



## Política de Segurança da Informação do Grupo Benner

## Sumário

1. INTRODUÇÃO .....	3
2. CAMPO DE APLICAÇÃO .....	4
3. DEFINIÇÕES.....	4
4. ENUNCIADO .....	4
5. OBJETIVO .....	5
6. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO .....	5
7. PAPÉIS E RESPONSABILIDADES.....	8
8. SANÇÕES.....	11
9. ELIGIBILIDADE E VALIDADE.....	12
10. REGISTRO DE ALTERAÇÕES .....	12
11. FORMALIZAÇÃO .....	12

## 1. INTRODUÇÃO

Como parte do Programa de *Compliance* do **Grupo Benner** (“Grupo Benner” ou “Empresa”), foi desmembrada e atualizada a presente Segurança da Informação do **Grupo Benner** (“Política”) que tem por objetivo assegurar que os seus colaboradores e representantes entendam os requisitos e procedimentos das Leis, bem como servir como uma ferramenta efetiva de adequação e prevenção, de modo a orientá-los a identificar e evitar conflitos e infrações a essas leis.

No caso de irregularidades e/ou infrações detectadas, espera-se que sejam adotados os necessários procedimentos para assegurar a interrupção das irregularidades e a tempestiva remediação dos danos gerados. Assim, a falha no cumprimento das Leis poderá resultar em sérias e diversas penalidades para o **Grupo Benner** e para seus colaboradores e/ou representantes.

Este documento foi elaborado visando implementar as orientações das mais atualizadas e confiáveis diretrizes de segurança, em especial as normas NBR ISO IEC 27001, NBR ISO IEC 27002, NBR ISO IEC 15408, Lei Geral de Proteção de Dados (Lei 13.709/2018) (“LGPD”) e outras, tendo por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades, e criar uma cultura educativa empresarial de proteção aos dados do **Grupo Benner**.

A justificativa da necessidade de implementação da presente Política se faz ainda mais evidente, tendo em vista que o **Grupo Benner** é uma empresa nacional de solução em softwares, que trabalha no desenvolvimento de softwares que gerencia dados de outra empresa e para tanto, conta com um parque tecnológico, composto de redes de microcomputadores e prestação de serviços em desenvolvimento de soluções de softwares.

Esta Política suplementa, mas não substitui e nem altera os demais documentos que compõem o Programa de *Compliance* do **Grupo Benner**, os quais devem ser lidos de forma conjunta para a efetiva compreensão.

Nesse sentido, disponibilizamos em nossa intranet página específica sobre os temas de *compliance*, por meio do qual é possível consultar as principais ações implementadas, orientações corporativas, demais procedimentos internos, legislações e documentos importantes, como os já mencionados acima.

## 2. CAMPO DE APLICAÇÃO

Aplicável a todas as áreas da organização Benner.

## 3. DEFINIÇÕES

**Ativos de Informação:** Toda e qualquer pessoa, processo, tecnologia ou ambiente que manipule, processe, armazene, transporte, transmita e descarte informações corporativas.

**Informação:** patrimônio imaterial de propriedade ou sob custódia do Grupo Benner. Consiste em informações que podem ser de caráter comercial, estratégico, técnico, códigos-fonte, projetos, financeiro, mercadológico, legal, de recursos humanos ou de qualquer outra natureza, não importando se protegidas ou não de confidencialidade, disponíveis na forma física ou armazenadas digitalmente, não limitadas à infraestrutura tecnológica do Grupo Benner.

**Segurança da Informação:** adoção de medidas para assegurar a preservação da confidencialidade, integridade e disponibilidade das informações do Grupo Benner; desta forma contribuindo para a continuidade do negócio.

**Colaboradores:** pessoas com vínculo contratual, não importando o regime jurídico a que estejam submetidos; provedores que estejam alocados na prestação de serviços no ambiente Benner por força de contrato, que utilizem – direta ou indiretamente – a infraestrutura tecnológica do Grupo Benner para o desenvolvimento de suas atividades profissionais.

**Usuários:** pessoas ou organizações que utilizam um determinado tipo de serviço e podem ser classificados segundo a área de interesse. Usuários em sistemas de informação são agentes externos ao sistema que usufruem da tecnologia para realizar determinado trabalho.

