

# **guia de vendas (latu)** Seguros

Resumo das coberturas, benefícios, exclusões, selling points  
e possíveis respostas a objeções comuns.

## aviso legal

Todas as informações apresentadas neste material são meramente para referência e servem como um guia geral. Este documento não pretende substituir nem complementar as condições gerais dos seguros oferecidos pela Latú Seguros.

A Latú Seguros atua como representante de seguros, um tipo de associação devidamente regulamentado pela resolução de número 431 de 11 de Novembro de 2021 do Conselho Nacional de Seguros Privados (CNSP). Como representantes de seguros, somos autorizados a promover, ofertar e distribuir produtos de seguros em nome da sociedade seguradora BS2 Seguros S/A.

Seguro garantido por BS2 Seguros S.A, CNPJ 07.163.211/0001-94. Processo SUSEP 15414.608318/2024-24. As Condições Contratuais podem ser consultadas em [www.susep.gov.br](http://www.susep.gov.br) sob a busca "Consulta Pública de Produtos". A aceitação da proposta de seguro está sujeita à análise do risco. O registro do produto é automático e não representa aprovação ou recomendação por parte da SUSEP.

# Apresentando o **Seguro Cyber**.



## O que é?

É um **seguro** que protege empresas contra **incidentes cibernéticos**, sendo acionado sempre que ocorrer um evento desse tipo.



## Benefícios adicionais

O segurado conta, sem custo adicional, com acesso à **antivírus, firewall e backup em nuvem**, garantindo proteção abrangente.



## O que cobre?

- Custos incorridos para **recuperar-se** do ataque.
- Custos legais no caso de **vazamento de dados de terceiros**.
- **Multas** por vazamento de dados.



## Quem pode contratar?

**Qualquer empresa** que possua alguma atividade na internet, como:

- E-commerces.
- Contabilidade.
- Provedores de e-mail.
- Servidores.

# Como funcionam as **coberturas**?

## INCIDENTE CIBERNÉTICO



### Danos à Empresa

- Perda de dados.
- Indisponibilidade de sistemas.
- Ataques de *Ransomware*.



### Danos a Terceiros

- Vazamento de dados.
- Investigação Regulatória.
- Ações Judiciais.

### O Seguro cobre:

- Custos de restauração de dados.
- Custos forenses.
- Custos de monitoramento de crédito.
- Custos de extorsão cibernética.
- Custos de comunicação.
- Lucros Cessantes.

### O Seguro cobre:

- Custos de defesa.
- Indenizações à terceiros.
- Acordos judiciais e extrajudiciais.
- Multas e Penalidades.

# Detalhamento das **coberturas**.

**Danos à Empresa.** Em caso de **descoberta** de um incidente cibernético, são passíveis de cobertura:

## **CUSTOS DE REPRESENTAÇÃO LEGAL.**

Honorários e despesas para consultoria ou representação legal após um evento cibernético. Por exemplo, em caso de vazamento de dados, a seguradora contrata um escritório especializado em LGPD para comunicar o incidente à ANPD, cumprindo as obrigações legais e minimizando possíveis penalidades.

## **CUSTOS DE MONITORAMENTO DE CRÉDITO.**

Despesas para serviços de monitoramento de crédito e roubo de identidade para indivíduos afetados por um evento cibernético, normalmente por um período de 12 meses, visando prevenir danos adicionais. Isso é necessário porque é comum criminosos realizarem abertura de contas bancárias com base em credenciais vazadas em ataques cibernéticos.

## **LUCROS CESSANTES.**

Referem-se à perda de lucro líquido e às despesas fixas e operacionais que são necessárias para manter o funcionamento normal dos negócios, causadas por uma interrupção das atividades. Isso inclui custos para evitar ou minimizar os efeitos de uma queda de sistema ou interrupção de rede, bem como ações para descobrir e limitar essa interrupção, preservar evidências e justificar as perdas de negócios.

## **CUSTOS DE RESTAURAÇÃO DE DADOS.**

Despesas para restaurar ou substituir dados e programas perdidos, apagados, corrompidos ou criptografados devido a um incidente cibernético, incluindo a compra de licenças de software.

