Departamento: Segurança da Informação

Tipo de informação: pública

Ano: 2026 **Versão:** 03

Bits

Política de

Gestão da Segurança da Informação

3ª versão

1. Introdução

A Bits tem como objetivo transformar documentos jurídicos complexos em documentos claros e fáceis de entender, por meio da aplicação de Legal Design. A Bits também desenvolve produtos de tecnologia, incluindo plataformas digitais e soluções com inteligência artificial, que permitem a criação, análise e transformação de documentos de forma eficiente e escalável.

Diante da natureza sensível das informações tratadas, a Bits adota processos e controles de Segurança da Informação voltados à preservação da integridade, disponibilidade e confidencialidade dos dados, atuando de forma preventiva na identificação, monitoramento e resposta a incidentes de segurança cibernética.

2. Qual o objetivo desta Política?

O objetivo desta política é estabelecer diretrizes claras para a gestão eficiente, segura e ética das informações dentro da Bits. Essa política visa garantir a **integridade, confidencialidade e disponibilidade das informações,** bem como o cumprimento de regulamentações aplicáveis.

3. Aplicabilidade da Política

Equipe

Esta Política se aplica aos:

- colaboradores,
- C-levels,
- diretores,
- prestadores de serviços,
- consultores,
- auditores,
- temporários,
- fornecedores,
- estagiários,
- parceiros diversos e
- demais contratados que estejam a serviço da Bits.

Todos os destinatários desta Política são responsáveis por:

- Utilizar as informações da Bits exclusivamente para fins profissionais e autorizados;
- Proteger credenciais de acesso, mantendo-as pessoais, sigilosas e intransferíveis;
- Utilizar apenas sistemas, ferramentas e repositórios autorizados pela Bits;
- Preservar o sigilo e a confidencialidade das informações às quais tenham acesso;

- Comunicar imediatamente ao Comitê de Segurança da Informação sobre qualquer incidente, suspeita de violação ou uso indevido de informações;
- Cumprir integralmente esta Política e os demais normativos internos relacionados à Segurança da Informação.

Produtos e serviços

A Política de Segurança da Informação abrange:

a. Os processos de desenvolvimento, operação, manutenção e suporte dos produtos e serviços oferecidos pela Bits, incluindo:

- UX DOC
- BITS A.I.
- Studio de Legal Design
- Cursos e treinamentos

4. Princípios

O compromisso da Bits com o tratamento adequado das informações se baseia nos seguintes princípios:

Integridade

Garantia de que as informações permaneçam completas, corretas e íntegras ao longo de todo o seu ciclo de vida, protegidas contra alterações, exclusões ou destruições não autorizadas ou acidentais.

Confidencialidade

Garantia de que as informações sejam acessadas apenas por pessoas, sistemas ou processos devidamente autorizados, prevenindo acesso, uso ou divulgação não autorizados.

Disponibilidade

Garantia de que as informações e sistemas estejam acessíveis e utilizáveis por usuários autorizados sempre que necessário, de acordo com os níveis de serviço e requisitos operacionais estabelecidos.

5. Classificação da informação

A informação é classificada da seguinte forma:

Pública

Informação da Bits ou de seus clientes que **pode ser divulgada ao público em geral**, com caráter informativo, comercial ou promocional.

É **destinada ao público externo** ou ocorre devido ao cumprimento de legislação vigente que exija publicidade.

Interna

Informação que **a Bits não tem interesse em divulgar,** em que o acesso por parte de indivíduos externos à empresa deve ser evitado.

Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da empresa.

Pode ser acessada sem restrições por todos os colaboradores e prestadores de serviços.

Confidencial

É uma **informação crítica para os negócios da Bits** ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à Bits ou aos seus clientes. É sempre **restrita a um grupo específico de pessoas,** podendo ser este composto por colaboradores, clientes e/ou fornecedores.

6. Comitê de Segurança da Informação e Privacidade

Composição

O Comitê será composto por colaboradores da:

- **área jurídica,**
- **tecnologia e**
- **representantes da Diretoria Executiva.**

São obrigações do Comitê:

Discutir **a cada 03 meses** novas estratégias de segurança da informação;

Realizar **semestralmente treinamentos** para conscientizar os colaboradores sobre as práticas relacionadas à Segurança da Informação;

Atualizar **anualmente** esta e das demais políticas de segurança da informação;

Receber denúncias de violações e vazamento de dados, e tomar as medidas cabíveis de acordo com cada caso.

Como posso contatar o Comitê em caso de irregularidades?

