



## CARTA DE COMPROMISSO DE SEGURANÇA DA INFORMAÇÃO DA BENNER

## SUMÁRIO

1. COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO .....	3
2. COMO GARANTIMOS A QUALIDADE E SEGURANÇA DAS NOSSAS SOLUÇÕES? .....	3
3. NOSSOS PROCESSOS INTERNOS .....	4
4. CAPACITAÇÃO DE COLABORADORES .....	5
5. ZERO TRUST E SEGURANÇA DE IDENTIDADE .....	7
6. FIREWALL .....	7
7. PROTEÇÃO DE ENDPOINTS, COMUNICAÇÃO E INFRAESTRURA .....	8
8. MDR, SOAR E SOC .....	8
9. MEDIDAS DE SEGURANÇA ADOTADAS NO GRUPO BENNER .....	10
10. RECOMENDAÇÕES PARA OS NOSSOS CLIENTES .....	13
11. LINK PARA CERTIFICACOES DOCUMENTAÇÕES .....	13
12. REGISTRO DE ALTERAÇÕES .....	14
13. FORMALIZAÇÃO .....	14

## **1. COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO**

A Benner adota um modelo de segurança em camadas para garantir confidencialidade, integridade e disponibilidade das informações.

Nosso compromisso com a proteção de dados se traduz em um conjunto robusto de medidas e estratégias de segurança, que asseguram a resiliência operacional dos serviços da Benner e a mitigação de riscos cibernéticos.

## **2. COMO GARANTIMOS A QUALIDADE E SEGURANÇA DAS NOSSAS SOLUÇÕES?**

A segurança não é um complemento nos produtos da Benner – ela é essencial desde o início. Adotamos uma abordagem de Security by Design e Privacy by Design, garantindo que privacidade, proteção de dados e segurança cibernética sejam incorporadas desde a concepção das nossas soluções.

### **O que isso significa na prática?**

**Security by Design:** Desenvolvemos nossos produtos com mecanismos de defesa nativos, prevenindo vulnerabilidades e garantindo resistência a ataques desde a primeira linha de código.

**Privacy by Design:** Garantimos que a privacidade dos usuários e a conformidade com a LGPD sejam prioridades desde a arquitetura das soluções, permitindo que clientes tenham controle sobre seus dados.

Para reforçar essa abordagem, implementamos:

- Análises de segurança contínuas para identificar e corrigir riscos antes que se tornem um problema.
- Simulações de ataques controlados, garantindo que nossas soluções resistam a ameaças reais.
- Testes de privacidade e conformidade, assegurando que os dados dos clientes sejam tratados com segurança e transparência.

**Benefícios diretos para nossos clientes:**

- Soluções mais seguras e confiáveis, reduzindo riscos de incidentes cibernéticos.
- Maior conformidade com normas e regulamentações de proteção de dados.
- Menos preocupações com vulnerabilidades, permitindo foco total nos negócios.

Mas segurança não se trata apenas de como desenvolvemos nossas soluções – ela precisa estar presente em toda a nossa operação. Da concepção dos produtos à sua gestão diária, contamos com processos estruturados que garantem resiliência, continuidade e prevenção de ameaças.

**3. NOSSOS PROCESSOS INTERNOS**

A governança da segurança na Benner vai além da tecnologia – ela é integrada a cada processo interno, garantindo que nossos serviços sejam confiáveis, auditáveis e resilientes.

Nossa estrutura de segurança é baseada em três pilares fundamentais:

- **Prevenção ativa:** antecipamos riscos antes que eles possam impactar a operação.
- **Monitoramento contínuo:** asseguramos visibilidade total sobre o ambiente, detectando qualquer anomalia.
- **Resposta rápida a incidentes:** estamos preparados para agir imediatamente diante de qualquer ameaça.

Como isso se traduz na prática?

**Políticas de segurança definidas**

Seguimos boas práticas reconhecidas internacionalmente, como as recomendações do NIST (National Institute of Standards and Technology), garantindo que nossos processos estejam alinhados aos padrões mais rigorosos do mercado.

**Gestão ativa de vulnerabilidades**

- Avaliações diárias para identificar possíveis riscos antes que eles possam impactar nossos serviços.
- Correções e atualizações semanais, priorizando vulnerabilidades críticas para manter a integridade da nossa infraestrutura.

