Política Geral de Segurança da Informação (PGSI)

Código: P.SI.01
Versão: 001
Uso interno

Código: P.SI.01
Versão: 001
Uso interno

1. Introdução

1.1 Sobre a BEAR BEAR

A **BEAR BEAR** é uma empresa brasileira dedicada ao desenvolvimento e à comercialização de roupas esportivas inteligentes, com foco em conforto, performance e inovação tecnológica. Seu principal diferencial competitivo é a tecnologia **AARRGH®**, projetada para garantir maior durabilidade ao tecido, a respiração ativa da pele e controles térmicos e anti odores.

A empresa atua majoritariamente no modelo B2C (Business to Consumer), com vendas realizadas por meio de plataforma de e-commerce própria e em marketplaces de terceiros. Com uma equipe de 50 a 100 colaboradores e estrutura enxuta, mas robusta, a **BEAR BEAR** adota princípios de segurança da informação e privacidade de dados desde a concepção de seus processos, reconhecendo a informação como ativo estratégico essencial para a continuidade e confiança do negócio.

1.2 Finalidade da Política

Esta Política Geral de Segurança da Informação **(PGSI)** tem como finalidade estabelecer as diretrizes, princípios e responsabilidades necessários para proteger os ativos de informação da **BEAR BEAR**, garantindo a **confidencialidade, integridade, disponibilidade, autenticidade e auditabilidade** das informações sob sua guarda.

A **PGSI** visa orientar a adoção de práticas e controles de segurança em todos os níveis da organização — estratégico, tático e operacional — alinhando-se aos objetivos de negócio da empresa e às exigências legais e contratuais aplicáveis,

especialmente aquelas relacionadas à proteção de dados pessoais conforme a **Lei Geral de Proteção de Dados (LGPD)**.

Esta política também tem como propósito promover a cultura da segurança da informação entre todos os colaboradores, parceiros e demais partes interessadas, contribuindo para a prevenção de incidentes, a continuidade dos serviços, a melhoria contínua e a preservação da confiança dos clientes e da reputação da **BEAR BEAR** no mercado.

1.3 Aplicabilidade e Escopo

Esta **Política Geral de Segurança da Informação** aplica-se a todos os colaboradores, inclusive aqueles cujo vínculo contratual com a **BEAR BEAR** já tenha sido encerrado, bem como prestadores de serviço, parceiros, fornecedores, estagiários, terceiros contratados e quaisquer outras partes que tenham acesso, direto ou indireto, aos ativos de informação da **BEAR BEAR**, independentemente do vínculo ou da localização geográfica.

A **PGSI** abrange todos os ativos de informação da organização, incluindo, mas não se limitando a:

- Dados armazenados, processados ou transmitidos em meios físicos ou digitais;
- Sistemas e serviços utilizados pela empresa, inclusive em ambientes de computação em nuvem;
- Equipamentos corporativos e, quando autorizado, dispositivos pessoais utilizados em regime de **BYOD**;
- Ambientes internos e remotos de trabalho;
- Informações relativas a clientes, colaboradores, fornecedores, processos e propriedade intelectual.

Esta política também contempla a proteção da propriedade intelectual da **BEAR BEAR**, considerando como tal todo material, artefato, dado, processo, design, código ou qualquer outra criação desenvolvida no contexto das atividades laborais ou contratuais, ou mediante uso de ativos da empresa.

A política é aplicável a todas as unidades, operações e áreas da **BEAR BEAR**, e serve como base para o desenvolvimento de normas, procedimentos e controles técnicos e administrativos específicos que compõem o **Sistema de Gestão de Segurança da Informação da organização**.

1.4 Referências Normativas e Legais

Esta **Política Geral de Segurança da Informação** foi desenvolvida com base nas exigências legais aplicáveis e em boas práticas amplamente reconhecidas no mercado, servindo como referência para a estruturação do **Sistema de Gestão da Segurança da Informação (SGSI)** da **BEAR BEAR**.

