



PROSEGUR

Documento de Apoio 3P às Condições Gerais de Compra

ÁREA DE GESTÃO DE MEIOS - COMPRAS.

1. Proprietário

Diretor Corporativo de Gestão de Meios

2. Sumário

Marco normativo que regula as condições aplicáveis a qualquer tipo de contrato ou pedido da Prosegur, na ausência de condições específicas acordadas entre as partes e consubstanciadas em contrato.

3. Elaboração y Aprovação

Elaborado por:	Área de Gestão de Meios - Compras			
Revisado por:	Área Legal Global			
Aprovado por:	Área Global de Compras	David Jose Gestal	Data:	23/06/2023
Substitui a:	DS/GLO/GdM/COM/01 DS/GLO/GdM/COM/06	Edição:	03 02	Data: 31/03/2023 31/05/2022

4. Documentos Associados

Código	Nome
NG/GLO/GdM/COM/01	Norma Geral 3P de Compras

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed.04 23/06/2023 Página 1
------------	--	---

5. DEFINIÇÕES

Para maior clareza e compreensão das presentes Condições Gerais, são estabelecidas as seguintes definições:

- **Prosegur:** Empresa do Grupo agindo como parte compradora e/ou contratante em cada Compra e/ou Contrato.
- **Filial** refere-se a uma empresa ou grupo de empresas registadas ou não, sob controlo comum. al como utilizado nesta definição, "controlo" (e as variantes utilizadas) significa o poder, direto ou indiretamente, de dirigir os interesses de outra empresa, quer como proprietária ou de outra forma.
- **Compra:** Transação em que o montante corresponde principalmente a aquisições de bens.
- **Contratação:** Transação em que o montante corresponde principalmente à aquisição de obras e/ou serviços e, portanto, à mão de obra. Tanto uma compra como uma contratação podem ter componentes de obras, bens e serviços. No desenvolvimento destas Condições, os termos de compra e contratação serão considerados termos equivalentes.
- **Pedido:** Documento vinculativo para as partes emitido pela Prosegur ao fornecedor em que são estabelecidos preços, prazos e condições para o fornecimento de um bem ou prestação de um serviço para o qual a compra ou contrato tenha sido previamente adjudicado. Por vezes, este documento é simultaneamente um contrato e um pedido de aquisição.
- **Contrato:** Acordo vinculativo entre as partes em que são estabelecidos preços, prazos e condições para a execução de uma obra, subcontratação ou prestação de um serviço.
- **Condições Gerais:** Documento que estabelece as bases para o processo de Compra de bens e/ou Contratação de obras e/ou serviços e que é aplicável a todo o Grupo Prosegur.
- **Fornecedor:** A entidade a quem foi concedido um Pedido.
- **Contratante:** A entidade a quem foi concedido um Contrato.
- **Condições Especiais:** Também denominado Pedido de Proposta. Qualquer documento que inclua todos os requisitos, de qualquer natureza, necessários para o Fornecedor/Contratante fornecer os bens ou realizar as obras e serviços da forma e qualidade exigidas.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 2
------------	--	--

6. CONDIÇÕES GERAIS DE COMPRA E CONTRATAÇÃO

6.1. Validade e prioridade da documentação contratual

6.1.1. As Condições Gerais serão dadas a conhecer aos Fornecedores/Contratantes no processo da gestão de Compras/Contratação e integrarão a documentação contratual estabelecida no Pedido/Contrato, em todos os seus termos e condições.

6.1.2. Estas Condições Gerais poderão ser complementadas com Condições Especiais e/ou os correspondentes Pedidos/Contratos gerados. Em caso de discrepância entre os documentos que compõem uma Compra/Contratação, o particular prevalecerá sobre o geral, sendo a ordem de prioridade a seguinte:

- Quaisquer alterações ao Pedido/Contrato, expressamente acordadas por escrito e posteriores à sua data de subscrição ou emissão.
- O Pedido/Contrato e a sua documentação anexa.
- Quaisquer alterações nas especificações técnicas solicitadas
- As especificações técnicas solicitadas.
- As alterações às Condições Especiais e/ou Gerais.
- As Condições Especiais.
- As Condições Gerais
- Os esclarecimentos feitos por escrito pelo Fornecedor/Contratante, após a sua oferta ter sido aceite pela Prosegur.

6.1.3. Não serão aceites outras Condições Gerais propostas pelo Fornecedor/Contratante para além das estabelecidas neste documento, a menos que sejam expressamente aceites, no todo ou em parte, pela Prosegur.

6.1.4. Quaisquer condições e especificações inseridas pelo Fornecedor/Contratante nas suas guias de remessa, faturas ou outros documentos trocados entre as partes, que contradigam as condições expressas estabelecidas no Pedido/Contrato, serão nulas e sem efeito.

6.1.5. Os contratos de obras e/ou serviços permanecem em vigor durante o período de execução das obras em conformidade com as disposições da documentação contratual. Se uma data de expiração tiver sido predeterminada e a duração dos trabalhos exceder essa data, o Contrato será tacitamente prorrogado por períodos mensais sucessivos, a menos que qualquer uma das partes avise por escrito com antecedência de pelo menos quinze dias antes da referida data de expiração ou de qualquer prorrogação deste tipo.

No entanto, o Contrato poderá incluir as cláusulas que serão aplicadas ao cumprimento dos prazos de execução e respetivas prorrogações.

6.2. Sistema de avaliação e homologação de Fornecedores

6.2.1. A Prosegur utiliza uma plataforma online gestionada por um fornecedor externo à Prosegur (GoSupply Advanced Applications, S.L., doravante "GoSupply"), para a pré-qualificação, avaliação e homologação preliminar dos seus Fornecedores/Contratantes. Para a qualificação e homologação definitiva de um Fornecedor/Contratante, é obrigatório o registo e participação do

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 3
------------	--	--

Fornecedor/Contratante no processo de análise de risco do Fornecedor implementado pela Prosegur através desta plataforma.

6.2.2. O Fornecedor/Contratante deve ser qualificado como adequado no processo de análise da Prosegur, antes do início de qualquer fornecimento de serviços, bens e/ou materiais nos termos destas Condições Gerais e/ou do respetivo Contrato/Pedido. Da mesma forma, o Fornecedor/Contratante garante e compromete-se a manter as condições aprovadas na referida análise durante todo o período estabelecido nas presentes Condições Gerais e/ou no Contrato/Pedido correspondente e, para o efeito, compromete-se a fornecer à Prosegur as informações e/ou documentação atualizada solicitada de acordo com os critérios estabelecidos pela Prosegur.

6.2.3. O Fornecedor/Contratante é informado e assume que a Prosegur fica excluída dos serviços prestados pela “GoSupply”, sendo responsabilidade do fornecedor desta plataforma os serviços de acesso e outras circunstâncias associadas ao registo na mesma. A Prosegur é apenas a destinatária das informações que o Fornecedor/Contratante inclui na plataforma.

6.2.4. Para completar o processo interno de pré-qualificação, avaliação e homologação preliminar, a Prosegur implementou o serviço de pré-qualificação, avaliação e homologação preliminar de Fornecedores/Contratantes, centrado na melhoria constante dos seus Fornecedores/Contratantes, para melhorar a sustentabilidade e qualidade dos bens e serviços comercializados à Prosegur. Este serviço de pré-qualificação, avaliação e homologação preliminar, de contratação direta entre os Fornecedores e a Prosegur é obrigatório e envolve o pagamento à Prosegur de um montante anual, que será designado em função do nível de faturação anual do Fornecedor/Contratante e das categorias de produtos e serviços a que dedica a sua atividade. Em qualquer caso, a Prosegur determinará a categoria atribuída ao Fornecedor/Contratante e o montante anual correspondente, que consiste em:

- Fornecedor autónomo: 59€ por ano + IVA
- Fornecedor básico: 99€ por ano + IVA
- Fornecedor padrão: 199€ por ano + IVA
- Fornecedor crítico: 299€ por ano + IVA

Estes montantes e/ou a categoria inicialmente atribuída ao Fornecedor/Contratante podem ser revistos e atualizados pela Prosegur em qualquer altura e a seu exclusivo critério, e o Fornecedor/Contratante compromete-se a aceitar os novos montantes e/ou a nova categoria atribuída assim que for comunicado pela Prosegur.

6.2.5. O Fornecedor/Contratante aceita que o pagamento dos montantes pelo serviço de pré-qualificação, avaliação e homologação preliminar dos Fornecedores seja efetuado à Prosegur, através de débito direto na mesma conta bancária que o Fornecedor/Contratante indique à Prosegur para que a Prosegur pague as faturas das obras, serviços ou fornecimento de bens e/ou materiais prestados ou entregues à Prosegur. Do mesmo modo, em caso de reembolso ou impossibilidade de pagamento de acordo com o acima exposto, a Prosegur terá o direito de deduzir e/ou compensar o montante correspondente às referidas prestações das faturas pendentes de pagamento ao Fornecedor/Contratante.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 4
------------	--	--

6.3. Obrigações e responsabilidades do Fornecedor/Contratante

6.3.1. O Fornecedor/Contratante compromete-se a realizar as obras, serviços e fornecimento de bens, de acordo com o estabelecido no Pedido/Contrato e/ou nos seus anexos e a cumprir todas as obrigações técnicas, administrativas, fiscais, de trabalho, legais e qualquer outra ligada à relação contratual.

6.3.2. O Fornecedor/Contratante deverá entregar toda a documentação exigida pela Prosegur no Pedido/Contrato, tanto em termos de tempo como qualquer outra informação ou documento de qualquer tipo que possa ser exigido pelas leis, normas ou regulamentos aplicáveis ao fornecimento, obra ou serviço.

6.3.3. O Fornecedor/Contratante, a pedido da Prosegur, deve fornecer prova documental do cumprimento das obrigações referidas nos pontos anteriores. A não apresentação ou insuficiência de tal prova documental constituirá uma grave violação das suas obrigações.

6.3.4. De acordo com a natureza do Pedido/Contrato, o Fornecedor/Contratante nomeará os responsáveis, no âmbito da sua organização, pelo fornecimento de bens e/ou contratação de obras e/ou serviços estabelecidos nas Condições Particulares, e comunicará essa nomeação ao respetivo Coordenador da Prosegur.

6.3.5. O Fornecedor/Contratante e, quando aplicável, os seus subcontratantes são responsáveis pelo pagamento atempado de salários, segurança social e qualquer outra compensação ou indemnização de natureza profissional ou de qualquer outra natureza que, por qualquer razão, os seus empregados devem receber e manter a Prosegur isenta de responsabilidade contra qualquer reclamação decorrente da violação desta obrigação.

6.3.6. O Fornecedor/Contratante e, quando aplicável, os seus subcontratantes, devem cumprir as normas legais em vigor e outras como as das Convenções Fundamentais da Organização Internacional do Trabalho relativas aos direitos dos trabalhadores e segurança social.

O Fornecedor/Contratante e, quando aplicável, os seus subcontratantes, devem cumprir todas as disposições relativas ao Ambiente, Prevenção de Riscos Profissionais e Segurança e Saúde em vigor e aplicáveis ao Pedido/Contrato, devem respeitar as políticas e procedimentos da Prosegur e, em qualquer caso, devem respeitar o Código de Ética e Conduta da Prosegur, que é publicado em espanhol e inglês nos seguintes links contidos no website da Prosegur:

- [Código Ético y de Conducta Prosegur - ES](#)
- [Code of Ethics and Conduct Prosegur – EN](#)
- [Código de Ética e Conduta da Prosegur - PT](#)

6.3.7. O Fornecedor/Contratante e, quando aplicável, os seus subcontratantes serão responsáveis e indemnizarão e isentarão a Prosegur e todo o Grupo Prosegur de danos diretos, indiretos e/ou consequentes, incluindo perda de negócio, danos à imagem ou perda de lucro, perda ou destruição de propriedade do primeiro e/ou de terceiros ou por morte, doença ou ferimento no pessoal do segundo e/ou de terceiros resultantes da realização pelo Fornecedor/Contratante e/ou, quando aplicável, pelos seus subcontratantes das suas obrigações contratuais ou legais. Esta responsabilidade incluirá honorários e custos legais, e os montantes dos Seguros subscritos nos termos da Cláusula 2.10 não constituirão um limite à sua responsabilidade.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 5
------------	--	--

6.3.8. O Fornecedor/Contratante e, quando apropriado, os seus subcontratantes serão responsáveis para com a Prosegur e todas as Empresas do Grupo Prosegur, por quaisquer danos diretos, indiretos e/ou consequentes, incluindo perda de negócio, danos à imagem e perda de lucro que ele/ela ou as pessoas pelas quais ele/ela são legal ou contratualmente responsáveis, podem causar à Prosegur ou às empresas do Grupo Prosegur danos, perdas ou destruição dos seus bens ou morte, doença ou ferimentos ao seu pessoal, e que sejam causados por uma ação ou omissão no cumprimento das obrigações derivadas do Pedido/Contrato pelo Fornecedor/Contratante e, quando apropriado, pelos seus subcontratantes ou pelo seu pessoal. Esta responsabilidade incluirá honorários e custos legais, e os montantes dos Seguros subscritos nos termos da Cláusula 2.10. não constituirão um limite à sua responsabilidade.

6.3.9. O Fornecedor/Contratante garante a indemnização da Prosegur contra eventuais reclamações dos empregados do Contratante envolvidos no cumprimento do Pedido/Contrato ou dos seus subcontratantes, que serão defendidos ou liquidados pelo Fornecedor/Contratante, que também suportará os custos de defesa e os montantes ou declarações objeto da liquidação ou contidos numa condenação final.

6.3.10. Da mesma forma, o Fornecedor/Contratante garante a isenção da Prosegur de qualquer sanção administrativa ou de qualquer outro tipo que possa ser imposta, direto ou indiretamente, da execução do Pedido/Contrato.

6.3.11. Em caso de não cumprimento pelo Fornecedor/Contratante das obrigações indicadas nos parágrafos anteriores, a Prosegur terá o direito de deduzir na seguinte ou seguintes certificações/faturas os montantes pagos pela Prosegur de tais reclamações ou sanções não cumpridas pelo Fornecedor/Contratante, bem como os custos de defesa assumidos pela Prosegur como resultado do não cumprimento.

6.3.12. O regime de responsabilidade legal referido neste documento não é aplicável às responsabilidades pelas quais cada uma das Partes pode ser obrigada a cumprir, de acordo com a lei de prevenção de riscos profissionais ou os regulamentos aplicáveis nesta área e os seus regulamentos de aplicação, caso em que será aplicado o regime legal e regulamentar estabelecido para tal responsabilidade.

6.3.13. A responsabilidade estabelecida na cláusula 6.3.8 será ampliada, e será igualmente exigível, durante o Período de Garantia.

