grupo de acesso. Para outras pessoas fora desse grupo somente com autorização do gestor responsável.	Somente para o grupo de acesso. Para outras pessoas fora do grupo de acesso, somente com autorização do gestor responsável.
Eliminação de mídia digital e/ou analógica	Sem Restrições	Somente dentro das áreas do Santos Bevilaqua Advogados	O dispositivo deverá ser destruído fisicamente ou as informações são destruídas, apagadas ou sobre gravadas por meio de técnicas que tornem as informações originais irrecuperáveis. Não utilizar apenas a função padrão de apagar ou formatar.	O dispositivo deverá ser destruído fisicamente ou as informações são destruídas, apagadas ou sobre gravadas por meio de técnicas que tornem as informações originais irrecuperáveis. Não utilizar apenas a função padrão de apagar ou formatar
Eliminação de mídia impressa	Sem Restrições	Triturar as informações dentro das dependências do Santos Bevilaqua Advogados	Fragmentar as informações preferencialmente dentro das dependências do setor responsável e na presença de alguém do grupo de acesso daquela informação.	Fragmentar as informações preferencialmente dentro das dependências do setor responsável e na presença de alguém do grupo de acesso daquela informação

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar

CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro

Rua Lauro Muller, 116, sala 1903

CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Eliminação de arquivos de computadores	Sem Restrições	Excluir da pasta onde está arquivada.	Excluir da pasta onde está arquivada e da lixeira também	Excluir da lixeira dos dispositivos e adotar soluções tecnológicas visando garantir que as informações não possam ser recuperadas.

8. SEGURANÇA DE RECURSOS TECNOLÓGICOS

É estritamente proibido usar quaisquer dispositivos de Tecnologia da Informação (como servidores, bancos de dados, roteadores, softwares de desenvolvimento etc.) que não tenham sido previamente aprovados e estejam sob a gestão da área de TI ou segurança da informação.

8.1 Segurança Mínima dos Recursos Tecnológicos Corporativos

Os recursos tecnológicos corporativos devem ter implementado, no mínimo:

Segurança de Servidores: Monitoramento constante para eliminar vulnerabilidades e aplicar correções de segurança imediatas.

Segregação de Rede: Implementação de segregação de rede (física ou lógica) com mecanismos e tecnologias adequadas para garantir a confidencialidade, integridade e disponibilidade das informações que trafegam.

Antivírus: Instalação de softwares antivírus em todas as estações de trabalho, com procedimentos definidos para garantir sua atualização e funcionamento correto.

Proteção de E-mails: Soluções de proteção de e-mails, incluindo anti-spoofing, filtro de reputação, AntiSpam e antiphishing.

- ⇒ Barreiras de Segurança: Equipamentos que estabeleçam barreiras de segurança, como Firewalls e WAF (Web Application Firewall).
- ⇒ Segurança em Computadores de Usuários: Computadores de usuários com firewall pessoal, configurações de segurança e atualização de *patches* para reduzir a chance de invasões, evasão de informações e acessos não autorizados.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

8.1.1 Monitoramento e Prevenção de Incidentes

Controles tecnológicos são implementados para monitorar, proteger e minimizar os riscos associados às informações ou ativos de processamento, visando preservar a confidencialidade, integridade e disponibilidade. Esses controles devem atuar na prevenção, restrição, monitoração e detecção de incidentes de segurança (ex: NOC - *Network Operations Center* e SOC - *Security Operations Center*). Além disso, os relógios dos ambientes e sistemas corporativos são sincronizados com uma fonte de tempo precisa e única para todos.

8.2 Criptografia

A criptografia de disco é obrigatória em todos os notebooks e dispositivos móveis do escritório. Essa medida visa proteger informações confidenciais e prevenir vazamento de dados em caso de perda ou roubo de equipamentos.

Para a segurança das informações do escritório, qualquer aplicação hospedada externamente deve usar o protocolo HTTPS para comunicação e criptografia avançada na transmissão dos dados.

A transmissão de informações confidenciais pela internet (via APIs, serviços ou comunicação com parceiros) exige a implementação de mecanismos de criptografia dedicados. As chaves criptográficas usadas são armazenadas de forma segura e centralizada, utilizando softwares de gerenciamento ou cofres de senhas corporativos.

.

