

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Classificação: Interna
	PRIVACIDADE	Data: 05/09/2025

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta política apresenta os princípios gerais adotados pela Bravium para proteger informações e recursos relacionados às suas atividades. O documento foi preparado para divulgação externa e não descreve procedimentos internos, configurações técnicas, canais operacionais, responsabilidades nominais ou detalhes de controles que possam comprometer a segurança da organização, de seus clientes, parceiros ou colaboradores.

1. OBJETIVO

A Bravium estabelece diretrizes para proteger a confidencialidade, a integridade e a disponibilidade das informações sob sua responsabilidade, incluindo dados pessoais e informações recebidas de clientes, parceiros e fornecedores. A segurança da informação é considerada parte da condução responsável dos negócios e da proteção das pessoas e relações de confiança

2. ABRANGÊNCIA

As diretrizes aplicam-se às informações tratadas pela Bravium, em qualquer formato ou meio, e aos recursos utilizados para criá-las, armazená-las, processá-las ou compartilhá-las. Devem ser observadas por pessoas que atuem em nome da organização e por terceiros quando tiverem acesso a essas informações ou recursos, conforme os respectivos vínculos e obrigações.

3. PRINCÍPIOS

A Bravium orienta a proteção da informação por meio de controles proporcionais à sua sensibilidade, aos riscos envolvidos, às necessidades do negócio e às obrigações legais, regulatórias e contratuais aplicáveis. As medidas de segurança devem apoiar o uso legítimo das informações e reduzir riscos de acesso, alteração, perda, indisponibilidade ou divulgação não autorizados.

A proteção de dados pessoais integra essas diretrizes e deve considerar as finalidades do tratamento, a necessidade de acesso, a privacidade das pessoas e as salvaguardas adequadas ao contexto.

4. DIRETRIZES DE SEGURANÇA

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Classificação: Interna
	PRIVACIDADE	Data: 05/09/2025

4.1. Governança e melhoria contínua

A segurança da informação é uma responsabilidade compartilhada. A Bravium define orientações e atribui responsabilidades compatíveis com suas atividades, avalia riscos e promove a melhoria de suas práticas. As pessoas abrangidas por esta política devem agir com cuidado, seguir as orientações aplicáveis e comunicar situações que possam afetar a segurança.

4.2. Acesso e autenticação

Cada usuário é responsável por toda atividade desempenhada com sua identificação de usuário designada através login e senha associado à sua identidade nos sistemas, equipamentos ou no uso da rede corporativa e/ou outros recursos aos quais a Bravium disponibilize acesso.

4.3. Uso de recursos e tratamento da informação

Os recursos disponibilizados para as atividades devem ser utilizados de forma responsável e segura. Informações devem ser acessadas, armazenadas, compartilhadas e descartadas por meios apropriados ao seu conteúdo e finalidade. É vedada a divulgação ou transferência não autorizada, inclusive para contas, dispositivos ou serviços sem aprovação para aquele uso.

As informações devem receber proteção compatível com sua sensibilidade. Quando houver dúvida sobre a autorização ou a forma adequada de uso, a pessoa deve buscar orientação pelos canais indicados pela Bravium.

4.4. Proteção de sistemas e gestão de vulnerabilidades

A Bravium adota práticas de segurança ao selecionar, desenvolver, configurar, operar e manter sistemas e serviços. Riscos e vulnerabilidades são identificados e tratados de acordo com sua criticidade e com as prioridades definidas pela organização. Medidas de proteção devem buscar reduzir a exposição a códigos maliciosos, falhas, alterações não autorizadas e interrupções.

4.5. Continuidade e recuperação

A organização considera os riscos de interrupção e estabelece medidas de continuidade e recuperação compatíveis com a importância de suas atividades e informações. Essas medidas são avaliadas e aprimoradas conforme a necessidade, para apoiar a retomada segura das operações.

4.6. Privacidade, confidencialidade e monitoramento

Informações confidenciais e dados pessoais devem ser tratados somente por pessoas autorizadas e para finalidades legítimas. Eventuais atividades de monitoramento de recursos corporativos devem observar a legislação aplicável, os avisos pertinentes, a necessidade e a proporcionalidade, com acesso às informações geradas restrito a finalidades autorizadas.

4.7. Terceiros e parceiros

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Classificação: Interna
	PRIVACIDADE	Data: 05/09/2025

Quando terceiros acessarem informações ou recursos da Bravium, o acesso deve ser compatível com a atividade contratada e protegido por obrigações adequadas. A organização pode avaliar riscos relacionados a fornecedores e parceiros e solicitar medidas de proteção proporcionais ao tipo de serviço e às informações envolvidas.

4.8. Conscientização

A Bravium promove orientações e ações de conscientização para apoiar práticas seguras. Pessoas abrangidas por esta política devem manter-se atentas a tentativas de fraude, solicitações incomuns, perda de equipamentos, exposição indevida de informações e outros sinais de risco.

5. COMUNICAÇÃO E TRATAMENTO DE INCIDENTES

Situações suspeitas ou confirmadas que possam afetar a segurança das informações devem ser comunicadas prontamente pelos canais disponibilizados pela Bravium. O tratamento pode incluir avaliação, contenção, investigação, recuperação e adoção de medidas para reduzir a recorrência, considerando as obrigações aplicáveis de comunicação às partes pertinentes.

6. RESPONSABILIDADES

A administração da Bravium apoia a aplicação desta política e a gestão dos riscos de segurança. As áreas responsáveis por segurança, tecnologia, privacidade e demais funções pertinentes contribuem para implementar e acompanhar medidas de proteção, cada qual dentro de suas atribuições.

Todas as pessoas abrangidas devem proteger as informações às quais têm acesso, preservar suas credenciais, respeitar os limites de autorização e comunicar incidentes ou fragilidades de que tenham conhecimento. Fornecedores e parceiros devem cumprir as obrigações de segurança aplicáveis à relação mantida com a Bravium.

7. EXCEÇÕES E DESCUMPRIMENTOS

Exceções a esta política devem ser justificadas, avaliadas quanto aos riscos e autorizadas pela instância competente, com medidas de proteção apropriadas. O descumprimento pode resultar em providências administrativas ou contratuais e, quando aplicável, nas consequências previstas em lei.

7.1. REVISÕES E DISPOSIÇÕES FINAIS

Esta política é mantida sob revisão e pode ser atualizada quando necessário para refletir mudanças relevantes nos riscos, nas atividades ou nas obrigações aplicáveis. As diretrizes aqui apresentadas são complementadas por orientações e procedimentos internos que não integram esta versão pública.