6.3.14. Nos casos em que a condição de Fornecedor/Contratista seja detida por uma joint venture temporária, ou por qualquer entidade sem personalidade jurídica própria que não seja a dos seus componentes, a responsabilidade que possa derivar deste Pedido/Contrato contra a Prosegur será solidária de todas as pessoas ou empresas que façam parte das empresas em questão.

6.3.15. Em consequência do exposto, e de acordo com as disposições dos artigos 1.137 e 1.144 do Código civil espanhol, a Prosegur poderá tomar medidas, indistinta e individualmente, contra qualquer uma das pessoas singulares ou coletivas que constituem a joint venture temporária ou a entidade sem personalidade jurídica, para exigir o cumprimento de todas as obrigações decorrentes do Pedido/Contrato.

6.3.16. A Prosegur, não será em caso algum e em nenhuma circunstância responsável por danos diretos, indiretos e/ou consequentes que o Fornecedor/Contratante possa sofrer, derivados direta ou indiretamente da execução do Pedido/Contrato, incluindo, mas não limitado a perdas de utilização, perdas de lucros e interrupções de negócio.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 6
------------	--	--

6.3.17. A Prosegur incentiva a contratação de fornecedores que atendam a critérios de sustentabilidade e responsabilidade social corporativa, que promovam e subscrevam os objetivos de desenvolvimento sustentável das Nações Unidas e que possuam algum tipo de certificação ESG, seja por adesão a Índices sustentáveis ou através de certificações na matéria. A Prosegur promove e incentiva os fornecedores e associados com os quais trabalha a aceitar os seguintes princípios:

- Respeitar as leis aplicáveis de todas as jurisdições onde o Grupo Prosegur está presente
- Funcionar como um empregador socialmente responsável que está comprometido com:
 - pagar um salário digno aos seus empregados sempre acima do salário mínimo Interprofissional
 - respeitar a prevenção do trabalho infantil e do trabalho forçado,
 - respeitar a não discriminação e a igualdade de oportunidades,
 - respeitar a liberdade de associação, o direito à negociação coletiva e a eliminação de horários excessivos de trabalho.
- Oferecer um ambiente de trabalho seguro, em conformidade com todas as normas de segurança e saúde no trabalho.
- Utilizar práticas sustentáveis que respeitem o ambiente, exigindo dos seus fornecedores compromissos em:
 - Utilização de energias renováveis
 - Ações destinadas a reduzir as emissões e os poluentes para prevenir as alterações climáticas
 - Respeito pela biodiversidade
 - Utilização sustentável dos recursos naturais
 - Redução de resíduos
- Respeite o Código de Ética e Conduta da Prosegur.

6.4. Obrigações e responsabilidades da Prosegur

6.4.1. O pagamento dos bens, obras e/ou serviços nos preços e condições estabelecidos no pedido/contrato de acordo com o estabelecido nas cláusulas 2.6 e 2.7.

6.5. Cessão do Pedido/Contrato e subcontratação

6.5.1. As obras, bens e serviços objetos deste Pedido/Contrato não poderão ser delegados ou subcontratados, total ou parcialmente, sem a autorização prévia por escrito da Prosegur, caso em que o subcontratante será expressamente sub-rogado em todas as condições deste documento.

6.5.2. Para obter autorização prévia para subcontratação, o Fornecedor/Contratante deverá exigir do Subcontratante toda a documentação prevista no Pedido de Proposta e nestas Condições Gerais, bem como o seu compromisso escrito de cumprimento de cada uma das cláusulas do Pedido/Contrato e a sua documentação anexa, todos os quais devem ser entregues imediatamente à Prosegur.

6.5.3. No caso de utilização de subcontratantes, o Fornecedor/Contratante continuará a ser o principal responsável para com a Prosegur pelo cumprimento das obrigações decorrentes do Pedido/Contrato, mesmo no caso de bens, obras e/ou serviços fornecidos/prestados diretamente pelo subcontratante autorizado. Independentemente disto, a Prosegur pode, a qualquer altura, inspecionar e controlar o trabalho do subcontratante e o cumprimento das suas obrigações.

6.6. Condições económicas e impostos

6.6.1. Os preços indicados no Pedido/Contrato e/ou nos seus anexos, devem ser entendidos como fixos e não revisíveis até o cumprimento total e correto do Pedido/Contrato, exceto indicação expressa em contrário, e devem incluir todos os impostos, encargos, imposições, taxas e direitos, presentes ou futuros, exceto o Imposto sobre o Valor Acrescentado ou imposto semelhante, que deve aparecer separadamente como um item independente.

6.6.2. Como exceção adicional ao parágrafo anterior e no caso de ser aplicado retenção na fonte de acordo com a Legislação aplicável, o montante da retenção correspondente à Legislação aplicável não deve ser entendido como incluído no preço. Portanto, o Fornecedor deverá pagar o montante total da fatura ao Cliente e pagar adicionalmente o montante da retenção correspondente à Administração Fiscal do Fornecedor. No caso de redução da retenção na fonte devido à aplicação de uma Convenção para Evitar a Dupla Tributação entre os dois países, o Cliente deverá, a pedido do Fornecedor, entregar, antes de qualquer pagamento, um certificado de residência fiscal em conformidade com o mencionado, para que o Fornecedor possa pagar o montante retido na fonte aplicável de acordo com a referida Convenção. O Fornecedor, uma vez pago o imposto retido na fonte, deverá fornecer ao Cliente um certificado de pagamento da retenção.

6.6.3. Os bens, obras e/ou serviços não incluídos no Pedido/Contrato não serão pagos se a sua execução não tiver sido previamente oferecida pelo Fornecedor/Contratante, por escrito, e aceite, também por escrito, pela Prosegur, a correspondente alteração do Pedido/Contrato.

6.6.4. O pagamento de adiantamentos por conta será realizado, de acordo com o caso, através da apresentação da correspondente garantia bancária pelo mesmo montante a pagar, irrevogável e sem reservas, conjunta e solidariamente, à primeira solicitação e com renúncia aos benefícios de excusão e divisão, e desde que tal adiantamento seja previsto no Pedido/Contrato correspondente.

6.6.5. O pagamento do preço do Pedido/Contrato não implicará qualquer renúncia aos direitos da Prosegur previstos.

6.6.6. O Fornecedor/Contratante será responsável por qualquer diferença no frete, transporte, impostos ou quaisquer outros gastos resultantes do não cumprimento das instruções de envio ou de qualquer outra das condições estabelecidas ou aplicáveis ao Pedido/Contrato.

6.6.7. Todos os impostos aplicados sobre as transações comerciais referidas nestas Condições Gerais, serão a cargo das partes, em conformidade com a lei. O contribuinte do imposto é responsável, em cada caso, pela correta tributação das suas obrigações fiscais.

6.7. Forma de pagamento

6.7.1. Todos os pagamentos serão realizados no prazo de 60 dias de calendário da data da fatura, exceto se acordado entre as partes um prazo diferente ou se for estabelecido outro período de pagamento por imperativo legal. As faturas apenas serão pagas se a Prosegur possuir documentos que demonstrem a receção adequada dos serviços realizados de acordo com as disposições do Pedido/Contrato. No caso de fornecimento de bens, aplica-se o estabelecido nos Incoterms e/ou as condições de entrega incluídas no Pedido.

O meio de pagamento habitual é por transferência bancária ou confirmação.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 8
------------	--	--

6.7.2. As outras condições de pagamento estarão perfeitamente definidas no Documento de Condições Especiais, bem como no Pedido/Contrato.

6.8. Aceitação do Pedido/Contrato

6.8.1. Aceitação do Contrato: A assinatura do Contrato pelas Partes será considerada a sua total aceitação.

6.8.2. Aceitação do Pedido: A assinatura ou aviso de receção como sinal de aceitação do Pedido pelo Fornecedor/Contratante à Prosegur. Em qualquer caso, a simples execução do Pedido pelo Fornecedor implica a aceitação implícita do mesmo pelo Fornecedor e exclui qualquer exceção não aceite por escrito pela Prosegur.

6.9. Prazos de entrega e execução

6.9.1. O prazo de entrega/execução estabelecido no Pedido/Contrato deverá ser firme e deve ser realizado de acordo com as quantidades, datas e locais especificados nos programas de entrega/execução definidos e fornecidos pela Prosegur.

6.9.2. Em caso de atraso no prazo de entrega/execução estabelecido, a Prosegur poderá aplicar as sanções estabelecidas e/ou, quando aplicável, rescindir o Pedido/Contrato de acordo com as disposições da cláusula 2.16.

6.9.3. A Prosegur pode alterar os prazos de entrega/execução ou solicitar a suspensão temporária das entregas programadas. Para isto, buscará o acordo correspondente e poderá solicitar o ajuste necessário do Pedido/Contrato.

6.10. Garantia

6.10.1. As Garantias que, dependendo das características do bem, obra e serviço, podem ser estabelecidas pela Prosegur são as seguintes:

Garantia do fiel cumprimento e dos bens, obras e/ou serviços para o fim requerido. Será estabelecido pelo Fornecedor/Contratante para garantir o cumprimento de todas as suas obrigações contratuais de acordo com o Pedido/Contrato, desde a altura da aceitação/assinatura do Pedido/Contrato, até a receção definitiva pela Prosegur dos bens, obras e /ou serviços requeridos. A exigência ou não da referida Garantia será estabelecida no Pedido de Oferta e/ou no Pedido/Contrato correspondente.

A referida Garantia será estabelecida através do Modelo de Garantia do Anexo II (emitido por um banco com uma classificação mínima de BBB- da Standard & Poor ou aprovado pelo departamento de Tesouraria da Prosegur) ou por um seguro caução (emitido por uma seguradora com uma classificação mínima de BBB- da Standard & Poor ou aprovado pelo departamento de Seguros da Prosegur) ou por uma retenção direta na fatura.

6.10.2. O Fornecedor garante que, no caso de fornecimento de bens, estes são da sua plena propriedade, adequados ao fim destinado e de primeira qualidade e primeira utilização, e que cumprem os requisitos de segurança e qualidade especificados no Pedido. O Contratante garante que a realização das obras e/ou serviços cumpre os requisitos de segurança e qualidade especificados no Contrato. O Fornecedor/Contratante também garante a conformidade com a legislação correspondente em vigor, bem como da própria regulamentação da Prosegur, e que cumprirá os programas de trabalho/execução estabelecidos.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 9
------------	--	--

6.10.3. O Fornecedor/Contratante, também garante que os bens, obras e serviços são isentos de taxas e encargos a favor de terceiros, livres de defeitos e adequados para a sua comercialização/utilização, bem como que têm as patentes, licenças e outros direitos de propriedade industrial/intelectual necessários para a realização do objeto do Pedido/Contrato.

6.10.4. Retenções de Garantia: As retenções para garantia serão estabelecidas no Pedido/Contrato.

6.10.5. O Período de Garantia dos bens, obras e/ou serviços fornecidos/realizados pelo Fornecedor/Contratante será estabelecido no Pedido/Contrato. Caso contrário, será:

Para bens, 12 meses a partir da data de entrada em serviço ou 24 meses a partir da data de receção no destino ou de disponibilização, de acordo com o Incoterm aplicável, o que ocorrer primeiro, se o Fornecedor tiver condições de maior duração, estas deverão ser cumpridas.

Para contratos de obras e/ou serviços, 12 meses a partir da data de assinatura do registo de receção provisória.

Outros prazos poderão ser exigidos quando previsto pela legislação aplicável e/ou natureza específica do fornecimento, obra e/ou serviço em questão.

6.10.6. Durante o período de garantia, o Fornecedor/Contratante será responsável por todas as violações e/ou danos, sem prejuízo do disposto na Cláusula 6.3.16 e seguintes, decorrentes do não cumprimento ou cumprimento defeituoso ou inadequado por parte do Fornecedor/Contratante das condições contratuais aplicáveis ao fornecimento, obra ou serviço, bem como, quando aplicável, por defeitos na qualidade dos materiais utilizados.

O período de garantia será interrompido pelo tempo utilizado nas respetivas reparações ou substituições, que por sua vez serão garantidas, após a sua conclusão, pelo mesmo período de tempo que o da garantia inicial estabelecida.

6.10.7. O não cumprimento ou cumprimento defeituoso ou inadequado do fornecimento, obra e/ou serviço, ou defeito na qualidade em questão, quando o Fornecedor/Contratante não tiver realizado as ações corretivas pertinentes, ou quando não demonstrar a diligência adequada na resolução dos problemas levantados., pode dar origem a: à retenção pela Prosegur de pagamentos pendentes; à execução da(s) garantia(s) económica(s) e/ou bancária(s) e ainda à rejeição total ou parcial do fornecimento, obra ou serviço executado, sendo neste caso a exigência da devolução dos montantes pagos sem que tal circunstância possa ser causa de qualquer reclamação do Fornecedor/Contratante.

6.10.8. A Prosegur deduzirá, quando aplicável, quaisquer sanções aplicáveis das faturas pendentes de pagamento ao Fornecedor/Contratante.

Do mesmo modo, para compensar as suas próprias despesas e custos derivados da contratação com terceiros para a reparação ou execução do que não foi cumprido ou incorretamente cumprido pelo Fornecedor/Contratante, e por qualquer outra dívida que o Fornecedor/Contratante mantenha com a Prosegur, poderá deduzir tais montantes das faturas pendentes de pagamento ao Fornecedor/Contratante.

O pagamento ou dedução de tais sanções e despesas não isentará o Fornecedor/Contratante de nenhuma das suas outras obrigações e responsabilidades nos termos do Pedido/Contrato.

6.10.9. A dívida do Fornecedor/Contratante para com a Prosegur é automaticamente considerada como qualquer montante reclamado a esta última, devido a descobertos ou não cumprimentos do

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 10
------------	--	---

Fornecedor/Contratante em relação a salários, segurança social, obrigações fiscais e qualquer outro montante que possa ser reclamado à Prosegur de acordo com os termos legais ou regulamentares.

6.10.10. Quaisquer deduções feitas de acordo com os pontos anteriores, serão totalmente independentes do montante depositado, no seu caso, como Garantia.

6.10.11. No caso do Fornecedor pretender deixar de fabricar o produto objeto do Pedido de Compra, deverá enviar uma notificação escrita com aviso de receção ao Departamento de Compras da Prosegur com seis meses de antecedência à data em que pretende deixar de fabricar o produto. Esta notificação deve conter, pelo menos: (i) identificação do produto; (ii) identificação dos Pedidos de Compra afetados; (iii) lista dos países afetados; e (iv) data em que o produto deixa de ser fabricado.

A partir da emissão do Pedido de Compra, o Fornecedor garante o atendimento técnico adequado e a existência de sobresselentes durante um período mínimo de dez (10) anos em todos os países afetados e a partir da data em que o produto deixa de ser fabricado. O preço das peças sobresselentes ou produtos e serviços será oferecido à Prosegur por um preço máximo equivalente ao contratual dos produtos substituídos; e com o mesmo nível de conformidade e requisitos técnicos solicitados pela Prosegur para o produto a ser reparado ou substituído.

