Seguro de Riscos Cibernéticos (CyberClear 360º)

Condições Especiais

Seguro de Riscos Cibernéticos (CyberClear 360º)
Condições Especiais

Condições aplicáveis a toda a apólice

Por favor, leia atentamente estas condições especiais, assim como as condições gerais e particulares e quaisquer atas adicionais. Todos estes documentos fazem parte da sua **apólice** de seguro. Se detetar algum erro em qualquer deles, por favor contacte o seu mediador de seguros ou segurador o mais rapidamente possível.

O segurador compromete-se a cobrir o que está incluído neste seguro em contrapartida do pagamento do prémio acordado.

1. Definições

As palavras sublinhadas a negrito têm o mesmo significado ao longo desta apólice, conforme se encontram abaixo definidas.

Afetado

Qualquer pessoa singular titular dos **dados pessoais**.

Ameaça de extorsão

Qualquer ameaça direta à **entidade** por terceiros, caso a **entidade** não pague o resgate exigido, de:

1. cometer um ataque deliberado contra o **sistema informático**, ou contra dados no **sistema informático**, incluindo o ataque através da introdução de um **vírus**; ou
2. cometer um ataque deliberado ao sistema informático de um terceiro recorrendo ao uso do **sistema informático** da **entidade**, incluindo o ataque através da transmissão de um **vírus**; ou
3. divulgar publicamente **informações confidenciais, informações corporativas** ou **dados pessoais** dos quais se tenham indevidamente apropriado do **sistema informático**.

Ataque de engenharia social

O ato, cometido por terceiros, de enganar uma **pessoa segura,** através da apropriação da identidade de i) outra **pessoa segura**, ou ii) um cliente ou prestador de serviços da **entidade**, através de e-mail (phishing), mensagens de texto (smishing), voz sobre IP (vishing) ou atos semelhantes, a fim de obter **dados pessoais, informações confidenciais ou informações corporativas**.

Cauções / Fianças

A prestação de caução que possa ser exigida a uma **pessoa segura** para garantir a sua eventual responsabilidade civil, bem como as despesas que uma **pessoa segura** incorra na constituição e manutenção de uma fiança penal para garantir a sua libertação provisória, não ficando neste caso coberto o valor da própria fiança, como resultado de uma **reclamação.**

Ciberataque

Qualquer falha em garantir segurança do **sistema informático** que resulte:

1. no acesso ou utilização não autorizada do **sistema informático**; ou
2. numa alteração, corrupção, destruição ou perda de **dados pessoais**, **informações corporativas ou informações confidenciais**; ou
3. na introdução ou receção de um **vírus**, independentemente do seu modo de transmissão; ou
4. num **ataque de negação de serviço** ao **sistema informático**, entendendo-se este como uma privação maliciosa temporária, total ou

parcial, do acesso ou utilização do **sistema informático**, incluindo, mas não se limitando a, um ataque de negação de serviço distribuído.

Entende-se por um ataque de negação de serviço distribuído, aquele que é produzido através de um ataque desde vários computadores (ou vetores) em vez de um único.

Conta bancária

Qualquer conta detida pela **entidade** numa instituição financeira, através da qual uma **pessoa segura** pode ordenar a transferência de fundos:

i) Através de uma ordem eletrónica ou telefónica; ou

ii) através de instruções escritas que estabeleçam as condições em que as transferências serão processadas por um sistema de transferência de fundos eletrónicos.

Custos de defesa

Despesas incorridas, com o consentimento prévio por escrito do segurador, para investigar, regularizar ou defender uma **reclamação** contra o **segurado**.

Dados pessoais

Qualquer informação pessoal pela qual a **entidade** seja responsável, independentemente do formato em que se encontre, que permita a identificação do lesado e que não se encontre no domínio público, tal como definido nos regulamentos aplicáveis relativos aos cuidados, guarda, controlo e utilização de informações pessoais, incluindo, mas não se limitando, às informações protegidas pelo Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, ou qualquer outro regulamento que o substitua.

Descoberto/a

A primeira vez que a **entidade** tomou conhecimento de um facto ou de uma suspeita, que possa ativar a presente apólice, ainda que nessa altura sejam desconhecidos os detalhes e o possível impacto dos mesmos.

Despesas de mitigação

Entendem-se como as despesas incorridas pela **entidade**, distintas das que possam ficar abrangidas pelas restantes coberturas e serviços facultados pela presente apólice, com o nosso consentimento prévio por escrito, que tenham o propósito de minimizar potenciais perdas decorrentes de um **incidente** coberto por esta apólice, até ao sublimite indicado nas **condições particulares**. A**s despesas de mitigação** incluem, mas não se limitam:

a. Ao aluguer de equipamento informático de terceiros;

b. Aos honorários de um prestador externo, especialmente contratado com o objetivo de coordenar a implementação de um plano de continuidade de negócios da **entidade**;

c. Despesas necessárias e razoáveis para restaurar o ranking atribuído pelo motor de busca à **entidade** na posição anterior ao **incidente**;

d. O aumento dos custos de mão-de-obra da **entidade**, cujo âmbito inclui, mas não se limita a contratação de trabalhadores temporários ou o pagamento de horas extraordinárias aos **empregados**;

e. A atualização ou substituição de hardware ou software já existente e que faça parte do **sistema informático**;

f. Pagamento de recompensas a informadores, sob a forma de reembolso ao **segurado** das quantias anteriormente pagas por este ao Informador, em troca de informações que contribuam para a detenção e condenação de qualquer pessoa ou grupo de pessoas que cometam ou tentem cometer qualquer **ciberataque** ou **ameaça de extorsão**;

Informador: Entende-se como um terceiro que não mantém ligações direta ou indiretamente com o **segurado** e que forneça informações que não podem ser obtidas de outra forma, em troca de uma recompensa oferecida pelo **segurado**. Entre outros, estão excluídos os **empregados**, gestores e quaisquer outras pessoas relacionadas com as empresas contratadas pelo **segurado** para investigar qualquer ato ilegal ou para realizar trabalhos de auditoria ou análise forense.

As **despesas de mitigação** não podem, em caso algum, exceder o montante que teríamos pago pelo **incidente** se a **entidade** não tivesse incorrido nessas despesas.

Empregado

Qualquer **pessoa segura** que mantenha um contrato de trabalho com a **entidade**, e que preste trabalho para esta.

Entidade

O **Tomador do Seguro**, as suas **subsidiárias**, as **novas entidades**, assim como qualquer fundação onde o **tomador do seguro** ou uma **subsidiária** detenha a maioria dos direitos de voto do órgão decisor.

Erro humano

Uma interrupção não intencional e não programada, parcial ou total, do **sistema informático**, ou a indisponibilidade dos dados da **entidade** no **sistema informático**, que não resulte de uma **violação de dados** ou de um **ciberataque**, e que seja causada por:

1. Um erro humano por parte de uma **pessoa segura**, incluindo um erro na programação, parametrização, atualização ou seleção de um **programa**, desde que esse **programa** não esteja em fase de testes e tenha sido testado com sucesso por um período mínimo de 30 dias, ou a alteração, corrupção, destruição ou perda de **informações corporativas** ou **informações confidenciais**; ou
2. Uma falha elétrica, incluindo sobretensão ou queda de tensão do sistema elétrico ou o ato de desligar o **sistema informático** da corrente elétrica, quando causado acidental e exclusivamente por uma **pessoa segura**, desde que não resulte de um dano material, entendendo-se como tal a perda, dano, desgaste, deterioração gradual ou destruição de qualquer bem tangível.

Fornecedor externo tecnológico

Sem prejuízo da exclusão 1 (Infraestrutura) da secção «O que não está coberto», entende-se como pessoa coletiva ou singular (na qualidade de profissional independente) a quem a **entidade** contrata serviços para uso próprio através de um contrato escrito, em troca do pagamento de honorários a um terceiro e relacionados com: (1) instalação, administração

ou segurança dos equipamentos de tecnologias da informação; (2) operação, supervisão ou manutenção de infraestruturas tecnológicas; (3) assistência técnica aos utilizadores; e/ou 4) serviços de computação na nuvem (‘cloud computing’) e serviços de armazenamento (hosting).

Franquia

Os montantes e/ou período de tempo expressamente definidos nas **Condições Particulares** que são deduzidos do valor a ser pago pelo segurador por qualquer participação coberta ao abrigo desta apólice.

Incidente

Uma **violação de dados**, **ciberataque**, **erro humano**, **ameaça de extorsão** ou **ataque de engenharia social**.

Informações Confidenciais

Informações comerciais de terceiros com caráter confidencial, qualificadas contratualmente como tal, pelas quais a **entidade** seja responsável, independentemente do formato em que se encontrem.

Informação corporativa

A informação própria da **entidade,** que não seja do domínio público e que não seja informação de **dados pessoais,** independentemente do formato em que se encontre.

Novas entidades

1. Qualquer entidade que o **tomador do seguro** adquira (entendida a aquisição como a aquisição de titularidade de mais de metade das ações, participações sociais ou ativos de qualquer entidade) durante o **período do seguro**, mas exclusivamente na medida em que exerça a mesma atividade que o **tomador do seguro**, que tenha as mesmas medidas de segurança informática que o **tomador do seguro** ou as suas **subsidiárias,** que seja domiciliada no Espaço Económico Europeu ou no Reino Unido e que a faturação anual dessa entidade seja inferior a 20% da faturação anual do **tomador do seguro** e das suas **subsidiárias**;
2. Qualquer entidade que o **tomador do seguro** adquira (entendida a aquisição como a tomada de titularidade de mais de metade das ações, participações sociais ou ativos de qualquer entidade), durante o **período do seguro** e que não realize necessariamente a mesma atividade que o **tomador do Seguro,** ou cuja faturação anual exceda 20% da faturação anual do **tomador do seguro** e das suas **subsidiárias**, ou cujas medidas de segurança informáticas sejam diferentes das do **tomador do seguro** e das suas **subsidiárias**, mas apenas no caso:
    a. do **tomador do seguro** avisar previamente o segurador da aquisição, por escrito e num prazo de 30 dias após a aquisição e o segurador ter dado o seu consentimento por escrito, concordando em estender a cobertura da **apólice** a essa entidade; e
    b. o **tomador do seguro** ter pago o prémio adicional e aceitado os termos, condições e exclusões adicionais propostos pelo segurador;
    c. da entidade estar domiciliada no Espaço Económico Europeu ou no Reino Unido.