## 4. ENUNCIADO

O Grupo Benner afirma o seu compromisso com a proteção das informações de sua propriedade e/ou sob sua custódia, por meio de diretrizes e práticas de segurança orientadas para a preservação da sua confidencialidade, integridade e disponibilidade.

Esta política está suportada por um conjunto de normas, manuais, planos e procedimentos adicionais, e aplica-se a todas as empresas do Grupo Benner e suas subsidiárias, seus colaboradores, sistemas, serviços e demais ativos de informação.

## **5. OBJETIVO**

Definir as diretrizes para que os objetivos de negócio do Grupo Benner sejam alcançados de forma adequada, no que diz respeito privacidade e à segurança das informações, privacidade e a conformidade com as leis e normas aplicáveis às empresas do grupo e sua proteção de dados de clientes que estejam sob a nossa custódia, mesmo que eventualmente.

Todas as diretrizes desta Política visam o desenvolvimento de um comportamento ético e profissional, com a finalidade de eliminar e/ou reduzir os riscos a níveis aceitáveis para o negócio.

## **6. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO**

### **6.1 Sistema de Gestão da Segurança da Informação (SGSI)**

A gestão da segurança da informação deve ser uma atividade contínua e sistemática, abrangendo todos os ativos de informação existentes no Grupo Benner.

As diretrizes, normas, planos, procedimentos, registros e controles são definidos de acordo com o nível de maturidade (atual e desejado), considerando as capacidades técnicas e operacionais para mantê-los. Desta forma, a abordagem adotada para implantação e manutenção do SGSI consiste em melhorias contínuas e sucessivas, com o objetivo de assegurar a sustentabilidade das diretrizes implementadas.

O sistema de gestão de segurança da informação está baseado em uma hierarquia de documentos. De acordo com o seu nível de abrangência dentro da organização, os documentos que compõem o SGSI são identificados da seguinte forma:

- **Corporativos:** Envolvem informações, instruções e diretrizes que devem ser de conhecimento de toda a organização;
- **Intersetoriais:** Relativos às normas, procedimentos e controles que requerem a participação de várias áreas na organização;
- **Técnicos:** Referem-se às normas, procedimentos e controles que estão restritos às áreas de Tecnologia e Segurança da Informação.

### **6.2 Responsabilidade e Comprometimento**

Todos os colaboradores, em qualquer vínculo, função ou cargo, são responsáveis pela segurança da informação e devem estar comprometidos com a proteção e salvaguarda dos ativos de informação sob sua responsabilidade, dos ambientes físicos e computacionais a que tenham acesso, independente das demais medidas de segurança existentes.

### **6.3 Gestão de Riscos**

O Grupo Benner adota mecanismos de monitoramento e gestão de riscos, visando atingir o grau de segurança necessário, dentro dos limites orçamentários e padrões de qualidade definidos.

As decisões de segurança da informação e as diretrizes dessa política e das normas que a suportam são determinadas conforme a percepção de risco aos objetivos e negócios da Empresa.

### **6.4 Uso Aceitável dos Ativos de TI**

Os ativos de TI disponibilizados aos colaboradores devem ser utilizados essencialmente para as finalidades determinadas, sempre em harmonia com os interesses da empresa. Para isso, os colaboradores devem conhecer e concordar com os termos e condições descritos no MSI - Manual de Segurança da Informação.

### **6.5 Classificação e Tratamento da Informação**

As informações de propriedade do Grupo Benner ou terceiros sob sua custódia devem ser classificadas de acordo com seu grau de sigilo, e receber tratamento adequado para assegurar sua proteção durante todo o ciclo de vida.

Os dados pessoais e os dados sensíveis de propriedade ou sob custódia do Grupo Benner são tratados em conformidade com a legislação vigente, de acordo com as diretrizes definidas na Política de Privacidade (<https://universobenner.mybeehome.com/cms/145/folder/>).

### **6.6 Gestão de acessos**

O acesso às instalações, sistemas, redes, dados e informações de propriedade ou sob responsabilidade do Grupo Benner deve ser monitorado, controlado e restrito às necessidades profissionais de cada colaborador. O acesso de terceiros (clientes, fornecedores e parceiros comerciais) aos ativos de informação da Empresa deve seguir as normas, procedimentos e critérios estabelecidos, com a finalidade de mitigar os riscos de violação dos requisitos de segurança da informação.