Como garantia deste compromisso, a Prosegur reserva-se o direito de exigir ao Fornecedor uma garantia bancária na primeira solicitação, de acordo com o modelo de Garantia do Anexo II deste documento.

O não cumprimento da referida garantia ou a capacidade de cumprir pelo Fornecedor, terá os seguintes efeitos:

- Retenção de qualquer pagamento pendente pela Prosegur
- Aplicação da garantia bancária
- Cancelamento total ou parcial das Ordens de Compra em curso, sem que implique qualquer compensação a favor do fornecedor.
- Direita da Prosegur de reclamar todos os danos, perdas, custos e despesas (incluindo honorários legais) incorridos para cumprir as obrigações não cumpridas do Fornecedor pelos seus próprios meios ou através de terceiros.

Para além, o Fornecedor, a seu próprio custo, deverá disponibilizar à Prosegur todos os desenvolvimentos de software feitos à medida, incluindo código-fonte, código-objeto, manuais e qualquer outra informação relevante.

6.11. Seguros

6.11.1. Sem prejuízo da sua responsabilidade, estabelecida no Pedido/Contrato, e sem que esta cláusula a limite, o Fornecedor/Contratante deverá assinar e manter em vigor, a expensas próprias durante todo o período de duração do Pedido/Contrato, e com empresas de reconhecida solvência financeira, os seguros descritos abaixo. As coberturas e montantes cobertos por esse seguro nunca serão inferiores aos obrigatórios pelas leis em vigor. A sua manutenção não alterará as obrigações de isentar a Prosegur estabelecidas pelo Pedido/Contrato.

6.11.1.1 Contratos de Obras e/ou Serviços.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04 23/06/2023 Página 11
------------	--	---

a) Seguro de acidentes de trabalho e de doença para todos os colaboradores designados para os Trabalhos, de acordo com a lei aplicável, incluindo as leis do Estado de origem dos colaboradores expatriados.

b) Seguro de construção/edificação, montagem e danos em equipamentos de construção alugados, arrendados ou propriedade do Contratante, com um limite não inferior ao seu valor de substituição. No caso do seguro de construção, será necessário contratar a cobertura adicional de adjacentes e pré-existentes. Em caso de reclamação, e independentemente da causa, o Contratante renuncia expressamente ao direito de recurso contra a Prosegur por qualquer dano ou prejuízo sofrido pelos referidos bens, comprometendo-se a notificar por escrito as suas empresas seguradoras desta renúncia de recurso.

c) Seguro de responsabilidade civil das empresas, incluindo, entre outros, responsabilidade do empregador e profissional, produtos, remoção de produtos, pós-trabalhos e poluição e contaminação com uma cobertura igual ao montante das obras/serviços contratados nas Condições Especiais de cada Contrato e que no mínimo, será dos montantes padrão indicados no Anexo I.

No caso de apólices de responsabilidade civil, se estas forem contratadas no âmbito temporário de cobertura, o Contratante deverá manter as referidas apólices em vigor até o termo do período de garantia ou responsabilidade legal. Se as apólices forem subscritas no âmbito temporário da cobertura da reclamação, o Contratante deverá manter as apólices em vigor durante pelo menos dois (2) anos, após o termo do período da garantia ou responsabilidade legal.

Estes seguros incluirão a Prosegur como um segurado adicional, sem perder a sua condição de terceiro.

d) Se for necessária a utilização de automóveis, máquinas automotoras, máquinas industriais, aviões ou embarcações para a realização da obra, deverá haver um seguro de responsabilidade civil, com um limite que será fixado por reclamação nas Condições Especiais de cada Contrato e que, pelo menos, será o dos montantes padrão que constam do Anexo I.

Caso necessária a contratação de embarcações, será exigida a cobertura de proteção e indemnização (proprietário/fretador) com um clube do Grupo Internacional.

Independentemente do acima exposto, o Contratante poderá subscrever o seguro adicional que considerar necessário para a cobertura total das suas responsabilidades nos termos do Contrato.

6.11.1.2 Pedidos de Bens.

a) Seguro de acidentes de trabalho e de doença para todos os colaboradores designados para os trabalhos, de acordo com a lei aplicável, incluindo as leis do Estado de origem dos colaboradores expatriados.

b) Seguro de transporte dos bens e/ou equipamentos objeto do Pedido, de acordo com as condições de compra e do Incoterm acordado nas Condições Especiais.

c) Seguro de responsabilidade civil empresarial, incluindo, mas não limitando, a responsabilidade do empregador, profissional, produtos, recolha de produtos, pós-trabalho, poluição e contaminação com uma cobertura igual ao montante dos bens adquiridos que, no mínimo, será o montante determinado nas Condições Especiais de cada Pedido.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 12
------------	--	---

No caso de apólices de responsabilidade civil, se forem contratadas no âmbito da cobertura temporária, o Fornecedor deverá manter as referidas apólices em vigor até o termo do período de garantia ou responsabilidade legal. Se as apólices forem contratadas no âmbito temporário da cobertura da reclamação, o Fornecedor deverá manter as apólices em vigor durante pelo menos dois (2) anos após o termo do período da garantia ou responsabilidade legal.

Estes seguros incluirão a Prosegur como um segurado adicional, sem perder a sua condição de terceiro.

Independentemente do acima exposto, o Fornecedor poderá subscrever o seguro adicional que considerar necessário para a cobertura total das suas responsabilidades nos termos do Pedido.

6.11.2. Antes da entrega dos bens ou do início das obras/serviços, o Fornecedor/Contratante deverá entregar à Prosegur um certificado do seguro contratado. Este certificado será incorporado ao Contrato/Pedido como um Anexo. A não entrega do certificado autorizará a Prosegur a rescindir o Contrato/Pedido por motivos imputáveis ao Fornecedor/Contratante.

6.11.3. A Prosegur, a qualquer altura, poderá solicitar ao Fornecedor/Contratante a entrega do original das apólices, ou cópias autenticadas, das apólices de seguro que contratou, bem como recibos ou comprovantes atualizado do pagamento dos prémios correspondentes. O Fornecedor/Contratante tem a obrigação de entregar tudo o que antecede em um prazo não superior a sete (7) dias.

6.11.4. O Fornecedor/Contratante tem a obrigação de informar a Prosegur por escrito sobre qualquer incidente que afete a validade e as condições dos seguros contratados.

6.11.5. Em qualquer caso, a Prosegur nunca será responsável por limites, franquias ou limitações nas condições das políticas do Fornecedor/Contratante.

6.11.6. Em todos os seguros referidos na cláusula 2.10.1., será incluída uma menção que isenta a seguradora de responsabilidade e não repetição contra a Prosegur.

6.11.7. O Fornecedor/Contratante, sob a sua exclusiva responsabilidade, exigirá, quando aplicável, que os subcontratantes mantenham a mesma responsabilidade e apólices de seguro exigidas ao Fornecedor/Contratante. Isto não isentará o Fornecedor/Contratante da sua responsabilidade para com a Prosegur.

6.11.8. Dependendo do âmbito ou natureza do Contrato/Pedido, a Prosegur reserva-se o direito de:

- Solicitar limites por reclamação superiores aos estabelecidos no Anexo I,
- Solicitar cobertura ou seguros adicionais não incluídos no ponto 2.10.1

6.12. Sanções por não conformidade

6.12.1. As sanções ou penalidades por não cumprimento por parte do Fornecedor/Contratante serão estabelecidas nas Condições Especiais e no Pedido/Contrato e, na falta, serão sujeitas à legislação comercial em vigor.

6.12.2. No caso de não estarem especificadas nas condições especiais do Pedido/Contrato, serão aplicadas as seguintes sanções quando houver uma violação objetiva das obrigações do Fornecedor/Contratante:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 13
------------	--	---

- Entrega de Materiais: Sanção de até 10% semanal
- Atraso na execução de obras ou prestação de serviços: Sanção de até 5% semanal.

6.13. Cessão de direitos e créditos

6.13.1. Os Pedidos/Contratos e os créditos e/ou faturas decorrentes destas relações jurídicas não poderão ser cedidos, total ou parcialmente, ou penhorados sobre elas, sem a prévia e expressa autorização da Prosegur, por escrito, de acordo com a forma estabelecida.

6.13.2. A Prosegur poderá ceder, sem o consentimento prévio do Fornecedor/Contratante, parte ou a totalidade dos seus direitos e obrigações ao abrigo do Pedido/Contrato a favor de qualquer empresa do Grupo Prosegur ou como consequência de qualquer transação societária que envolva uma sucessão, total ou parcial, dos direitos e obrigações correspondentes.

6.14. Inspeções/Ativações

6.14.1. O Fornecedor/Contratante deverá realizar, por sua conta e risco, as inspeções necessárias antes da entrega dos bens, obras ou serviços para garantir que todos os requisitos especificados no Pedido/Contrato são cumpridos.

Com o objetivo de acelerar as disposições para o cumprimento do prazo de entrega, o Fornecedor deve ter um sistema de controlo para monitorizar os seus fornecedores de materiais, componentes e serviços que afetam o(s) bem(s) objeto do Pedido.

O Fornecedor/Contratante deverá inspecionar, através do Organismo de Controlo competente, os bens sujeitos a requisitos legais (regulamento técnico, segurança, ambiente, etc.) e/ou conforme especificado nas condições contratuais do Pedido/Contrato.

6.14.2. A Prosegur reserva-se o direito de realizar inspeções dos bens objeto do Pedido/Contrato e exigir quaisquer testes necessários, que serão por conta do Fornecedor, tanto nas instalações do Fornecedor como nas dos seus fornecedores.

Para isto, a PROSEGUR nomeará inspetores que terão livre acesso às oficinas e processos de fabrico, sem que esta inspeção diminua a responsabilidade do Fornecedor.

6.14.3. O Fornecedor/Contratante realizará revisões semestrais das instalações ou oficinas temporárias nas instalações da Prosegur ou dos seus clientes. O Fornecedor/Contratante deverá informar a Prosegur sobre o resultado destas inspeções e revisões.

6.14.4. Quando o Pedido/Contrato exigir a entrega de documentação (planos, especificações, etc.) à Prosegur, esta deverá ser previamente assinada pelo Fornecedor/Contratante como aprovação. A Prosegur reserva-se o direito de verificar a veracidade da documentação e informações fornecidas pelo Fornecedor/Contratante onde está localizada ou onde a Prosegur assim o indique ou solicite. Para este efeito, a Prosegur poderá nomear inspetores que terão livre acesso à documentação de apoio sem que esta inspeção diminua a responsabilidade do Fornecedor/Contratante.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04 23/06/2023 Página 14
------------	--	---

6.15. Entrega e envio de bens

6.15.1. Todos os bens fornecidos devem estar devidamente embalados para evitar qualquer dano. A Prosegur não aceitará qualquer taxa de embalagem caso não tenha sido previamente acordado. Os bens de Pedidos/Contratos diferentes não devem ser embalados em conjunto.

6.15.2. Todos os envio devem ser acompanhados por uma guia de entrega ou comprovante de entrega indicando a quantidade, descrição do produto, número do Pedido/Contrato, referência do Fornecedor/Contratante e lista de pacotes, com a distribuição do documento de acordo com o especificado no Pedido/Contrato e/ou Condições Especiais.

6.15.3. Todos os pacotes serão marcados externamente com o destino da mercadoria e o número do Pedido/Contrato correspondente, bem como indicações para manuseio ou precauções a serem tomadas nos casos necessários.

6.15.4. Para os bens que pela sua natureza são entregues em embalagens discretas (por exemplo, produtos de laboratório), o Fornecedor deve cumprir as seguintes instruções:

- a) Cada embalagem deve ser identificada com o número do lote, fabrico e data
- b) Os bens correspondentes a mais de dois lotes não serão incluídos na mesma entrega, a menos que previamente notificado pelo Fornecedor à Prosegur, e aceites por escrito pela Prosegur.
- c) O Fornecedor notificará as limitações de validade do bem, quando existam, indicando nas embalagens a data de validade de utilização dos bens.
- d) As normas de identificação, marcação, transporte e manuseamento estabelecidas na ficha de segurança e as específicas para mercadorias perigosas.

6.15.5. Para os bens que pela sua natureza sejam entregues em tanques, o Fornecedor deverá cumprir e fazer cumprir o seguinte:

- a) As obrigações e responsabilidades do remetente e do transportador, tanto na contratação como nas tarefas de carga, seguem as disposições da legislação aplicável (Lei de Regulação do Transporte Terrestre, Acordo ADR, etc.).
- b) O transportador assume a execução das tarefas de carregamento de material nas instalações da Prosegur.
- c) O transportador é obrigado a cumprir rigorosamente as normas do centro de carga (tanto em aspeto operacionais como de segurança).
- d) O Fornecedor será sempre responsável para com a Prosegur e para com terceiros por quaisquer danos que possam ser causados durante as atividades de carregamento no centro de carga (ação negligente ou inadequada).
- e) Antes de facilitar o acesso ao transporte para as instalações, o Fornecedor deve justificar à Prosegur, no local de entrega, que os transportes MMPP têm a seguinte documentação em vigor:

- Seguro(s)
- ITV
- Carta de condução e ADR do condutor
- Certificado ADR para trator e tanque
- EPI do condutor
- Painéis laranja e etiquetas de perigo.
- Guia de remessa ADR
- EPI a ser utilizado pelo condutor de acordo com os regulamentos em vigor.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 15
------------	--	---

6.15.6. A simples receção pela Prosegur de uma remessa ou expedição de mercadorias do Fornecedor não será considerada como aceitação final da mesma, que será sujeita a revisão posterior. A Prosegur tem o direito de reclamar por defeitos e/ou deficiências na qualidade ou quantidade, etc., e o Fornecedor deve tomar as medidas necessárias para satisfazer tais reclamações.

6.15.7. Para a entrega do fornecimento, será aplicado o Incoterm (última edição) definido nas Condições Especiais e no Pedido correspondente.

6.15.8. A Prosegur reserva-se o direito de devolver os bens, por conta do Fornecedor, em caso de não conformidade com as especificações e quantidades solicitadas.

6.16. Receção de obras, bens e/ou serviços

6.16.1. Receção Provisória: Uma vez concluídas as obras e/ou serviços, entregue toda a documentação exigida, se a execução foi correta, com todos os testes e ensaios de instalação realizados com sucesso, a Prosegur elaborará um relatório de receção provisório indicando se as condições estabelecidas no Pedido/Contrato relativamente aos trabalhos efetivamente executados, datas de disponibilidade, qualidade, funcionamento correto e quaisquer outras observações foram ou não cumpridas. A partir da assinatura deste documento provisório, o período de garantia estabelecido entrará em vigor. O documento provisório deverá ser assinado em aceitação pelo Contratante.