As mesmas regras são aplicáveis às entidades constituídas direta ou indiretamente (quando sejam constituídas por uma **subsidiária**) pelo **tomador do seguro** durante o **período de seguro**.

A cobertura só será aplicável às **reclamações** apresentadas ou aos **incidentes descobertos** pela primeira vez durante o **período de seguro** quando as causas dos mesmos tiverem sido geradas durante o **período de seguro** após a aquisição ou constituição da **nova entidade**.

Período do seguro

O período, indicado nas **condições particulares**, durante o qual o presente contrato se encontra em vigor, em contrapartida do pagamento do prémio aceite pelo segurador e pelo **tomador**. O **período do seguro** não inclui qualquer período adicional de notificação.

Pessoa segura

Entende-se como:

1. Qualquer pessoa singular que, durante o **período do seguro**, seja, tenha sido ou que se torne sócio, administrador, diretor, membro do conselho de administração, encarregado de proteção de dados, estagiário com contrato de estágio ou **empregado** da **entidade**, mas apenas no exercício das suas funções para a **entidade**;
2. Qualquer trabalhador temporário, contratado ou subcontratado independente, que seja uma pessoa singular, incluindo os trabalhadores independentes, ou qualquer trabalhador com contrato de trabalho de um contratado ou subcontratado, mas apenas no exercício das suas funções para com a **entidade,** e quando utilizem o **sistema informático** da **entidade** com um utilizador próprio fornecido pela **entidade**;

Ficam excluídos da definição de pessoa segura, os auditores, liquidatários ou administradores judiciais ou de insolvência.

Poluentes

Entende-se como qualquer irritante ou contaminante sólido, líquido, gasoso, biológico, radiológico ou térmico, incluindo, mas não se limitando a, fumo, vapor, **amianto**/asbestos, sílica, poeira, nanopartículas, fibras, fuligem, gases, ácidos, alcalis, químicos, materiais nucleares, germes e resíduos. Os resíduos incluem, mas não se limitam a materiais para reciclagem, reacondicionamento ou recuperação.

Programa

Uma sequência de instruções escritas que interagem com equipamentos informáticos ou de telecomunicações para a execução de uma tarefa de processamento de dados ou interação com outros equipamentos.

Reclamação

Qualquer pedido escrito, reclamação escrita ou instauração de processo civil, criminal, administrativo ou arbitral apresentado contra qualquer **segurado** com o propósito de obter uma indemnização em consequência de um **incidente**. Também se considerará como uma reclamação um procedimento administrativo de proteção de dados iniciado contra qualquer **segurado** por um organismo regulador no domínio da proteção de dados.

Segurado

1. A **Entidade.**
2. A **pessoa segura**.

Sistema informático

Todos os computadores eletrónicos interligados ou sem fios e os seus componentes, incluindo, mas não se limitando a:

- sistemas operativos, hardware ou software;
- dispositivos associados de entrada e saída, dispositivos de armazenamento de dados e serviços, dispositivos ou ferramentas de cópia de segurança;
- dispositivos móveis utilizados pela **pessoa segura** e autorizados pela **entidade** a aceder aos seus sistemas;
- componentes periféricos relacionados, tais como dispositivos 'Internet das Coisas' ('Internet of Things' o IOT)
- Sítio Web (incluindo extranet e intranet) e contas de redes sociais;
- sistemas na nuvem;

desde que seja propriedade da **entidade**, esteja diretamente sob o controlo e administração da **entidade** e seja utilizado pela **entidade** para seu próprio proveito, pelo que não inclui os que sejam fornecidos por um **fornecedor externo tecnológico**.

Subsidiária

Qualquer pessoa coletiva em que o **tomador do seguro**:

1. Detenha, à data início da apólice, mais de 50% das ações ou participações, ou mais de 50% dos direitos de voto, direta ou indiretamente; ou
2. que, não cumprindo a alínea 1) anterior, tenha o direito legal de eleger a maioria do seu conselho de administração ou de um órgão de administração semelhante;
3. e em qualquer dos dois casos acima referidos, seja domiciliada dentro do Espaço Económico Europeu (EEE) ou no Reino Unido, ou fora dos ditos territórios, sempre e quando nos tenham sido comunicadas e seja aceite por **nós** por escrito.

Vírus

Programas maliciosos introduzidos no **sistema informático**, sem a permissão ou conhecimento da **entidade**, incluindo, mas não se limitando a, "worms", "cavalos de troia", "malware" ou "spyware".

Violação de dados

A apropriação ou roubo, cópia, divulgação, acesso, utilização, perda, divulgação não autorizadas, de:

a) **dados pessoais**; e/ou

b) **informação corporativa**; e/ou

c) **Informação confidencial**.

2. O que está coberto

Em contrapartida do pagamento do prémio, de acordo com o Questionário de risco ou a proposta de seguro e sujeito à contratação efetiva das coberturas indicadas abaixo, de acordo com o estipulado nas **Condições Particulares** da **apólice**, o segurador e o **segurado** acordam as seguintes coberturas:

2.1 Serviço de Resposta a Incidentes

Ativação do serviço

Se, durante o **período do seguro**, o **segurado descobrir** um **incidente**, real ou presumível, o segurador**:**

a. Pagará o custo dos Serviços de Resposta a Incidentes indicados nesta seção fornecidos pelos especialistas indicados no Anexo destas condições especiais.

   Poderá aceder através do número de telefone indicado no referido anexo.

   Caso algum dos referidos especialistas não possa prestar o serviço requerido, o segurador reembolsará as despesas que o **segurado** possa incorrer na contratação de outro especialista fora do Painel de especialistas, mediante a prévia verificação e aprovação escrita das mesmas, ou

b. reembolsará as despesas em que o segurado possa incorrer, após validação prévia e aprovação escrita das mesmas, e descontada a **franquia** indicada nas **Condições Particulares**, para contratar outro especialista fora do Painel de especialistas para prestação dos Serviços de Resposta a Incidentes indicados nesta secção.

   Em qualquer caso, não pagaremos despesas de correção ou melhoria, nem despesas superiores às que teríamos com o uso de nosso painel de especialistas.

Franquia e utilização do painel de fornecedores especializados

Sempre que o **segurado** recorra ao Serviço de Resposta a Incidentes, através do Painel de Especialistas em anexo, não haverá lugar à aplicação de **franquia** nos seguintes serviços:

a. serviços de contenção tecnológica;

b. aconselhamento jurídico e serviço de comunicação e relações-públicas;

c. nas despesas de notificação e de monitorização previstos no ponto i. c. no Âmbito dos Serviços de Resposta a Incidentes;

d. no pagamento de horas extraordinárias de **pessoas seguras** dedicadas exclusivamente aos serviços acima mencionados.

Exoneração de responsabilidade

- O segurador não será responsável por, nem se associará a, qualquer serviço que venha a ser acordado com qualquer uma das empresas especializadas que integram o Serviço de Resposta a Incidentes e o

segurado, salvo pelas despesas de resposta a **incidentes** incorridas na ativação do referido serviço.

O segurador não garante a capacidade nem o serviço dos especialistas disponibilizados no painel do Serviço de Resposta a Incidentes.

A responsabilidade máxima que as empresas especializadas que integram o Serviço de Resposta a Incidentes assumirão relativamente aos **tomadores** / **segurados** da apólice, será equivalente ao valor do Serviço de Resposta a Incidentes que tenha sido prestado.

Âmbito dos Serviços de Resposta a Incidentes :

a. **Serviços de contenção tecnológica**

O serviço especializado em cibersegurança tem como finalidade:

i. Prestar aconselhamento acerca da paragem ou contenção de um **incidente**;

ii. Determinar, na medida do possível, a causa e a extensão de um **incidente**;

iii. Confirmar a ocorrência de uma **violação de dados** e identificar, na medida do possível, os **afetados**;

iv. Emitir recomendações de forma a evitar a repetição de um **incidente**, desde que a causa possa ser detetada.

b. **Serviço de aconselhamento jurídico, comunicações e relações-públicas**.

i. O serviço de aconselhamento jurídico externo para assessorar nas ações que devam ser tomadas para gerir a resposta a um **incidente**, sempre que necessário.

ii. Despesas de relações-públicas, nomeadamente:

a) um consultor especializado para ajudar o segurado a restabelecer a sua reputação e gerir a sua comunicação externa decorrente de um **incidente**, incluindo o desenvolvimento e comunicação de uma estratégia para o efeito, sempre que necessário;

b) Emissão de comunicados via e-mail ou através do website institucional da **entidade** e redes sociais; e

c) qualquer outra medida razoável e proporcional para restaurar a sua reputação, com o nosso consentimento prévio por escrito.

c. **Despesas de notificação e monitorização**

i. despesas, com o nosso consentimento prévio, relacionadas com a notificação da ocorrência de uma **violação de dados** a qualquer entidade reguladora, ou outras autoridades competentes em matéria de **violação de dados**, desde que o **segurado** esteja legalmente obrigado a fazê-lo;

ii. Custos incorridos, com o nosso consentimento prévio, com a utilização de um *call center* externo para resposta às questões dos **afetados**, previamente notificados, em resultado de uma **violação de dados**,

iii. Despesas de monitorização de identidade: contratação de um serviço de monitorização em sites públicos da Internet das informações comprometidas dos **afetados**, a fim de evitar uso indevido, pelo prazo máximo de um ano a partir da data de ativação. O serviço deve ser ativado somente após a notificação, previamente acordada com o segurador, aos **afetados**, como consequência de uma **violação de dados**;

iv. Despesas com a notificação dos **afetados** da **violação de dados**, com o nosso consentimento prévio;

v. Despesas de monitorização de crédito: reembolso das despesas razoáveis e necessárias incorridas pela **entidade**, com nosso consentimento prévio, para a contratação de um serviço de monitorização de crédito ou similar para os **afetados**, previamente notificados, em consequência de uma **violação de dados**.

