Guia de Vendas

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

Apresentando o **seguro cyber**

O que é?

É um **seguro** que protege empresas contra incidentes cibernéticos.

O seguro é acionado se a empresa tiver um **incidente cibernético.**

Benefícios adicionais

O segurado tem acesso, **sem custo**:

- **Antivírus**
- **Firewall**
- **LatúScan Mensal**

O que cobre?

- Os custos incorridos para **recuperar-se** de um ataque cibernético.
- Os custos legais caso terceiros **responsabilizem** a empresa por **vazamento de seus dados.**
- **Multas** por vazamento de dados.

Quem pode contratar?

Qualquer empresa que possua alguma atividade na internet.

- Vendas ou serviços on-line;
- Faturamento de notas on-line;
- Website; e-mail; servidores.

Como funcionam as **coberturas**?

Evento Cibernético

Danos à Empresa

- Perda de dados
- Indisponibilidade de Sistemas
- Ataques de *Ransomware*

O Seguro cobre:

- Custos de restauração de dados
- Custos forenses
- Custos de monitoramento de crédito
- Custos de extorsão cibernética
- Custos de comunicação

Resp. por danos a Terceiros

- Vazamento de Dados
- Investigação Regulatória
- Ações Judiciais

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 Evento Cibernético, são passíveis de cobertura:

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

- **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 realizaram abertura de contas bancárias com base em credenciais vazadas em ataques cibernéticos.

- **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.

Detalhamento das **Coberturas**

Responsabilidade por danos a terceiros

Em caso de uma *reclamação* apresentada por terceiros associadas a um Evento 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, relacionadas a incidentes cibernéticos.

- **Custos de Multas e Penalidades**
  Multas ou penalidades civis impostas por autoridades competentes ou pelo poder judiciário, excluindo multas contratuais, decorrentes de uma reclamação por incidentes cibernéticos.

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.
- **Dispositivo Portátil não Criptografado**
  Qualquer dado que tenha sido perdido ou vazado que estava armazenado em dispositivo portátil não criptografado por biometria ou senha.
- **Serviços Públicos**
  Danos por Interrupções ou falhas em serviços públicos, salvo se fornecidos pelo próprio segurado.
- **Atos Dolosos**
  Danos causados intencionalmente pelo segurado ou seus representantes, válida após comprovação judicial ou confissão escrita.
- **Violação de Leis de *spam*; telemarketing**
  Violações de legislação anti-spam ou de telemarketing.
- **Mesmo Grupo Econômico**
  Reclamações feitas por empresas ou indivíduos que pertencem ao mesmo grupo econômico do segurado.
- **Eventos anteriores**
  Eventos cibernéticos previamente conhecidos ou notificados e fatos ocorridos antes do início da apólice
- **Atualização e Melhorias**
  Custos com a atualização ou melhoria de sistemas computacionais.
- **Radiação, Energia Nuclear, Magnetismo**
  Danos causados por ou devidos à radiação, energia nuclear ou eletromagnetismo
- **Danos Materiais e Corporais**
  Danos físicos a bens ou pessoas e danos morais relacionados, exceto quando causados diretamente por eventos cibernéticos.
- **Não Relacionadas a Resp. Cibernética**
  Responsabilidades imputadas ao segurado que estejam diretamente ligadas a eventos cibernéticos.
- **Guerra ou Desordem Civil**
  Danos resultantes de guerra ou desordem civil.
- **Operação Cibernética Estatal**
  Operações cibernéticas perpetradas por Estados, com caracterização condicionada à atribuição governamental ou análise objetiva.
- **Obrigações Contratuais**
  Qualquer inadimplemento de obrigações contratuais, exceto se tal obrigação prevalecesse no caso da ausência da obrigação contratual
- **Sanções Internacionais**
  Questões decorrentes de sanções internacionais (ex: negócios com Rússia, Irã, Coréia do Norte etc)

Benefícios Adicionais – Soluções de **cibersegurança**

Todos os segurados terão acesso até 15 licenças do software de cibersegurança que poderão utilizar para proteger os dispositivos da empresa, contando com as seguintes características:

Antivírus

Proteção multicamadas projetada para prevenir e neutralizar vírus e *malwares*.

Anti-Hacker

Ferramentas para impedir acesso não autorizado e sequestro do seu computador, incluindo *anti-phishing* e *firewall*.

Remoção de ameaças

Tecnologias para detectar vulnerabilidades, remover vírus e reparar seu PC caso ele já tenha sido infectado.