6.16.2. Se as obras e/ou serviços executados apresentarem quaisquer defeitos, a Prosegur dará ao Contratante um prazo para os corrigir. Se tal não for realizado no prazo indicado, a Prosegur poderá realizá-lo por si ou por terceiros, cobrado ao montante retido como garantia, ou cobrado ao Contratante pelo montante das obras e/ou serviços não cobertos pela garantia retida.

6.16.3. Receção final: Após o período de garantia estabelecido para as obras e/ou serviços ter expirado e desde que não haja reclamações da Prosegur pendentes de resolução pelo Contratante, a receção final das obras e/ou serviços terá lugar. A Prosegur é obrigada a reembolsar ao Contratante o montante, se existir, dos fundos de garantia e reparação não afetados a pagamentos às suas custas.

6.16.4. O Contratante deverá refazer, às suas próprias custas, os trabalhos defeituosos devido a erros ou omissões do Contratante. Para além, os custos de reparação, alteração ou substituição dos materiais necessários para corrigir tais erros ou omissões serão à suas custas.

6.16.5. A entrega de bens, obras e serviços e a disponibilização do documento de entrega ou guia de entrega correspondente não implica que a Prosegur tenha aceite a qualidade das obras, bens e/ou serviços entregues. Independentemente dos períodos de garantia especificados para cada produto, obra ou serviço, a Prosegur tem quinze (15) dias de calendário para verificar a qualidade das obras, bens e/ou serviços entregues e para os devolver, por conta do Fornecedor/Contratante, no caso de não cumprirem as especificações de qualidade ou técnicas exigidas no Pedido/Contrato.

6.16.6. Caso a entrega de bens, obras e/ou serviços não tenha sido realizada em sua totalidade, a Prosegur apenas será obrigada a pagar ao Fornecedor/Contratante o preço das obras, bens e/ou serviços que tenham sido corretamente entregues e aceites pela Prosegur. Isto sem prejuízo do direito da Prosegur de exigir o cumprimento por parte do Fornecedor/Contratante da sua obrigação de entrega das outras obras, bens e/ou serviços ou o cancelamento do Pedido/Contrato em relação aos mesmos e, em qualquer caso, de ser indemnizada por quaisquer danos sofridos.

6.17. Rescisão do Pedido/Contrato

6.17.1. O Pedido/Contrato será rescindido pela sua cessação ou expiração.

6.17.2. Rescisão do Pedido/Contrato por causa do Fornecedor/Contratante.

6.17.2.1 Para além dos estabelecidos por lei, a Prosegur reserva-se o direito de rescindir o Pedido/Contrato pelas razões abaixo indicadas, a título de exemplo e sem limitação:

a) Venda ou transferência inter vivos ou mortis causa da empresa do Fornecedor/Contratante ou a sua transformação noutra pessoa coletiva, por meios legalmente estabelecidos, sem a aprovação escrita da Prosegur.

b) Não cumprimento pelo Fornecedor/Contratante de qualquer uma das cláusulas ou obrigações contidas nas presentes Condições Gerais, Pedido/Contrato ou em qualquer dos documentos contratuais assinados pelas partes.

c) Alcançadas as sanções máximas aplicáveis, tal como estabelecidas no Pedido/Contrato.

d) Não cumprimento da legislação em vigor, pelo Fornecedor/Contratante.

e) Existência de embargos e retenção de créditos decretados por órgãos judiciais ou administrativos de natureza executória (Agência do Estado, Agência Fiscal, Segurança Social, etc.) ou a dissolução da empresa Fornecedor/Contratante.

f) Mais de 20% das obras, bens e serviços pendentes de execução/entrega, após a finalização do prazo estabelecido no Pedido/Contrato.

g) Em caso de reclamação ou acidente que cause danos a pessoas, bens ou ambiente.

h) Existência de imprecisões graves nas informações fornecidas pelo Fornecedor/Contratante, nomeadamente no que diz respeito à qualidade, prevenção de riscos profissionais, segurança e saúde, sistemas de gestão ambiental, condições e cumprimento dos requisitos de trabalho.

i) Não cumprimento das normas de ética e conduta da Prosegur.

j) Violação das obrigações de confidencialidade.

k) Quando detetado um caso de conflito de interesses entre o Fornecedor/Contratante e qualquer colaborador da Prosegur e tal situação não tenha sido previamente comunicada e expressamente autorizada.

l) Quando o Fornecedor/Contratante, os seus acionistas ou diretores estão envolvidos em casos de fraude, corrupção ou qualquer outro tipo de crime.

6.17.2.2 Quando ocorrer qualquer das causas acima referidas, o Pedido/Contrato será rescindido e sem efeito a partir da data em que a Prosegur comunicar a sua decisão a este respeito ao Fornecedor/Contratante ou, quando apropriado, aos seus sucessores por título.

6.17.2.3 Nos casos em que o Pedido/Contrato for rescindido, a Prosegur poderá adotar todas ou algumas das seguintes medidas:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 17
------------	--	---

- a) Suspender os pagamentos pendentes
- b) Executar as garantias que o Fornecedor/Contratante estabeleceu.
- c) Conservar em caução os bens e elementos do Fornecedor/Contratante que se encontravam na posse da PROSEGUR.

6.17.3. Rescisão do Pedido/Contrato por vontade da Prosegur

6.17.3.1 A Prosegur reserva-se o direito de rescindir unilateralmente o Pedido/Contrato em qualquer altura, justificando e comunicando a sua decisão por escrito e notificando o Fornecedor/Contratante com antecedência de pelo menos trinta (30) dias da data em que a rescisão deva entrar em vigor.

6.17.4. O pedido de declaração de insolvência, falência, suspensão de pagamentos ou início de qualquer processo de insolvência, do Fornecedor/Contratante de acordo com as leis ou regulamentos aplicáveis em cada caso, dará à Prosegur, no prazo de trinta (30) dias após tomar conhecimento da existência do referido pedido, o direito de exigir que o Fornecedor/Contratante acredite, no prazo de dez (10) dias após a receção pelo mesmo do pedido feito para o efeito pela Prosegur, os seguintes pontos:

- Que dispõe dos meios materiais e pessoais necessários e suficientes para continuar a executar os trabalhos contratados (pessoal, meios técnicos, etc.).
- Que dispõe dos meios económicos necessários para realizar os trabalhos contratados até à sua conclusão, para o que deverá apresentar à Prosegur uma garantia bancária solidária, à primeira solicitação e renunciando expressamente aos benefícios de exclusão e divisão, pelo montante total dos trabalhos contratos até à sua execução mais 25% desse montante, para garantir o cumprimento por parte do Fornecedor/Contratante de todas as suas obrigações contratuais.

Se dentro do referido prazo de dez (10) dias, o Fornecedor/Contratante não acreditar todos os pontos referidos neste secção, a Prosegur terá o direito de rescindir o Pedido/Contrato, com direito a ser indemnizada pelo Fornecedor/Contratante por todos os danos que tal resolução contratual possa causar.

6.18. Força Maior

6.18.1. Nenhuma das partes será considerada responsável pelo não cumprimento das suas obrigações decorrentes do Pedido/Contrato, na medida em que o seu cumprimento seja atrasado ou tornado impossível por Força Maior.

Para estes fins, considera-se Força Maior os fenómenos naturais, acidentes inevitáveis, pandemias, incêndio, revolta ou motim popular, atos de guerra, por imposição, regra, ordem ou ato de qualquer governo ou agência governamental, bem como de qualquer outra autoridade competente, ou qualquer outra causa de natureza semelhante que seja imprevisível ou que seja previsível, inevitável, irresistível ou independente da vontade das partes e fora do seu controlo.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 18
------------	--	---

Não obstante as disposições do parágrafo anterior, a suspensão das obrigações contratuais causada pelo pessoal do Fornecedor/Contratante ou dos seus Subcontratantes não poderá ser invocada como causa de Força Maior.

6.18.2. A suspensão das obrigações contratuais durará enquanto continuar a causa de força maior. A parte afetada pela suspensão deve informar imediatamente a outra e fazer esforços razoáveis para resolver a causa da suspensão no mais curto espaço de tempo possível.

Se a causa de força maior durar mais de um mês, a Prosegur reserva-se o direito de cancelar o Pedido/Contrato com o pagamento ao Fornecedor/Contratante dos montantes devidos pela realização dos trabalhos, prestação de serviços ou entrega dos bens que tenham sido efetuados pelo Fornecedor/Contratante à altura do cancelamento, sem que isto dê ao Fornecedor/Contratante o direito de cobrar qualquer montante adicional ou sanção ou indemnização a favor do Fornecedor/Contratante.

6.19. Propriedade Intelectual e Industrial

2.19.1. Garantias do Fornecedor em relação aos serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur.

2.19.1.1. O Fornecedor garante, sem exceção, a exploração e utilização plena e pacífica dos serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur, colocados à disposição da Prosegur em todo o mundo, bem como (i) que os serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur, não infringem, nem irão infringir as normas vigentes ou os Direitos de Propriedade Intelectual e Industrial, ou semelhantes, de terceiros e que não existe qualquer reivindicação, exigência ou litígio; (ii) que está suficientemente autorizado para o fornecimento de serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur, e que não possui um acordo com terceiros que o impeça, total ou parcialmente, de executar o contrato ao qual está vinculado; (iii) obter e assumir o custo das licenças, cessões e Direitos de Propriedade Intelectual e Industrial com o alcance obrigatório para garantir a exploração plena e pacífica pela Prosegur. Em conformidade com a garantia acima, o Fornecedor isenta a Prosegur de qualquer responsabilidade por infrações relacionadas com a exploração e a utilização dos serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur disponibilizados pelo Fornecedor, que a Prosegur possa incorrer.

Assim, o Fornecedor deve obter o consentimento prévio, expresso e por escrito da Prosegur antes de incorporar nos serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur, qualquer elemento de propriedade de terceiros e/ou que possa estar protegido por Direitos de Propriedade Intelectual e Industrial de terceiros.

2.19.1.2. O Fornecedor garante à Prosegur e tem a obrigação de fornecer uma prova documental à Prosegur e, se necessário, que possui os Direitos de Propriedade Intelectual e Industrial necessários para a execução do objeto do presente Contrato.

2.19.1.3. O Fornecedor compromete-se a notificar a Prosegur de quaisquer informações que tenha de reclamações de terceiros em relação aos Direitos de Propriedade Intelectual e Industrial sobre os serviços, produtos, entregas e/ou desenvolvimentos ad hoc para a Prosegur, ou que possam afetar os Direitos da Prosegur e abster-se-á de iniciar qualquer ação sem o consentimento prévio por escrito da Prosegur.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 19
------------	--	---

2.19. 2. Indemnização.

Na eventualidade de qualquer reclamação, judicial ou extrajudicial contra Prosegur, relacionada com a violação dos Direitos de Propriedade Intelectual e Industrial utilizados pelo Fornecedor ou como resultado de qualquer ação, reclamação ou procedimento, público ou privado, que seja iniciado em virtude de ações, tanto por ação como por omissão, realizadas ou permitidas pelo Fornecedor ou por qualquer um dos respetivos administradores, agentes ou funcionários, em relação ao cumprimento das obrigações referidas, o Fornecedor isenta a Prosegur de qualquer responsabilidade e procederá à indemnização da Prosegur pelos danos e prejuízos sofridos, comprometendo-se a isentar os respetivos consultores, diretores e funcionários de qualquer perda, responsabilidade, danos, prejuízos, gastos e custos (incluindo custos jurídicos) incorridos pela Prosegur, bem como quaisquer danos causados a terceiros, garantindo à Prosegur a utilização dos Direitos de Propriedade Intelectual e Industrial que deram origem à reclamação ou através da disponibilização de outros diferentes que permitam a continuidade dos serviços, produtos ou do contrato.

2.19.3. Direitos de Propriedade Intelectual e Industrial da Prosegur.

19.3.1 Por Direitos de Propriedade Intelectual e Industrial entende-se qualquer direito de propriedade intelectual e industrial ou de natureza análoga sobre quaisquer resultados que estejam ou possam estar sujeitos a proteção, de acordo com a regulamentação para esse fim específico. O Fornecedor compromete-se a respeitar os Direitos de Propriedade Intelectual e Industrial e qualquer outro de natureza semelhante de propriedade da Prosegur, e reconhece que nada no presente documento é uma transferência, cessão ou licença sobre os referidos Direitos em favor do Fornecedor. O Fornecedor reconhece que só pode utilizar os Direitos de Propriedade Intelectual e Industrial da Prosegur com a sua instrução expressa e consentimento por escrito, e apenas no âmbito da execução do contrato, tendo a obrigação de respeitar as instruções da Prosegur.

19.3.2 Em particular, o Fornecedor não poderá utilizar a denominação, nome comercial, logótipo ou marcas registadas da Prosegur, nem utilizá-los ou utilizar a aceitação de qualquer oferta, nem a assinatura ou execução do presente Contrato, nem a prestação dos serviços referidos no mesmo, como referência para a obtenção de novos clientes ou captação de negócios, ou para manter um determinado nível profissional.

2.19.4. Titularidade dos Direitos sobre potenciais Desenvolvimentos ad hoc do Fornecedor para a Prosegur.

2.19.4.1. Na hipótese de, em resultado da relação entre as partes, o Fornecedor ter de realizar um Desenvolvimento ad hoc para a Prosegur, a Prosegur será a proprietária exclusiva, sem limite geográfico ou temporal, de todos os Direitos de Propriedade Intelectual e Industrial sobre os referidos Desenvolvimentos ad hoc que o Fornecedor, ou qualquer pessoa que o Fornecedor tenha contratado para esse fim, desenvolva para a Prosegur em resultado da relação regulada no presente documento.

Caso a titularidade dos Direitos de Propriedade Intelectual e Industrial sobre os Desenvolvimentos ad hoc da Prosegur não possa ser originalmente atribuída à Prosegur de acordo com a legislação vigente, então, por força do presente documento, o Fornecedor atribui à Prosegur a titularidade de todos os Direitos de Propriedade Intelectual e Industrial, em regime de exclusividade, e na máxima extensão permitida por lei, ou seja, durante toda a vigência dos Direitos de Propriedade Intelectual e Industrial cedidos, para todo e qualquer tipo de exploração, mesmo que não seja o setor de atividade habitual da Prosegur. Consequentemente, a Prosegur poderá exercer livremente e da forma que entender, os Direitos de Propriedade Intelectual e Industrial dos Desenvolvimentos ad hoc, incluindo a sua exploração, transmissão, cessão, licença a terceiros, tudo nos termos e condições que entender.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 20
------------	--	---

2.19.4.2. O Fornecedor compromete-se a colaborar com a Prosegur no cumprimento das respetivas obrigações e, em particular, a (i) colaborar na obtenção dos registos e inscrições relativos aos Direitos de Propriedade Intelectual e Industrial da Prosegur (ii) informar imediatamente a Prosegur de quaisquer resultados obtidos no âmbito da relação contratual com a Prosegur, fornecendo toda a documentação e outros suportes necessários para garantir a propriedade da Prosegur sobre os Desenvolvimentos ad hoc para a Prosegur.