Extensão de cobertura para sistemas armazenados na nuvem de um **Fornecedor externo tecnológico**

Faz-se constar que fica abrangido, nos mesmos termos, o Serviço de Resposta a Incidentes em caso de **incidente** que afete um sistema:

a. utilizado pela **entidade** para o desenvolvimento da sua atividade e em seu benefício próprio;

b. que seja fornecido por um **fornecedor externo tecnológico**; e

c. que esteja armazenado na nuvem de um **fornecedor externo tecnológico**;

desde que o **incidente** seja **descoberto** durante o **período do seguro** e tenha origem no **sistema informático** da **entidade ou** tenha ocorrido através do **sistema informático** da **entidade**.

2.2. Perdas do segurado

Se, durante o **período do seguro** da **apólice,** o **segurado** sofrer um **incidente**, real ou presumível, o segurador **pagará** o seguinte:

a. Despesas de recuperação de dados ou sistemas

Despesas incorridas, com o prévio consentimento por escrito do segurador para:

i. recuperação do acesso aos **programas**, **sistemas informáticos** ou dados eletrónicos da **entidade**;

ii. reconfigurar, instalar a partir de cópias de segurança, cópias originais ou outras fontes ou, se necessário, substituir um **programa** de terceiros (adquirido legalmente) no **sistema informático**;

iii. recriar os dados eletrónicos da **entidade**;

iv. **despesas de mitigação**

Se os **programas** ou dados eletrónicos não puderem ser acedidos, recuperados, substituídos, reparados ou recriados, as despesas a serem pagas pelo segurador não excederão os custos incorridos para obter essa conclusão.

Em caso algum pagaremos os custos de recuperação de dados decorrente do furto ou roubo de hardware que façam parte integrante do sistema informático.

Extensão de cobertura para sistemas armazenados na nuvem de um fornecedor externo tecnológico.

Faz-se constar que as despesas de recuperação estão cobertas nos mesmos termos dos dados ou sistemas em caso de **incidente** que afete um sistema:

a. utilizados pela **entidade** para o desenvolvimento da sua atividade e em benefício próprio;

b. que seja fornecido por um **fornecedor externo tecnológico**; e

c. que esteja armazenado na nuvem de um **fornecedor externo tecnológico**;

Desde que o **incidente** seja **descoberto** durante o **período do seguro** e tenha origem no **sistema informático** da **entidade ou** tenha ocorrido através do **sistema informático** da **entidade**.

b. Extorsão cibernética

O segurador reembolsará:

i. o valor económico do resgate pago pelo **segurado** ou, caso o terceiro exija o pagamento do resgate em forma de bens ou serviços, o valor de mercado desses mesmos bens ou serviços no ato de entrega do resgate;

ii. os honorários e demais despesas incorridas com serviços de consultoria especializados para auxílio do **segurado** na gestão e negociação do resgate;

iii. o valor de um resgate roubado por um terceiro, desde que o referido roubo ocorra num local acordado para o pagamento do resgate, ou a caminho dele;

iv. **Despesas de mitigação.**

O segurador apenas reembolsará as despesas incorridas pela **entidade** decorrentes da **ameaça de extorsão** sempre que ocorram as seguintes circunstâncias:

i. a legislação permita o reembolso dessas despesas, sendo que em caso algum o segurador reembolsará o **Segurado**, quando este esteja sito em território português, de valores referentes ao pagamento de resgates

ii. o **segurado** informe imediatamente o segurador, mantendo-o sempre atualizado sobre a **ameaça de extorsão**, e obtenha o consentimento por escrito do segurador antes do pagamento do resgate;

iii. o **segurado** notifique a **ameaça de extorsão** à polícia ou a outra autoridade competente;

iv. o **segurado** faça prova ao segurador de que o resgate foi pago, ou os bens ou serviços foram entregues, sob coação ou ameaça, e que envidou todos os esforços para determinar que a ameaça era real e não fictícia, assim como todas as ações necessárias para evitar a **ameaça de extorsão**; e

v. um administrador, diretor (ou cargo equivalente) da **entidade** tenha dado o seu consentimento para o pagamento do resgate ou para a entrega de bens ou serviços.

vi. o valor do resgate exigido seja proporcional às perdas que a **entidade** poderia sofrer caso não aceitasse o pagamento do resgate.

<u>Extensão de cobertura para sistemas armazenados na nuvem de um fornecedor externo tecnológico</u>

Faz-se constar que está coberta, nos mesmos termos, a **ameaça de extorsão** à **entidade** sobre um **sistema informático**:

a. utilizado pela **entidade** para o desenvolvimento da sua atividade e em benefício próprio;

b. que seja fornecido por um **fornecedor externo tecnológico**; e

c. que esteja armazenado na nuvem de um **fornecedor externo tecnológico**.

Sempre que a **ameaça de extorsão** seja **descoberta** durante o **período do seguro** da **apólice** e resulte de um acesso não autorizado ao **sistema informático** da **entidade**.

c. Proteção de equipamentos

Até ao sublimite indicado nas **condições particulares**, o segurador reembolsará a **entidade**, do custo de reparação ou substituição de equipamento informático (hardware ou móvel) que faça parte do **sistema informático**, sempre e quando:

- o equipamento informático contenha **dados pessoais**, **informações confidenciais** ou **informações corporativas** da **entidade**; e
- o equipamento informático tenha sido afetado por um **incidente** e já não possa ser utilizado para as funções para as quais se destinava; e

- a cobertura de **despesas de mitigação** não seja ativada.

O segurador apenas assumirá o custo de substituição de um equipamento informático quando:

- o equipamento não possa ser reparado; ou
- o custo da reparação ultrapasse o custo da substituição.

Garantias adicionais – consulte as condições particulares para confirmar se estão contratadas

d. Perda de lucros

O segurador pagará, até ao limite estabelecido nas **Condições Particulares**, a Perda de Lucros resultante da interrupção parcial ou total do **sistema informático** quando a mesma i) ocorra durante o **período do seguro** da **apólice**, ii) o período de interrupção ultrapasse a **franquia temporal**, e iii) a interrupção seja consequência direta e exclusiva de um **incidente** no **sistema informático da entidade**.

A referida Perda de lucros será calculada de acordo com uma das seguintes hipóteses:

1. Caso as **Condições Particulares** estabeleçam um limite por dia para a cobertura de Perda de Lucros, o segurador pagará, durante a interrupção do **sistema informático** e de acordo com o **período de indemnização**, o limite de indemnização por dia fixado nas **Condições Particulares**.

   O montante a pagar a título de indemnização pela Perda de Lucros não pode, em caso algum, exceder os prejuízos efetivamente sofridos.

   O segurador reserva-se no direito de averiguar e comprovar a perda sofrida pela **entidade** e de solicitar a documentação necessária para o seu apuramento, conforme abaixo indicado, podendo pagar um valor inferior ao indicado nas **Condições Particulares** se a perda real for inferior ao limite da indemnização diária definida nas mesmas.

   Cálculo da redução do resultado operacional

   O cálculo da Perda de Lucros será feito com base na comparação entre o resultado operacional (lucro ou prejuízo) obtido durante a paralisação da atividade, e o resultado operacional (lucro ou prejuízo) que a **entidade** obteve no mesmo período do ano anterior. Caso estejamos perante o primeiro ano de atividade, o cálculo do resultado líquido será feito comparando o período de interrupção do **sistema informático** e o período idêntico imediatamente anterior à interrupção.

2. Caso as **Condições Particulares** estabeleçam um limite de indemnização por **período do seguro** para a cobertura de Perda de Lucros, o segurador pagará, quer durante a interrupção do **sistema informático**, quer após a cessação de tal interrupção, e durante o **período de indemnização**:

i. a redução do resultado operacional (lucro ou prejuízo), incluindo os custos operacionais fixos incorridos pela **entidade** afetada; e

ii. as **despesas de mitigação**.

Cálculo da redução do resultado operacional

O segurador pagará a diferença entre o resultado operacional real (lucro ou prejuízo) obtido durante o **período de indemnização**, em comparação com o resultado operacional (lucro ou prejuízo) que a **entidade** obteve no mesmo período do ano anterior. Se este for o seu primeiro ano de atividade, o cálculo do resultado operacional será efetuado comparando o **período de indemnização** com o período imediatamente anterior à interrupção.

Caso seja previsível que a **entidade** possa recuperar parcial ou totalmente os prejuízos sofridos durante a interrupção do seu **sistema informático**, o segurador reserva-se ao direito de esperar até ao final do **período de indemnização** para calcular a compensação a que a **entidade** tem direito, por Perda de Lucros.

Extensão de cobertura para sistemas armazenados na nuvem de um fornecedor externo tecnológico

Faz-se constar que fica coberta, nos mesmos termos, a Perda de Lucros da **entidade** decorrente da interrupção parcial ou total de um sistema:

a. utilizado pela **entidade** para o desenvolvimento da sua atividade e para seu benefício próprio;

b. que seja fornecido por um **fornecedor externo tecnológico**; e

c. que esteja armazenado na nuvem de um **fornecedor externo tecnológico**.

desde que o **incidente** seja **descoberto** durante o **período do seguro** e tenha a sua origem no **sistema informático** da **entidade ou** tenha ocorrido através do **sistema informático** da **entidade**.

Definições aplicáveis a esta cobertura

Para efeitos da presente cobertura, aplicam-se as seguintes definições:

Franquia temporal: corresponde ao período de tempo, indicado nas **condições particulares**, durante o qual a cobertura de Perda de Lucros não se encontra em vigor, não podendo o **tomador/segurado** acionar a mesma.

