

A intenção deste questionário é conhecer como a organização protege a sua informação, os seus sistemas, como deteta possíveis incidentes, a resposta que oferece para a gestão dos mesmos, incluindo os serviços externalizados e com base nisso, apresentar a nossa proposta de seguro e serviços. Em função do nível de risco que tenhamos detetado poderemos solicitar a realização de uma avaliação de risco mais detalhada.

Informação geral

Corretor de seguros

Nome do Tomador

NIF

Morada

Código Postal

Ano de Constituição

Página web

Outras Entidades **Necessita de cobertura para as subsidiárias** Sim Não

Se respondeu Sim, tenha em consideração que as seguintes perguntas neste questionário se referem a todas as empresas a segurar nesta apólice, incluindo faturação e sinistralidade. Também deverá anexar uma lista de todas as subsidiárias.

Informação Financeira do Tomador e das suas Subsidiárias

| | | | |
|-----------------------------|---|---|---|
| Faturação anual | € | Faturação por País / Subsidiária (valor ou percentagem) | |
| Ano | | | |
| % Venda online | % | | |
| Resultado Operacional Anual | € | Europa | |
| Ano | | EUA e Canadá | |
| | | Resto do mundo | |
| | | Total anual | € |

Número de empregados O número total de empregados, incluindo das subsidiárias

Atividades

Por favor detalhe a sua atividade (inclua as atividades das suas subsidiárias)

1. Para entender melhor a sua atividade, por favor selecione as áreas onde a desenvolve

| Área | Se a realiza total ou parcialmente coloque "Sim" | É realizada Online? |
|--|---|---|
| Fabrico | Sim <input type="checkbox"/> Não <input type="checkbox"/> | Não se aplica |
| Venda de bens e Serviços ao Consumidor Final | Sim <input type="checkbox"/> Não <input type="checkbox"/> | Sim <input type="checkbox"/> Não <input type="checkbox"/> |
| Venda de bens e Serviços a um Intermediário | Sim <input type="checkbox"/> Não <input type="checkbox"/> | Sim <input type="checkbox"/> Não <input type="checkbox"/> |
| Distribuição (Produtos ou Serviços) | Sim <input type="checkbox"/> Não <input type="checkbox"/> | Sim <input type="checkbox"/> Não <input type="checkbox"/> |
| Serviços de Hosting / SaaS / PaaS / IaaS a terceiros | Sim <input type="checkbox"/> Não <input type="checkbox"/> | Não se aplica |

Em caso afirmativo, por favor forneça detalhes do serviço oferecido

2. Indique, por favor, o número de pessoas físicas de quem você, ou alguém em seu nome, processa, armazena ou transfere dados sensíveis*

| | | | |
|---------------------|--------------------------|-----------------------|--------------------------|
| <20.000 | <input type="checkbox"/> | 1.000.001 – 3.000.000 | <input type="checkbox"/> |
| 20.001 – 100.000 | <input type="checkbox"/> | 3.000.001 – 6.000.000 | <input type="checkbox"/> |
| 100.001 – 250.000 | <input type="checkbox"/> | > 6.000.000 | <input type="checkbox"/> |
| 250.001 – 1.000.000 | <input type="checkbox"/> | | |

* Por dados sensíveis, entende-se:

- NIF, Número de Segurança Social, BI ou Cartão de Cidadão, Carta de Condução, Passaporte.
- Dados Bancários, como por exemplo, números de Cartões de Crédito.
- Informação sobre raça, etnia, orientação sexual, estado de saúde, dados genéticos, biométricos, de crenças religiosas, políticas ou sindicais.

3. Você cumpre com as normas de Proteção de Dados? Sim Não

4. Caso tenha a obrigação legal de o fazer, existe um DPO (Delegado de Proteção de Dados), Interno ou Externo? Sim Não
Sem Obrigação Legal

5. Indique o cargo, anos de experiência e certificações das pessoas responsáveis pela Proteção de dados e de Segurança da Informação

Não temos responsável (s) nessas áreas.