8.3 Gestão de logs e trilhas de auditorias

É fundamental que todos os sistemas de importância crítica para o escritório possuam mecanismos de auditoria habilitados. Esses mecanismos devem registrar todas as ações privilegiadas, como o início e o término de acesso ao sistema, a conexão e desconexão de dispositivos, tentativas de acesso não autorizadas e violações de segurança, entre outros eventos relevantes. A segurança dos registros de eventos (logs) e seus recursos exige proteção contra acesso não autorizado e adulteração, assegurando a veracidade e a confidencialidade das informações.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

8.4 Gestão de backup

Todos os backups são automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.
As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) são acondicionadas em local seco, climatizado, seguro (de preferência, e se possível, em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As mídias de backup são devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.
A necessidade de renovação das mídias em razão de seu desgaste natural, bem como a existência de estoque dessas mídias para qualquer uso emergencial, é determinada, e controlada, pelos responsáveis pela atividade.
Mídias que apresentam erros devem, primeiramente, ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.
As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente, e se possível, com estrutura de sala-cofre.
Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do Santos Bevilaqua Advogados, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

O executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem realizar a operação. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

Mais informações podem ser encontradas na "*Diretrizes de Backup*".

9. Suporte de Segurança Da Informação (Gestão de Acessos e Service Desk)

O Santos Bevilaqua Advogados mantém uma parceria com uma empresa terceirizada especializada em suporte de segurança da informação. Essa colaboração abrange a gestão de acessos e o service desk, contando com expertise em tecnologia da informação aplicada ao contexto jurídico.

A atuação abrange as seguintes demandas:

⇒ Suporte e manutenção de máquinas;

⇒ Gestão de acessos aos sistemas e ambientes do escritório;

⇒ Gerir e publicar o inventário de sistemas, máquinas, matriz de acessos;

⇒ Gerir atividades de proteção, coordenar e comunicar eventos de segurança cibernética;

⇒ Avaliação de requisitos de segurança em novos projetos;

⇒ Gestão e Detecção de Vulnerabilidades;

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

⇒ Resposta a Incidentes de Segurança;

⇒ Suporte ao Comitê de Segurança da Informação para atualizações das Políticas, Normas e procedimentos relacionadas à SI.

10. DIRETRIZES, TERMOS E PROCEDIMENTOS INTERNOS COMPLEMENTARES

Documentos que compõem os esforços de Segurança da Informação e Privacidade do Santos Bevilaqua Advogados, sem prejuízo de outras políticas, termos e normas não especificadas aqui, são:

⇒ Ações de Conscientização e Treinamento em Segurança da Informação -SBA

⇒ Diretrizes de Notificação de Incidentes - SBA

⇒ Plano de Resposta aos Incidentes de Segurança da Informação

⇒ Diretrizes de Criptografia – SBA

⇒ Diretrizes de Hardening - SBA

⇒ Plano de Continuidade de Negócios e Gestão de Crises

11. SANITIZAÇÃO

A sanitização visa proteger informações confidenciais garantindo a conformidade com leis de privacidade (LGPD) e mantendo a integridade dos dados.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

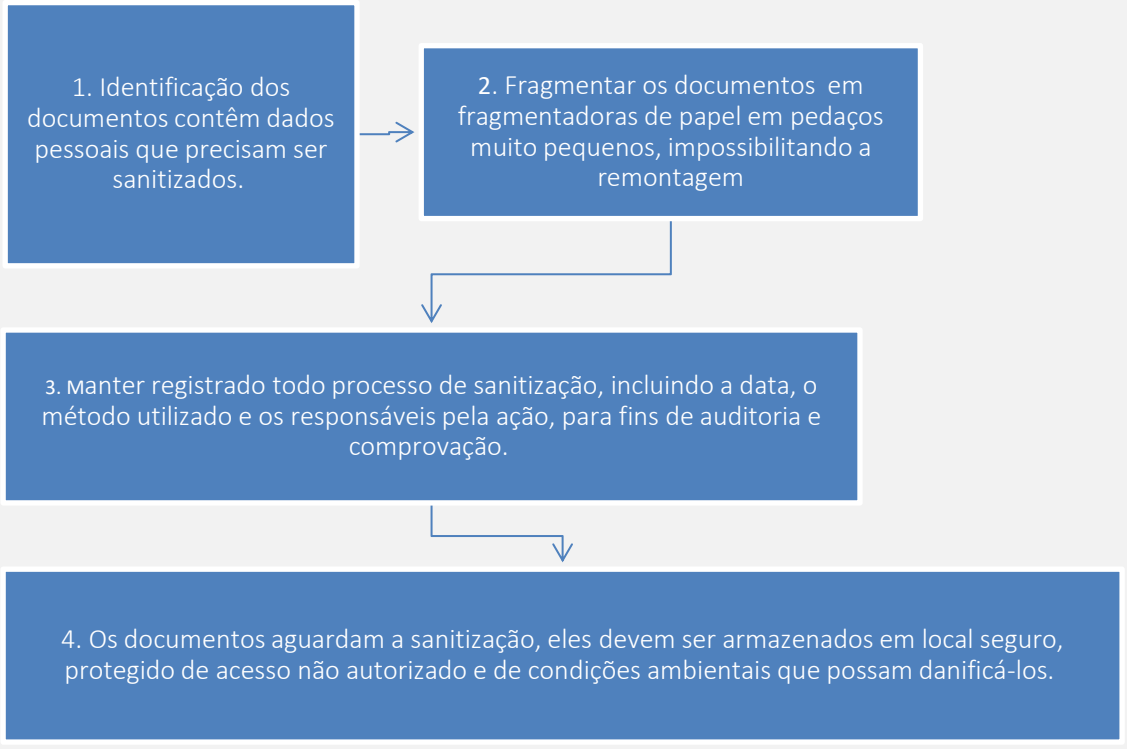
Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