Período de indemnização: o período máximo decorrido nos dias de calendário, indicado nas **condições particulares**, uma vez decorrida a **franquia temporal**, durante o qual **o segurador** assumirá a perda de lucros previstos na cobertura. O **período de indemnização** não será interrompido se uma nova interrupção do **sistema informático** ocorrer pelo mesmo motivo num prazo máximo de uma hora a partir da resolução da primeira interrupção.

O **segurado** deve fornecer todas as informações solicitadas pelo segurador**,** de forma que esta possa apurar a redução do resultado líquido real que possa ter ocorrido. Para mais detalhes, consulte a secção 1.2 do anexo “Processo de notificação de incidentes e reclamações" desta **apólice**.

e. Fornecedor externo tecnológico

No seguimento de um **ciberataque** ao seu **Fornecedor externo tecnológico**, e até ao sublimite e **período de indemnização**, e deduzidas as **franquias** correspondentes indicadas nas **condições particulares**, o segurador cobrirá a **entidade** relativamente a:

i. Despesas incorridas, com o consentimento prévio do segurador, na medida em que sejam necessárias para restaurar os **programas** ou dados eletrónicos da **entidade** alojados na nuvem de um **fornecedor externo tecnológico** a partir de cópias de segurança, desde que a cópia de segurança esteja disponível; ou despesas incorridas com o consentimento prévio por escrito do segurador para recriar os dados eletrônicos da **entidade** alojados por um **fornecedor externo tecnológico**;

   Se os **programas** ou dados eletrónicos não puderem ser restaurados ou recriados, as despesas que o segurador pagará não ultrapassarão as despesas incorridas para chegar a essa conclusão.

ii. A Perda de Lucro da **entidade** resultante de uma interrupção parcial ou total do **sistema informático de um fornecedor externo tecnológico** desde que i) ocorra durante o **período do seguro**, ii) o **período de interrupção** ultrapasse a **franquia temporal**, e iii) a interrupção seja uma consequência direta e exclusiva de um **ciberataque** no **sistema informático de um fornecedor externo tecnológico**.

   O cálculo da perda de lucros é feito conforme indicado na secção 2.2. d. “Perda de Lucros”.

iii. As **Despesas de mitigação**, para restabelecer o serviço à **entidade** prestado pelo **fornecedor externo tecnológico**.

O limite máximo a pagar através da presente cobertura, independentemente do número de **ciberataques** ou **incidentes** abrangidos nesta apólice, não excederá o sublimite indicado nas **condições particulares** para a cobertura do **Fornecedor externo tecnológico**.

Consulte a documentação que será solicitada para o processamento do pedido de pagamento desta secção no **Anexo “Processo de notificação de incidentes e reclamações”**.

Definições aplicáveis a esta cobertura

Para efeito de ativação desta cobertura:

- Aplicam-se as definições de **período de indemnização** e **franquia temporal** constantes da secção "**Perda de Lucros**".
- A definição de "**sistema informático**" é substituída por "**sistema informático de um fornecedor externo tecnológico** ", nos termos a seguir indicados:

Sistema informático de um fornecedor externo tecnológico

Todos os computadores interligados ou sem fios e os seus componentes, incluindo, entre outros:

- sistemas operativos, hardware ou software;
- dispositivos de entrada e saída associados, dispositivos de armazenamento de dados e serviços de backup, dispositivos ou ferramentas de back-up;
- componentes periféricos relacionados, tais como dispositivos de Internet das Coisas (em inglês, *Internet of Things*);
- site web (incluindo extranet e intranet) e contas de redes sociais; e
- Sistemas de armazenamento em nuvem, incluindo, entre outros a infraestrutura subjacente (hardware).

desde que estejam diretamente sob o controlo e administração do **fornecedor externo tecnológico**, e utilizados por este para a prestação dos seus serviços à **entidade**.

Faz-se constar que a cobertura não é ativada caso não se possa acreditar a ocorrência de um **ciberataque** ao **sistema informático de um fornecedor externo tecnológico**. Cabe ao **Segurado** provar que o referido **ciberataque** ocorreu e que isso significou uma paralisação total ou parcial do **sistema informático** da **entidade**.

2.3 Responsabilidade tecnológica

Se, durante o **período do seguro,** o **segurado,** em consequência de um **incidente**:

1. **Sanção de proteção de dados**

Receber uma **reclamação** na qual se alegue:

a) incumprimento, violação ou infração involuntária de qualquer legislação e demais normativos aplicáveis em matéria de proteção de **dados pessoais** ou direito à privacidade, desde que a **reclamação** não se baseie direta ou indiretamente na recolha e/ou tratamento de **dados pessoais** pela **entidade**, ou por qualquer pessoa que atue em seu nome, sem ter obtido consentimento prévio nos termos do quadro legal ou regulamentar aplicável. Faz-se constar que as **reclamações** apresentadas pelos **empregados** são abrangidas por esta secção, caso os seus **dados pessoais** sejam violados. As **reclamações** apresentadas por qualquer sócio, administrador ou diretor não estão cobertas.

b) Violação de qualquer dever de confidencialidade de **dados pessoais** ou **informações confidenciais**; ou

c) violação de qualquer dever contratual de manutenção da segurança ou confidencialidade dos **dados pessoais**, **informações confidenciais** ou **informações corporativas**, incluindo uma violação da política de privacidade **da entidade**.

2. **Inspeção de Proteção de Dados**

For sujeito a uma **inspeção de dados** ou a qualquer outro procedimento normativo no domínio da proteção de dados.

3. **PCI DSS Incumprimento**

For objeto de procedimento por incumprimento da norma de segurança de dados da Indústria de Cartões de Pagamento (em inglês: Payment Card Industry Data Security Standard).

4. **Responsabilidade por conteúdos digitais**

Receber uma **reclamação** decorrente diretamente da modificação por terceiros ou por um **empregado** (excluindo sócios, administradores ou diretores) e que resulte de um **ciberataque** ao conteúdo do e-mail, redes sociais, intranet, extranet ou website da **entidade,** alegando:

a) Uma violação de qualquer direito de propriedade intelectual; ou

b) difamação, incluindo injúria, calúnias ou depreciação de um produto ou serviço; ou

c) violação de qualquer licença.

5. **Devido a falha de segurança cibernética**

Receber uma **reclamação** com base na transmissão de um **vírus**, no acesso ou uso não autorizado do **sistema informático de terceiros** ou num **ataque de negação de serviço a terceiros**, realizado por meio ou usando o **sistema informático** da **entidade**.

Para efeitos desta cobertura entende-se como:

Sistema informático de terceiros

Todos os computadores interligados ou sem fios e os seus respetivos componentes, que sejam propriedade de terceiros, controlados e administrados por terceiros e utilizados pelo terceiro para seu próprio benefício.

Ataque de Negação de Serviço a terceiros

Privação maliciosa temporária, total ou parcial, do acesso ou uso do **sistema informático de terceiros** como resultado de um ataque desde um computador. Também fica abrangido por esta definição um ataque de negação de serviço distribuído, que é produzido por um ataque desde vários computadores (ou vetores) em vez de a apenas um.

De acordo com os pontos 1 a 5 acima indicados no parágrafo 2.3, o **segurador** pagará:

a) Os montantes acordados entre o **segurado** e o segurador após uma negociação de boa-fé, uma mediação ou qualquer outra forma alternativa de resolução de litígios, para resolver a **reclamação**, ou os montantes em que o **segurado** foi condenado por sentença ou resolução arbitral.

Para efeitos desta cobertura, são também consideradas **reclamações** aquelas em que seja pedida uma compensação financeira por sofrimento mental ou emocional resultante de um **incidente**;

b) A **Sanção de proteção de dados** imposta à **entidade**;

c) Os **custos e sanções de PCI** impostos à **entidade**;

d) **despesas forenses de proteção de dados**;

e) **despesas de inspeção da proteção de dados** incorridos **pela entidade**;

f) **custos de defesa** do **segurado** e **cauções / fianças** impostas ao **segurado;**

g) **despesas de mitigação**; e/ou

h) as **despesas de comparência em julgamento**.

Para efeitos desta cobertura e para determinar o que o **segurador** pagará, aplicam-se as "Definições aplicáveis a esta cobertura" indicadas abaixo.

Caso, durante a defesa de uma **reclamação**, o **segurado** tenha que comparecer em tribunal, o **segurador** suportará as despesas justificadas por cada dia, ou parte de cada dia**,** que o **segurado** ou qualquer um dos seus **empregados** deva dedicar a tal assistência, a pedido do seu advogado ou perito do **segurador**, de acordo com as seguintes taxas:

a. Qualquer sócio, administrador ou membro do conselho de administração da **entidade**, até 500€ por dia;

b. Qualquer **empregado** até 250 euros por dia.

Não será aplicada qualquer **franquia** a estas despesas.

Definições aplicáveis a esta cobertura

Despesas forenses de proteção de dados: entendem-se como as despesas incorridas pelo **segurado**, com o consentimento prévio do **segurador**, para utilizar os serviços de peritos externos, de forma a preparar a defesa contra uma **reclamação**.

Despesas de inspeção de proteção de dados: entende-se como os honorários de advogados e peritos, incorridas pelo segurado, com o consentimento prévio do segurador, para a investigação, defesa, recurso ou regularização no âmbito de uma inspeção de dados.

Inspeção de dados: qualquer investigação, consulta ou exame oficial não rotineiro decorrente de uma **violação de dados** por parte de um regulador, organismo governamental ou qualquer outra autoridade de supervisão que vise garantir o cumprimento da legislação de proteção de **dados pessoais.**

Custos e sanções do PCI: entende-se como multas, sanções e reembolsos de despesas (incluindo, mas não se limitando a despesas operacionais, despesas relacionadas com a reemissão de cartões de pagamento e recuperações de fraudes) que a **entidade** é legalmente obrigada a pagar em consequência do incumprimento da norma de segurança de dados da indústria de cartões de pagamento (em inglês: Payment Card Industry Data Security Standard).