**Proteção contínua para nossos colaboradores e sistemas**

- Monitoramento inteligente com EDR (Endpoint Detection and response), detectando e bloqueando ameaças automaticamente.
- Camadas adicionais de segurança no tráfego de dados, garantindo que a comunicação entre sistemas seja criptografada e protegida contra interceptação.
- Proteção contra-ataques externos, incluindo DNS sobre HTTPS (DoH) para prevenir ataques como *spoofing* (falsificação de identidade para enganar usuários e sistemas) e man-in-the-middle (interceptação de comunicações para roubo ou alteração de dados transmitidos).

A segurança não é apenas um processo interno – é o que garante que cada cliente da Benner possa operar com tranquilidade, sabendo que seus dados e operações estão protegidos por uma estrutura confiável e robusta.

**4. CAPACITAÇÃO DE COLABORADORES**

A Benner promove uma cultura sólida de conscientização em segurança cibernética, garantindo que nossos colaboradores estejam constantemente atualizados sobre as políticas e procedimentos de segurança da empresa, bem como as diretrizes da LGPD (Lei Geral de Proteção de Dados).

Para que todos sigam as boas práticas de segurança e saibam como agir diante de situações de risco, realizamos treinamentos obrigatórios para toda a equipe, incluindo novos colaboradores durante o *onboarding*.

**Portal de Treinamentos Interno – Educa Benner**

Além disso, contamos com o **Educa Benner**, um portal interno de treinamentos, que disponibiliza **cursos obrigatórios e diversos conteúdos de capacitação**, incluindo:

- Segurança da Informação – práticas essenciais para proteção de dados e mitigação de riscos.
- LGPD – conceitos e responsabilidades sobre privacidade e proteção de dados.
- Prevenção e Combate ao Assédio – garantindo um ambiente de trabalho seguro e respeitoso.
- ESG e Sustentabilidade – abordagens modernas de responsabilidade corporativa.
- Treinamentos técnicos e operacionais – capacitação para áreas específicas da empresa.

**Plataformas Complementares**

Além do portal **Educa Benner**, incentivamos a participação ativa dos colaboradores em plataformas online de aprendizado contínuo, abrangendo temas essenciais para segurança, tecnologia e inovação.

Os cursos oferecidos cobrem áreas estratégicas como:

- **Segurança Cibernética e Conscientização** – boas práticas para proteção digital.
- **Programação e Desenvolvimento** – incluindo Front-end, Back-end, DevOps e Mobile.
- **Ciência de Dados e Inteligência Artificial** – capacitação em Data Science, Machine Learning e Big Data.
- **UX & Design** – aprimoramento em Experiência do Usuário e Interfaces Digitais.
- **Gestão & Inovação** – abordagens modernas para liderança, transformação digital e metodologias ágeis.

Essas iniciativas permitem que nossos colaboradores aprimorem continuamente suas habilidades, mantendo-se alinhados às melhores práticas de segurança da informação e às tendências do mercado.

## 5. ZERO TRUST E SEGURANÇA DE IDENTIDADE

Adotamos o conceito de Zero Trust Security, assegurando que todo acesso, seja de usuários ou sistemas, é concedido com base em regras explícitas e continuamente validadas.

Nossos controles de segurança incluem:

- **MFA (Autenticação Multifator)** obrigatório para serviços de e-mail e colaboração.
- **Governo de acesso baseado em privilégios mínimos**, restringindo permissões apenas ao necessário.
- **Segregação de rede com controle de fluxo de tráfego**, garantindo que servidores e sistemas só possam se comunicar com **domínios, portas e serviços explicitamente autorizados**.
- **Análise contínua de credenciais vazadas**, com monitoramento ativo na *dark web*.
- **Revalidação periódica de acessos**, eliminando permissões desnecessárias ou obsoletas.
- **Uso segregado de contas administrativas**, reduzindo a exposição de contas privilegiadas e mitigando riscos de movimentação lateral em caso de comprometimento.
- **Revogação automática de acessos, baseada no Sistema de RH**, garantindo que mudanças como desligamento, afastamento ou alteração de função resultem na **desativação ou ajuste imediato das permissões**.

## 6. FIREWALL

Nossa infraestrutura está protegida por um sistema de firewall robusto (NGFWs), seguindo um modelo amplamente reconhecido por sua alta performance e recursos avançados de segurança, como bloqueio de geolocalização, prevenção de intrusões, inspeção e decodificação de TLS/SSL, controle de aplicativos, entre outros. Essas medidas garantem a integridade e a confiabilidade das comunicações e transferências de dados em nossa infraestrutura.

## 7. PROTEÇÃO DE ENDPOINTS, COMUNICAÇÃO E INFRAESTRUTURA

A Benner implementa um modelo de segurança robusto para proteger dispositivos, redes e comunicações contra ameaças digitais. Isso inclui medidas para garantir a segurança de *endpoints*, do ambiente de mensageria e da infraestrutura geral.