As principais fontes normativas e regulatórias utilizadas como base incluem:

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais **(LGPD)**;
- Lei nº 12.965/2014 – **Marco Civil da Internet**;
- Normas da família **ISO/IEC 27000**, com destaque para:
    - **ISO/IEC 27001:2022** – Requisitos para Sistemas de Gestão de Segurança da Informação;
    - **ISO/IEC 27002:2022** – Diretrizes para implementação de controles de segurança;
    - **ISO/IEC 27701:2019** – Requisitos e diretrizes para gestão de informações de privacidade;
    - **ISO/IEC 29100:2024** – Estrutura para proteção da privacidade da informação pessoal (Personally Identifiable Information – PII);

- Diretrizes do **NIST Cybersecurity Framework**, quando aplicáveis ao contexto organizacional;
- Cláusulas contratuais firmadas com parceiros, fornecedores e plataformas externas, que envolvam obrigações de segurança da informação e proteção de dados;
- Regulamentos e orientações da **Autoridade Nacional de Proteção de Dados (ANPD)**, conforme aplicável.

2. Dos Princípios da Segurança da Informação

2.1 Confidencialidade

A **confidencialidade** consiste na garantia de que a informação estará acessível somente a pessoas, sistemas ou processos devidamente autorizados. Na **BEAR BEAR**, este princípio visa proteger informações sensíveis e estratégicas contra acessos não autorizados, vazamentos, exposições indevidas ou uso indevido, seja por colaboradores, terceiros, agentes externos ou falhas operacionais.

As informações tratadas pela organização, incluindo dados pessoais de clientes, especificações técnicas da tecnologia **AARRGH®**, estratégias comerciais, contratos e quaisquer outros ativos classificados como confidenciais, devem ser protegidas mediante controles físicos, lógicos e administrativos adequados.

O acesso será concedido com base nos princípios do **menor privilégio (least privilege)** e da **necessidade de saber (need to know)**, respeitando as funções e responsabilidades atribuídas.

2.2 Integridade

A **integridade** garante que as informações e sistemas permaneçam íntegros, exatos, completos e livres de alterações não autorizadas ou acidentais.

Na **BEAR BEAR**, esse princípio assegura que dados de clientes, registros financeiros, ordens de compra e outras informações operacionais essenciais sejam **confiáveis, consistentes e auditáveis**, do momento de sua criação até o descarte ou anonimização.

A **integridade** será preservada mediante a aplicação de controles de validação, monitoramento, versionamento, trilhas de auditoria e permissões adequadas de edição e alteração.

2.3 Disponibilidade

A **disponibilidade** assegura que as informações e os recursos estejam acessíveis e utilizáveis sob demanda por usuários autorizados, sempre que necessário para o cumprimento das atividades da organização.

A **BEAR BEAR** manterá medidas de continuidade de negócios, planos de contingência e políticas de *backup* para garantir que dados críticos, sistemas de venda, meios de pagamento, suporte ao cliente e operações logísticas permaneçam funcionais mesmo diante de falhas, incidentes ou desastres.

Serviços em nuvem, como os oferecidos pela AWS, deverão ser configurados para garantir redundância, escalabilidade e tolerância a falhas.

2.4 Autenticidade

A **autenticidade** garante que a origem, autoria ou identidade da informação, do usuário ou do sistema seja verificável e confiável, evitando fraudes, falsificações ou acessos indevidos.

Na **BEAR BEAR**, esse princípio é essencial para a segurança de comunicações internas e externas, validação de identidade em acessos remotos, transações digitais e na integridade de registros e logs.

Serão adotados controles como credenciais individuais, autenticação multifator (MFA), uso de certificados digitais e registros de acesso para fortalecer esse pilar.

2.5 Auditabilidade

A **auditabilidade** garante que as ações realizadas sobre os sistemas e ativos de informação sejam registradas, rastreáveis e passíveis de verificação posterior.

Esse princípio é fundamental para a **BEAR BEAR** manter a transparência, responsabilidade (***accountability***) e conformidade com leis como a **LGPD** e o **Marco Civil da Internet.**

Todos os sistemas críticos deverão registrar logs de atividades de forma segura, permitindo auditorias, investigações e análises forenses sempre que necessário.

3. Das Diretrizes Gerais de Segurança

A **BEAR BEAR** adota um conjunto de diretrizes de segurança da informação com o objetivo de proteger seus ativos informacionais e garantir a continuidade, confiabilidade e conformidade de suas operações. Tais diretrizes estão alinhadas

aos princípios descritos neste documento e serão detalhadas por meio de normas complementares específicas, que integram o Sistema de Gestão da Segurança da Informação **(SGSI)** da organização.