6. Tem implementado um programa de formação anual para os seus Empregados (incluindo Diretores e Administradores), sobre as ameaças e boas práticas em CiberSegurança, Proteção de Dados e Privacidade? Sim Não

Em caso afirmativo, por favor forneça mais detalhes:

7. Relativamente aos seus sistemas informáticos, por favor responda às questões abaixo:

- a. Realiza um inventário anual do seu Software e Firmware? Sim Não
- b. Confirma que não utiliza Sistemas ou Programas sem suporte do Fabricante (como, por exemplo Windows 7 ou XP)? Sim Não

Em caso de resposta negativa, por favor responda às questões abaixo:

- c. Estão os mesmos totalmente desligados da Internet e do resto da sua Rede? Sim Não
- d. Dispõe de uma extensão de suporte especial por parte do Fabricante? Sim Não

Por favor indique a sua política no que diz respeito a Patches / Atualizações, indicando, entre outras coisas, a frequência, e se são realizados em ambientes de teste ou não:

- e. As atualizações / Patches e testes do seu Software Próprio (caso seja aplicável) realizam-se em ambiente de teste? Sim Não
- f. Desenvolve software próprio como parte do seu Negócio? Sim Não

No caso de resposta afirmativa, por favor responda às questões abaixo:

- a. Realiza frequentemente testes, com ferramentas de terceiros, para detetar possíveis vulnerabilidades? Sim Não
- b. Existe separação de funções durante as fases distintas de desenvolvimento do Software? Sim Não

8. Relativamente aos seus sistemas informáticos, por favor responda às questões abaixo:

- a. Descreva a sua estratégia de cópias de Segurança, indicando, entre outras coisas: a frequência, o tipo de dispositivos ou meios onde as armazena, se são realizadas por si ou não, número de cópias e confirmação de que, pelo menos uma delas está permanente desconetada dos seus sistemas (Offline);

- b. Você realiza (ou alguém em seu nome), cópias de todos os seus sistemas e informação crítica para o seu negócio? (por crítica significa aqueles sistemas e informações que, em caso de indisponibilidade por mais de 48 Horas, causariam uma Perda Financeira? Sim Não

- c. De que forma protege a integridade das suas cópias de segurança, num cenário de um acesso não autorizado com mais de 45 dias?

- d. Dispõe de um procedimento de restauração de cópias de Segurança, e testa-o, pelo menos, uma vez por ano? Sim Não

9. No caso de ter clientes nos Estados Unidos da América, por favor responda ao seguinte:

- a. Tem subsidiária nesse país? Sim Não
- b. Exporta os seus produtos ou oferece os seus serviços remotamente desde Portugal ou Europa para esse país? Sim Não
- c. No caso de resposta positiva, indique a % que representa da sua Faturação %
- d. Está ligado / conectado à rede informática dos seus clientes nos Estados Unidos da América? Sim Não
- e. Por favor indique qual (ais) das seguintes opções se aplicam em relação à informação que gere ou armazena desses clientes:
- | | | | |
|--------------------------------------|--------------------------|--------------------------|--------------------------|
| Informação não pessoal, mas Sensível | <input type="checkbox"/> | Dados pessoais Sensíveis | <input type="checkbox"/> |
| Informação não Sensível | <input type="checkbox"/> | Não armazena, nem gere | <input type="checkbox"/> |

10. Confirme, por favor, se você ou alguém em seu nome, aplica criptografia / encriptação à informação, nos seguintes momentos:

- a. Quando está armazenada em qualquer ponto da rede (incluindo dispositivos móveis, de armazenamento, servidores, entre outros), com uma encriptação de 256 bits Sim Não
- b. Quando é transmitida, incluindo quando se utiliza uma rede privada virtual (VPN) Sim Não
11. Dispõe de políticas e procedimentos relativos à retenção, destruição e depuração de dados pessoais, informação corporativa e informação confidencial? Sim Não
12. Dispõe de políticas e procedimentos relativos à retenção, destruição e depuração de dados pessoais, informação corporativa e informação confidencial? Sim Não
13. Todos os administradores dispõem, nos seus sistemas de dois tipos de utilizadores (um para o dia-a-dia, sem privilégios de administrador, e outros com privilégios de administrador)? Sim Não
14. Sempre que é terminada uma relação laboral, o acesso de utilizador dessa pessoa é eliminado? Sim Não
15. Realiza um processo anual de verificação e correção de autorizações e acessos aos seus sistemas? Sim Não
16. Relacionado com os processos de autenticação dos utilizadores, por favor seleccione as opções aplicáveis:
- a. Passwords com, pelo menos 8 caracteres, combinando, pelo menos dois tipos de caracteres (por exemplo números e letras)
- b. Gestor de passwords
- c. Teclado virtual
- d. Duplo ou múltiplo fator de autenticação (por exemplo para o e-mail, via web ou acesso remoto)
- e. Outras:

17. Relativamente à segmentação da sua rede. Aplica alguma das seguintes opções abaixo para segmentar a sua rede?

- a. Dispõe de uma DMZ (Zona Desmaterializada) Sim Não
- b. As Subsidiárias ou empresas do grupo a segurar, dispõem de redes fisicamente independentes; Sim Não
- c. A parte IT está separada da parte OT Sim Não
- d. A rede separa utilizadores internos de externos (clientes, similares, ou fornecedores) Sim Não
- e. Não dispõe de nenhuma Segmentação. Sim Não
18. Confirma que dispõe de Firewall nos seguintes locais e equipas?
- a. Todos os locais de acesso à Internet Sim Não
- b. Aplicações Web (ou “web application firewall”, em inglês) Sim Não

c. PCs, computadores portáteis, e equipamentos semelhantes Sim Não

d. Outros:

19. Para uma melhor compreensão da segmentação do seu sistema informático, por favor faça uma descrição abaixo:

20. Relativamente aos seus fornecedores de serviços ou encarregados de tratamento de dados, por favor responda ao seguinte:

a. Tem contratos com todos os encarregados de tratamento de dados, com acesso a dados sensíveis, que incluam cláusulas de cumprimento da norma de Proteção de Dados? Sim Não

b. Inclui cláusulas de indemnização nos respetivos contratos? Sim Não

a. Tem procedimentos para avaliar ou auditar os controlos de segurança da informação ou proteção de dados aplicados pelo provedor de Serviços? Sim Não

b. Inclui nos seus contratos medidas mínimas a cumprir em termos de Segurança da Informação? Sim Não

21. Complete o quadro seguinte, tendo em conta os sistemas informáticos mais críticos para o seu negócio (aqueles que num caso de indisponibilidade de mais de 48 horas, causariam uma perda financeira, depois de um ataque ou falha informática), por ordem de importância para a sua faturação:

| Nome do Sistema | É um Sistema em Nuvem/Cloud? Se sim, indicar o tipo de Provedor: Grupo 1: Amazon Web Services, Google, Oracle, Alibaba ou Salesforce; Grupo 2: Outros | Demoraria mais de 12 Horas a recuperar o acesso? |
|-----------------|--|---|
| | Sim <input type="checkbox"/> Não <input type="checkbox"/> Grupo 1 <input type="checkbox"/> Grupo 2 <input type="checkbox"/> Qual | Sim <input type="checkbox"/> Não <input type="checkbox"/> |
| | Sim <input type="checkbox"/> Não <input type="checkbox"/> Grupo 1 <input type="checkbox"/> Grupo 2 <input type="checkbox"/> Qual | Sim <input type="checkbox"/> Não <input type="checkbox"/> |
| | Sim <input type="checkbox"/> Não <input type="checkbox"/> Grupo 1 <input type="checkbox"/> Grupo 2 <input type="checkbox"/> Qual | Sim <input type="checkbox"/> Não <input type="checkbox"/> |
| | Sim <input type="checkbox"/> Não <input type="checkbox"/> Grupo 1 <input type="checkbox"/> Grupo 2 <input type="checkbox"/> Qual | Sim <input type="checkbox"/> Não <input type="checkbox"/> |

22. Relativamente aos sistemas informáticos críticos para o seu negócio anteriormente indicados, encontram-se os mesmos alojados em duas ou mais regiões, separados pelo menos por 350 Km's entre cada um deles? Sim Não

23. Relativamente à sua capacidade de deteção e gestão de incidentes, incluindo os serviços contratados, por favor responda ao seguinte:

a. Existe um processo de monitorização do tráfego de entrada e saída? Sim Não

b. Quanto tempo (em dias), mantém os logs e alertas de segurança dos seus sistemas, antes de os apagar? Sim Não

c. Tem contratado um sistema de identificação e prevenção de intrusos (IDS/IPS)? Sim Não

d. Tem contratado um serviço de proteção contra ataques de negação de serviço (DDoS)? Sim Não

- e. Realiza cópia dos logs e eventos de segurança armazenados? Sim Não
- f. Qual das seguintes opções usa, ou alguém em seu nome, para analisar os logs e alertas de Segurança?
- SIEM SOC Interno
- SOC Externo Outros;
- Nenhuma Outros;
24. Realiza, com recurso ao trabalho de terceiros, alguma auditoria ou testes (por exemplo Pentesting, Scan de Vulnerabilidades) aos seus sistemas informáticos, pelo menos uma vez por ano? Sim Não

