Hiscox CyberClear - Indústria

Proposta de Seguro

A intenção deste questionário é conhecer a forma 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 solicitaremos a uma empresa especialista mais informação ou solicitaremos 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.

Normas de segurança da informação

Tem alguma certificação de segurança da informação? (por exemplo ISO/IEC 27002) Sim ☐ Não ☐

Se respondeu Sim, por favor faculte detalhes adicionais

Faturação

	Último ano	Ano em curso	Estimada para o próximo ano
Faturação total	€	€	€
Faturação nos EUA	€	€	€
Faturação na Europa	€	€	€
Faturação Online	€	€	€

Número de empregados

O número total de empregados, incluindo das subsidiárias

Atividades

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

HISCOX
CYBERCLEAR®

Hiscox CyberClear - Indústria

Proposta de Seguro

Distribua a sua faturação por:

Local de risco	% de faturação

Informação da Gestão do Risco

1. Gestão da Segurança de Informação (ao nível da entidade)

a. Existe um responsável da segurança de informação? Sim ☐ Não ☐

b. Dispõe de alguma equipa ou pessoa responsável por pôr em prática as medidas de proteção definidas? Sim ☐ Não ☐

c. Dispõe de uma equipa ou terceiro que verifique que as medidas de proteção se encontram em prática, diferente do Departamento de Sistemas ou TI? Sim ☐ Não ☐

2. Políticas de Gestão da Segurança de Informação

a. Na sua organização a aplicação das medidas definidas para a proteção dos seus sistemas de informação está centralizada? Sim ☐ Não ☐

b. Dispõe de uma política de proteção de dados pessoas e de segurança adaptada à legislação, sector e jurisdição onde atua a entidade? Sim ☐ Não ☐

c. Tem algum programa de consciencialização de segurança da informação para os seus empregados? Sim ☐ Não ☐

d. Dispõe de algum dos seguintes planos implementados e testados na sua organização relacionados com a segurança dos seus sistemas? Sim ☐ Não ☐

Contingência Sim ☐ Não ☐

Resposta a incidentes Sim ☐ Não ☐

Recuperação perante desastres Sim ☐ Não ☐

3. Sistema Informático

a. Quantos utilizadores têm atualmente acesso aos seus sistemas? ☐

b. Realiza um inventário dos seus ativos/equipamentos informáticos? Sim ☐ Não ☐

c. De quantos servidores dispõe? (quer próprios como de terceiros)? ☐

d. Por favor indique, se souber, o número de IP's públicas que tem atribuído a sua organização? ☐

e. Indique por favor os sistemas ou áreas mais críticas para o seu negócio. Caso tenho sido avaliado, indique o tempo máximo que demoraria a voltar à normalidade após sofrer um incidente (queda, bloqueio, etc.):

Sistema (ou atividade)	Tempo de recuperação

4. Medidas de segurança da sua infraestrutura tecnológica

a.	Dispõe de antivírus atualizado em todos os equipamentos e as atualizações são periódicas e estão centralizadas?	Sim ☐ Não ☐
b.	Existe um processo formal de implementação de patches?	Sim ☐ Não ☐
c.	Em caso de resposta afirmativa à pergunta anterior, qual é a frequência de implementação de patches?	
d.	Necessita de um nome de utilizador e palavra passe para aceder a todos os seus sistemas?	Sim ☐ Não ☐
e.	O princípio do privilégio mínimo é usado para a configuração dos diferentes perfis dos utilizadores?	Sim ☐ Não ☐
f.	Existem utilizadores que não pertençam ao departamento de Sistemas/ TI ou terceiro autorizado, com acesso aos sistemas e que tenha um perfil de 'administrador' (acesso sem limitações ao sistema)?	Sim ☐ Não ☐
g.	Existe uma política de palavra passe complexa e uma mudança periódica da mesma?	Sim ☐ Não ☐
h.	Existe um controlo de acesso, bloqueio ou medidas restritivas no caso de sucessivas tentativas falhadas de acesso a uma conta?	Sim ☐ Não ☐
i.	Existe um segundo fator de autenticação para o acesso a sistemas críticos?	Sim ☐ Não ☐
j.	Realiza um processo anual de verificação e correção de autorizações de acesso ao seu sistema?	Sim ☐ Não ☐
k.	Existe um procedimento para desativar os utilizadores após o término de um contrato de trabalho?	Sim ☐ Não ☐
l.	Existem medidas de segurança mínimas definidas para os diferentes equipamentos informáticos (incluindo servidores, computadores e portáteis), e controla-se periodicamente a sua correta implementação?	Sim ☐ Não ☐