As diretrizes a seguir devem ser observadas por todos os colaboradores, parceiros e prestadores de serviço, e servirão de base para a implementação e manutenção de controles técnicos, físicos e administrativos apropriados.

3.1 Classificação da Informação

As informações devem ser classificadas com base em seu grau de sensibilidade e criticidade, a fim de definir níveis adequados de proteção, acesso e tratamento.

Os critérios e responsabilidades para essa classificação estão descritos na Norma de **Classificação da Informação.**

3.2 Controle de Acesso

O acesso a sistemas, dados e recursos da **BEAR BEAR** deve ser controlado com base em critérios de necessidade, função e autorização formal.

As diretrizes para concessão, revisão e revogação de acessos estão descritas na Norma de **Controle de Acesso.**

3.3 Uso de Ativos de Informação

Os ativos de informação e os equipamentos utilizados para fins corporativos devem ser utilizados de forma segura, ética e responsável.

Os critérios de uso aceitável, responsabilidades e restrições estão definidos na Norma de **Uso Aceitável de Ativos.**

3.4 Segurança em Ambientes de TI e Nuvem

A infraestrutura tecnológica, incluindo ambientes em nuvem utilizados pela **BEAR BEAR**, deve ser projetada e mantida com foco na segurança, integridade e disponibilidade das informações.

Os controles específicos estão descritos nas normas técnicas e operacionais pertinentes.

3.5 Acesso Remoto e Uso de Dispositivos Pessoais (BYOD)

O acesso remoto e o uso de dispositivos não corporativos devem ocorrer sob critérios rigorosos de autorização e controle, conforme diretrizes estabelecidas na Norma de **Acesso Remoto e BYOD**.

3.6 Continuidade de Negócio e Recuperação de Desastres

A **BEAR BEAR** manterá mecanismos e procedimentos que garantam a continuidade de suas atividades e a recuperação de serviços críticos em caso de incidentes.

As orientações sobre planos, testes e responsabilidades estão descritas na Norma de **Continuidade de Negócio e Recuperação de Desastres**.

3.7 Gestão de Incidentes de Segurança

Todos os incidentes de segurança da informação devem ser prontamente reportados, registrados, analisados e tratados conforme os procedimentos definidos pela organização.

As etapas, responsabilidades e critérios estão definidos na Norma de **Gestão de Incidentes de Segurança da Informação**.

4. Dos Papéis e Responsabilidades

A estrutura de governança da segurança da informação da **BEAR BEAR** é organizada em três níveis: **estratégico, tático e operacional.** Cada nível possui atribuições específicas que garantem a efetividade da Política Geral de Segurança da Informação **(PGSI)** e promovem a proteção adequada dos ativos informacionais da organização.

4.1 Nível Estratégico – Comitê de Segurança da Informação

O **Comitê de Segurança da Informação** é o órgão responsável pela definição de diretrizes, aprovação de políticas, avaliação de riscos relevantes e tomada de decisões estratégicas relacionadas à segurança da informação e à proteção de dados pessoais.

Composição:

- Representante da Diretoria Executiva;
- Representante do Departamento Jurídico;
- Representante do Departamento de TI e Segurança da Informação;
- Representantes das áreas de RH, Marketing e Financeiro;
- Outros membros indicados conforme necessidade estratégica.

Principais responsabilidades:

- Aprovar políticas, normas e planos relacionados à segurança da informação;
- Avaliar riscos estratégicos e aprovar medidas de mitigação;
- Acompanhar indicadores de segurança e relatórios de incidentes críticos;
- Deliberar sobre casos de exceções, sanções e medidas corretivas;
- Integrar temas de segurança da informação e privacidade ao planejamento institucional da empresa.

4.2 Gestores e Responsáveis de Área

Os **gestores das áreas da organização** são responsáveis por implementar e garantir o cumprimento das diretrizes da **PGSI** e das **normas complementares** no âmbito de suas equipes e processos.

Principais responsabilidades:

- Assegurar a aplicação das normas de segurança da informação em sua área;
- Identificar e reportar riscos e vulnerabilidades operacionais;
- Apoiar a gestão de acessos, uso de ativos e segurança de sistemas;
- Promover a orientação de suas equipes quanto às práticas exigidas;
- Reportar incidentes ou desvios de conformidade ao Comitê de Segurança.