### Ambiente de Mensageria e Colaboração Seguro

- Utilizamos **Microsoft Office 365** como solução corporativa de e-mail, garantindo proteção contra *phishing*, *malware* e ataques de engenharia social.
- Monitoramos continuamente **tentativas de login suspeitas e ataques de força bruta**, bloqueando acessos não reconhecidos.

### Proteção de *Endpoints* e Controle de Software

- Implementamos **soluções EDR (Endpoint Detection and Response)** para **identificar, isolar e mitigar ameaças** em tempo real.
- Aplicamos restrições de software, impedindo a instalação de centenas de aplicativos não autorizados nos *endpoints* corporativos.
- Monitoramos o arquivo hosts dos *endpoints* para evitar acessos indevidos a sites não autorizados.

### Infraestrutura e Controle de Comunicação

- **Segregação de Rede:** Aplicamos **Zero Trust Networking**, onde servidores e sistemas só podem se comunicar com **domínios, portas e serviços explicitamente autorizados**.
- **Monitoramento e restrições de tráfego:** Garantimos que **servidores e endpoints tenham acesso apenas ao necessário**, evitando comunicação indevida entre sistemas.
- **Referência ao Firewall:** Para controle avançado de tráfego, utilizamos **Firewalls de Próxima Geração (NGFWs)**, conforme detalhado no **item 7**.

## 8. MDR, SOAR E SOC

Para reforçar a detecção e resposta a incidentes, implementamos um MDR (Managed Detection and response) que monitora *endpoints*, servidores e o ambiente BennerCloud.



**SOAR: Automação e resposta orquestrada**

O MDR está integrado a um **SOAR (Security Orchestration, Automation, and Response)**, permitindo:

- **Automação da resposta a incidentes**, reduzindo drasticamente o tempo de reação.
- **Correlação avançada de eventos**, permitindo detecção proativa de ameaças antes que elas causem impacto.
- **Orquestração entre múltiplos sistemas de segurança**, garantindo uma defesa integrada e coordenada.
- **Investigação acelerada de ameaças**, com análise automatizada de eventos em tempo real.

**Principais Benefícios do MDR e SOAR**

- **Detecção precoce de ameaças**, permitindo ações preventivas e mitigação antecipada.
- **Isolamento automático de *endpoints* comprometidos**, impedindo movimentação lateral de atacantes.
- **Bloqueio automatizado de ataques em andamento**, reduzindo o tempo de resposta e mitigação.
- **Aprimoramento da resposta a incidentes**, com workflows automatizados reduzindo a necessidade de intervenção manual.

**SOC e Monitoramento de Serviços Críticos**

O SOC (Security Operations Center) da Benner é responsável pelo monitoramento contínuo de serviços críticos da infraestrutura produtiva e de clientes, garantindo disponibilidade e estabilidade operacional, realizando:

- Supervisão de serviços essenciais, como infraestrutura, bancos de dados e aplicações críticas.
- Detecção de falhas operacionais e indisponibilidades, garantindo que ações corretivas possam ser tomadas pelo time responsável.

- Correlação de eventos em sistemas monitorados, permitindo rápida identificação de incidentes técnicos.
- Geração de alertas e notificações para as equipes responsáveis pela operação, sem intervenção direta.

## **9. MEDIDAS DE SEGURANÇA ADOTADAS NO GRUPO BENNER**

Na Benner, segurança da informação não é apenas uma prioridade – é um compromisso com a confiança e a continuidade dos negócios dos nossos clientes. Adotamos medidas de proteção que garantem disponibilidade, privacidade e conformidade, assegurando que os serviços e dados estejam sempre protegidos contra ameaças cibernéticas.

### **Segurança de Infraestrutura e Cloud**

A infraestrutura da Benner foi projetada para oferecer confiabilidade, escalabilidade e segurança avançada para os nossos clientes.

Para isso, utilizamos o Benner Cloud, uma plataforma baseada na Oracle Cloud Infrastructure (OCI), reconhecida por sua alta resiliência e proteção contra riscos operacionais.

### **O que isso significa para nossos clientes?**

- Alta disponibilidade: Garantimos que os serviços permaneçam estáveis e acessíveis, minimizando riscos de interrupção.
- Ambiente seguro e monitorado: Nossa infraestrutura é continuamente auditada e monitorada para garantir proteção contra ameaças e ataques cibernéticos.
- Conformidade com padrões globais: O Benner Cloud segue os mais altos padrões de segurança, atendendo a certificações como SOC 1, SOC 2, SOC 3, ISO 27001, PCI DSS e HIPAA.
- Implementação de controles de segurança, disponibilidade e integridade operacional, garantindo que os processos de TI e infraestrutura sejam monitorados, auditáveis e confiáveis.