Sanção de proteção de dados: entende-se como multas ou sanções por violação involuntária dos regulamentos de proteção de dados, impostas à **entidade** por qualquer entidade governamental ou qualquer órgão de supervisão, desde que sejam seguráveis por lei na jurisdição em que a

sanção é aplicada pela primeira vez, excluindo Penalidades PCI, sendo que caso algum o **segurado** pagará quaisquer valores no caso em que a jurisdição em que a sanção é aplicada pela primeira vez for a Portuguesa.

2.4 Fraude tecnológica

O **segurador** reembolsará a **entidade**, conforme indicado neste parágrafo, até ao sublimite indicado nas **condições particulares** e até ao máximo de 60 dias seguidos por **período do seguro**, pelas perdas financeiras diretas da **entidade, descobertas** pela primeira vez durante o **período do seguro** da apólice, como resultado de um **ciberataque** de terceiros, exclusivamente nos casos abaixo indicados:

a. **Uso fraudulento da identidade eletrónica do segurado**

Devido ao uso fraudulento ou desonesto da identidade eletrónica da empresa, incluindo, de forma limitativa:

i. Obtenção de crédito em nome do **segurado**;

ii. Assinatura eletrónica de qualquer contrato;

iii. Criação ou utilização de um website concebido para copiar ou imitar o negócio do **segurado**;

b. **Furto ou Roubo eletrónico de fundos**

Pelo furto ou roubo eletrónico de dinheiro ou valores mobiliários da **entidade**, desde que a respetiva perda resulte de instruções fraudulentas por meios eletrónicos através das quais o terceiro, sem autorização, ordene um movimento financeiro para o débito de valores em **conta bancária**.

c. **Modificação de preços on-line**

Pela diferença entre os preços oficiais autorizados pela **entidade,** publicados nos seus websites e os preços modificados, que se traduzam numa redução, feita de forma intencional, por um terceiro não autorizado.

d. **Fraude nos serviços contratados**

Decorrente da utilização fraudulenta do **sistema informático**, que resulte no aumento das despesas incorridas pela **entidade** em/nos:

i. serviços de fornecimento de eletricidade;

ii. serviços de telecomunicações (quer seja através de telefones fixos ou móveis, ou através da Internet);

iii. Serviços de Internet, incluindo dados móveis;

iv. Custos de qualquer pagamento por clique malicioso;

v. mineração de criptomoedas (criptojacking).

Em qualquer caso, não garantimos qualquer aumento nas despesas incorridas pela **entidade** relacionadas com a utilização fraudulenta de sistemas na nuvem.

Caso se verifique algum dos casos acima mencionados nas alíneas a. a d., o segurador indemnizará o **segurado** relativamente:

i. ao valor ou quantia de qualquer dinheiro, título ou propriedade, furtado ou roubado e/ou,

ii. às despesas necessárias e razoáveis incorridas com o nosso consentimento prévio por escrito, para dissociar o negócio do **segurado**

de qualquer contrato ou acordo celebrado através do uso fraudulento ou desonesto da identidade eletrónica do seu negócio.

Para efeitos da alínea d), o pagamento de qualquer indemnização fica sujeito a que tais despesas sejam cobradas ao **segurado** através de fatura periódica emitida pelo prestador de tal serviço, nos termos de um contrato ou acordo escrito celebrado entre ambas as partes**,** antes da descoberta da fraude do serviço e a que o contrato não assente na existência de uma tarifa fixa

Consulte a documentação que será solicitada para o processamento do pedido de reembolso ao abrigo desta secção no Anexo referente ao “processo de notificação de incidentes e reclamações”.

O que não está coberto O segurador não fará nenhum pagamento que seja, direta ou indiretamente, baseado em, que decorra de ou que seja atribuível a:

1. Infraestrutura Qualquer falha ou interrupção de um serviço prestado por um prestador de serviços de internet, prestador de serviços do sistema de nome de domínio (ou DNS, na sigla em inglês), autoridades de certificados (ou CA, na sigla em inglês), rede de entrega de conteúdos (ou CDNs, na sigla em inglês), telecomunicações, satélites, fornecimento de energia ou qualquer outro prestador de serviço público (incluindo, mas não se limitando a, água, gás, hidrogénio); no entanto, esta exclusão não se aplica a uma **violação de dados**, quando estes estejam armazenados na nuvem, servidores remotos ou armazenados num centro de processamento de dados/data center externo e a falha ou interrupção resulta desses serviços.

2. Propriedade intelectual e industrial Qualquer violação, utilização, apropriação indevida ou transmissão de qualquer propriedade intelectual ou industrial, incluindo, mas não se limitando a patentes, segredos comerciais ou marcas registadas; todavia, esta exclusão não se aplica a:

a. uma **violação de dados**

b. um **ciberataque**; ou

c. a uma **reclamação** de responsabilidade de conteúdo digital.

3. Danos materiais A perda, dano, desgaste normal, deterioração gradual ou destruição de qualquer bem tangível. Todavia, esta exclusão não se aplica a:

a. perda, dano ou destruição de dados eletrónicos;

b. uma **violação de dados**, ou um ataque cibernético, resultante de danos ou destruição de qualquer bem tangível

c. ao que está incluído na alínea 2.2. c. “Proteção de equipamentos”.

4. Danos pessoais Morte, doença ou lesão física sofridos por qualquer pessoa. No entanto, esta exclusão não se aplicará a qualquer parte de uma **reclamação** por sofrimento mental ou emocional decorrente de um **incidente**.

5. Conflitos, Atos de Violência e Guerra

a) Invasão, greve, motim, revolta, tomada de poder à força (militar ou não)

b) **guerra**; ou

c) Uma **operação cibernética** que seja atribuível a um **Estado** e:

i. Que ocorra durante a **guerra**; e/ou

ii. Que devido ao seu efeito, direto ou indireto, cause impacto no funcionamento de um **Estado**, na disponibilidade, integridade ou prestação de um **serviço essencial** nesse **Estado**; e/ou

iii. Que cause impacto na segurança ou na defesa daquele **Estado**.

Uma **operação cibernética** pode ser imputável a um **Estado**, se o governo ou uma agência de segurança (incluindo agências de inteligência) de um **Estado relevante** a comunicar publicamente.

Caso haja conflito na atribuição de uma **operação cibernética** dentro de um **Estado relevante**, deve prevalecer a atribuição feita pelo governo do **Estado relevante** nas comunicações oficiais.

No caso de existir um conflito na atribuição de uma **operação cibernética** entre diferentes **Estados relevantes**, a atribuição feita pelo **Estado afetado** deve prevalecer.

Se o **Estado afetado** não efetuou uma atribuição de uma **operação cibernética**, a atribuição efetuada por um **Estado relevante** deve ser suficiente, mesmo que outros **Estados relevantes** discordem ou o contradigam.

No caso de ausência de atribuição de uma **operação cibernética** por um **Estado relevante**, uma **operação cibernética** também pode ser imputável a um **Estado** se o segurador o demonstrar com provas adequadas.

As seguintes definições aplicam-se a esta exclusão:

Operação cibernética: entende-se como o acesso ou uso não autorizado de um computador, rede ou sistema no território de um **Estado** por ou em nome de outro **Estado**, bem como o uso de um computador, rede ou sistema por um **Estado** ou em seu nome, para afetar adversamente um computador, rede ou sistema de outro **Estado**, incluindo, mas não limitando a, a introdução de um **vírus** ou um ataque de negação de serviço contra um computador, rede ou sistema no território de um **Estado**.

Serviço essencial: entende-se como o serviço essencial para a manutenção de atividades sociais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um **incidente** possa ter efeitos perturbadores relevantes na prestação desse serviço, conforme estabelecido pela Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, ou qualquer outro diploma que a substitua.

Estado: é entendido como um país soberano, reconhecido como tal na ordem internacional, estabelecido em território determinado e dotado dos seus próprios órgãos governativos.

Estado afetado: qualquer **Estado** que sofra um impacto negativo na sua operação, devido ao efeito direto ou indireto de uma **operação cibernética** na disponibilidade, integridade ou prestação de um **serviço essencial** ou na sua segurança ou defesa.

Guerra: entende-se como o uso da força física por um **Estado** contra outro **Estado**, declarada ou não, bem como uma guerra civil.

Estado relevante: um **Estado afetado**, um **Estado**-Membro da União Europeia ou um **Estado**-Membro da NATO.

5. Apreensão, confiscação e/ou proibição de acesso	a. Qualquer ação de um governo ou autoridade pública com vista à apreensão, expropriação, confisco, apropriação ou destruição de bens, ou qualquer ordem desse governo ou autoridade pública para desativar, bloquear ou não permitir o acesso ou utilização da totalidade ou de parte do **sistema informático** da **entidade** ou do **sistema informático de um fornecedor externo tecnológico**. b. Qualquer ação do governo ou autoridade pública que direta ou indiretamente regule, limite ou proíba o uso de energia pela **entidade** ou **fornecedor externo tecnológico**. c. Qualquer ordem do governo ou autoridade pública que impeça ou restrinja o acesso a qualquer espaço físico ou local de trabalho da **entidade** ou de um **fornecedor externo tecnológico**, incluindo, mas não se limitando ao acesso a data centers.
6. Problemas pré-existentes	a) Qualquer facto, circunstância ou **incidente** do qual o **segurado** tenha tomado conhecimento antes da data início da apólice. b) Qualquer procedimento civil, comercial, criminal, laboral, administrativo, regulatório ou de arbitragem, ou qualquer procedimento alternativo de resolução de litígios iniciado antes da primeira data de início desta apólice, ou com base nos mesmos ou essencialmente nos mesmos factos alegados no procedimento referido anteriormente.
7. Atos deliberados ou desonestos	a) Qualquer ato ou omissão fraudulento, doloso, desonesto, ilegal ou malicioso cometido pelo segurado, bem como por qualquer outra pessoa que o **segurado** tenha consentido ou tolerado, incluindo o uso ou obtenção não autorizados de dados de forma intencional ou em violação da Lei. b) Qualquer ato ou omissão com a finalidade de obter benefício indevido ou vantagem indevida a que o **segurado** não tivesse legalmente direito. Esta exclusão tem as seguintes ressalvas: a Só é aplicável se o referido ato ou omissão for comprovado por sentença transitada em julgado ou outra deliberação final, ou se o **segurado** o reconhecer; b. Os atos de um **empregado** não serão imputados à **entidade**, a menos que tais atos tenham sido cometidos ou tenham sido do conhecimento de anterior ou atual sócio, administrador ou diretor. A **entidade** reembolsará o segurador por qualquer pagamento efetuado por este que esteja relacionado com tal ato ou omissão.
8. Cobertura Internacional	Qualquer **reclamação** ou **incidente** fora da jurisdição aplicável, entendendo-se como tal os processos que corram em tribunal situados, ou com base na jurisdição do referido país ou território e/ou fora dos territórios definidos (âmbito territorial) nas **condições particulares**, sem prejuízo de qualquer limitação legal adicional que possa existir em qualquer território ou jurisdição.