### **6.7 Aquisição de hardware e software**

Toda aquisição de hardware e software necessária para o desempenho das atividades dos colaboradores deverá ser assessorada pela área de Governança de TI, para assegurar que estejam aderentes à arquitetura definida para a Organização e aos requisitos técnicos e funcionais de TI e proteções com relação a segurança da informação.

#### **6.8 Gestão da Continuidade de Negócios**

A Empresa deve identificar as ameaças potenciais e os impactos operacionais e estratégicos aos seus negócios, e desta forma desenvolver e manter mecanismos que garantam a continuidade de seus processos críticos.

#### **6.9 Aquisição, desenvolvimento e manutenção de sistemas**

Com o objetivo de promover a redução de riscos e manutenção dos níveis de segurança já existentes, o desenvolvimento de sistemas de gestão da informação por equipe própria ou por terceiros deve atender as diretrizes e normas de segurança da informação (LGPD). De forma similar, a aquisição de sistemas contratados com terceiros e os contratos de suporte e manutenção das aplicações utilizadas na Empresa estão também sujeitos aos mesmos controles.

#### **6.10 Gerenciamento de Projetos**

Todos os projetos iniciados e em andamento na Empresa devem levar em conta os requisitos relevantes em segurança da informação. Os aspectos de confidencialidade, disponibilidade e integridade dos ativos de informação devem ser preservados pelas equipes envolvidas no projeto, independentemente de serem os colaboradores próprios ou terceirizados.

#### **6.11 Notificação, Registro e Tratamento de Incidentes**

Os colaboradores devem reportar quaisquer incidentes que possam comprometer a segurança das informações corporativas da Empresa. A Equipe Infraestrutura de TI é responsável por avaliar e tratar os incidentes de segurança da informação, implantando as medidas necessárias para evitar a sua recorrência. Quando necessário, contatos apropriados com autoridades relevantes devem ser mantidos.

#### **6.12 Auditoria e Conformidade**

As práticas de segurança da informação adotadas pelos colaboradores serão auditadas periodicamente, de forma a avaliar a conformidade das ações executadas em relação ao estabelecido nesta Política e demais normas e procedimentos que a suportam.

#### **6.13 Monitoramento**

O Grupo Benner reserva-se o direito de monitorar os acessos (físico e lógico), e a utilização de todos os ativos de informação disponibilizados aos seus colaboradores, para que softwares não legalizados e ameaças ou ações diversas não autorizadas sejam detectadas e tratadas tempestivamente.

#### **6.14 Treinamento e Conscientização**

Todos os colaboradores devem receber treinamento relativo às diretrizes, normas e procedimentos da Empresa em segurança da informação, além de contínua conscientização sobre os riscos emergentes, precauções e boas práticas para a utilização adequada dos ativos de informação.

Os profissionais envolvidos com tecnologia e segurança da informação devem assegurar a participação em grupos de discussão, associações profissionais ou fóruns especializados, com a finalidade de se manter continuamente atualizados sobre os avanços tecnológicos e o surgimento de novas ameaças cibernéticas.

#### **6.15 Revisão e análise crítica**

O conjunto de documentos que compõe a Política de Segurança da Informação deve passar por revisões e análises críticas a cada dois anos, ou sempre que ocorrer algum fato ou evento relevante que justifique a sua revisão ou adequação.

#### **6.16 Penalidades**

O descumprimento ou inobservância das diretrizes estabelecidas nesta Política e em seus documentos complementares constitui conduta inadequada do colaborador. É importante ressaltar que condutas inadequadas podem resultar em prejuízos financeiros, operacionais, além de impactos legais, regulatórios, de reputação e imagem para a Empresa. Sendo assim, eventuais medidas administrativas, cíveis e judiciais aplicáveis em cada situação serão definidas pelo Comitê de Segurança da Informação – CSI.

Todo o colaborador assina um documento que leu, entendeu e se compromete com os termos da política.

### **7. PAPÉIS E RESPONSABILIDADES**

A responsabilidade pela segurança das informações é dada a todos os envolvidos com as atividades do Grupo Benner, (funcionários, fornecedores, parceiros comerciais, clientes, fornecedores que tenham acesso a informação da Benner ou cliente, prestadores de serviços etc.). Cada um dos responsáveis pela segurança da informação tem papel fundamental para garantir a confidencialidade, integridade e disponibilidade das informações.