Em caso afirmativo, por favor forneça preencha a tabela abaixo:

| Tipos de Auditorias ou Provas | Nome do sistema ou área | Data em que foi realizada |
|-------------------------------|-------------------------|---------------------------|
| | | |
| | | |
| | | |
| | | |

- a. Houve recomendações nas auditorias ou provas? Sim Não
- b. Caso a resposta tenha sido afirmativa relativamente à pergunta anterior: as mesmas recomendações foram aplicadas? Sim Não
25. Tem implementado, e comprovado, pelo menos anualmente, um plano de contingência (BCP) ou um de recuperação perante um desastre (DRP), em caso de haver um incidente nos seus sistemas informáticos (por exemplo um ataque por Ransomware)? Sim Não

Reclamações e Incidentes

26. Nos últimos 24 meses sofreu alguma violação de dados, falha de segurança, extorsão cibernética, interrupção ou bloqueio dos seus sistemas, destruição de dados, acesso de pessoas não autorizadas ao seu sistema ou qualquer outro incidente que tenha dado origem a uma reclamação ou inspeção de dados? Sim Não
27. Tem conhecimento de qualquer facto ou circunstancia que possa dar origem a uma reclamação, inspeção de dados ou ativação de qualquer uma das coberturas da apólice que oferecemos? Sim Não

Caso tenha respondido “sim” às questões 26. Ou 27. por favor faculte uma descrição do incidente, indicando as suas consequências económicas e operacionais, os arquivos ou componentes da sua infraestrutura tecnológica afetados, e as medidas corretivas aplicadas.

Coberturas Adicionais

Perguntas relativas a Fraude Tecnológica:

28. Indique, por favor o valor médio (ou um intervalo de valor) das suas transações €
29. É realizado algum procedimento de verificação de antecedentes relativamente a novos Empregados? Sim Não
30. São aplicados, ao nível da direção, controlos para verificar que todos os pagamentos são legítimos? Sim Não
31. Confirme que, para aceder à sua conta bancária online (da Empresa), tem em vigor, para além da sua Password de acesso habitual, pelo menos uma das três seguintes formas de autenticação: Token (Hardware ou Software); Password de um só uso (por exemplo um SMS); Biométrica (por exemplo impressão digital ou reconhecimento facial). Sim Não
32. As transferências superiores a 5.000€ são sempre autorizadas por duas ou mais pessoas? Sim Não

33. No caso de um pedido de alteração dos números de conta e outros dados de beneficiário: verifica-se com a pessoa que fez o pedido se o mesmo é legítimo, de uma forma diferente da mesma em que foi feita o pedido (por exemplo se foi recebido por e-mail, verifica-se telefonicamente)? Sim Não
34. Cumpre com as recomendações dadas pela sua instituição Financeira no que diz respeito a pagamentos por transferência bancária e no uso da Banca Online? Sim Não
35. Verifica diariamente nas suas contas bancárias que os movimentos das mesmas (Conciliação Bancária) foram realizados por si, ou outras pessoas com autorização para o fazer? Sim Não
36. Nos últimos 3 anos, a Empresa foi alvo de alguma tentativa ou perda por roubo de identidade ou de qualquer outra perda por atos fraudulentos (internos ou externos)? Sim Não

Caso a resposta à questão 36. seja positiva, por favor forneça informação detalhada dos incidentes, data dos mesmos, indicando as consequências económicas e operacionais, o sistema afetado, a pessoa alvo de roubo de identidade, e, especialmente as medidas correcionais aplicadas.

Hiscox CyberClear – Grandes Riscos

Proposta de Seguro

Tratamento de dados pessoais – Política de privacidade Innovarisk

Os dados pessoais recolhidos serão processados e armazenados informaticamente pela **Innovarisk**, atuando na sua condição de entidade encarregada do processamento da informação, que tratará os seus dados em nome e por conta do Segurador, e unicamente para os fins estabelecidos por este.

Quaisquer omissões, inexactidões e falsidades, quer no que respeita a dados de fornecimento obrigatório, quer facultativo, são da sua inteira responsabilidade.