4.3 Usuários e Equipe Técnica

Os **usuários e a equipe técnica**, ou seja, todos os colaboradores, prestadores de serviço, estagiários e técnicos que utilizam os recursos e ativos de informação da organização ou atuam na manutenção de seus sistemas e processos.

Principais responsabilidades:

- Cumprir as políticas, normas e procedimentos estabelecidos;
- Proteger senhas, dispositivos e dados sob sua responsabilidade;
- Utilizar os recursos tecnológicos da empresa de forma segura e ética;
- Reportar imediatamente qualquer anomalia, falha ou incidente de segurança;
- Participar de treinamentos e iniciativas de conscientização promovidos pela organização.

4.4 Encarregado pelo Tratamento de Dados Pessoais (DPO)

O **Encarregado pelo Tratamento de Dados Pessoais (DPO)**, cuja função principal é atuar como elo entre a organização, os titulares dos dados pessoais e as autoridades reguladoras, promovendo a conformidade com as normas de proteção de dados.

Principais responsabilidades:

- Atuar como canal de comunicação com os titulares de dados pessoais e autoridades competentes;
- Apoiar as áreas internas na implementação de práticas compatíveis com a proteção de dados;
- Orientar colaboradores e terceiros sobre boas práticas de privacidade e segurança da informação;
- Apoiar o tratamento e a resposta a incidentes envolvendo dados pessoais;
- Coordenar a elaboração e atualização de registros de tratamento de dados;
- Avaliar os impactos de novas operações de tratamento e apoiar na elaboração de relatórios específicos;
- Atuar como responsável institucional pela **Política de Privacidade** da **BEAR BEAR**, promovendo seu cumprimento e atualização;
- Promover a cultura de proteção de dados em todos os níveis da organização.

5. Da Conscientização e do treinamento

A **BEAR BEAR** reconhece que o fator humano é essencial para a eficácia da segurança da informação e da proteção de dados pessoais. Por esse motivo, a organização mantém o **compromisso de promover ações contínuas de conscientização, capacitação e orientação** de seus colaboradores, terceiros e parceiros, com o objetivo de **fortalecer a cultura de segurança**, reduzir riscos

operacionais e garantir o cumprimento das políticas, normas internas e exigências legais aplicáveis.

Os objetivos, formatos, abrangência, responsabilidades e demais critérios relativos aos programas de conscientização e treinamento serão definidos em normas e planos específicos, a serem mantidos e atualizados pelas áreas responsáveis.

6. Das sanções e consequências por não conformidade

O **descumprimento** das diretrizes estabelecidas **nesta Política Geral de Segurança da Informação e das normas complementares** associadas poderá acarretar a aplicação de sanções disciplinares, contratuais ou administrativas, conforme a natureza da infração e o vínculo do infrator com a **BEAR BEAR**.

6.1 Colaboradores e Funcionários Internos

Os colaboradores da **BEAR BEAR** que infringirem as disposições desta política ou das normas internas correlatas estarão sujeitos às medidas disciplinares cabíveis, de acordo com a legislação trabalhista vigente, incluindo, mas não se limitando a:

- Advertência verbal ou escrita;
- Suspensão das atividades laborais;
- Rescisão do contrato de trabalho por justa causa, conforme previsto no **art. 482 da Consolidação das Leis do Trabalho (CLT)** e disposições correlatas.

As penalidades serão aplicadas observando o grau da infração, a reincidência, a gravidade do risco ou dano envolvido, e os princípios do contraditório e da ampla defesa.

6.2 Terceiros, Fornecedores e Parceiros

Em casos de **descumprimento contratual** relacionado à segurança da informação ou proteção de dados por parte de terceiros, fornecedores, prestadores de serviço ou parceiros comerciais, poderão ser aplicadas as **cláusulas penais** previstas nos contratos firmados, incluindo, quando aplicável:

- Notificação formal e prazo para correção;
- Suspensão de acesso aos sistemas da **BEAR BEAR**;
- Rescisão contratual;
- Aplicação de penalidades financeiras ou outras medidas previstas contratualmente.

A **BEAR BEAR** poderá ainda adotar medidas judiciais ou extrajudiciais cabíveis para a reparação de danos ou responsabilização civil, penal ou administrativa.

6.3 Tratamento Interno e Registros

Todos os casos de **não conformidade** serão registrados e avaliados pelo **Comitê de Segurança da Informação**, que definirá as ações corretivas e, quando necessário, escalará o caso às instâncias competentes. As medidas aplicadas deverão ser proporcionais, documentadas e alinhadas à **política de conduta** da organização.