9. Responsabilidade contratual	Qualquer garantia, promessa ou obrigação assumida contratualmente pelo segurado. No entanto, esta exclusão não é aplicável: a. À responsabilidade que o **segurado** teria assumido na ausência do referido contrato; b. quando descubra uma **violação de dados**; c. quando ocorra uma violação das normas de segurança da Indústria dos Cartões de Pagamento (PCI Data Security Standard).
10. Segurado contra Segurado	Qualquer **reclamação** apresentada: a. pelo próprio segurado; ou b. por qualquer pessoa individual ou coletiva que detenha, direta ou indiretamente, mais de 15% das ações ou participações emitidas pela **entidade**, ou que, direta ou indiretamente, a gira, controle ou dirija total ou parcialmente; c. por qualquer pessoa coletiva em que a **entidade** detenha, direta ou indiretamente, mais de 15% das ações ou participações emitidas, ou que a **entidade** gira, controle ou dirija total ou parcialmente. Esta exclusão não se aplica a uma **reclamação** apresentada por um **empregado** como resultado de uma **violação de dados**.
11. Multas, penalizações e sanções	Multas ou sanções, penalizações contratuais, danos punitivos ou exemplares, não reembolsáveis ou não compensatórios. Esta exclusão não é aplicável: a. a sanções decorrentes do incumprimento dos regulamentos do PCI Data Security Standard; ou b. a qualquer **Sanção de proteção de dados**.
13. Fundos e valores imobiliários	O furto, roubo, perda ou transferência de dinheiro, fundos, valores ou bens tangíveis, exceto o que está incluído na secção “Fraude Tecnológica”.
14. Melhoria	Qualquer custo referente à reparação, melhoria, correção, remoção, substituição, eliminação ou outro qualquer processo, na medida em que o mesmo deixe o **segurado** numa situação mais vantajosa do que aquela que existiria na ausência do sinistro. No entanto, esta exclusão não se aplica: a. às **despesas de mitigação**; b. às despesas de recuperação de dados e sistemas indicadas como cobertas na seção 2.2.a “Despesas de recuperação de dados ou sistemas” ou; c. à cobertura 2.2.c) “Proteção de equipamentos”.
15. Exclusões aplicáveis à	Aplicável apenas no que diz respeito à cobertura 2.3 alínea “4. Responsabilidade por conteúdos digitais”.

responsabilidade tecnológica (conteúdo digital)	a. Qualquer violação, utilização, apropriação indevida ou transferência de qualquer patente ou segredo comercial; ou b. À obrigação de pagar taxas de licenciamento ou royalties; e/ou c. qualquer **incidente** cometido por uma **pessoa segura** que não seja um **empregado**.
16.Exclusões aplicáveis à cobertura 2.2.a) Despesas de recuperação de dados ou sistemas	Aplicável apenas no que diz respeito à cobertura 2.2.a) "Despesas de recuperação de dados ou sistemas": a. despesas para identificar ou corrigir vulnerabilidades no **sistema informático** da **entidade**, no **sistema informático de um fornecedor externo tecnológico** ou **programa**; b. O valor económico de **programas**, **dados pessoais**, dados eletrónicos, **informações corporativas** ou **informações confidenciais**, incluindo segredos comerciais, sem prejuízo do disposto na alínea a. ii. da cobertura 2.2.a. "Despesas de recuperação de dados ou sistemas"; c. despesas destinadas a substituir, restaurar ou atualizar **programas** ou dados eletrónicos para um nível superior ao que existia antes da ocorrência do **incidente**. d. despesas incorridas no desenvolvimento de novos **programas** ou dados eletrónicos.
17. Contaminação e radiação nuclear	Qualquer descarga, libertação ou fuga (real, suspeita, presumível ou ameaça de) de **poluentes**, incluindo quaisquer instruções ou solicitações para testar, monitorizar, limpar, remover, conter, tratar, desintoxicar ou neutralizar **poluentes**, bem como qualquer perda derivada de um acidente nuclear que cause, entre outros aspetos, um pulso eletromagnético (ou EMP, na sigla em inglês).
18. Responsabilidade Civil Profissional e Responsabilidade de Produtos	Qualquer **reclamação** contra o **segurado** decorrente da sua prestação de serviços ou de produtos fornecidos ou produzidos pela **entidade** (incluindo, mas não se limitando à retirada ou substituição de produtos). No entanto, esta exclusão não se aplica a uma **reclamação** contra o **segurado** com fundamento: 1) na transmissão de um **vírus** a partir do **sistema informático**, 2) num ataque de negação de serviço a terceiros com a utilização do **sistema informático** da **entidade** ou com a utilização do **sistema informático de um fornecedor externo tecnológico**, 3) numa **violação de dados**.
19. Riscos da natureza	Danos decorrentes de um risco da natureza, incluindo, mas não limitando a, terramotos, incêndios, ventos, inundações, vulcões, supervulcões, inversão dos polos magnéticos da Terra, tempestade solar ou erupção solar. Faz-se igualmente constar que estão excluídos os danos causados pelo clima espacial, entendendo-se como tal, as condições do sol e do vento

	solar, a magnetosfera, a ionosfera e a termosfera que podem afetar o desempenho e a fiabilidade dos sistemas tecnológicos espaciais e terrestres e que de alguma forma afetam as infraestruturas, a tecnologia, a saúde e a vida humana. Esta exclusão abrange, não ficando, porém, limitada aos danos causados por asteroides, fulgurações, erupções solares, ou ejeções de massa coronal que possam produzir, entre outras coisas, apagões de rádio ou tempestades de radiação solar.
20. Recolha e tratamento ilícito de dados pessoais	**Incidentes** e/ou **reclamações** decorrentes de negligência ou incumprimento de disposições legais ou regulamentares em matéria de proteção de dados, no âmbito da recolha e/ou tratamento de **dados pessoais** pela **entidade**, ou por quem atue em seu nome, sem que tenha sido obtido consentimento válido nos termos do quadro legal ou regulamentar aplicável.
21. Transações financeiras	Qualquer **reclamação** ou perda baseada em, ou decorrente de, ou que seja atribuível a, direta ou indiretamente, compra ou venda de qualquer fundo, valores ou títulos, ações, derivados ou outros ativos financeiros. Ficam igualmente excluídos quaisquer danos resultantes da perda de oportunidade para realizar uma transação financeira.
22. Sanções internacionais	O Segurador não proporcionará qualquer cobertura, nem será responsável por efetuar algum tipo de pagamento por qualquer sinistro, reclamação, dano ou perda, nem satisfará qualquer benefício nos termos da presente **apólice**, na medida em que tal cobertura, pagamento ou satisfação de prestação ou benefício exponha o Segurador ou qualquer membro do grupo económico a que pertença o Segurador, a qualquer sanção, proibição ou restrição aplicável nos termos de resoluções emitidas pelas Nações Unidas ou a regulamentação, leis, sanções económicas ou comerciais, impostas pela União Europeia, Reino Unido ou Estados Unidos da América.

3. Disposições gerais

3.1 Quanto é que pagaremos?

a. O limite máximo total agregado de indemnização que o segurador pagará pelo conjunto de todas coberturas previstas nestas Condições Especiais, é o limite de indemnização indicado nas **condições particulares**.

b. O **segurado** obriga-se a pagar a **franquia** indicada nas **Condições Particulares**.

c. Qualquer sublimite de indemnização que venha a ser estabelecido fará parte integrante do limite de indemnização indicado nas **condições particulares** para este módulo de cobertura ou **apólice**, e não será em nenhum caso adicional ao mesmo, sendo também o valor máximo a pagar por **incidente** e **período do seguro** para a cobertura correspondente.

d. Caso duas ou mais coberturas sejam acionadas pela mesma causa ou evento, o **segurado** pagará uma única **franquia**. A **franquia** a aplicar neste caso será a mais elevada das indicadas nas **condições particulares**. Este critério não se aplica à **franquia temporal**, que será aplicada de forma independente.

e. Dois ou mais **incidentes/reclamações** com origem na mesma causa ou facto gerador serão considerados apenas como um **incidente/reclamação**, independentemente do número de reclamantes ou **segurados** envolvidos e ainda que tenham sido apresentados em momentos e locais diferentes. Os referidos **incidentes/reclamações** serão aplicados apenas ao **período do seguro** em que ocorreu a primeira comunicação dos referidos **incidentes/reclamações**.

f. Caso existam duas ou mais apólices de seguro emitidas pelo segurador ou por qualquer outra empresa pertencente ao Grupo Hiscox e que garantam cobertura para o mesmo **incidente** ou **reclamação**, o valor total a pagar pelo conjunto de todas essas apólices não ultrapassará o maior dos limites ou sublimites de indemnização entre todas estas apólices.

3.2 Âmbito temporal

As coberturas desta apólice só são concedidas para os **incidentes descobertos** e notificados ao segurador durante o **período do seguro**.