## **CUSTOS DE COMUNICAÇÃO.**

Despesas para comunicar incidentes cibernéticos a indivíduos afetados ou autoridades competentes, incluindo notificações de violação de dados à ANPD.

## **CUSTOS DE RELAÇÕES PÚBLICAS.**

Honorários e despesas de consultoria para proteger ou mitigar danos à reputação do segurado, incluindo ações para manter a imagem pública após um incidente cibernético.

## **CUSTOS DE EXTORSÃO CIBERNÉTICA.**

Reembolso de despesas para encerrar ou mitigar um ataque de ransomware ou qualquer ameaça crível de um evento cibernético resultante de extorsão com o consentimento da seguradora.

## **CUSTOS FORENSES.**

Despesas para investigar a causa, escopo e extensão de incidentes cibernéticos, incluindo análise de segurança de dados e sistemas afetados.

# Detalhamento das **coberturas**.

**Danos a Terceiros.** Em caso de uma **reclamação** apresentada por terceiros associadas a um incidente cibernético, são passíveis de cobertura:

## **CUSTOS DE DEFESA.**

Despesas legais para defender o segurado contra reclamações relacionadas a incidentes cibernéticos. Inclui honorários advocatícios, custas judiciais e despesas para apresentar defesas e recursos.

## **CUSTOS DE INDENIZAÇÃO.**

Pagamentos devidos a terceiros determinados por decisões judiciais, arbitrais, ou administrativas como resultado de uma reclamação, devido a danos causados por incidentes cibernéticos.

## **CUSTOS DE ACORDOS.**

Despesas para resolver reclamações por meio de acordos judiciais ou extrajudiciais, com a anuência da seguradora,

## **CUSTOS DE MULTAS E PENALIDADES.**

Despesas para comunicar incidentes cibernéticos a indivíduos afetados ou autoridades competentes, incluindo notificações de violação de dados à ANPD.

# Detalhamento das **exclusões.**

## **TRANSFERÊNCIA DE FUNDOS.**

Transferências eletrônicas indevidas de fundos ou valores do segurado. Ou seja, em uma transferência bancária, o valor em si NÃO está coberto.

## **ATOS DOLOSOS.**

Danos causados intencionalmente pelo segurado ou seus representantes, válida após comprovação judicial ou confissão escrita.

## **EVENTOS ANTERIORES.**

Eventos cibernéticos previamente conhecidos ou notificados e fatos ocorridos antes do início da apólice.

## **DANOS MATERIAIS E CORPORAIS.**

Danos físicos a bens ou pessoas e danos morais relacionados, exceto quando causados diretamente por eventos cibernéticos.

## **OPERAÇÃO CIBERNÉTICA ESTATAL.**

Operações cibernéticas perpetradas por Estados, com caracterização condicionada à atribuição governamental ou análise objetiva.

## **DISPOSITIVO PORTÁTIL NÃO CRIPTOGRAFADO.**

Qualquer dado que tenha sido perdido ou vazado que estava armazenado em dispositivo portátil não criptografado por biometria ou senha.

## **VIOLAÇÃO DE LEIS DE SPAM E TELEMARKETING.**

Violações de legislação anti-spam ou de telemarketing.

## **ATUALIZAÇÃO E MELHORIAS.**

Custos com a atualização ou melhoria de sistemas computacionais.

## **NÃO RELACIONADAS A RESPONSABILIDADE CIBERNÉTICA.**

Responsabilidades imputadas ao segurado que estejam diretamente ligadas a eventos cibernéticos.

## **OBRIGAÇÕES CONTRATUAIS.**

Qualquer inadimplemento de obrigações contratuais, exceto se tal obrigação prevalecesse no caso da ausência da obrigação contratual

## **SERVIÇOS PÚBLICOS.**

Danos por Interrupções ou falhas em serviços públicos, salvo se fornecidos pelo próprio segurado.

## **MESMO GRUPO ECONÔMICO.**

Reclamações feitas por empresas ou indivíduos que pertencem ao mesmo grupo econômico do segurado.

## **RADIAÇÃO, ENERGIA NUCLEAR, MAGNETISMO.**

Danos causados por ou devidos à radiação, energia nuclear ou eletromagnetismo.