- Next-generation firewalls (NGFWs): Proteção avançada com bloqueios geo-IP, prevenção de intrusões, IDS/IPS e inspeção TLS/SSL.
- Conexões criptografadas e WAF: Implementação de TLS 1.2 no mínimo e WAF sob demanda, garantindo comunicação segura e mitigação de ataques web.

Além do cuidado com a nossa infraestrutura, adotamos um conjunto de camadas adicionais de segurança para mitigar ameaças e garantir a integridade das aplicações e serviços. Essas medidas protegem desde o tráfego de rede até a integridade das informações processadas em nossos sistemas.

### **Proteção avançada para aplicações e tráfego**

Para mitigar ameaças e garantir a integridade das aplicações e serviços, aplicamos camadas adicionais de proteção:

#### **Mecanismos de inspeção e filtragem de tráfego:**

- **Redução de riscos cibernéticos:** Inspeção automática para bloquear tráfego suspeito antes que ele alcance a infraestrutura interna.
- **Prevenção contra ataques na web:** Implementação de regras avançadas para impedir ataques de injeção de código, exploração de vulnerabilidades e acessos indevidos.

#### **Fortalecimento das políticas de segurança HTTP:**

- Aplicação de **Strict-Transport-Security (HSTS)** para evitar ataques de *downgrade* de protocolo.
- Uso de **Content-Security-Policy (CSP)** para prevenir carregamento de scripts maliciosos.
- Implementação de **X-Frame-Options** para evitar ataques de *clickjacking*.

#### **Gestão segura de conexões criptografadas:**

- Criptografia TLS 1.2+ para garantir segurança na comunicação e impedir interceptação de dados.

- HSTS (HTTP Strict Transport Security) para reforçar o uso de HTTPS e evitar ataques de *downgrade* de protocolo.
- DNS over HTTPS (DoH) para proteger consultas DNS contra manipulação e espionagem.
- Firewalls e Monitoramento IDS/IPS, garantindo que tráfego malicioso ou tentativas de adulteração de pacotes sejam bloqueadas.

**Gestão de vulnerabilidades e proteção contra ameaças.**

- Gestão de vulnerabilidades ativa com avaliações diárias e correções semanais, mitigando riscos de segurança continuamente.
- Segurança de *endpoints* com EDR: Implementação de proteção avançada contra ameaças cibernéticas em dispositivos e servidores.
- Segurança de e-mails com Microsoft Office 365 e MFA, protegendo contra *phishing*, malware e ataques direcionados.

**Governança de Acessos e Conformidade**

- LAPS (Local Administrator Password Solution): Gerenciamento seguro de credenciais administrativas em servidores.
- Plano de treinamento e conscientização em segurança, incluindo treinamentos internos e plataformas online para colaboradores.
- Medidas de segurança estendidas para colaboradores, garantindo cultura de segurança e conformidade contínua.

**Monitoramento e Resposta a Incidentes**

- Monitoramento com NOC: Supervisão contínua de serviços críticos do ambiente produtivo e de clientes.

- MDR e SOAR 24/7: Resposta automatizada a incidentes e monitoramento contínuo de ameaças cibernéticas, garantindo ação proativa contra ataques e vazamentos de dados.

## **10. RECOMENDAÇÕES PARA OS NOSSOS CLIENTES**

Segurança e conformidade vão além da tecnologia – exigem processos bem definidos dentro das empresas. Nossa equipe está à disposição para apoiar nossos clientes na implementação de políticas de segurança eficazes, ajudando a fortalecer sua estrutura de TI e assegurar conformidade com a LGPD e demais regulamentações.

## **11. LINK PARA CERTIFICACOES DOCUMENTAÇÕES**

- [Certificados Oracle e PSI-Benner](#)

**12. REGISTRO DE ALTERAÇÕES**

Versão	Data	Etapa	Responsável
1.0	07.02.2025	CRIAÇÃO	JORGE ESPINHARA

**13. FORMALIZAÇÃO**

ELABORAÇÃO		APROVAÇÃO	
Jorge Espinhara – GOV DE TI		Severino Benner - CEO	
26.02.2025	<small>DocuSigned by:</small> <i>Jorge Luiz Carvalho Espinhara</i> <small>46FC1E7A18DC49D...</small>	26.02.2025	<small>DocuSigned by:</small> <i>Severino Benner</i> <small>B5112A47CD594F7...</small>