É dever de todos reportar qualquer violação a esta Política, suas normas e diretrizes ao Comitê de Segurança da Informação através do e-mail:

compliance@bitsacademy.com.br

7. Diretrizes

Para desenvolver as suas atividades, a Bits estabelece as seguintes diretrizes:

Sistema de Segurança da Informação

Essa Política foi desenvolvida em conformidade com o Sistema de Segurança da Informação implementado na empresa;

Princípios

As informações devem ser utilizadas de forma ética, segura e transparente, para o estrito fim de cumprimento do plano de negócios da empresa;

Monitoramento

A Bits reserva-se no direito de monitorar e registrar o acesso e armazenamento de informações veiculadas na empresa.

Identificação dos ativos

Todos os ativos de infomação estão devidamente identificados, classificados e monitorados;

Tratamento

As informações devem ser tratadas, armazenadas e descartadas com as proteções necessárias, para garantir a segurança interna e dos dados dos clientes;

Identificação dos usuários

A identificação de cada usuário dentro dos sistemas utilizados pela Bits é única, pessoal e intransferível;

Proteção dos equipamentos

Todos os computadores devem ter instalados e atualizados um dos softwares indicados pela equipe de tecnologia, com objetivo de proteger a máquina contra códigos maliciosos;

Contratos

A Bits garante que os contratos com fornecedores, parceiros e terceiros, estejam pautados em uma postura ética compatível com seus princípios e valores;

Atenção às leis

A Bits identifica, segue, documenta e se mantém atualizada de acordo com as leis que regulamentam suas atividades, bem como dos aspectos de propriedade intelectual;

Atuação do Comitê de Segurança da Informação

- **Riscos:** O Comitê identificará os riscos por meio de um processo que analisará de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação. Todos os riscos deverão ser apresentados ao Comitê que deliberará sobre o tratamento adequado para cada situação;
- **Incidentes de segurança:** Todos os incidentes de segurança devem ser reportados ao Comitê de Segurança da Informação para que sejam analisados, avaliados e tratados pela área responsável;

8. Armazenamento e organização

Todos os documentos e informações da Bits, independentemente do formato ou meio, devem ser armazenados exclusivamente em **sistemas previamente autorizados**, em conformidade com esta Política e com as demais normas internas de Segurança da Informação.

O armazenamento das informações deve observar sua **classificação**, de modo que controles de acesso, compartilhamento e edição sejam aplicados de forma proporcional ao nível de sensibilidade da informação.

Política de Backup

A Bits manterá procedimentos regulares de backup das informações consideradas críticas para a continuidade de suas operações, conforme política específica. Os backups devem:

- ser realizados de forma periódica;
- ser armazenados em ambientes seguros e protegidos contra acesso não autorizado;

- permitir a restauração das informações em caso de incidente, falha técnica ou perda de dados.

8.1. Uso de inteligência artificial

A Bits autoriza e incentiva o uso de recursos de inteligência artificial com intuito de aumentar a eficiência, a qualidade e a escalabilidade de suas entregas.

O uso de IA na Bits deve observar as diretrizes a seguir:

Uso responsável e alinhado à finalidade

As soluções de Inteligência Artificial devem ser utilizadas **exclusivamente para finalidades legítimas, autorizadas e compatíveis com as atividades da Bits**, sendo vedado o uso de ferramentas de IA para fins pessoais, ilícitos ou incompatíveis com os objetivos do negócio.

O uso da IA deve respeitar o princípio da **necessidade**, evitando o tratamento excessivo ou inadequado de informações.

Proteção de dados e informações

É proibida a inserção, treinamento ou processamento, por meio de ferramentas de Inteligência Artificial, de:

- informações classificadas como confidenciais;
- dados pessoais ou dados pessoais sensíveis;
- informações de clientes, parceiros ou terceiros fora dos ambientes e ferramentas autorizados pela Bits.

Sempre que possível, devem ser utilizados **dados anonimizados ou pseudonimizados** nos processos que envolvam Inteligência Artificial.

Ferramentas e ambientes autorizados

Somente poderão ser utilizadas soluções de Inteligência Artificial:

- aprovadas pela Bits;
- integradas aos produtos e sistemas oficiais da empresa;
- contratadas ou validadas pelo Comitê de Segurança da Informação.

É vedado o uso de ferramentas externas de IA que não tenham sido previamente avaliadas quanto a riscos de segurança da informação, privacidade e conformidade legal.

Incidentes relacionados ao uso de I.A.

Qualquer suspeita ou confirmação de incidente de segurança, vazamento de dados, uso indevido ou comportamento inesperado relacionado a soluções de Inteligência Artificial

deverá ser imediatamente reportada ao Comitê de Segurança da Informação, nos termos previstos nesta Política.

9. Controle de acesso

O acesso aos documentos será concedido com base no princípio do menor privilégio, garantindo que apenas pessoas devidamente autorizadas possam visualizar, modificar, compartilhar ou excluir informações, de acordo com suas funções e responsabilidades.

O acesso aos sistemas de informação da Bits deve ser controlado de acordo com o **valor, sensibilidade e criticidade** da informação.