A seguir são descritos os **papéis e responsabilidades** específicos para cada grupo de colaboradores:



**A. Diretoria: Composta pela Alta Administração. Responsável por:**

- Fornecer apoio organizacional e ser exemplo de liderança quanto ao cumprimento de todas as diretrizes descritas nesta Política de Segurança da Informação e demais documentos relacionados.
- Garantir a aplicação das Políticas de Segurança da Informação.
- Prover os recursos humanos, materiais e financeiros necessários para implementar e manter os mecanismos de segurança da informação.
- Analisar, revisar e aprovar a Política de Segurança da Informação (PSI), incluindo as revisões e o desdobramento de normas específicas, quando necessário.
- Designar os representantes do Comitê de Segurança da Informação - CSI.
- Avaliar e tomar decisões relativas às solicitações encaminhadas pelo CSI, incluindo eventuais medidas administrativas e/ou disciplinares decorrentes do descumprimento das normas estabelecidas.

**B. Comitê de Segurança da Informação (CSI):** Equipe multidisciplinar, constituída por representantes (titulares e suplentes) de áreas-chave para o desenvolvimento e manutenção da cultura de segurança da informação no Grupo Benner. Responsável por:

- Estabelecer requisitos e diretrizes para preservar a confidencialidade, integridade e disponibilidade dos ativos de informação da Empresa.
- Atuar como facilitador para a implantação das orientações descritas nesta Política e demais Normas e Procedimentos relacionados à Segurança da Informação.
- Validar a documentação relacionada com a Política de Segurança da Informação e realizar revisões periódicas e/ou sempre que necessárias.
- Facilitar a realização de treinamentos e programas de conscientização em Segurança da Informação, para todos os colaboradores que tenham acesso a ativos de informação do Grupo Benner.
- Avaliar eventuais solicitações de exceção a esta Política e demais normas e procedimentos de segurança da informação, considerando a real necessidade e possíveis riscos ao negócio.
- Acompanhar os incidentes em segurança da informação e analisar casos de descumprimento a esta Política e demais Normas, encaminhando-os para a Diretoria quando necessário.

**C. Departamento de Gente e Gestão (RH):** Área dedicada ao recrutamento, seleção, contratação, desenvolvimento e administração de pessoal. Responsável por:

- Garantir que todos assinem o documento de concordância da Política de Segurança da Informação e demais documentos de compliance.

- Assegurar o cumprimento das diretrizes de segurança da informação na administração de pessoal próprio ou terceirizado sob sua responsabilidade.
- Coordenar treinamentos e campanhas de conscientização relacionados às normas e diretrizes em Segurança da Informação.
- Manter os registros que evidenciem a participação dos colaboradores nos treinamentos e demais eventos relacionados à Segurança da Informação.
- Garantir e disponibilizar treinamento sobre Política de Segurança e LGPD.

**D. Gestores:** Líderes (Gerentes ou Coordenadores) que gerenciam equipes de colaboradores próprios ou terceiros. Responsáveis por:

- Assegurar que os colaboradores sob sua responsabilidade conhecem e cumprem as normas de segurança da informação.
- Controlar a disponibilização e utilização dos ativos de informação fornecidos aos colaboradores sob sua responsabilidade.
- Zelar pelo cumprimento das normas e diretrizes de segurança da informação nas atividades desempenhadas dentro da sua área de atuação.
- Avaliar as solicitações abertas pelos colaboradores sob sua responsabilidade, e emitir parecer baseado na real necessidade dos colaboradores.

**E. Colaboradores:** Integrantes do Conselho de Administração, diretores, gestores, colaboradores, estagiários e jovens aprendizes do Grupo Benner;

**F. Prestadores de Serviços:** funcionários temporários que atuam nas unidades da Empresa ou acessam remotamente a sua infraestrutura de TI; indivíduos e/ou empresas que atuam em nome do Grupo Benner como consultores, despachantes ou agentes.