2.19.4.3. O Fornecedor reconhece que a remuneração acordada em favor do Fornecedor também satisfaz as obrigações e compromissos assumidos por este na presente cláusula, renunciando à sua reclamação.

2.19.5 Software.

2.19.5.1. Caso o Fornecedor efetue o licenciamento do Software Padrão (software desenvolvido genericamente para a mesma utilização por várias pessoas) à Prosegur para a execução do presente contrato, a referida licença será exclusiva, irrevogável e sublicenciável para utilização (inclusive em favor do Grupo Prosegur) em todo o mundo e pelo prazo máximo de vigência dos referidos direitos.

2.19.5.2. O Fornecedor garante que não utilizará software de código aberto (ao abrigo de uma licença de código aberto) para a execução do presente contrato sem o consentimento prévio por escrito da Prosegur. Para este fim, irá informar a Prosegur quanto aos termos e condições da licença aplicável, irá confirmar que o programa de computador enquanto um todo não pode ser considerado software de código aberto e que a respetiva utilização não restringe a utilização dos serviços, produtos, entregas e desenvolvimentos ad hoc para a Prosegur. No caso de uma utilização autorizada, o Fornecedor compromete-se e garante o cumprimento dos termos e condições da licença aplicável.

2.20. Confidencialidade das informações e documentos

2.20.1. As informações confidenciais serão consideradas informações protegidas contra o acesso de pessoas não autorizadas e especificamente:

a) Todas as informações (escritas ou verbais) e materiais, de qualquer tipo ou natureza mostradas ou fornecidas (antes ou depois da data do Pedido/Contrato pela Prosegur ou os seus administradores, empregados, representantes, filiais ou pelos seus consultores, advogados, auditores ou Fornecedores externos, ou tratadas no âmbito das atividades objeto do Pedido/Contrato e toda a informação a que o Fornecedor/Contratante tenha acesso ou conheça durante a execução dos serviços objeto do Pedido/Contrato e, em qualquer caso, quaisquer dados relacionados ou associados a uma pessoa singular específica ou determinável, sejam informações ou materiais relacionados à Prosegur ou a terceiros (seja, sem limitação, informações ou dados relativos a clientes, fornecedores, empregados ou qualquer outro terceiro que mantenha relação de qualquer natureza com a Prosegur ou qualquer das empresas ou entidades do Grupo Prosegur);

b) O conteúdo do serviço, a existência de conversas e negociações anteriores entre a Prosegur e o Fornecedor/Contratante, a existência de qualquer oferta de bens, obras e/ou serviços, de qualquer documento aceitando qualquer oferta de bens, obras e/ou serviços, ou qualquer outro acordo, contrato ou documento relacionado ou destinado ao fornecimento de bens, obras e/ou serviços pelo Fornecedor/Contratante à Prosegur, bem como o conteúdo de tais conversas, negociações, oferta de bens, obras e/ou serviços, carta, contrato, acordos, contratos ou documentos.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 21
------------	--	---

c) a título de exemplo e sem limitação, abrange o modo de funcionamento do Grupo Prosegur, segredos comerciais, segredos empresariais, ideias, planos de negócios, planos de expansão, informações de marketing ou vendas, novas oportunidades de negócios, projetos de desenvolvimento, direitos de propriedade intelectual e industrial, qualquer informação científica ou técnica, invenção, design, processo, procedimento, fórmula, melhoria, tecnologia ou método; quaisquer conceitos, amostras, relatórios, dados, know-how, trabalhos em curso, designs, fotografias, ferramentas de desenvolvimento, especificações, programas para computadores, código-fonte, código objeto, organogramas e bases de dados, independentemente de que a informação seja escrita, documental, oral, visual, eletrónica ou formato legível por máquina, amostras, modelos ou outros. As Partes concordam que as Informações Confidenciais não têm de ser novas, únicas, patenteáveis, protegidas por direitos de autor ou por um segredo comercial, a fim de serem classificadas como Informações Confidenciais e, como tal, protegidas.

A seguir, qualquer das informações referidas nos pontos a), b) e c) serão denominadas "Informações Confidenciais".

2.20.2. Obrigação de confidencialidade:

a) As Informações Confidenciais serão tratadas de forma confidencial pelo Fornecedor/Contratante e não serão divulgadas pelo Fornecedor, no todo ou em parte, direta ou indiretamente (através dos seus empregados, colaboradores externos ou internos, subcontratados, auditores ou outras entidades relacionadas) a terceiros., em quaisquer circunstâncias, exceto com o consentimento prévio por escrito da Prosegur. Em particular, o Fornecedor/Contratante compromete-se a tomar as medidas necessárias para impedir o acesso de terceiros não autorizados às Informações Confidenciais e a limitar o acesso às mesmas a empregados autorizados que necessitem acesso para a realização dos bens, obras e/ou serviço, transferindo a eles a mesma obrigação de confidencialidade.

b) O Fornecedor/Contratante garante que as Informações Confidenciais não serão utilizadas ou exploradas, em benefício próprio ou de terceiros, para utilização ou fins diferentes do fornecimento de bens, obras e/ou serviços.

c) O Fornecedor/Contratante compromete-se a não copiar, divulgar, comunicar, emprestar ou de outra forma reproduzir, revelar ou divulgar as Informações Confidenciais a terceiros, bem como não publicá-las ou de qualquer outra forma, diretamente, através de terceiras pessoas ou empresas disponibilizá-las a terceiros, sem o prévio consentimento escrito da Prosegur.

d) O Fornecedor/Contratante compromete-se a que todas as Informações Confidenciais a que tenha acesso permaneçam nas instalações da Prosegur e não possam ser transferidas para outro local, exceto com o consentimento prévio por escrito da Prosegur.

e) As obrigações estabelecidas para o Fornecedor/Contratante no Pedido/Contrato serão também de obrigatório cumprimento para os seus empregados, colaboradores, externos e internos, subcontratantes, advogados e auditores, e o Fornecedor/Contratante será responsável para com a Prosegur se tais obrigações forem violadas por tais empregados, colaboradores, subcontratantes, advogados e auditores. O Fornecedor/Contratante compromete-se a obter dos seus colaboradores externos ou subcontratantes autorizados pela Prosegur um compromisso por escrito em termos idênticos aos estipulados nesta cláusula com relação às Informações Confidenciais na sua posse dos mesmos.

2.20.3. Exceções à obrigação de confidencialidade. Auditorias:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 22
------------	--	---

a) A obrigação de confidencialidade não será aplicável e, portanto, não serão consideradas Informações Confidenciais as informações que são ou serão acessíveis ao público por outras razões que não a violação da obrigação de confidencialidade pelo Fornecedor/Contratante; que tenham sido publicadas antes da data deste Pedido/Contrato; que já estejam na posse legítima do Fornecedor/Contratante e não estejam sujeitas a um acordo de confidencialidade entre as partes, desde que isto seja levado ao conhecimento da outra parte antes da divulgação; que seja recebida através de um terceiro sem restrições e sem violação de qualquer obrigação legal ou contratual do terceiro; ou que tenha sido desenvolvida independentemente pelo Fornecedor/Contratante para outros fins que não os bens, obras e/ou serviços a prestar à Prosegur e que tenha sido desenvolvida sem a utilização ou assistência de Informações Confidenciais.

b) A divulgação de Informações Confidenciais para cumprir uma ordem judicial ou administrativa não está sujeita à obrigação de confidencialidade desde que o Fornecedor/Contratante que tenha recebido a ordem correspondente informe a Prosegur por escrito, com antecedência, da obrigação de proceder a essa divulgação.

c) A Prosegur está autorizado a supervisionar o desenvolvimento dos bens, obras e/ou serviços encomendados, para garantir que os mesmos estejam de acordo com as instruções emitidas e regulamentos aplicáveis existentes, e pode solicitar ao Fornecedor/Contratante quaisquer informações que considere relevantes, aceder ao local físico onde os serviços são feitos e realizar, diretamente ou através de terceiros, quaisquer auditorias e verificações que considere de interesse.

2.20.4. Devolução das Informações Confidenciais: No final da obra ou entrega de bens e/ou prestação do serviço objeto do Pedido/Contrato, ou antes desta data se assim solicitado pela Prosegur e não for necessário que o Fornecedor/Contratante os tenha para prestar serviços à Prosegur, o Fornecedor/Contratante deverá devolver à Prosegur quaisquer Informações Confidenciais que estejam em poder do Fornecedor/Contratante.

2.20.5. Propriedade das Informações Confidenciais: Nenhum direito de propriedade ou outro direito ou título das Informações Confidenciais é reconhecido a favor do Fornecedor/Contratante, exceto os direitos de utilização estabelecidos no Pedido/Contrato e com as limitações nele indicadas.

2.20.6. Duração: A duração das presentes obrigações de confidencialidade será indefinida, permanecendo em vigor após a cessação, por qualquer razão, da relação entre a Prosegur e o Fornecedor/Contratante.

2.20.7. Não cumprimento: O Fornecedor/Contratante será responsável e indemnizará a Prosegur por todos os danos causados como consequência da violação de qualquer das obrigações de confidencialidade estabelecidas.

2.20.8 Em qualquer caso, a prestação dos serviços objeto de qualquer oferta de serviços do Fornecedor, ou através de subcontratantes autorizados pelo Cliente, não deverá prejudicar os direitos de inspeção do Banco de Espanha e/ou outros organismos reguladores da atividade do Cliente. O Fornecedor compromete-se a permitir ao Banco de Espanha e a outros organismos reguladores o acesso direto e sem restrições às informações do Cliente na posse do Fornecedor ou dos seus subcontratantes autorizados pelo Cliente, para que o Banco de Espanha ou outros organismos reguladores possam realizar nas instalações do Fornecedor ou dos seus subcontratantes as verificações relevantes em relação a essas informações, incluindo a verificação da adequação dos sistemas e aplicações utilizadas. O Fornecedor compromete-se a obter dos seus subcontratantes autorizados pelo Cliente um compromisso escrito em termos idênticos aos estipulados nesta estipulação no que respeita às informações na sua posse, acesso às suas instalações e verificação da adequação dos sistemas e aplicações utilizadas.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 23
------------	--	---

6.21. Proteção de dados pessoais

6.21.1. No caso do Fornecedor ter de aceder aos dados pessoais pertencentes à Prosegur, será necessário assinar o contrato de Encarregado de Tratamento previsto no Anexo III.

6.21.2. Em qualquer caso, o Fornecedor que tem de ter acesso aos dados pessoais detidos pela Prosegur (doravante, os "Dados") estará sujeito ao cumprimento do regime jurídico previsto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE - Regulamento Geral sobre a Proteção de Dados (doravante, "GDPR"), bem como na Lei Orgânica 3/2018, de 5 de dezembro, relativa à Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDGDD).

Em geral, em conformidade com as disposições dos regulamentos de proteção de dados aplicáveis, o Fornecedor que tem acesso aos dados pessoais declara expressamente e compromete-se a:

- a. Utilizar e tratar os Dados com o único e exclusivo fim de cumprir este Contrato e seguir em todos os casos as instruções recebidas da Prosegur. O Fornecedor deverá abster-se expressamente de utilizar os Dados para qualquer outra utilização para além da acordada e, em particular, abster-se de alterar, utilizá-los para os seus próprios interesses comerciais ou comunicá-los ou permitir o acesso de terceiros, nem mesmo para fins de armazenamento.
- b. Observar a máxima confidencialidade e reserva em relação aos dados pessoais fornecidos pela Prosegur com respeito ao desenvolvimento do objeto do presente Contrato, comprometendo-se a não divulgar estes dados a terceiros, bem como qualquer outra informação que possa ter sido fornecida relativamente à Prosegur.
- c. Devolver à Prosegur, uma vez concluída a prestação dos serviços objeto do presente Contrato, todos os documentos e ficheiros em que constem todos ou alguns dos Dados, qualquer que seja o seu suporte ou formato, bem como as suas cópias.
- d. Restringir o acesso e a utilização dos Dados aos seus empregados, agentes e colaboradores a quem é absolutamente essencial que tenham acesso e conhecimento para o desenvolvimento do objeto do presente Contrato, comprometendo-se a impor-lhes as obrigações de confidencialidade e proibição de utilização dos Dados, nos mesmos termos previstos no presente Contrato, comprometendo-se a responder por qualquer violação das referidas obrigações por parte de qualquer dos seus empregados, agentes e colaboradores acima mencionados.
- e. Adotar, implantar e exigir as medidas de segurança de índole técnica e organizacional necessárias, que assegurem uma segurança adequada dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizacionais adequadas («integridade e confidencialidade»), bem como atualizar as medidas de segurança conforme as exigências legalmente decorrentes durante a duração do presente Contrato e quaisquer outras que sejam objeto de notificação fidedigna por parte da Prosegur.

Especificamente, em conformidade com o artigo 32 do RGPD, o Fornecedor implementará as medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, tendo em conta o nível de sensibilidade dos dados e as atividades de tratamento realizadas, incluindo, entre outras, as seguintes:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 24
------------	--	---

- pseudonimização e encriptação de dados pessoais, quando apropriado;
 - capacidade de assegurar a contínua confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços de tratamento;
 - capacidade de restaurar rapidamente a disponibilidade e o acesso aos dados pessoais em caso de incidente físico ou técnico;
 - um processo de verificação, avaliação e controlo regular da eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento.
- f. O fornecedor não poderá subcontratar nenhum dos serviços que fazem parte do objeto deste Contrato que implique o tratamento de dados pessoais, exceto com a prévia autorização expressa concedida por escrito pela Prosegur.

Caso seja necessário subcontratar algum tratamento, tal deverá ser comunicado previamente e por escrito à Prosegur, indicando os tratamentos que se pretendem subcontratar e identificando de forma clara e inequívoca a empresa subcontratante e os seus dados de contacto.

Em caso de autorização, o subcontratante, que também terá o estatuto de encarregado do tratamento, será também obrigado a cumprir as obrigações estabelecidas neste Contrato para o Fornecedor e as instruções da Prosegur. Cabe ao Fornecedor inicial regular a nova relação em conformidade com o artigo 28 do RGPD, para que o novo encarregado esteja sujeito às mesmas condições (instruções, obrigações, medidas de segurança, etc.) e aos mesmos requisitos formais que o Fornecedor inicial, no que diz respeito ao adequado tratamento dos dados pessoais e à garantia dos direitos das pessoas em causa.

Em caso de não cumprimento por parte do subencarregado, o Fornecedor inicial permanecerá totalmente responsável junto a Prosegur pelo cumprimento das obrigações.