9.1. Como o controle de acesso é feito?

O controle de acesso será feito de acordo com as **funções e atividades** desempenhadas pelo colaborador dentro da empresa, analisando-se a imprescindibilidade ou não de acesso à determinada informação.

Quaisquer informações e documentos relacionados à Bits, seus clientes, fornecedores e investidores serão armazenadas nos apenas **repositórios indicados** pela área responsável por aquele dado.

> ⚠ **Todos os colaboradores, internos ou externos, que manipulem ou tenham acesso a informações sob custódia ou de propriedade da Bits devem garantir a confidencialidade e o sigilo dessas informações.**

9.2. Compartilhamento

O compartilhamento de informações confidenciais e restritas à terceiros só poderá ser feito para:

- cumprimento de obrigação contratual (desde que autorizado pelo titular da informação); ou
- mediante autorização expressa da liderança responsável pela área.

10. Retenção e descarte

A Bits compromete-se a reter informações pessoais apenas pelo tempo estritamente necessário para cumprir as finalidades para as quais foram coletadas, conforme determinado pela Lei Geral de Proteção de Dados (LGPD).

Dados pessoais

Após o período necessário de retenção, a Bits assegurará o descarte seguro e adequado das informações pessoais, de modo a evitar o acesso não autorizado ou o tratamento indevido

Dados comuns

As informações que não contenham dados pessoais serão armazenadas por tempo indeterminado.

11. Realização de auditorias

A Bits monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Por conta disso, auditorias podem ser realizadas nos sistemas e aplicações da empresa, em momentos definidos pelo Comitê de Segurança da Informação.

12. Treinamento

O Comitê de Segurança da Informação será responsável por divulgar esta Política dentro da empresa, com objetivo de que todos os destinatários tenham consciência de seu conteúdo e de suas responsabilidades.

Os colaboradores, prestadores e parceiros devem ser capacitados **semestralmente** sobre o uso dos ativos de informação dentro de suas atividades. Os treinamentos serão realizados nos formatos e modalidades definidos pelo Comitê.

As alterações realizadas em quaisquer políticas relacionadas à segurança da informação deverão ser amplamente divulgadas aos destinatários, através de reuniões com os colaboradores e envio de e-mails.

13. Violações à Política

O descumprimento das disposições previstas nesta Política de Segurança da Informação, bem como a ocorrência de incidentes ou quebras de segurança decorrentes de ação ou omissão, dolosa ou culposa, por parte de colaboradores, prestadores de serviços, parceiros ou terceiros, poderá resultar na aplicação de medidas administrativas, contratuais e/ou legais cabíveis.

As penalidades serão aplicadas de forma **proporcional à gravidade da infração**, considerando, entre outros fatores:

- a natureza da violação;
- o impacto causado à Bits, a seus clientes, parceiros ou terceiros;
- a reincidência;
- a intenção ou negligência envolvida;
- a existência de descumprimento de obrigações legais, regulatórias ou contratuais.

Sem prejuízo de outras medidas previstas no ordenamento jurídico vigente, as penalidades poderão incluir, conforme o caso:

- advertência verbal ou escrita;
- aplicação de medidas disciplinares previstas na legislação trabalhista e nos contratos aplicáveis;
- suspensão de acessos a sistemas, plataformas ou informações;
- rescisão contratual, nos termos da legislação e dos instrumentos firmados;
- adoção de medidas judiciais ou extrajudiciais cabíveis para reparação de danos.

A apuração das violações será conduzida de forma confidencial, garantindo-se a análise adequada dos fatos, além da observância do contraditório e da ampla defesa.

14. Disposições gerais

A presente Política de Gestão da Segurança da Informação integra o Sistema de Gestão da Segurança da Informação (SGSI) da Bits e é de observância obrigatória por todos os seus colaboradores, prestadores de serviços, parceiros e demais terceiros que tratem informações da organização.

Esta Política será revisada, no mínimo, anualmente, ou sempre que ocorrerem mudanças relevantes no contexto organizacional, nos processos, nas tecnologias, nos requisitos legais ou nos riscos de segurança da informação que impactem as diretrizes aqui estabelecidas.

15. Revisão e atualização

Esta política será revisada **anualmente**, no mês de janeiro. As alterações serão comunicadas a todos os colaboradores através de e-mails, apresentações nas reuniões gerais e novos programas de conscientização.

16. Vigência

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

17. Histórico do documento

Histórico de versões

VERSÃO	DATA	AUTOR	COMENTÁRIOS
1	24.01.2024	Lorena Cardoso	Criação do documento

Histórico de revisões

REVISÃO	DATA	AUTOR	COMENTÁRIOS
2	06.01.2025	Lorena Cardoso	Revisão
3	20.01.2026	Lorena Cardoso	Revisão