Navegação privada

Ferramentas para evitar rastreamento on-line não autorizado, exibição de anúncios não autorizados ou qualquer pessoa que use seus periféricos.

Otimização de performance

Permite liberar espaço em seus dispositivos e melhorar o desempenho do sistema.

Proteção bancária on-line

Tecnologias avançadas para proteger suas transações online e aplicativos bancários.

Benefícios adicionais: Avaliação de Riscos Cibernéticos Mensal **LatúScan**

Mapeamos a Superfície de Ataque

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

Avaliamos mais de 100 mil vulnerabilidades

Com um banco de dados atualizado em tempo real, analisamos a existência de quaisquer vulnerabilidades já identificadas pela comunidade de cibersegurança global

Buscamos Vazamentos de Dados

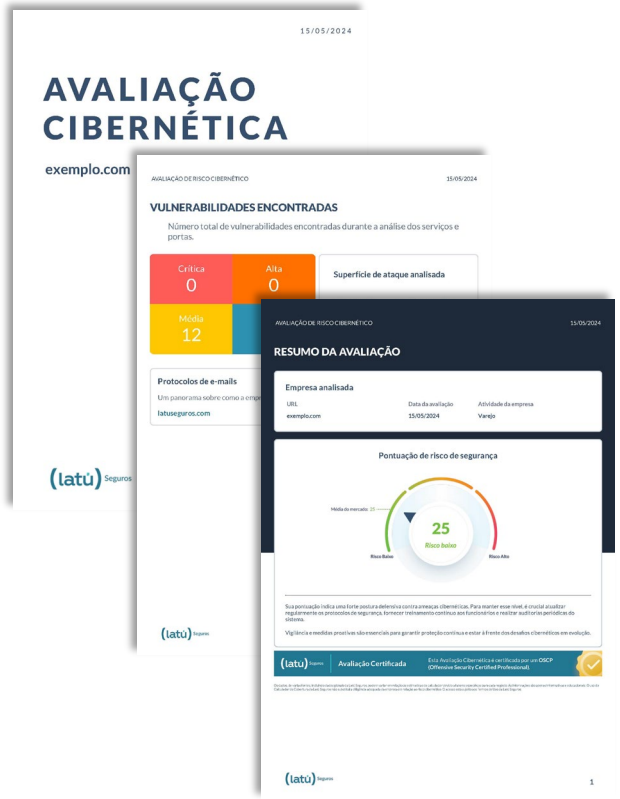
Monitoramos fontes abertas e a dark web para detectar vazamentos de dados sensíveis, informando rapidamente seu cliente para mitigar os danos.

Estimamos Potenciais Perdas Financeiras

Analisamos o impacto financeiro potencial de acordo com as vulnerabilidades encontradas e o perfil do cliente, fornecendo estimativas das possíveis perda.

Priorizamos e Apresentamos Soluções

Classificamos as vulnerabilidades identificadas por nível de risco, oferecendo soluções para correção



Principais ***Sellings Points*** **(1 de 2)**

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

Pergunta de Qualificação		*Selling point*
Sua empresa manipula ou armazena dados dos clientes ou parceiros?	O seguro cyber...	...cobre os **custos legais** caso terceiros responsabilizem a empresa por vazamento de seus dados.
Você possui alguma medida de segurança cibernética existente?	O seguro cyber...	...oferece acesso à **um pacote de proteção cibernética** para proteger seus dispositivos eletrônicos e mitigar riscos.
Sua empresa ou você já sofreou algum incidente cibernético no passado?	O seguro cyber...	...proporciona **acesso imediato a especialistas em segurança cibernética** para avaliação de riscos, resposta rápida a incidentes e orientação estratégica.
Você está ciente das consequências legais e financeiras de uma violação de dados?	O seguro cyber...	...inclui **cobertura financeira para prejuízos causados por ataques cibernéticos** e violações de dados, incluindo perdas devido a fraudes, custos de recuperação de dados ou extorsão cibernética.