## **GUERRA OU DESORDEM CIVIL.**

Danos resultantes de guerra ou desordem civil.

## **SANÇÕES INTERNACIONAIS.**

Questões decorrentes de sanções internacionais (ex: negócios com Rússia, Irã, Coreia do Norte etc).

# Apresentando o **Seguro Cyber**.



## **Central de Atendimento 24/7**

Nosso 0800 oferece **suporte imediato** e está disponível **a qualquer hora do dia**, garantindo resposta rápida a incidentes cibernéticos.



## **Equipe de Especialistas em Cibersegurança**

**Profissionais altamente capacitados** para análise e mitigação de incidentes identificados, atuando de modo a mitigar danos e conter custos.



## **Planos de Resposta Adaptáveis**

**Protocolos específicos e adaptáveis** para diferentes tipos de incidentes, assegurando uma abordagem eficaz e coordenada para cada situação.



## **Painel Jurídico Especializado em Direito Digital**

Atuamos com **escritórios parceiros especializados** para garantir conformidade com a LGPD e apoio em questões legais relacionadas a incidentes cibernéticos.



### **A relevância de uma resposta a incidentes efetiva**

Agir de modo rápido e eficiente a incidentes cibernéticos é crucial para **minimizar danos, proteger dados sensíveis, reduzir custos e preservar a confiança dos clientes** e a reputação da empresa.

# Benefícios adicionais: Avaliação de riscos cibernéticos mensal **LatúScan e Antivírus.**

## LatúScan

### Mapeamos a superfície de ataque

A partir da URL do seu cliente, **mapeamos todos os subdomínios, endereços de IP, protocolos de e-mails** entre outros serviços.

### Avaliamos vulnerabilidades presentes

Com uma base de dados em tempo real, **buscamos por +100 mil vulnerabilidades** já catalogadas globalmente.

### Buscamos vazamentos de dados

**Monitoramos fontes abertas e a dark web** para detectar vazamentos de dados sensíveis.

### Estimamos potenciais perdas financeiras

**Analisamos o impacto financeiro potencial** de acordo com as vulnerabilidades encontradas e o perfil do cliente.

### Priorizamos e apresentamos soluções

**Classificamos as vulnerabilidades identificadas por nível de risco**, oferecendo soluções para cor-



## Antivírus

### Pacote de antivírus incluso:

- **Proteção multicamadas**, com prevenção e neutralização de vírus.
- **Deteção de vulnerabilidades**, remove vírus e repara seu PC
- **Impede acesso não autorizado** e sequestro com anti-phishing e firewall.

### Instalação opcional,

não necessária se já possuir antivírus.

**Até 10 licenças** por segurado.

# Principais **Sellings Points**.

**Perguntas de qualificação** que auxiliam a planejar e nortear o processo de venda.

## Pergunta de Qualificação

1. Sua empresa **manipula ou armazena dados dos clientes** ou parceiros?
2. Você possui alguma **medida de segurança cibernética** existente?
3. Sua empresa ou você **já sofreu algum incidente cibernético** no passado?
4. Você está ciente das **consequências legais e financeiras** de uma violação de dados?

**O SEGURO CYBER...**

**O SEGURO CYBER...**

**O SEGURO CYBER...**

**O SEGURO CYBER...**

## Selling Points

... **cobre os custos legais** caso terceiros responsabilizem a empresa por vazamento de seus dados.

... **oferece acesso à um pacote de proteção cibernética** para proteger seus dispositivos eletrônicos e mitigar riscos.

... **proporciona acesso imediato a especialistas em segurança cibernética** para avaliação de riscos, resposta rápida a incidentes e orientação estratégica.

... **inclui cobertura financeira para prejuízos** causados por ataques cibernéticos e violações de dados, incluindo perdas devido a fraudes e custos de recuperação de dados ou extorsão cibernética.