Os dados podem ser utilizados para divulgação da nossa atividade e dos nossos produtos, sendo que, quanto a este caso, você nos tenha que autorizar expressamente.

Assinale por favor aqui caso pretenda autorizar.

O consentimento poderá a qualquer momento ser revogado mediante informação direta à Innovarisk.

Tratamento de dados pessoais – Política de privacidade Hiscox

A Hiscox, S.A. – Sucursal em Portugal é a entidade Responsável pelo tratamento dos seus dados pessoais.

Trataremos os seus dados pessoais para lhe conseguir propor, disponibilizar e gerir a sua apólice de seguro. Por exemplo, necessitamos de tratar os seus dados pessoais logo na fase pré-contratual, mesmo antes de celebrarmos um contrato, para lhe enviar a nossa proposta de seguro. Precisamos de tratar os seus dados pessoais, para proceder a avaliações de risco, tramitar e gerir processos decorrentes de sinistros que se encontrem cobertos pela sua apólice, pagar-lhe eventuais indemnizações a que tenha direito, ou outras prestações de serviços relacionadas com a execução do seu contrato de seguro.

O tratamento dos seus dados pessoais é necessário para garantir que conseguimos realizar as diligências pré-contratuais que nos tenha solicitado, bem como, cumprir adequadamente com a execução dos termos do contrato de seguro que celebrou connosco. Para outros casos, o tratamento dos seus dados pessoais pode estar legitimado em outros fundamentos. Para saber quais os fundamentos em que sustentamos o tratamentos dos seus dados pessoais, consulte a nossa Política de Privacidade através do link <https://www.hiscox.pt/privacidade>

Em determinadas circunstâncias e por necessidades decorrentes da normal execução do seu contrato de seguro, ou por imposição legal ou regulatória a que estejamos obrigados, poderemos ter de transmitir os seus dados pessoais a outras empresas do Grupo Hiscox, entidades reguladoras, agencias relacionadas com prevenção de fraude ou prestadores de serviços externos, como mediadores, peritos ou advogados.

Enquanto titular dos dados e desde que se encontrem preenchidos os necessários pressupostos legais, poderá ter o direito de aceder, retificar, limitar e de se opor ao tratamento dos seus dados pessoais, bem como o direito de solicitar que os mesmos sejam apagados ou que lhe seja entregue uma cópia dos mesmos em formato estruturado, de uso corrente e de leitura automática.

Lembramos que poderá consultar o texto integral da nossa Política de Privacidade através do link <https://www.hiscox.pt/privacidade> e caso subsistam quaisquer dúvidas, não hesite em nos contactar, pelo seguinte número de telefone +351 210 027 330 ou endereço de e-mail info_portugal@hiscox.com

Declaração

Por favor, leia cuidadosamente as informações que se seguem e assine no final.

A cobertura do risco só terá início após confirmação formal por parte do Segurador.

Tenha em conta que esta apólice funciona por ano e seguintes, que terá validade até que qualquer das partes a denuncie de acordo com o previsto nas Condições Gerais e Especiais ou por falta de pagamento de qualquer prémio por Si devido.

Declaração inicial do risco Você declara que (a) este formulário foi preenchido após realização das averiguações apropriadas; (b) os seus conteúdos são verdadeiros e exatos e (c) todos os eventos e circunstâncias que possam ser relevantes para a consideração da nossa proposta de seguro foram comunicados. Se qualquer informação prestada neste questionário, ou anexos, sofrer alterações antes da data de início da apólice para a qual este questionário se realizou, ou tiver conhecimento de novos factos ou circunstâncias que possam afetar a cobertura de seguro, você deverá notificar a Innovarisk, podendo a Seguradora modificar ou retirar a cobertura de seguro.

Você concorda que este formulário e toda a informação por si facultada seja incorporada no contrato de seguro e farão parte integrante do mesmo.

**Informação
pré-contratual**

O Segurado reconhece expressamente que recebeu as Condições Gerais e Especiais, e que leu, examinou e compreendeu o conteúdo e o alcance de todas as cláusulas contidas nessas mesmas Condições. Por último, o Segurado reconhece expressamente ter recebido a informação relativa à legislação aplicável ao contrato de seguro, às diferentes instâncias de reclamação, bem como à identificação e ao estatuto legal do Segurador e do respetivo representante.

Assinatura do Presidente, Diretor Geral ou equivalente

Data

Deverá ficar com uma cópia desta proposta em seu poder, para seu registo.