11.1 Rotina de Sanitização - SBA

11.1.1 Sanitização de Documentos Físicos



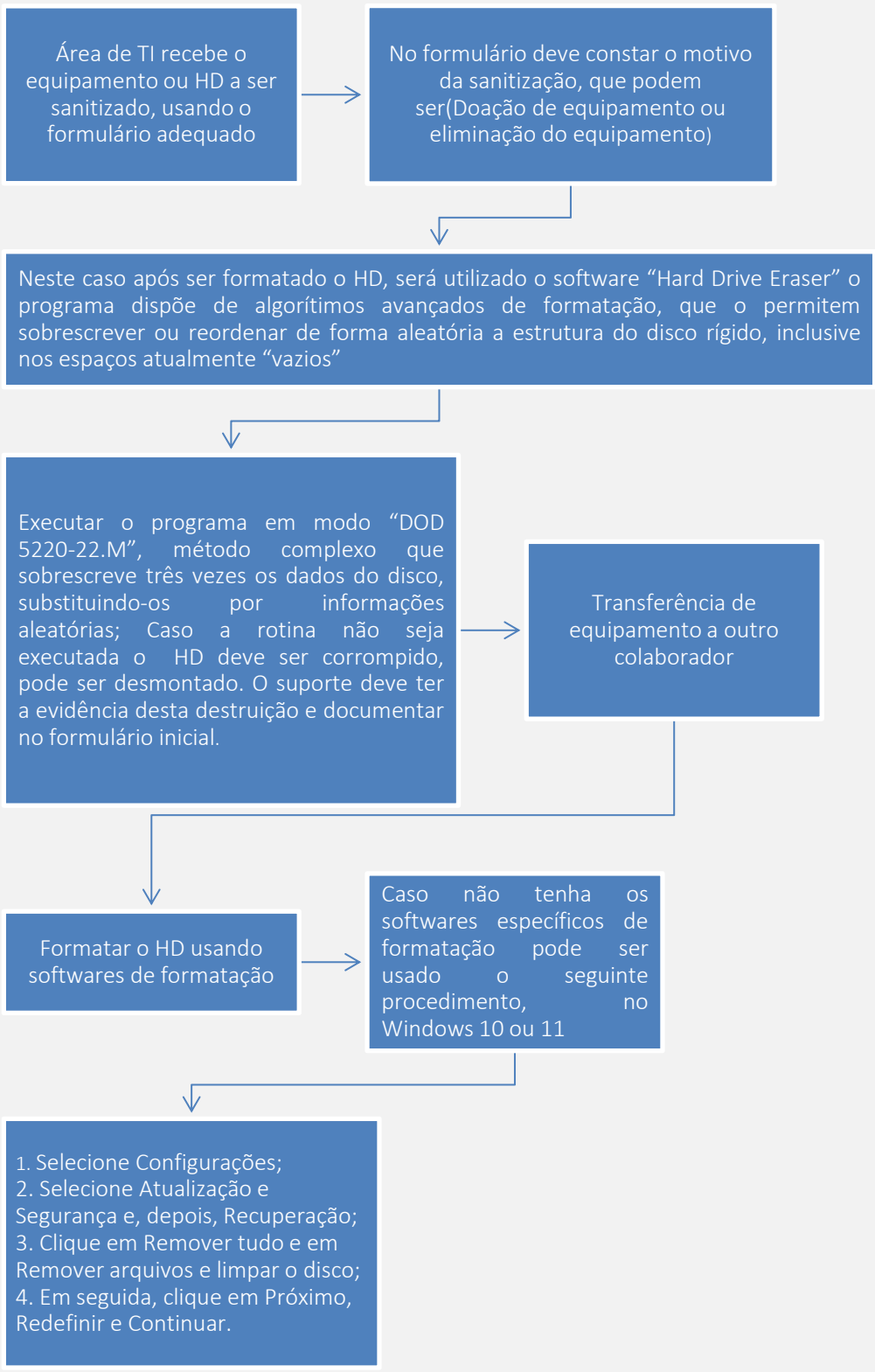
São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