7. Da Gestão da Política

A **Política Geral de Segurança da Informação** da **BEAR BEAR** é um documento institucional que deve ser mantido atualizado, acessível e compatível com a realidade organizacional, legal e tecnológica da empresa. Sua gestão será

conduzida de forma estruturada, com **revisões periódicas e comunicação adequada** a todos os públicos envolvidos.

7.1 Responsabilidade pela Manutenção

A responsabilidade pela atualização, revisão e disseminação desta política é do **Comitê de Segurança da Informação**, com apoio das áreas de **Segurança da Informação, Jurídico e Recursos Humanos**.

7.2 Revisão e Atualização

A política será revisada periodicamente, preferencialmente a cada 12 meses, ou sempre que houver:

- Alterações relevantes na legislação ou regulamentações aplicáveis;
- Mudanças significativas na estrutura da organização ou nos ativos informacionais;
- Incidentes de segurança que justifiquem ajustes de controle ou diretrizes;
- Identificação de oportunidades de melhoria por auditorias, avaliações internas ou externas.

As revisões devem ser documentadas e aprovadas formalmente pelo **Comitê de Segurança da Informação**.

7.3 Comunicação e Divulgação

A versão vigente da **PGSI** será disponibilizada aos colaboradores e partes interessadas, preferencialmente por meio dos canais institucionais da empresa. Sempre que atualizada, os usuários deverão ser notificados e, quando necessário, novos treinamentos ou comunicações formais poderão ser promovidos para garantir a ciência e o alinhamento organizacional.

7.4 Vigência

Esta Política entra em vigor na data de sua aprovação pelo **Comitê de Segurança da Informação** e permanecerá válida até que nova versão a substitua. As versões anteriores serão devidamente arquivadas para fins de histórico e rastreabilidade.

Aprovado e publicado em 23 de maio de 2025,
Belo Horizonte/MG.

Grizzly Bear
CISO

Polar Bear
Sócio Diretor

8. Glossário

Termo	Definição
Ativo de Informação	Qualquer dado, sistema, processo, serviço, equipamento ou recurso que possua valor para a organização.
Auditoria	Processo sistemático, independente e documentado para obter evidência e avaliá-la objetivamente.
Autenticidade	Garantia de que a informação, usuário ou sistema é genuíno e não foi alterado ou forjado.
BYOD	Sigla de *Bring Your Own Device*: uso de dispositivos pessoais para fins profissionais.
CLT	Consolidação das Leis do Trabalho: legislação brasileira que rege as relações de trabalho formal no país.
Confidencialidade	Garantia de que a informação seja acessível apenas a pessoas autorizadas.
Controle de Acesso	Processo de restrição e autorização de acesso a sistemas e informações com base em critérios definidos.
DPO	Sigla de Data Protection Officer (Encarregado de Dados): profissional responsável pela comunicação com titulares e autoridades e pela orientação interna sobre proteção de dados.
Disponibilidade	Garantia de que a informação e os recursos estejam acessíveis quando necessário.
Integridade	Garantia de que a informação é exata, completa e não foi alterada indevidamente.

ISO/IEC	Sigla para a International Organization for Standardization e a International Electrotechnical Commission. Ambas as organizações desenvolvem normas internacionais reconhecidas mundialmente, incluindo aquelas voltadas à segurança da informação.
ISO/IEC 27000	Conjunto de normas internacionais que definem requisitos, diretrizes e boas práticas para estabelecer, implementar, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI), com foco na proteção de ativos informacionais.
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que regulamenta o tratamento de dados pessoais no Brasil.
NIST	Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, referência global em cibersegurança e autor do Cybersecurity Framework (CSF).
Política de Segurança da Informação	Documento que estabelece diretrizes e princípios para proteção dos ativos de informação da organização.
Risco	Possibilidade de ocorrência de um evento que afete negativamente os ativos de informação.
SGSI	Sistema de Gestão da Segurança da Informação: estrutura de políticas, procedimentos e controles para proteger os ativos de informação da organização.
Titular de dados pessoais	Pessoa natural a quem se referem os dados pessoais tratados pela organização.
Lei de Acesso à Informação (LAI)	Lei nº 12.527/2011, que regula o acesso a informações públicas e estabelece regras de transparência no setor público.