5. Segurança na rede

a.	Estão todos os pontos de acesso à Internet protegidos por Firewalls?	Sim ☐ Não ☐
b.	Existe uma segmentação da rede entre recursos críticos e outros recursos?	Sim ☐ Não ☐
c.	Os sistemas críticos são configurados de acordo com uma arquitetura ativa/passiva ou ativa/ativa?	Sim ☐ Não ☐
d.	Realiza um teste de intrusão interno ou externo pelo menos uma vez por ano, com um plano de ação destinado a mitigar as vulnerabilidades identificadas?	Sim ☐ Não ☐
e.	Existe um processo de recolha, monitorização e análise de acessos (ou histórico dos eventos que ocorreram na rede)?	Sim ☐ Não ☐
f.	O acesso de utilizadores internos à Internet é feito através de uma proxy, com controlo de antivírus e filtragem de conteúdo?	Sim ☐ Não ☐
g.	Os acessos remotos são feitos através de uma rede privada virtual (VPN) ou outros mecanismos que garantam a encriptação do canal de comunicação?	Sim ☐ Não ☐
h.	Existe um sistema de identificação e prevenção de intrusão (IDS/IPS)?	Sim ☐ Não ☐
i.	Existe um processo de monitorização do tráfego de entrada e saída?	Sim ☐ Não ☐

6. Gestão de dados pessoais e informação confidencial de terceiros

a.	Existe um responsável de Proteção de Dados ou pessoa que tenha a sua função dentro da sua organização?	Sim ☐ Não ☐
b.	Obriga os seus empregados a cumprir com a política de Proteção de Dados (ou equivalente)?	Sim ☐ Não ☐
c.	Realiza formações para os seus empregados no âmbito do tratamento e Proteção de Dados?	Sim ☐ Não ☐
d.	Classifica a informação que gere (você ou um terceiro em seu nome) com base na sensibilidade ou na natureza crítica para o seu negócio, de acordo com as normas de Proteção de Dados?	Sim ☐ Não ☐

e. Com que frequência faz cópias de segurança (back-up) dos seus sistemas ou dados críticos?

Pelo menos uma vez por dia	☐
Pelo menos a cada 7 dias	☐
Entre 8 e 14 dias	☐
Entre 15 dias e um mês	☐
Outra periodicidade (indique)	

f. Confirma periodicamente que as cópias de segurança (back-up) foram feitas corretamente? Sim ☐ Não ☐

g. Existe algum procedimento estabelecido para restaurar as cópias de segurança? Sim ☐ Não ☐

h. Existem cópias de segurança adicionais em mais do que uma localização física e/ou serviço da Cloud? Sim ☐ Não ☐

i. É permitida a cópia de informações não encriptadas para dispositivos de armazenamento? Sim ☐ Não ☐

j. A encriptação é aplicada às informações armazenadas? Sim ☐ Não ☐

k. A encriptação é aplicada às cópias de segurança? Sim ☐ Não ☐

l. Indique por favor o tipo de dados que recolhe, armazena ou processa (você ou terceiro em seu nome), assim como o volume aproximado dos mesmos:

Tipo de dados		Número de dados
Dados pessoais (diferentes de nomes e apelidos)	Sim ☐ Não ☐	
Cartão de pagamento (débito ou crédito)	Sim ☐ Não ☐	
Números de contas	Sim ☐ Não ☐	
Dados médicos	Sim ☐ Não ☐	
Propriedade Intelectual / Segredos Comercial	Sim ☐ Não ☐	
Contratos/informação confidencial terceiros	Sim ☐ Não ☐	

m. No que diz respeito aos dados do cartão de pagamento, você ou o fornecedor com quem externaliza o processo de pagamento, cumprem os regulamentos do sector de cartões de pagamento em termos de segurança do mesmo (PCI-DSS)? Sim ☐ Não ☐

n. Em caso de resposta afirmativa à pergunta anterior, por favor indique o nível atribuído:

7. Conteúdos em meios digitais

a. Os conteúdos do seu website e redes sociais (como por exemplo: imagens, vídeos, textos) são de terceiros ou facultados por terceiros? Sim ☐ Não ☐

b. Em caso de resposta afirmativa à pergunta anterior, tem o consentimento por escrito para poder fazer uso do conteúdo e sua publicação? Sim ☐ Não ☐

c. O conteúdo (próprio e de terceiros) é legalmente revisto no seu website e redes sociais antes de ser publicado? Sim ☐ Não ☐

d. Você alterou, por defeito, as palavras-passe do administrador de gestão da sua página web? Sim ☐ Não ☐

8. Rede industrial

a. A rede industrial encontra-se segregada da rede corporativa ou administrativa? Sim ☐ Não ☐

b. Faz uso de controladores lógicos programáveis (ou PLC em inglês) nos seus processos de produção? Sim ☐ Não ☐

c. Acede-se remotamente à rede industrial? Sim ☐ Não ☐

d. Existe um processo formal de identificação, avaliação e aplicação de correções na rede industrial? Sim ☐ Não ☐

e. Realiza-se, pelo menos uma vez por ano, uma análise de vulnerabilidades dos distintos componentes da rede industrial, com um plano de ação para mitigar as falhas identificadas? Sim ☐ Não ☐

f. Existe um plano de recuperação de desastres (DRP) sobre a rede industrial, conhecido pelo pessoal envolvido e testado pelo menos uma vez por ano? Sim ☐ Não ☐

g. Faz uso de sistemas operativos ou bases de dados sem suporte técnico por parte do prestador correspondente por questões de compatibilidade com a rede industrial? Sim ☐ Não ☐

h. Existe um processo de monitorização dos diferentes componentes da rede industrial, com a definição e gestão de alarmes perante casos críticos? Sim ☐ Não ☐

i. Modificam-se, por defeito, as palavras passe dos equipamentos que compõem a rede industrial? Sim ☐ Não ☐

9. Medidas de segurança física

a. As medidas mínimas de segurança física dos Centros de Processamento de Dados (CPD), encontram-se definidas com um controlo periódico de cumprimento? Sim ☐ Não ☐

b. Existe um controlo de acessos apropriado aos centros de produção? Sim ☐ Não ☐

c. Existe um sistema de deteção e extinção automáticos de incêndios? Sim ☐ Não ☐

d. A fonte de alimentação está protegida com um sistema de alimentação ininterrupto? Sim ☐ Não ☐

10. Externalização de serviços

a. Quais dos seguintes serviços de TI são externalizados e quem são os prestadores correspondentes?

Serviços externalizados		Nome do prestador
Segurança dos sistemas	Sim ☐ Não ☐	
Serviços de armazenamento na Cloud ou serviços na nuvem (SaaS)	Sim ☐ Não ☐	
Plataforma cartões de pagamento	Sim ☐ Não ☐	
Cópias de segurança	Sim ☐ Não ☐	
Manutenção/Atualização dos sistemas	Sim ☐ Não ☐	
Gestão de equipamentos informáticos	Sim ☐ Não ☐	

b. Os contratos para os serviços externalizados incluem cláusulas de confidencialidade da informação e cumprimento com a correspondente normativa de proteção de dados? Sim ☐ Não ☐

c. Os contratos para os serviços externalizados incluem medidas ou requerimentos mínimos de segurança a cumprir e a possibilidade de serem auditados? Sim ☐ Não ☐

d. Os contratos para os serviços externalizados exigem a notificação de incidentes de segurança que os possam afetar? Sim ☐ Não ☐

e. Contratualmente exige aos seus prestadores de serviço a manutenção de uma apólice de seguro de riscos cibernéticos? Sim ☐ Não ☐

Reclamações, incidentes e apólices de seguros

a. 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 ☐

b. 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 ☐

c. Tem em vigor ou já teve anteriormente um seguro de riscos cibernéticos? Sim ☐ Não ☐

Caso tenha respondido "sim" às questões a. ou b. 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.

Hiscox CyberClear - Indústria

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, inexatidões 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

Hiscox CyberClear - Indústria

Proposta de Seguro

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.