11.1.2 Sanitização de Equipamentos



São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

12. VIOLAÇÕES E SANÇÕES

Os princípios desta política são totalmente endossados pela Comitê de sócios do Santos Bevilaqua Advogados e são rigorosamente cumpridos por todos os seus membros no exercício de suas atividades. Em nenhuma hipótese será admitida a alegação de desconhecimento para o não cumprimento desta política e derivadas.

12.1 Procedimentos Disciplinares e Violações

O Santos Bevilaqua estabelecerá procedimentos disciplinares formais para colaboradores, terceiros e prestadores de serviços que cometerem infrações, violações ou incidentes graves de segurança. Essas infrações incluem o não cumprimento das diretrizes desta política, assim como da Política de Código de Ética e Conduta.

São consideradas violações a esta política, mas não se limitam a, as seguintes situações:

- ⇒ Uso indevido e divulgação não autorizada de informações, segredos comerciais ou outras informações sem permissão formal.
- ⇒ Uso ilícito de dados, informações, equipamentos, sistemas e demais recursos tecnológicos, incluindo a violação de leis e regulamentos internos e externos.
- ⇒ Qualquer situação que exponha o Santos Bevilaqua Advogados a perdas financeiras ou de imagem devido à quebra de confidencialidade, integridade ou disponibilidade de suas informações ou das quais tenha custódia.

12.2 Sanções e Responsabilidades

Todos os colaboradores, terceiros e prestadores de serviços devem estar cientes de que o não cumprimento das diretrizes desta política resultará em sanções. Estas podem ser internas, administrativas, legais e/ou penais, dependendo da gravidade da infração.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

Para terceiros e prestadores de serviços, as sanções podem incluir a rescisão de contratos e penas de responsabilidade civil e criminal, na máxima extensão permitida por lei.

12.3 Detecção e Comunicação de Violações

Ao detectar uma violação, o usuário tem a responsabilidade de comunicá-la imediatamente aos responsáveis pela Segurança da Informação. Se for verificado que um colaborador não comunicou uma infração, mesmo sabendo de sua existência, ele poderá ser considerado coautor e, assim, ser indiciado e sofrer sanções.

13. VIGÊNCIA E REVISÃO

A presente norma entra em vigor na data de sua aprovação, sendo que sua revisão deve ser realizada no período máximo de 12 meses, ou em qualquer momento que se julgar necessário

14. CONTROLE DE VERSÕES

Item	Data	Atualização	Responsável
v.1.0	05/11/2021	Primeira versão do documento	3A Plus Serviços de Informática Ltda
v.1.0	05/12/2021	Revisão do documento	3A Plus Serviços de Informática Ltda
v.1.0	28/12/2021	Aprovação do documento	CSI - Santos Bevilaqua Advogados
v.2.0	05/12/2022	Revisão	3A Plus Serviços de Informática Ltda
v.2.0	28/12/2022	Aprovação do documento	CSI - Santos Bevilaqua Advogados
v.3.0	05/12/2023	Revisão	3A Plus Serviços de Informática Ltda
v.3.0	28/12/2023	Aprovação do documento	CSI - Santos Bevilaqua Advogados
v.4.0	01/02/2025	Revisão	3A Plus Serviços de Informática Ltda
v.4.0	28/02/2025	Aprovação do documento	CSI - Santos Bevilaqua Advogados
v.5.0	09/07/2025	Revisão	3A Plus Serviços de Informática Ltda
v.5.0	11/07/2025	Aprovação do documento	CSI - Santos Bevilaqua Advogados

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br

15. DISPOSIÇÕES FINAIS

Assim como a ética, a segurança é parte fundamental da cultura interna do Santos Bevilaqua Advogados. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pelo escritório.

São Paulo
Avenida Pedroso de Morais, nº 1553 – 4º andar
CEP 05419-001 - Pinheiros - São Paulo/SP

Brasília
SHIS QL22, Cj.02, Casa 01
CEP 71650-225 Brasília/DF
Tel.: +55 61 3366-2228

Rio de Janeiro
Rua Lauro Muller, 116, sala 1903
CEP 22290-160 – Botafogo - Rio

santosbevilaqua.com.br