# Principais **Sellings Points**.

**Perguntas de qualificação** que auxiliam a planejar e nortear o processo de venda.

## Pergunta de Qualificação

**5.** Você **está ciente das multas e penalidades impostas pela ANPD** por violações de privacidade de dados?

**6.** Você tem clientes ou parceiros que **se preocupam com a segurança de suas informações**?

**7.** Você sabe o que fazer caso sofra uma **extorsão cibernética**?

**8.** Você sabe como restaurar seu sistema caso um **ataque danifique seus ativos tecnológicos**?

**O SEGURO CYBER...**

**O SEGURO CYBER...**

**O SEGURO CYBER...**

**O SEGURO CYBER...**

## Selling Points

... **proporciona assistência financeira para custear despesas legais**, multas regulatórias e compensações devido a violações de privacidade.

... **contribui para o fortalecimento da imagem da empresa** ao demonstrar um comprometimento proativo com a segurança e privacidade de dados.

... **oferece cobertura para ataques de ransomware**, incluindo o pagamento de resgates sob consulta especializada, para evitar perdas maiores de dados ou danos ao sistema.

... **inclui cobertura dos custos associados à restauração de sistemas de TI e recuperação de dados**, garantindo a continuidade dos negócios com o mínimo de interrupção possível.

# Como lidar com **objeções comuns.**

## Objeção



**O seguro é muito caro.**



**Nossa empresa é pequena, não somos um alvo.**



**Já temos fortes medidas de segurança TI.**

## Fato

O valor médio de um ataque cibernético no Brasil é de **R\$ 7 milhões.**

**40%** foi o aumento no número de ataques cibernéticos a PMEs no Brasil.

**100 milhões** de ataques cibernéticos são feitos por ano no Brasil. O segundo maior destino do mundo!

## Valor do seguro

Esse é o custo potencial de um ciberataque em comparação com os prêmios acessíveis de nossa apólice. O seguro oferece uma rede de segurança financeira que pode ser muito mais acessível do que o custo de um incidente.

Mesmo que as empresas não lidem com dados sensíveis estão expostas a riscos cibernéticos, como ataques de negação de serviço (DDoS) que podem interromper suas operações. Além disso, qualquer informação de cliente pode ser valiosa para criminosos.

Qualquer um desses ataques pode explorar uma nova vulnerabilidade e penetrar nas camadas de segurança para realizar um ataque. A apólice de seguro é a única forma de transferir esse risco para uma terceira parte que irá pagar pelas perdas, caso isso aconteça.

# Como lidar com **objeções comuns.**

## Objeção

## Fato

## Valor do seguro



**As seguradoras nunca pagam sinistros.**

**R\$ 180 milhões** foi o valor pago pelas seguradoras em 2023 em sinistros cibernéticos.

Apólices patrimoniais podem não cobrir afirmativamente riscos cibernéticos - e normalmente os excluem explicitamente. Nossa apólice dedicada garante proteção abrangente contra esses riscos.



**Preferimos investir em prevenção.**

Empresas com **orçamentos milionários de tecnologia** como Fleury e Americanas, já foram vítimas de ataques cibernéticos.

Investimentos adicionais em segurança podem aumentar a proteção mas não eximem a empresa do risco de um ataque. A prevenção é fundamental, mas também é importante estar preparado para o pior cenário. O seguro cyber não substitui a prevenção; ele serve como uma camada adicional de proteção.



**Preocupação com a complexidade do processo.**

Nosso Seguro Cyber tem o processo de contratação **mais simples do mercado brasileiro.**

É muito simples. A cotação já está pronta. Basta você assinar e já emitimos a apólice. Parcelamos no boleto, em 12x.