- g. Quando as pessoas afetadas exercem os seus direitos de acesso, retificação, eliminação, oposição, de não estarem sujeitas a decisões individualizadas automatizadas, limitação do tratamento e portabilidade dos dados para com o Fornecedor, isto deve ser comunicado por correio eletrónico ao endereço indicado pela Prosegur. A comunicação deve ser feita imediatamente e, em nenhum caso, após o dia útil seguinte à receção do pedido, juntamente, quando apropriado, com outras informações que possam ser relevantes para a resolução do pedido.
- h. Em caso de qualquer violação da segurança dos Dados Pessoais, o Fornecedor deverá notificar o mesmo sem demora indevida e, em qualquer caso, num prazo máximo de vinte e quatro (24) horas e através de qualquer endereço de contacto, físico ou eletrónico, fornecido pela Prosegur durante o desenvolvimento da relação contratual entre as partes, juntamente com todas as informações relevantes para a documentação e comunicação do incidente.

6.21.3. Manter a Prosegur isenta de qualquer reclamação que possa ser apresentada contra a Prosegur à Autoridade de Controlo correspondente, que seja causada pela violação pelo Fornecedor e/ou seus subcontratantes das disposições do presente acordo e da legislação em vigor sobre proteção de dados pessoais e concordar em pagar o montante a que a Prosegur possa ser condenada como

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 25
------------	--	---

sanção, multa, indemnização, danos e juros, incluindo honorários de advogados, devido à violação acima referida.

6.22. Segurança da tecnologia da Informação

O Fornecedor compromete-se a ter um sistema operativo com as atualizações de segurança mais recentes, pelo menos as dos últimos três meses. Para além disso, garante que tem instalados antivírus atualizados na data atual com atualização automática predefinida.

O Fornecedor não irá ligar-se a partir de uma máquina que não seja propriedade da Prosegur para realizar tarefas administrativas em servidores da Prosegur.

Em caso de incumprimento destas obrigações, a Prosegur está excluída, na extensão máxima permitida por lei, de qualquer responsabilidade pelos danos diretos e prejuízos de qualquer natureza, diretos e indiretos, entre outros, lucro cessante ou perda de clientes, lucros ou de exploração, que possam dever-se a uma falha da segurança dos equipamentos, sistemas informáticos ou redes de comunicação do Fornecedor, incluindo situações de fuga de informação ou adulteração da informação, intervenção ou interferência ilegal dos sistemas informáticos, de comunicação e/ou software por malware (entre outros vírus, trojans, worms) e outras rotinas de programação prejudiciais de terceiros, sem que a presente enumeração seja limitativa de outras formas que possam modificar e/ou afetar os sistemas informáticos e/ou de comunicação da Prosegur.

O Fornecedor responderá, sem qualquer limitação, pelos danos e prejuízos de qualquer natureza, diretos e indiretos, entre outros, lucro cessante ou perda de clientes, lucros ou de exploração, por qualquer interrupção, perturbação ou diminuição do serviço prestado à Prosegur, causada por atos ou omissões de terceiros derivados do incumprimento destas obrigações.

Caso o Provedor identifique uma falha na segurança dos seus sistemas, deverá informar o responsável pelo projeto da Prosegur por qualquer meio que permita conservar registo escrito e num prazo de 24 horas a partir do momento em que tenha conhecimento da mesma. O cumprimento destas obrigações não isenta o Fornecedor de responsabilidade pelo incumprimento das obrigações anteriores.

O Fornecedor deve cumprir as disposições do Anexo V Utilização de Recursos e Sistemas de IT, bem como assinar o anexo "**DECLARAÇÃO DO USUÁRIO SOBRE A UTILIZAÇÃO DE RECURSOS E SISTEMAS DE IT**", que faz parte deste.

Todos os Fornecedores que requerem acesso às tecnologias da Informação do Grupo Prosegur, fornecem serviços/produtos tecnológicos e/ou digitais, bem como serviços não tecnológicos com capacidade de acesso às tecnologias da informação e/ou informação do Grupo, devem cumprir as disposições do Anexo IV. No caso do fornecedor prestar serviços que não exijam acesso às tecnologias da informação do Grupo Prosegur, aplicam-se os pontos do anexo que permitem avaliar o risco do fornecedor em relação à Prosegur.

2.22.1 Auditoria

A Segurança da Informação reserva-se o direito de realizar auditorias técnicas e rever o estado de conformidade do fornecedor com o Esquema de Controlo estabelecido por ele.

Relativamente às auditorias técnicas, os custos e despesas associados à intervenção da Prosegur serão assumidos pela Prosegur. No caso de serem detetadas vulnerabilidades, o Fornecedor será responsável pela sua reparação, de acordo com os procedimentos técnicos de gestão de vulnerabilidades do Grupo Prosegur e de acordo com os seguintes tempos de resolução:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 26
------------	--	---

- Crítica: 10 dias.
- Alta: 20 dias.
- Média: 90 dias.
- Baixa: 180 dias.

Em caso de não cumprimento dos prazos, será aplicada uma penalização de 5% do total da faturação anual, que será compensada em faturas futuras associadas ao serviço.

6.23. Resolução de conflitos e litígios

6.23.1. A legislação aplicável ao Pedido/Contrato será a do local do seu cumprimento. Entende-se por local de cumprimento aquele em que, de acordo com o Pedido/Contrato, devem ser entregues os bens ou a obra executada e/ou os serviços prestados.

6.23.2. Na ausência de um acordo, os bens serão entendidos como entregues e as obras e/ou serviços executados no local onde a empresa tem a sua sede a efeitos legais da correspondente empresa do Grupo Prosegur que assina o o Pedido/Contrato.

6.23.3. Para qualquer divergência que possa surgir quanto à interpretação, execução ou cumprimento do Pedido/Contrato, as partes devem submeter-se expressamente à jurisdição dos Tribunais ordinários da cidade da sede social da empresa do Grupo Prosegur que assina o Pedido/Contrato correspondente.

6.24. Ficheiros

6.24.1. O Fornecedor/Contratante deverá manter um registo completo e atualizado dos bens fornecidos e/ou obras e/ou serviços executados no âmbito do Pedido/Contrato, bem como de todas as transações a ele relacionadas. O Fornecedor/Contratante deverá manter todos estes registos durante um período de pelo menos três anos, após a conclusão do Pedido/Contrato. Estes registos estarão disponíveis para possível auditoria pela Prosegur. A auditoria, quando aplicável, não será aplicada às Patentes do Fornecedor/Contratante ou a quaisquer informações adicionais relacionadas a elas.

6.24.2. A Prosegur, com o objetivo de aumentar a exigência sobre os seus fornecedores em termos de sustentabilidade, reserva-se o direito de rever as políticas ambientais, de trabalho e de governo corporativo dos seus principais fornecedores.

7. ANEXOS.

7.1. Documentos Associados:

<u>Código</u>	<u>Nome</u>
DS-GLO-EF-COM-02	Anexo I: Lista de limites exigíveis nos seguros de acordo com produtos ou serviços

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 27
------------	--	---

MD-GLO-EF-COM-02	Anexo II: Modelo de garantia bancária fiel cumprimento e garantia de bens, obras e/ou serviços
MD-GLO-LEG-07	Anexo III: Contrato de Encarregado de Tratamento
	Anexo IV: Requisitos de Risco Tecnológico e Cibersegurança
	Anexo V: Utilização de Recursos de IT e Sistemas da Prosegur

7.2. ANEXO I: LISTA DE LIMITES DS-GLO-EF-COM-02

MONTANTES A PAGAR SOBRE PRODUTOS OU SERVIÇOS DE SEGUROS (POR RECLAMAÇÃO)

ATIVIDADE	PME	MULTINACIONAL
TODOS		
Seguro de Acidentes:	Mínimo legal	Mínimo legal
Seguro de Responsabilidade Civil para trabalhos realizados		
Responsabilidade Civil pelo produto, recolha do produto, pós-trabalho, união e mistura, contaminação e poluição	3.000.000 €	6 000 000 €
Seguro de Responsabilidade Civil do Empregador	3.000.000 €	6 000 000 €
Responsabilidade Civil para automóveis, máquinas automotoras, aviões, embarcações:	300.000 €	600.000 €
	Mínimo legal	Mínimo legal
Seguros adaptados ao local de prestação		
CONSTRUÇÃO		
Seguro de Construção/Edificação e Montagem:	Orçamento de obra	Orçamento de obra
Responsabilidade Civil pelo produto, recolha do produto, pós-trabalho, união e mistura, contaminação e poluição	3.000.000 €	
Responsabilidade Civil de Máquinas Industriais:	3.000.000 €	6.000.000 €
Danos próprios equipamento de construção; alugado ou propriedade do Contratante:	Valor de substituição	6.000.000 €
Seguro de dez anos:	Mínimo legal	Valor de substituição
	-	Mínimo legal
SERVIÇOS PROFISSIONAIS		
Responsabilidade Civil Profissional atividade profissional prestada	3.000.000 €	6.000.000 €
	3.000.000 €	6.000.000 €
SERVIÇOS PROFISSIONAIS TECNOLÓGICOS		
Responsabilidade Civil Profissional Tech PI	3.000.000 €	6.000.000 €
Riscos cibernéticos e proteção de dados	3.000.000 €	6.000.000 €
TECNOLOGIA		
Responsabilidade Civil Profissional Tech PI	3.000.000 €	6.000.000 €
Responsabilidade Civil pelo produto, recolha do produto, pós-trabalho, união e mistura, contaminação e poluição	3.000.000 €	6.000.000 €
Ciberrisco e proteção de dados	3.000.000 €	6.000.000 €
TRANSPORTE DE MERCADORIAS COMPRADAS		
Cobertura de transporte porta a porta	Valor transportado	Valor transportado
Transporte de carga e descarga		
ARMAZENAMENTO DE ESTOQUES EM ARMAZÉNS DO		
Cobertura total do armazém	Valor transportado	Valor transportado
GARANTIA DE PRODUTO E SERVIÇO		
Garantia do produto	Mínimo legal	Mínimo legal
Recolha de produto		
Garantia de falta de estoque		
Responsabilidade para com os clientes		
Perda de lucro / perda de atividade		

7.3. ANEXO II. MODELO DE GARANTIA MD-GLO-EF-COM-02

A entidade [•] (doravante, o “BANCO”), com CIF [•] com domicílio em [•], e em seu nome e representação Sr. [•] e o Sr. [•] com poderes suficientes para o vincular neste ato, tal como evidenciado pela procuração outorgada pelo Notário de [•], Sr. [•], na data [•] de [•] de [•], com o número [•] de protocolo

ENDOSSA

Incondicional, irrevogável e solidariamente, com renúncia expressa aos benefícios de divisão, exclusão e ordem, até os limites indicados e nas condições expressas abaixo, ao [] (doravante o [FORNECEDOR]), com sede em [] e NIF [], para garantir o pagamento pelo FORNECEDOR à PROSEGUR COMPAÑÍA DE SEGURUDAD, S.A. (doravante, "PROSEGUR") de todas as obrigações assumidas pelo FORNECEDOR no contrato de [] datado de [] (doravante, o "CONTRATO") ao abrigo do qual o FORNECEDOR [] à PROSEGUR (doravante os [BENS] [OBRAS] [SERVIÇOS]) e especialmente para responder pelo pagamento de quaisquer perdas, reclamações por danos, reclamações, causas de ação, responsabilidades, sanções, custos e, ou despesas quantificadas e determinadas de qualquer natureza imputadas pelo FORNECEDOR contra a PROSEGUR, devido à responsabilidade do FORNECEDOR agora ou no futuro, como resultado de qualquer declaração enganosa ou inexata, violação, contingência e/ou reclamação de terceiros da execução do CONTRATO.

PRIMEIRO. - EXECUÇÃO. Esta garantia bancária será efetivada, em uma ou mais vezes, no primeiro pedido de pagamento pela PROSEGUR, em uma ou mais vezes, até ao limite máximo de [...] ([...]) EUROS, relativamente ao pedido da PROSEGUR, ao qual é anexada uma cópia do pedido de pagamento enviada pela PROSEGUR ao FORNECEDOR e prova de que decorridos dez (10) dias úteis desde o envio da referida notificação do pedido de pagamento, sem que o FORNECEDOR tenha pago o referido montante.

O BANCO compromete-se a efetuar o pagamento do montante exigido até os montantes máximos (individuais e conjuntos) previstos acima, no prazo de três (3) dias a contar da receção de tal comunicação, e na conta indicada pela PROSEGUR para tal efeito.

SEGUNDO. - RENÚNCIA A EXCEÇÕES. Esta Garantia é irrevogável e é concedida em abstrato e à primeira solicitação, o BANCO não pode opor-se ou alegar contra a PROSEGUR qualquer tipo de exceção e, em particular, as exceções pessoais que o FORNECEDOR possa provar contra a PROSEGUR. Desta forma, uma vez apresentado o pedido descrito no ponto anterior, o BANCO não poderá de forma alguma questionar a validade da reclamação ao BANCO pela PROSEGUR.

TERCEIRO. - PRAZO DE VALIDADE. Esta garantia entrará em vigor na data de hoje e será válida por [...] ([...]) anos a partir de hoje. Na referida data, se o BANCO não tiver recebido qualquer comunicação fiável de pagamento do montante efetuado pelo FORNECEDOR, este expirará e será automaticamente terminado.

QUARTO. - CESSÃO. A PROSEGUR poderá ceder esta garantia a qualquer terceiro. Para que tal cessão seja válida relativamente ao BANCO, é suficiente que seja comunicada ao BANCO pela PROSEGUR. Neste caso, todas as referências à PROSEGUR nesta garantia serão entendidas como referências ao cessionário desta garantia.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 30
------------	--	---

QUINTO.- - DESPESAS. Quaisquer custos e despesas relacionados com esta garantia bancária deverão ser pagos e assumidos exclusivamente pelo FORNECEDOR.

Esta garantia foi registada na mesma data no Registo Especial de Garantias com o número [●].

[AUTENTICADO POR NOTÁRIO PÚBLICO]

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 31
------------	--	---

7.4. ANEXO III. CONTRATO DE PEDIDO DE TRATAMENTO

ENTRE

De uma parte, a PROSEGUR (doravante, o "Responsável pelo tratamento"), e da outra parte, o fornecedor (doravante, o "Subcontratante"), que serão denominadas coletivamente como as "**Partes**" e, individualmente, cada uma delas como a "**Parte**"

DECLARAM

- I. Que, como consequência da prestação dos serviços mencionados no Contrato de compra ou fornecimento, o Encarregado do Tratamento pode aceder a dados pessoais sob responsabilidade e proteção da **PROSEGUR**; tendo para estes efeitos o Fornecedor a condição legal de Encarregado do Tratamento no que diz respeito aos mesmos.
- II. Que, como consequência e em plena conformidade com as disposições dos regulamentos nacionais e comunitários aplicáveis, as Partes desejam incluir no presente Acordo as condições de tratamento dos dados por parte do Fornecedor, em conformidade com as disposições da legislação espanhola.
- III. Que, sem prejuízo do exposto, as Partes pretendem igualmente cumprir as exigências que, no que diz respeito à regulamentação da relação do Subcontratante, se encontram estabelecidas no artigo 28 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 e, para o efeito, subscrevem as seguintes

CLÁUSULAS

Primeira - Tratamento de dados pessoais

A prestação de serviços poderá implicar o acesso por parte do Subcontratante a informação confidencial e a dados pessoais sob responsabilidade da PROSEGUR. Para isto, o Fornecedor será considerado como Encarregado do tratamento, e o seu tratamento dos dados pessoais sob responsabilidade da PROSEGUR consistirá única e exclusivamente em aceder, e conforme o caso, armazenar os dados pessoais estritamente necessários para prestar os serviços mencionados no Contrato de compra ou fornecimento.