Principais ***Sellings Points*** **(2 de 2)**

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

Pergunta de Qualificação		***Selling point***
Você está ciente das multas e penalidades impostas pela ANPD por violações de privacidade de dados?	O seguro cyber...	... proporciona assistência financeira para custear despesas legais, **multas regulatórias e compensações** devido a violações de privacidade
Você tem clientes ou parceiros que se preocupam com a segurança de suas informações?	O seguro cyber...	... contribui para o **fortalecimento da imagem da empresa** ao demonstrar um comprometimento proativo com a segurança e privacidade de dados
Você sabe o que fazer caso sofra uma extorsão cibernética?	O seguro cyber...	... oferece **cobertura para ataques de ransomware, incluindo o pagamento de resgates** sob consulta especializada, para evitar perdas maiores de dados ou danos ao sistema.
Você sabe como restaurar seu sistema caso um atacante danifique seus ativos tecnológicos?	O seguro cyber...	... 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* (1 de 2)

Objeção	Fato	Valor do seguro
O seguro é muito caro	O valor médio de um ataque cibernético em Brasil é de **R$ 7 milhões**.	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
Nossa empresa é pequena, não somos um alvo	**40%** foi o aumento no número de ataques cibernéticos a PMEs no Brasil.	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
Já temos fortes medidas de segurança TI	**100 milhões** de ataques cibernéticos por ano são feitos no Brasil. O segundo maior destino do mundo!	Qualquer um desses ataques pode explorar uma nova vulnerabilidade e penetrar nas camadas de segurança para realizar um ataque bem-sucedido. 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* (2 de 2)

Objeção	Fato	Valor do seguro
As seguradora 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, 12x.

Apetite: Seguro Cyber

- Empresas com faturamento anual até **R$50M**
- Limites de Cobertura de até **R$ 300 mil**

Forte Apetite

- Atacadistas / Varejistas
- Administração de Imóveis / Síndicos
- Agricultura / Pecuária / Pesca
- Academias / Spas / Ginásios
- Hotéis / Pousadas
- Agências de Viagem e Turismo
- Agências de Recrutamento / RH
- Aluguel de Equipamentos
- Cafés / Bares / Restaurantes
- Arquitetos
- Construção Civil
- Caridade / ONGs
- Artistas, Músicos e Escritores
- Designers de Moda / Gráficos
- Designers de Interiores
- Bibliotecas e Arquivos
- Consultoria de Gestão
- Setor Marítimo
- Reservas Naturais e Parques
- Serviços Administrativos
- Associações Comerciais
- Logística e Armazenagem
- Reparos / Serviços de Carros
- Salões de Beleza
- Gráficas
- e mais...

Apetite Moderado

- Editoras (Jornais, Web)
- Emissoras de Rádio e TV
- Filmagem e Fotografia
- Água, Eletricidade, Esgoto
- Publicidade e Marketing
- Telecomunicações
- Instituições Financeiras
- Instituições Governamentais
- Empresas de Tecnologia
- Contadores
- Serviços Educacionais
- Industria de Alimentos e Bebidas
- Fundos de Investimento
- Gestores de Fundos Imobiliários
- Corretores de Investimento
- Corretores de Seguros
- Cartório
- Relações Públicas
- Serviços de Folha de Pagamento
- Escritório de Advocacia
- Manufatura
- Empresas de Segurança
- Indústria Extrativista
- Clínicas

Sem Apetite

- Agregadores de Dados / Analytics
- Companhias Aéreas
- Desenvolvedores de Jogos
- Entretenimento Adulto
- Jogos de Azar
- Plataformas de Jogos Online
- Processadoras de Pagamento
- Moedas Virtuais
- Instituições Religiosas
- Hospitais (exc. Clínicas)

Critério Mínimos de Aceitação

1. Implementação de um **firewall** de nível empresarial em todas as entradas externas da rede e de **software antivírus** de nível empresarial em toda a rede, incluindo servidores ou endpoints.

2. Os dados necessários para a operação das atividades comerciais são salvos em backup pelo proponente (ou seu Provedor de Serviços na Nuvem) pelo menos a cada 7 dias. Esses dados em backup são armazenados em um ambiente completamente separado da rede corporativa.

3. O Proponente instala patches críticos dentro de 15 dias após o lançamento. Um patch de software crítico é aquele cuja instalação é considerada obrigatória pelo fabricante de software por motivos de segurança.

4. O acesso remoto às aplicações necessárias para o segurado realizar suas atividades profissionais é protegido com, no mínimo, autenticação de 2 fatores.

→ Oferecemos gratuitamente até 15 licenças caso o cliente necessite.

→ Exemplo de provedores que atendem a este requisito: Google Drive, OneDrive, Dropbox, etc.

Mantenha contato conosco

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

Estamos disponíveis a qualquer horário, qualquer dia!

11 4040-2388
(número também aceita ligações)