- Conhecer e cumprir as diretrizes estabelecidas nesta Política e nas demais normas e procedimentos de Segurança da Informação, participando de treinamentos, campanhas de conscientização e outras atividades relacionadas que forem promovidas pela Empresa.
- Zelar pela segurança dos ativos de informação que lhe forem disponibilizados pela Empresa para desempenhar suas atividades.
- Reportar qualquer indício ou falha de segurança que possa colocar em risco a confidencialidade, integridade ou disponibilidade dos ativos de informação do Grupo Benner.

## 8. SANÇÕES

O Colaborador ou Prestador de Serviço do Grupo Benner tem por obrigação cumprir todas as políticas publicadas, caso contrário esta conduta será considerada um incidente.

O Comitê de Compliance exercerá seu poder perante o conhecimento desta Política para aplicar sanções aos infratores da mesma. Inicialmente o incidente será classificado em 3 níveis, quais sejam:

- **Casos Leves:** quando não há risco ao bom nome da Empresa ou exposição de informações classificadas como sensíveis. Um exemplo de caso leve é o uso eventual de recursos particulares, como acessos a websites fora do contexto de trabalho, destinados a compras e webmail particular.
- **Casos Médios:** reincidências de casos leves ou casos incidentes onde seja comprovada a não intenção de dolo.
- **Casos Graves:** quando a ação ou omissão do usuário exponha ou cause dano às informações classificadas como sensíveis. Tentativas deliberadas de acesso a dados sensíveis, não expressamente autorizado, constituem claramente um caso grave.

O Colaborador ou Prestador de Serviço, na constatação de incidentes (previamente classificado), sofrerá sanção, nos seguintes termos:

- **Notificação do Incidente ao Usuário:** O Colaborador será notificado pela Diretoria de forma pessoal, descrevendo o caso e se colocando à disposição para justificativas.
- **1ª Advertência por e-mail:** aplicada na constatação de incidente categorizado como Caso Leve. Esta advertência será enviada para o Colaborador, com cópia para o CI e terá valor jurídico.
- **2ª Advertência por e-mail:** aplicada pela reincidência de violação classificada como Caso Leve.

O método da advertência é o mesmo, mas aqui ficará dito que em caso de reincidência, uma **advertência escrita** será dada ao infrator:

- **1ª Advertência Escrita:** aplicada pelo acúmulo de incidentes categorizados como Caso Leve, após as duas advertências por e-mail enviadas ao infrator. Pode ser aplicada também com a constatação de um incidente classificado com Caso Médio. Uma carta de advertência do Departamento. Pessoal será dada ao infrator, com o devido aceite.
- **2ª Advertência Escrita:** aplicada pela reincidência de violação classificada como Caso Médio ou pela reincidência de qualquer violação após uma primeira advertência escrita. O método da advertência

é o mesmo, mas aqui ficará dito que em caso de nova reincidência, o Colaborador poderá ser desligado da Empresa.

- **Demissão com Justa Causa:** aplicado caso um incidente categorizado como Caso Grave aconteça e, neste existem provas suficientes para constatar um favorecimento ilícito do infrator sobre o **Grupo Benner**, bem como danos a sua imagem ou patrimônio. Nesta circunstância, caberá ao Jurídico da Empresa acompanhar o caso e a validade da demissão.

Não existe uma ordem para a aplicação das sanções, sendo assim, um incidente pode ter punição máxima sem que tenha havido qualquer outro incidente anterior.

## 9. ELIGIBILIDADE E VALIDADE

Esta política aplica-se a aplicável a todas as áreas da organização Benner, que utilizam ou tenham acesso a quaisquer ativos de informação das empresas do Grupo Benner.

Entra em vigor a partir de 20.04.2023.

## 10. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapas	Responsável
1.0	08/10/2019	Elaboração e Aprovação	Infraestrutura de TI e CEO
2.0	20/04/2023	Revisão e Aprovação.	Governança de TI e CEO

## 11. FORMALIZAÇÃO

ELABORAÇÃO/REVISÃO		APROVAÇÃO	
Jorge Espinhara – Governança de TI		Severino Benner - CEO	
20/04/2023	<small>DocuSigned by:</small> <i>Jorge Luiz Carvalho Espinhara</i> <small>46FCTE7A18DC49D...</small>	20/04/2023	<small>DocuSigned by:</small> <i>Severino Benner</i> <small>B5112A47CD594F7...</small>