Segunda - Confidencialidade e dever de sigilo

Salvo acordado em contrário pelas Partes, as mesmas e as restantes sociedades pertencentes ao grupo ou que tenham vínculo ao mesmo, manterão sigilo absoluto no que diz respeito a este acordo, ao seu negócio e à informação e documentação relativa à outra Parte das quais tenham tido conhecimento como consequência do cumprimento do contrato. Para além disso, o Subcontratante compromete-se especificamente a tratar como confidenciais todas as informações sob responsabilidade do Responsável ou de terceiros às quais possa ter acesso, para efeitos da prestação dos seus serviços e compromete-se a que esses dados permaneçam confidenciais.

Para este efeito, o Subcontratante compromete-se a tomar, relativamente aos seus empregados ou colaboradores, as medidas necessárias para os informar sobre a necessidade do cumprimento das suas obrigações como Subcontratante e que, conseqüentemente, devem respeitar, bem como garantir que os dados pessoais aos quais tenham acesso em virtude do presente contrato

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 32
------------	--	---

permaneçam confidenciais, mesmo após a resolução do presente acordo por qualquer motivo. Como tal, o Encarregado do tratamento levará a cabo todas as advertências (através de formação, mensagens de sensibilização, etc.) e subscreverá os documentos necessários com os seus empregados ou colaboradores, de forma a assegurar o cumprimento dessas obrigações. Estes deverão estar informados de forma compreensível da existência do presente acordo, das normas de segurança que afetam o desenvolvimento das suas funções, das consequências em caso de incumprimento e do carácter confidencial da informação e do dever de sigilo dos dados pessoais, mantendo-se a obrigação de confidencialidade e sigilo mesmo após finalizada a relação com o Subcontratante.

Esta obrigação de informação aos empregados e colaboradores do Subcontratante deverá realizar-se de modo a permitir a documentação e colocação à disposição da PROSEGUR do cumprimento dessa obrigação.

Adicionalmente, a informação e documentação confidencial não poderão ser utilizadas para um fim distinto do cumprimento do objeto do acordo, exceto se essa informação for do conhecimento geral e exceto ao que se refere à informação exigida por força de disposições ou por qualquer outra regulamentação aplicável e obrigatória.

No termo do presente acordo, a obrigação de confidencialidade e o dever de sigilo previstos nesta cláusula continuarão indefinidamente, mesmo após terminar o termo da sua relação com o Responsável pelo tratamento, por qualquer razão.

Caso se detete qualquer tipo de atuação indevida por qualquer pessoa que desempenhe funções profissionais para o Subcontratante (acesso a informação que não corresponde às suas funções, utilização indevida de utilizadores e palavras-chave, um utilizador com mais autorizações que as necessárias ou qualquer outra), será responsabilidade e obrigação expressa do Subcontratante a comunicação imediata à PROSEGUR, juntamente com um relatório detalhado dos factos.

Terceira - Instruções do Responsável pelo tratamento

O Encarregado do tratamento compromete-se a tratar os dados pessoais aos quais tenha acesso unicamente de acordo com as instruções por escrito que, para o efeito, sejam indicadas pelo Responsável pelo tratamento; seguindo sempre, pelo menos, a mesma política de proteção de dados pessoais e a política de medidas de segurança para a sua proteção como as utilizadas para o efeito pela PROSEGUR. Para além disso, este compromisso aplicar-se-á às transferências internacionais de dados pessoais para um terceiro país ou uma organização internacional.

Consequentemente, os dados conhecidos ou obtidos em virtude deste acordo:

- Não poderão ser utilizados para nenhuma outra finalidade diferente da execução do mesmo, terão carácter confidencial e não serão publicados ou dados a conhecer a terceiros sem a autorização prévia por escrito do Responsável pelo tratamento. Em caso algum os dados serão tratados para fins próprios.
- Não serão comunicados a terceiros sem a autorização prévia por escrito da PROSEGUR. Nesse sentido, o Subcontratante, por escrito e antes da PROSEGUR autorizar a comunicação, identificará a entidade ou entidades a quem os dados serão comunicados, quais os dados ou categoria de dados pessoais que serão objeto da comunicação e as medidas de segurança a aplicar para proceder à mesma.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 33
------------	--	---

Como tal, o Subcontratante compromete-se a informar imediatamente o Responsável pelo tratamento caso uma instrução por este dada possa infringir as disposições aplicáveis em matéria de proteção de dados encontradas no ordenamento comunitário ou dos Estados-Membros.

Caso o Subcontratante destine os dados para outro fim, os comunique ou os utilize em incumprimento das estipulações do presente contrato, será considerado igualmente Responsável pelo tratamento, respondendo pessoalmente pelas infrações nas quais tiver incorrido, bem como pelos danos e prejuízos que possa causar neste caso à PROSEGUR.

Quarta - Subcontratação dos serviços

O Encarregado do Tratamento não poderá subcontratar nenhuma das prestações que façam parte do objeto do Contrato que impliquem o tratamento de dados pessoais, exceto prévia autorização expressa e outorgada por escrito por parte da Prosegur.

Caso seja necessário subcontratar algum tratamento, tal deverá comunicar-se previamente e por escrito à Prosegur, indicando os tratamentos que se pretendem subcontratar e identificando de forma clara e inequívoca a empresa subcontratante e os seus dados de contacto.

Em caso de autorização, o subcontratante, que também terá o estatuto de encarregado de tratamento, estará igualmente obrigado a cumprir as obrigações estabelecidas no presente Contrato de Pedido de Tratamento e as instruções definidas pela Prosegur. O Subcontratante inicial é responsável por regular a nova relação em conformidade com o artigo 28 do RGPD, de forma a que o novo subcontratante esteja sujeito às mesmas condições (instruções, obrigações, medidas de segurança. etc.) e com os mesmos requisitos formais que ele, no que diz respeito ao adequado tratamento dos dados pessoais e à garantia dos direitos das pessoas afetadas.

No caso de não cumprimento por parte do sub-encarregado, o Encarregado do Tratamento inicial continuará a ser totalmente responsável para com a Prosegur no que diz respeito ao cumprimento das obrigações.

Quinta - Medidas de segurança

O Subcontratante compromete-se a cumprir as medidas de segurança, de carácter organizativo e técnico, adequadas para assegurar um nível de segurança apropriado ao risco que o tratamento possa originar, de forma a garantir a segurança e a integridade dos dados pessoais e evitar a sua alteração, perda, tratamento ou acesso não autorizado, tendo em conta o estado da tecnologia, os custos de aplicação, a natureza dos dados armazenados, o alcance do tratamento, bem como os riscos a que estão expostos e o impacto que tal pudesse ter sobre os direitos e liberdades das pessoas singulares, independentemente de estes riscos serem causados por atos humanos ou pelo ambiente natural, dando assim cumprimento ao exigido pela legislação em vigor.

O Subcontratante estará sujeito a medidas de segurança consideradas adequadas para a proteção dos dados pessoais e outras informações que deverá ser efetuada pelo Subcontratante e de acordo com o resultado da avaliação dos riscos realizada pela PROSEGUR tendo em conta o estado da tecnologia, os custos de aplicação, a natureza dos dados armazenados, o alcance do tratamento e os riscos a que estão expostos. Neste sentido, o Subcontratante deverá facultar à PROSEGUR a informação necessária nos casos em que a análise de risco realizada por esta ou pelo Subcontratante determine que o tratamento apresenta um risco elevado.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 34
------------	--	---

Assim, o Encarregado do tratamento deverá aplicar sobre os dados pessoais objeto das tarefas de tratamento, no mínimo, as medidas especificadas no APÊNDICE I do presente Contrato.

Sexta - Notificação de falhas de segurança

O Subcontratante terá a obrigação de garantir a implantação dos requisitos de segurança estabelecidos neste contrato e de comunicar à PROSEGUR qualquer incidente que afete a informação, documentação e dados pessoais responsabilidade da PROSEGUR, direta ou indiretamente.

Na eventualidade do Encarregado do tratamento ou qualquer pessoa envolvida nos serviços detetar uma incidência relacionada com roubo, perda ou dano da informação, o acesso à mesma por alguém sem autorização, ou que a informação tenha sido utilizada de forma inapropriada, o Encarregado do tratamento deverá informar imediatamente a PROSEGUR, especificando os detalhes da incidência e sempre antes do prazo de vinte e quatro (24) horas, através do correio eletrónico: dpo@prosegur.com, incluindo toda a informação relevante para a documentação e comunicação da incidência e, como mínimo, a seguinte informação (quando disponível):

1. Descrição da natureza da violação da segurança dos dados pessoais, inclusive, se possível, as categorias e o número aproximado de interessados afetados, e as categorias e o número aproximado de registos de dados pessoais afetados.
2. O nome e os dados de contacto do encarregado da proteção de dados ou de outro contacto junto do qual seja possível obter mais informações.
3. Descrição das possíveis consequências.
4. Descrição das medidas adotadas ou propostas para resolver a falha de segurança dos dados pessoais, incluindo, se necessário, as medidas para mitigar os possíveis efeitos negativos.

Se não for possível facultar as informações simultaneamente, serão facultadas gradualmente sem demoras indevidas.

O Subcontratante será responsável por realizar as ações de contenção e resolução do incidente que forem necessárias.

A PROSEGUR efetuará um acompanhamento periódico do estado da resolução do incidente, comprometendo-se o Subcontratante a responder com os relatórios que forem pedidos.

Sétima - Registo das categorias de tratamentos

O Subcontratante, nos casos determinados pelo Regulamento Geral de Proteção de Dados e pela restante legislação aplicável na matéria, deverá registar, por escrito, todas as categorias de tratamentos efetuados em nome da PROSEGUR incluindo:

1. Os dados de contacto da PROSEGUR e do Encarregado do tratamento bem como, se aplicável, dos seus representantes e gestores de proteção de dados.
2. As categorias de tratamentos realizados em nome da PROSEGUR.
3. Se aplicável, as possíveis transferências internacionais de dados que se podem efetuar no âmbito do tratamento específico.
4. Uma descrição geral das medidas de índole técnica e organizativa aplicadas.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04 23/06/2023 Página 35
------------	--	---

Oitava - Transferências Internacionais

Em termos gerais, o Subcontratante não poderá efetuar transferências internacionais dos dados sob responsabilidade do Responsável pelo tratamento fora do Espaço Económico Europeu, exceto se existir uma autorização prévia deste por escrito.

Caso o Subcontratante tenha de transferir dados pessoais para um país terceiro ou para uma organização internacional, em virtude do Direito da União ou dos Estados-Membros que seja aplicável, informará o responsável sobre essa exigência legal previamente, exceto se esse Direito o proibir por razões relevantes de interesse público.

Se o Responsável pelo tratamento autorizar as transferências internacionais de dados mencionadas e se os dados forem transferidos para um país sem um nível adequado de proteção ou equivalente, devem-se assinar as cláusulas contratuais-tipo estabelecidas para o efeito pela Comissão Europeia. Neste sentido, o Subcontratante deverá facultar estas formalidades ao Responsável pelo tratamento antes da realização da transferência internacional de dados.

Nona - Direitos dos interessados

O Encarregado dará assistência ao responsável, através da aplicação das medidas técnicas e organizacionais apropriadas, e em conformidade com a natureza dos dados tratados, em relação aos pedidos que tenham por objeto o exercício dos direitos dos interessados e, em particular, os seus direitos de acesso, retificação, apagamento ("direito a ser esquecido"), oposição ao tratamento dos seus dados, pedido de portabilidade dos seus dados pessoais, limitação do tratamento, bem como o direito a não ser objeto de uma decisão individual automatizada, incluindo a criação de perfis.

Caso as pessoas afetadas exerçam os direitos mencionados no parágrafo anterior para com o Encarregado do tratamento, este deverá comunicá-lo por correio eletrónico a: protecciondedatos@prosegur.com. A comunicação deverá ser feita de forma imediata e, em nenhum caso após o dia útil seguinte à receção do pedido, juntamente, se for necessário, com outras informações que possam ser relevantes para resolver o pedido.

Décima - Devolução ou destruição dos dados

Uma vez cumprido o serviço contratual, o Encarregado compromete-se a devolver à Prosegur os dados pessoais e, caso aplicável, os suportes onde estão armazenados, após cumprido o serviço. A devolução deve incluir o apagamento completo dos dados existentes nos equipamentos de computação utilizados pelo Encarregado do tratamento.

Para além disso, o Subcontratante deverá garantir que ao cessar a relação contratual com qualquer pessoa que desempenhe uma função profissional:

- A pessoa devolve e não conserva de forma alguma a informação e meios da PROSEGUR.
- O anterior será confirmado por escrito ou através de qualquer forma semelhante permitida pelo quadro jurídico em vigor.
- O cancelamento imediato das autorizações aos processos de informação.

Não obstante o acima indicado, o Encarregado do tratamento pode manter uma cópia, com os dados devidamente bloqueados, durante o período de tempo das responsabilidades pela realização dos serviços.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 36
------------	--	---

Décima primeira - Auditoria

A PROSEGUR, em cumprimento da sua capacidade de controlo, poderá realizar inspeções por conta própria que verifiquem o cumprimento das políticas e medidas de segurança exigidas neste contrato para a proteção de informação e dados pessoais. As inspeções podem ser aos sistemas de informação e instalações de tratamento de dados do Subcontratante ou através da recolha de informações que atestem o cumprimento por parte do Subcontratante.

De qualquer forma, o Subcontratante deverá manter à disposição da PROSEGUR a documentação (em suporte físico ou eletrónico) que ateste o cumprimento das suas obrigações conforme o contrato.

Para além disso, o Subcontratante deverá atestar que realizou as análises de riscos correspondentes e, se tal for indicado pela PROSEGUR, as avaliações de impacto sobre a proteção de dados relevantes.