# Conte conosco!

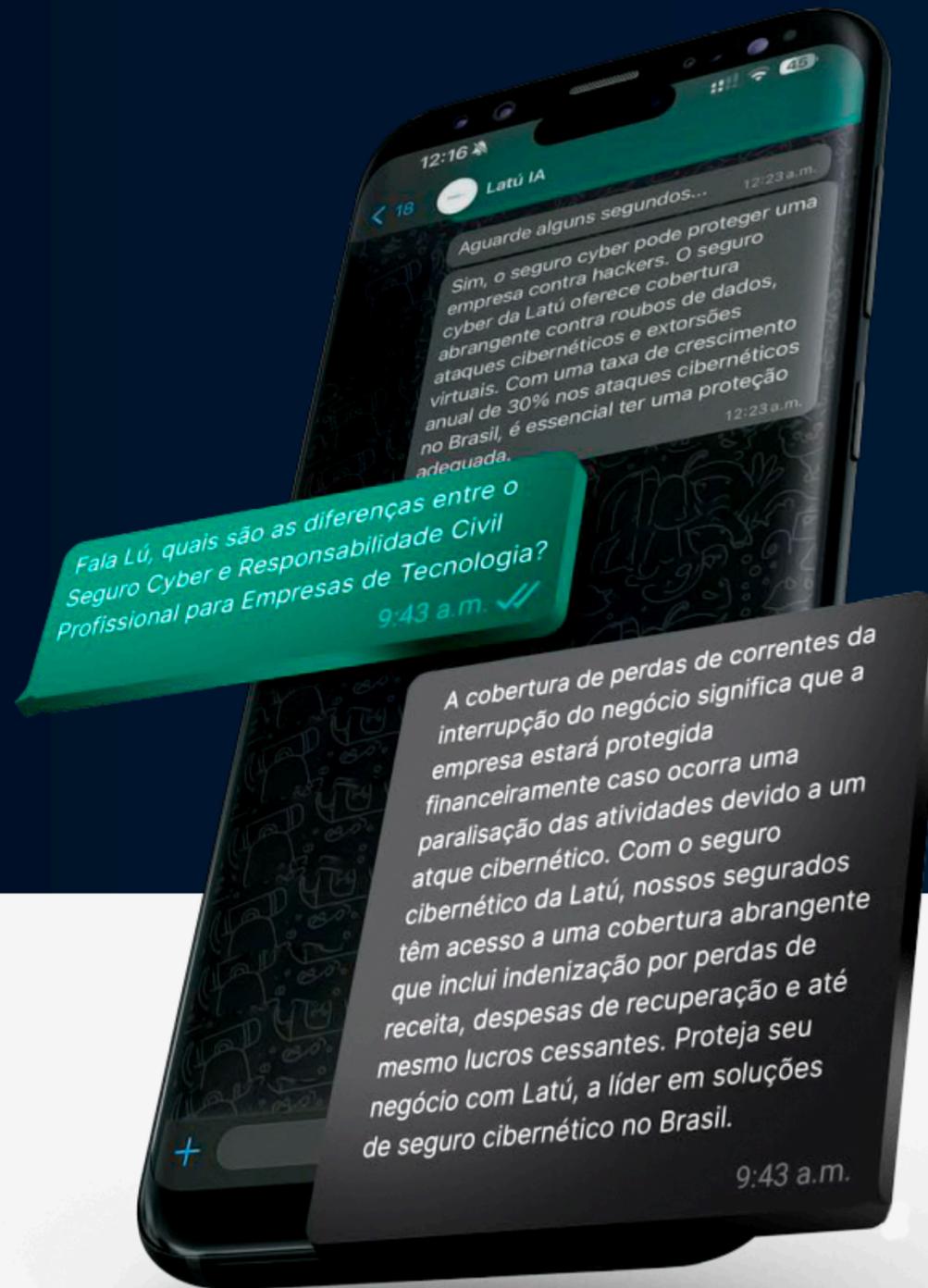
Caso tenha qualquer dúvida ou necessidade, **não hesite em entrar em contato** conosco!

**11 4040-2388**

Estamos disponíveis a qualquer horário, em qualquer dia, também por ligação!



WWW.LATUSEGUROS.COM



Fala Lú, quais são as diferenças entre o Seguro Cyber e Responsabilidade Civil Profissional para Empresas de Tecnologia?  
9:43 a.m. ✓

A cobertura de perdas de correntes da interrupção do negócio significa que a empresa estará protegida financeiramente caso ocorra uma paralisação das atividades devido a um ataque cibernético. Com o seguro cibernético da Latú, nossos segurados têm acesso a uma cobertura abrangente que inclui indenização por perdas de receita, despesas de recuperação e até mesmo lucros cessantes. Proteja seu negócio com Latú, a líder em soluções de seguro cibernético no Brasil.  
9:43 a.m.

**(latú)** Seguros