Adicionalmente, no que diz respeito às coberturas da alínea 2.3 da Responsabilidade Tecnológica, e desde que as mesmas estejam expressamente cobertas nas **Condições Particulares**, a cobertura é concedida às **reclamações** apresentadas contra o **segurado** durante o **período do seguro** ou o **período adicional de notificação**, independentemente da data de ocorrência do **incidente**, mas desde que **o incidente** tenha sido **descoberto** e notificado durante o **período do seguro.**

3.3 Âmbito territorial

As garantias deste módulo de cobertura estendem-se e limitam-se a **incidentes** ocorridos ou **reclamações** apresentadas nos territórios definidos nas **condições particulares**.

3.4 Controlo da defesa

O segurador tem o direito, mas não a obrigação, de assumir o controlo e dirigir em nome do **segurado** a investigação, o pagamento ou a defesa de qualquer **reclamação** ou **inspeção de dados**. Se o segurador considerar necessário, designará um perito/especialista, avaliador, advogado ou qualquer outra pessoa adequada para lidar ou gerir a **reclamação** ou a inspeção de dados.

O segurador não efetuará qualquer pagamento por qualquer **reclamação** ou inspeção de dados, ou parte dela, não coberta por este módulo.

3.5 Confidencialidade

O **segurado** deve adotar sempre todas as medidas necessárias e possíveis para que nenhum terceiro tenha conhecimento da existência desta apólice, exceto com o consentimento prévio por escrito do segurador. Esta cláusula não será aplicável aos seguradores das apólices em excesso quando o presente contrato atue como apólice primária.

3.6 Obrigações do segurado

a. O **segurado** deve notificar o segurador de qualquer **incidente** ou sinistro, nos termos do "processo de notificação" anexo a esta apólice, com a maior brevidade possível, mas sempre dentro do **período do seguro**.

b. O **segurado** poderá notificar o segurador de qualquer **incidente** ou circunstância que possa dar origem a uma **reclamação**, custo ou serviço coberto por este módulo de cobertura, com a maior brevidade possível e durante o **período do seguro**, salvo algum impedimento de ordem legal.

   Caso o segurador aceite a notificação do segurado, qualquer **reclamação**, despesa ou serviço coberto que derive dos mesmos factos, será entendido como tendo sido apresentados, para efeitos deste módulo de cobertura, quando os referidos factos foram comunicados pela primeira vez, desde que que, ao notificar os fatos, se tenha fornecido informação detalhada sobre os mesmos, incluindo datas e possíveis **afetados**.

c. A **entidade** compromete-se a prestar toda a assistência que o segurador possa requerer para recuperar junto de um terceiro as quantias que reembolsou.

3.7 Período adicional de notificação

Caso este módulo de cobertura seja cancelado ou não renovado, a **entidade** terá direito a um período adicional de notificação de:

a. 30 dias seguidos sem pagamento do prémio adicional, ou

b. 12 meses com um prémio adicional de 75% sobre o último prémio anual,

a partir da data do termo do **período do seguro**, durante o qual o **segurado** pode notificar pela primeira vez o segurador sobre um **incidente** apresentado contra o **segurado** durante o **período adicional de notificação**, cuja causa seja um **incidente descoberto** durante o **período de seguro**.

Exclusivamente no que diz respeito às coberturas da alínea 2.3 da Responsabilidade Tecnológica, a **entidade** terá sempre direito a um **período adicional de notificação** de 365 dias após a data termo da apólice, por atos ou omissões ocorridas durante o **período do seguro**

O **período adicional de notificação** significa o período de tempo a partir da data do termo do **período do seguro**, durante o qual o **segurado** poderá notificar o segurador de qualquer **reclamação** coberta por este módulo de cobertura para eventos que ocorram no **âmbito temporal** da **apólice**, mas antes da data de termo do **período do seguro**.

Este **período adicional de notificação** não se aplica se:

a. A apólice for cancelada por falta de pagamento do prémio ou de qualquer das suas frações;

b. Este módulo de cobertura tenha sido substituído por outra apólice que conceda, no todo ou em parte, a mesma cobertura.

O prémio correspondente ao **período adicional de notificação** deve ser pago integralmente no início do referido período.

O limite de indemnização aplicável durante o **período adicional de notificação** será o limite de indeminização remanescente da apólice cancelada ou não renovada. Em caso algum será concedido um limite separado ou adicional para este período.

3.8 Condições gerais Aplicáveis

São alteradas as seguintes cláusulas das Condições Gerais:

A cláusula “Condições gerais para a reclamação de sinistros” das Condições Gerais é substituída pela cláusula “3.6. Obrigações do segurado” destas condições especiais.

A cláusula “Segurados Conjuntos” das condições gerais é substituída pela cláusula «3.1. “Quanto é que pagaremos” destas condições especiais.

3.9 Declaração de Risco

O segurador celebrou o contrato considerando o estado dos riscos e com base na informação comunicada pelo **tomador do seguro** e/ou **segurado** antes da contratação e de acordo com o Questionário de Seguro apresentado ao segurador. Todas estas informações foram valorizadas como elementos essenciais para aceitar a cobertura, estimar o prémio e definir/estabelecer as obrigações entre as partes. Se esta informação não fosse correta, completa ou exata, o contrato não teria sido assinado ou teria sido aceito noutras condições mais onerosas.

O Questionário de seguro fornecido pelo **tomador do seguro** e/ou **segurado**, bem como a proposta do segurador, se for o caso, juntamente com esta apólice e as suas eventuais atas adicionais, constituem um todo unitário e são fundamento da apólice, a qual apenas abrange os riscos nela especificados, dentro dos limites acordados.

Caso o **tomador do seguro** e/ou **o segurado**, ao efetuar as declarações ao abrigo do questionário, incorra em omissão ou inexatidão sobre as circunstâncias e informações por si conhecidas que possam influenciar a avaliação do risco, aplicar-se-á o seguinte:

a) O segurador poderá, mediante declaração dirigida ao **tomador do seguro** no prazo de três meses a contar desde a data de conhecimento da reserva ou da inexatidão, fazer cessar o contrato, desde que demonstre que, em caso algum teria celebrado o contrato com o facto omitido ou declarado inexatamente. Salvo dolo ou negligência grave da sua parte, ao segurador caberão os prémios relativos ao **período de seguro** em vigor no momento da declaração.

b) Se a **reclamação** ou **incidente** ocorrer antes da declaração por parte do segurador, a indemnização será reduzida proporcionalmente à diferença entre o prémio acordado e o que teria sido aplicado caso se conhecesse a verdadeira entidade do risco. Havendo dolo ou culpa grave do **tomador**/segurado, o segurador ficará desobrigada do pagamento da indenização.

Se o conteúdo da apólice for diferente da proposta apresentada pelo segurador ou das cláusulas acordadas, o **tomador do seguro** poderá reclamar do segurador no prazo de um mês a partir da entrega da apólice para correção da divergência existente. Findo esse período sem que haja **reclamação**, aplicar-se-á o disposto na apólice.

3.10 Agravamento do risco

Durante a vigência do contrato, o **tomador do seguro** ou o **segurado** devem comunicar ao segurador, com a maior brevidade possível, quaisquer alterações nos fatores e circunstâncias declaradas e/ou que possam agravar o risco.

Entre outros aspetos que possam constituir um aumento do risco, serão considerados em qualquer caso como fatores ou circunstâncias que agravam o risco e que, portanto, o **tomador** e/ou **segurado** deve notificar o segurador, com base no questionário de risco que tenha sido preenchido, quando a **entidade**:

a. Tenha aumentado em mais de 20% a sua faturação anual consolidada ou, na falta deste dado em relação a todos os **segurados**, em relação aos valores declarados perante o segurador no último ano.
b. Realize uma atividade diferente, ou forneça um novo serviço a terceiros remotamente ou na nuvem.

c. Faça uso de sistemas de computador sem suporte do fabricante.
d. Instale os patches de prestador (ou atualizações) do fabricante nos sistemas com uma frequência superior a 30 dias, ou supere 15 dias no caso de patches críticos (CVSS 8.0 ou superior)
e. Deixe de utilizar o duplo fator de autenticação para acesso remoto a qualquer sistema, incluindo, entre outros, e-mail da web.
f. Deixe de restringir o acesso aos seus **empregados** apenas à informação e sistemas que necessitam para o desempenho das suas funções, e deixou de eliminar o acesso aos seus sistemas e informações aos seus **empregados**, quando deixam de o ser.
g. Não tenha cópias de segurança completas pelo menos a cada 7 dias de todos os seus dados e sistemas armazenados:
    i. num suporte físico desconectado dos seus sistemas, tanto durante o exercício da sua atividade, como durante a realização da cópia e as referidas cópias de segurança sejam feitas à vez em diferentes suportes externas (gravação única) ou
    ii. num prestador na nuvem, onde a autenticação de dois fatores não é necessária para aceder à consola de backup.
h. para todos os backups, não retenha pelo menos backups semanais dos últimos 30 dias.
i. Recorra a **prestadores de tecnologia externa** de serviços em nuvem que não sejam certificados com a norma ISO 27001 ou que não tenham um TIER inferior a 3 (aplicável apenas se a **entidade** tiver contratada a cobertura 2.2 e. **fornecedor externo tecnológico** e salvo se a **entidade** tiver comunicado no momento da emissão da apólice ou sucessivas renovações que utiliza um prestador que não cumpre com estas características, e isso tenha sido expressamente aceite pelo segurador).

O segurador pode, no prazo de 30 dias a contar da data da declaração do agravamento, propor a alteração do contrato incluindo qualquer das condições, limites de garantias ou coberturas contratadas, o prémio ou qualquer outro termo acordado.
Neste caso, o **tomador do seguro** tem 30 dias a contar da receção desta proposta para a aceitá-la ou recusá-la.
Em caso de recusa, ou ausência de resposta por parte do **tomador do seguro**, o **Segurador** poderá, decorrido o referido prazo, rescindir o contrato mediante aviso prévio ao **tomador do seguro**, concedendo-lhe novo prazo de quinze dias para se pronunciar, findo o qual e nos oito dias seguintes notificará o **segurado** da rescisão definitiva.

O segurador pode ainda optar pela resolução do contrato mediante comunicação escrita ao **segurado** no prazo de um mês, a contar do dia em que tomou conhecimento do agravamento do risco, demonstrando que, em caso algum, celebra contratos que cubram riscos com as características resultantes desse agravamento do risco.

.

Caso o **tomador do seguro** ou o **segurado** não tenha feito a sua declaração e ocorra um sinistro, o ***segurador*** fica exonerada da sua prestação se o **tomador do seguro** ou o **segurado** tiver agido de má-fé. Na inexistência de má-fé ou nos casos em que não tenha decorrido o prazo de dois meses indicado no n.º 3 ou caso o **tomador** ou **segurado** não tenha aceite e cumprido as obrigações de pagamento ou outras exigidas pelo segurador, a disposição do segurador será reduzido proporcionalmente à diferença entre o prêmio acordado e aquele que teria sido aplicado se a verdadeira entidade do risco fosse conhecida.

Anexo

Serviço de resposta a incidentes (cobertura 2.1)

Serviço de contenção tecnológica

Em caso de incidente, contacte o Prestador do Serviço de Resposta a Incidentes, disponível através do telefone 24x7x365

+351 211 219 400

Que informação deve fornecer?

1. Nome do **segurado** (entidade jurídica) e número da apólice
2. Contactos dos segurados (pessoa singular) para futuras comunicações
3. Breve descrição do **sinistro**

De que forma é aberto o processo de sinistro? O Prestador do Serviço de Resposta a Incidentes procederá, uma vez efetuadas as verificações preliminares necessárias, e desde que se trate de um **incidente** real e não um falso positivo, a abertura de um "ticket" no sistema de gestão de tarefas do Prestador do Serviço de Resposta a Incidentes e a comunicação do **incidente** à próprio segurador, que informará o seu mediador de seguros.

Quando começa a gestão de incidentes? Uma vez confirmado a receção da ocorrência através da abertura do "ticket", inicia-se o processo de à mesma por equipas e técnicos especializados, conforme previsto na apólice. Um técnico especializado estará sempre em contacto com o segurado.

Que informação será solicitada para a gestão do incidente? O Prestador do Serviço de Resposta a Incidentes solicitará ao **segurado** todas as informações necessárias para gerir o **incidente**, tais como diagramas de rede, máquinas afetadas, registos (e-mail, navegação), "dumps" de memória, discos rígidos, amostras de *malware*, e-mails originais, etc. Caso o cliente não tenha capacidade técnica para fornecer tais informações, o Prestador do Serviço de Resposta a Incidentes fornecerá as instruções necessárias para obtê-las.

É da responsabilidade do **segurado** fornecer as informações solicitadas pelo Prestador do Serviço de Resposta a Incidentes em tempo útil.

Onde será antecipada a gestão do incidente? O serviço será executado remotamente. Caso o **segurado** requeira a presença no local de técnicos especializados do Prestador do Serviço de Resposta a Incidentes nas instalações da pessoa afetada pelo acidente, procederá à resposta após aprovação prévia da Hiscox.

O que vai realizar o serviço de gestão de incidentes? O Prestador do Serviço de Resposta a Incidentes, sempre dentro da capacidade disponível,

realizará as ações necessárias para a prestação de serviços abrangidos pela apólice.

Que informações receberá após a prestação do serviço? Após a conclusão do processo de gestão de incidentes, o Prestador do Serviço de Resposta a Incidentes procederá à preparação, emissão e distribuição do correspondente relatório que será fornecido tanto ao **segurado** como à Hiscox.

Aconselhamento jurídico e serviço de comunicação e relações-públicas

Aquando da abertura do **incidente**, a Hiscox designará, quando necessário, um especialista jurídico e/ou de comunicação e relações-públicas do **painel de especialistas da Hiscox**, de forma a aconselhá-lo sobre as medidas a tomar para gerir a resposta ao **incidente**.

Despesas de notificação e monitorização

O **segurado** pode solicitar à Hiscox a prestação dos serviços adicionais incluídos na cobertura 2.1. **Serviço** de **resposta aos incidentes**, caso necessite que sejam prestados através do **painel de especialistas Hiscox**. A Hiscox deve dar o seu consentimento por escrito.

Processo de Notificação de Incidentes e Reclamações

1.1. Serviço de resposta a incidentes

Caso ocorra um **incidente**, e caso o **segurado** recorra a outro especialista que não o serviço de contenção tecnológica da Hiscox, deverá informar o **segurador**, no prazo máximo de sete dias a contar da sua ocorrência através do seu mediador de seguros, com a descrição da **ocorrência**, indicando a data, tipo e âmbito da mesma, bem como o relatório do especialista que a tem ou está a geri-lo.

1.2. Perdas do Segurado

Para a ativação destas coberturas, no caso em que não tenha utilizado **o serviço de contenção tecnológica**, deverá contactar o seu mediador de seguros para comunicar o **incidente**.

O **segurador** solicitará, caso a caso, a documentação que julgar necessária para fins de análise das coberturas da apólice. Entre outros, comprovativo da ocorrência do sinistro, justificativo das despesas a serem realizadas (orçamentos, atividades a serem realizadas, etc.), documentos contabilísticos para a cobertura de perda de lucros, etc.

Consulte a apólice para conhecer os processos a seguir para cada cobertura e as autorizações a solicitar à Hiscox.

a) Relativamente ao ponto 2.2, alínea **a**) **Custos de recuperação de dados ou sistemas e e) Fornecedor externo tecnológico.**

Em caso de sinistro coberto por esta garantia, assumiremos, nas condições previstas na apólice e até ao limite indicado nas **condições particulares**, o pagamento das faturas de recuperação de dados ou sistemas da **entidade**.

O segurador assumirá o reembolso do valor, excluindo quaisquer impostos aplicáveis, das faturas pagas pelo segurado, e mediante apresentação de documentação comprovativa, incluindo, mas não se limitando a/ao:

- Relatório sobre a extensão da perda de dados ou sistemas;
- Orçamento de intervenção do prestador designado pelo **segurado**, discriminado por ações a realizar e/ou horas a investir pelos técnicos.
- faturas da intervenção do prestador designado pelo **segurado**.

b) Em relação ao ponto 2.2, secção **d) Perda de lucros e e) Fornecedor externo tecnológico,** e somente no caso da **entidade** ter contratado um limite de indemnização:

Deve provar por escrito, no prazo máximo de 120 dias após a descoberta da existência de perda de lucros (salvo se o **segurador** tenha acordado alargar este prazo) a perda sofrida, fornecendo as seguintes informações:

- Uma descrição completa das circunstâncias relativas à perda de lucros, incluindo, mas não limitando, a hora, o local e a causa da perda;
- um cálculo detalhado de qualquer perda de lucros, ou no caso de pretender que o segurador calcule o valor de tais perdas, pedimos que nos forneça os mapas fiscais, a demonstração de resultados e o balanço dos últimos três anos das empresas afetadas; e
- toda a documentação e material de apoio que razoavelmente fazem parte ou relativos à comprovação de tal perda de lucros, incluindo as informações solicitadas nas alíneas a e b.

Os custos e despesas incorridos pelo **segurado** para provar ou justificar a perda dos benefícios sofridos serão da sua responsabilidade e não estão cobertos por esta apólice.

A redução do resultado operacional será calculada diariamente.

c) Relativamente à alínea 2.2, secção **b) Extorsão cibernética.**

Em caso de sinistro que possa ser abrangido por esta cobertura, o segurador solicitará a documentação que julgar conveniente, incluindo:

- a documentação incluída na secção **2.1. Serviço de Resposta a Incidentes** deste anexo;
- a descrição do **incidente**, indicando entre outras coisas data, tipo e impacto conhecido;
- a notificação pela **entidade** da **ameaça de extorsão** à polícia ou a outra autoridade policial;
- a autorização do pagamento do resgate por um administrador, gerente (ou cargo equivalente) da **entidade**;

- O(s) documento(s) que comprove(m) o pagamento do resgate.

d) Relativamente à secção 2.2, alínea **c) Proteção de equipamentos**.

O segurador solicitará faturas pela reparação ou substituição de equipamentos informáticos afetados por um **incidente**.

O segurador assumirá o reembolso do valor, excluindo eventuais impostos aplicáveis, das faturas por si pagas, e mediante apresentação dos documentos comprovativos indicados na cobertura.

1.3 Responsabilidade tecnológica

Caso receba uma **reclamação** ou esteja sujeito a uma inspeção de dados, agradecemos que contacte o seu mediador de seguros.

De forma a dar seguimento ao processamento do ficheiro corretamente, a Hiscox solicitará, através do seu mediador, a documentação necessária à análise da cobertura da apólice. Entre outros, a **reclamação** escrita formal do lesado, documentação judicial ou procedimento administrativo, versão detalhada dos factos por parte do **segurado**, informação sobre o erro alegadamente cometido, etc.

Caso o **segurado** pretenda nomear um advogado ou perito para auxílio na sua defesa, deverá solicitar a autorização prévia por escrito à Hiscox, e fornecer-lhe o orçamento de honorários para a sua aprovação. O **segurado** pode designar, se desejar, mediante solicitação à Hiscox, qualquer um dos profissionais incluídos no **painel de especialistas** da Hiscox.

Consulte a apólice para conhecer os processos a seguir para cada cobertura e as autorizações a solicitar à Hiscox.

1.4 Fraude tecnológica

O **segurador** pode solicitar documentação de suporte relativa às perdas do segurado, que podem incluir, mas não se limitam a/ao:

- Relatório sobre a extensão das perdas e/ou despesas incorridas;
- Perdas resultantes de diferenças entre preços oficiais e preços alterados em resultado de um **ciberataque**;
- Faturas emitidas pelo seu operador de telecomunicações.

Quaisquer despesas que o **segurado** incorra em relação à prova das perdas cobertas pela seção de **fraude tecnológica**, serão suportadas pela **entidade** e não são cobertas por esta **apólice**.

Painel de Especialistas Hiscox

Serviço de Resposta a Incidentes	+351 211 219 400