A fim de facilitar ou até mesmo evitar a inspeção por parte da PROSEGUR, o Subcontratante poderá fornecer as certificações relevantes cujos âmbitos de aplicação incluam os serviços e o pessoal facultados por esta à PROSEGUR. Se o Subcontratante optar por fornecer as certificações mencionadas, deverá para além disso fornecer a documentação relevante, certificação, âmbito de aplicação, bem como apresentar os relatórios das auditorias às que se encontra submetido de acordo com a certificação. Caso a PROSEGUR detete incumprimentos de segurança incompatíveis com a prestação do serviço, segundo a análise de riscos realizada por esta, dependendo da gravidade dos riscos poderá exigir ao Subcontratante a resolução imediata dos problemas detetados através da elaboração de um plano detalhado de medidas corretivas.

O acima exposto sem prejuízo de realizar quaisquer outras auditorias ou revisões para efeitos de verificação de outras obrigações contidas neste acordo.

Décima segunda - Dever de diligência

O Encarregado do tratamento compromete-se a proporcionar ao Responsável pelo tratamento todas as informações necessárias para provar o cumprimento das suas obrigações, e informará o Responsável pelo tratamento em relação à sua adesão a um código de conduta aprovado, ou ao seu vínculo a qualquer mecanismo de certificação que possa garantir o cumprimento das suas obrigações em relação ao tratamento de dados pessoais.

As pessoas que desempenham funções profissionais para o Subcontratante devem estar conscientes da importância da informação da PROSEGUR, tratar a mesma de forma segura e ter formação e qualificação em todas e cada uma das fases do processo da informação, para todas e cada uma das funções desempenhadas. Estas deverão observar todas as diligências possíveis e as medidas adequadas para proteger o processo da informação em cumprimento do seu dever de boa fé a que estão obrigadas contratualmente.

Décima terceira - Dever de informação

Os dados pessoais dos contactos do Subcontratante serão, por sua vez, tratados pela PROSEGUR, com sede social em calle Pajaritos, 24, Madrid, na qualidade de Responsável pelo tratamento, de forma a gerir a relação mantida com este na sua condição de fornecedor de serviços e com base na execução da prestação de serviços, podendo este exercer os seus direitos de acesso, retificação, apagamento, oposição, limitação do tratamento, portabilidade e a não ser objeto de decisões individualizadas automatizadas, enviando um correio eletrónico para o endereço de e-mail

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 37
------------	--	---

protecciondedatos@prosegur.com, anexando uma cópia do seu CC ou documento de identificação equivalente. O interessado terá igualmente direito a apresentar uma reclamação em matéria de proteção de dados à Agência Espanhola de Proteção de Dados. A Prosegur irá tratá-los enquanto durar a relação contratual, momento em que serão bloqueados durante os prazos de prescrição das ações legais aplicáveis.

Décima quarta – Inteligência Artificial

Caso a prestação dos serviços envolva a utilização de soluções de Inteligência Artificial pelo Encarregado do tratamento, este garantirá que a solução de Inteligência Artificial cumpre os princípios e requisitos detalhados no **APÊNDICE II** deste Contrato.

Da mesma forma, o Encarregado do Tratamento garante o cumprimento dos requisitos exigidos pela regulação em vigor aplicável ao caso específico.

A este respeito, o Encarregado do Tratamento implementará as medidas necessárias para garantir e demonstrar o cumprimento das obrigações estabelecidas no parágrafo anterior.

A PROSEGUR, em cumprimento da sua capacidade de controlo, poderá realizar revisões que verifiquem o cumprimento das políticas e medidas exigidas neste acordo para a implementação de soluções de Inteligência Artificial. O Encarregado do Tratamento compromete-se a participar no processo de avaliação e a implementar as medidas solicitadas pela PROSEGUR para cumprir a sua Política de Inteligência Artificial Responsável.

Décima quinta - Indemnidade.

O Encarregado do tratamento compromete-se a isentar a Prosegur em caso de qualquer reclamação que possa ser apresentada contra a Prosegur à Autoridade de Controlo correspondente, que tenha como origem o não cumprimento do Encarregado do Tratamento e/ou dos seus subcontratantes das disposições no presente contrato e na legislação em vigor em matéria de proteção de dados pessoais, e aceita pagar o montante que, em conceito de sanção, multa, indemnização, danos, prejuízos e juros a Prosegur possa ser condenada a pagar, incluindo honorários de advogados, em virtude do citado não cumprimento.

Décima sexta - Jurisdição

O presente acordo será regido e interpretado de acordo com as leis de Espanha com renúncia a qualquer outra jurisdição que possa corresponder, e submete-se à jurisdição exclusiva dos Tribunais da cidade de Madrid.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 38
------------	--	---

APÊNDICE I. - MEDIDAS DE SEGURANÇA

Em conformidade com os artigos 28 e 29 da GDPR, esta secção refere-se às medidas de segurança que o Encarregado do tratamento deve tomar para garantir o nível de segurança adequado ao risco.

O Encarregado do Tratamento deve implementar as seguintes medidas técnicas e organizacionais de segurança, de forma a garantir a segurança adequada dos dados pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danos.

1. Medidas organizativas

O Encarregado do Tratamento estará obrigado a cumprir as medidas em relação ao pessoal ao que será dado acesso aos dados pessoais:

I. Medidas organizativas genéricas

1. O Encarregado do Tratamento deverá garantir a existência e publicação de uma política de Segurança da Informação e de Proteção de Dados para garantir que o Encarregado do tratamento implemente as medidas necessárias para garantir um nível de segurança adequado ao risco, e a proteção de dados pessoais é realizada de acordo com a legislação aplicável em vigor.
2. O Encarregado do Tratamento deverá garantir a existência de uma estrutura (departamento atribuído/função) responsável pela segurança da informação e pela proteção de dados pessoais (dados internos e dados externos de outros clientes).
3. Realizar o inventário dos recursos (servidores, computadores, aplicações de software, cópias de segurança) que contêm dados pessoais.

II. Adesão e cumprimento das Políticas Corporativas da PROSEGUR

1. O Encarregado do Tratamento adere à Política de Segurança da Informação da PROSEGUR (NG/GLO/GR/04), ao documento sobre Requisitos de Segurança da Informação para projetos de novas tecnologias (NE/GLO/GR/SI/12), e à Política Geral de Proteção de Dados (NG-GLO-LEG-12 - 3P), até a sua versão mais recente. Para tal efeito, serão de aplicação as disposições dos referidos documentos e todas as medidas de segurança neles definidas ou referidas.

III. Medidas genéricas relativas ao pessoal

1. O Encarregado do Tratamento deve elaborar e aplicar uma Política de Segurança da Informação que se ajuste às melhores práticas de segurança e que inclua as obrigações relativas ao pessoal.
2. O Encarregado do Tratamento deve garantir que o pessoal atribuído ao serviço tenha as habilidades e capacidades adequadas para desempenhar as suas funções.
3. O Encarregado do Tratamento deverá garantir a elaboração de um programa de formação e sensibilização para os fornecedores, empregados e terceiros da organização que tratem dados pessoais. Todos os utilizadores que acedam aos dados pessoais devem ter recebido uma formação adequada sobre as funções a desempenhar.
4. Os contratos de trabalho devem incorporar cláusulas específicas de adesão às políticas de segurança e privacidade da organização e devem ser assinados pelos novos empregados antes de ser concedido o direito de acesso aos bens, recursos ou instalações para o tratamento de dados pessoais.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 39
------------	--	---

IV. Dever de confidencialidade e segredo

1. Com o objetivo de impedir o acesso de pessoal não autorizado aos dados pessoais, o Encarregado do Tratamento deve garantir a adoção de medidas para evitar que os dados pessoais sejam expostos a terceiros (monitores sem supervisão, documentos impressos deixados em áreas de acesso público, suportes com dados pessoais, etc.). Esta consideração inclui os ecrãs utilizados para ver imagens do sistema de videovigilância, caso existam. O pessoal bloqueará o ecrã ou terminará a sessão ativa sempre que deixar a sua mesa ou posto de trabalho.
2. O Encarregado do Tratamento deve garantir que os documentos impressos e os meios eletrónicos serão armazenados num local seguro (armários ou prateleiras de acesso restrito) 24 horas por dia e sob custódia quando estejam fora dos respetivos dispositivos de armazenamento ou salas de arquivo.
3. Os documentos impressos (em papel) ou eletrónicos (CD, pens, discos rígidos, etc.) que contenham dados pessoais não poderão ser eliminados a menos que a sua destruição possa ser garantida, para que a informação contida seja irrecuperável.
4. Os dados pessoais ou qualquer outro tipo de informações pessoais não poderão ser divulgados a terceiros, com especial cuidado para não revelar dados pessoais protegidos em conversas telefónicas, correios eletrónicos, etc.
5. O dever de confidencialidade e segredo permanece mesmo depois da conclusão da relação laboral ou da prestação de serviços.

V. Direitos dos titulares dos dados

1. O Encarregado do Tratamento deve dispor de um protocolo de ação para atender os interessados que exerçam os seus direitos, de forma a garantir uma resposta rápida e eficaz no exercício dos mesmos.
2. O Encarregado do Tratamento deve processar os pedidos de exercício dos direitos de proteção de dados, incluindo, mas não se limitando a, acesso, retificação e apagamento.
3. O Encarregado do Tratamento deve informar o Responsável pelo Tratamento sobre estes pedidos e ajudar o Responsável pelo Tratamento na atenção dos mesmos.

VI. Violações da segurança dos dados pessoais

1. O Encarregado do Tratamento deve dispor de um procedimento para gerir e notificar eventos (incidentes, vulnerabilidades, problemas, etc.) através do qual os eventos devem ser corretamente gestionados e comunicados ao Responsável pelo Tratamento.
2. Em caso de violação dos dados pessoais, como roubo ou acesso não autorizado a dados pessoais, o Responsável pelo Tratamento será imediatamente informado da violação, incluindo todas as informações necessárias para esclarecer os casos e acontecimentos que possam ter levado ao acesso não autorizado aos dados pessoais. Da mesma forma, será prestada assistência ao Responsável pelo Tratamento para notificar a Autoridade de Controlo e, se for caso, os interessados afetados, sobre a violação dos dados pessoais, tendo em conta as informações disponíveis pelo Encarregado do Tratamento.
3. O Encarregado do Tratamento deve manter um registo de todas as tarefas de manutenção e/ou suporte dos sistemas do Responsável pelo Tratamento.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 40
------------	--	---

2. Medidas técnicas.

I. Medidas relacionadas com o controlo do acesso físico e ambiental

1. As instalações deverão dispor de medidas de segurança perimetral (muros, vedações, portas de acesso, barreiras, videovigilância, mecanismos de autenticação de acesso às instalações, receção de visitantes, etc.) para proteger os sistemas de informação e os dados pessoais contra o acesso físico não autorizado e a manipulação.
2. Os acessos às salas e escritórios nos quais os dados pessoais são tratados deverão dispor de medidas técnicas e organizacionais de proteção contra o acesso não autorizado (controlo eletrónico de acesso, videovigilância, janelas equipadas com um sistema de deteção de quebra ou alterações, procedimento de pedido de acesso à sala ou escritório, identificação pessoal, sistema de alarme de deteção de intrusos).
3. Deve ser necessária uma autorização prévia para a retirada de dispositivos de suporte de armazenamento (discos rígidos, dispositivos amovíveis, fitas de cópias de segurança) das instalações.
4. As entradas e saídas das áreas de segurança das instalações deverão estar restringidas e controladas através de mecanismos de controlo de acesso e videovigilância para garantir que apenas o pessoal autorizado possa ter acesso a estas áreas.
5. O Encarregado do Tratamento deverá garantir a aplicação de medidas técnicas e organizacionais para proteger os dados contra ameaças imediatas, tais como fugas de água, incêndios no centro de tratamento de dados, falhas de energia, vandalismo, etc.

II. Medidas relativas ao controlo de acesso lógico

1. O Encarregado do Tratamento deverá definir, documentar e estabelecer um processo de gestão de contas normalizado para o acesso aos sistemas de informação que tratam dados pessoais (pedido de autorização, criação, edição e apagamento).
2. O acesso aos dados pessoais ou aos sistemas de tratamento de dados pessoais só poderá ser dado aos utilizadores que possuírem as autorizações correspondentes (de acordo com o processo estabelecido).
3. O Encarregado do Tratamento deve documentar e implementar um processo para garantir que as contas de acesso ao sistema sejam alteradas em conformidade, após alterações organizacionais (por exemplo, alterações funcionais, rescisões, despedimentos, etc.).
4. O Encarregado do Tratamento deve garantir que cada conta de utilizador tem um ID único atribuído e inequívoco.
5. As alterações feitas nas contas dos utilizadores devem ser rastreáveis (criação, edição, cancelamento) e deve ser mantido um registo (por exemplo, em documentos ou registos em sistemas de informação).
6. O Encarregado do Tratamento deverá garantir a revogação das autorizações dos utilizadores imediatamente após o fim da relação contratual (incluindo a subcontratação).
7. As contas de acesso privilegiado aos sistemas de tratamento de dados pessoais devem estar restritas apenas ao pessoal autorizado e limitadas em número.
8. As contas privilegiadas apenas devem ser concedidas ao pessoal qualificado tecnicamente que tenha feito previamente um curso específico de formação e sensibilização para a gestão e utilização de contas privilegiadas.

9. Os utilizadores que necessitem realizar atividades privilegiadas com dados pessoais devem ter duas contas no sistema: uma conta normal para levar a cabo as tarefas e operações de rotina e uma conta privilegiada para levar a cabo as tarefas que necessitem de autorizações privilegiadas.
10. As palavras-passe padrão das contas de utilizador devem cumprir os seguintes requisitos de complexidade e segurança:
 - Devem ser armazenadas de forma encriptada nos sistemas de informação.
 - As palavras-passe não devem ser mostradas durante o processo de introdução da palavra-passe pelo utilizador.
 - A palavra-passe deve ser alterada obrigatoriamente após a introdução da palavra-passe inicial de acesso ao sistema.
 - A validade máxima da palavra-passe deve ser de noventa (90) dias. O sistema deverá forçar a alteração obrigatória da palavra-passe após o prazo de validade máxima.
 - O comprimento mínimo da palavra-passe deve ser de oito (8) caracteres (incluindo 2 números ou caracteres especiais).
 - O histórico de palavras-passe deve ser, no mínimo, de três (3).
 - O número de tentativas incorretas consecutivas na altura de introduzir a palavra-passe antes que a conta fique bloqueada deve ser, no máximo, de três (3).
 - A conta ficará bloqueada automaticamente após, no mínimo, 15 minutos caso se tenha introduzido a palavra-passe incorreta repetidamente.
 - Será necessário impedir a introdução de palavras-passe comuns ou fáceis de adivinhar.
11. O controlo do acesso aos dados e aos sistemas de informação que tratam dados pessoais deve basear-se num conceito de funções e permissões formalmente documentadas.
12. A atribuição de autorizações/funções deve ser válida apenas por um período limitado e ser feita tendo em conta os princípios de segregação de funções (SoD) e o princípio do mínimo privilégio.
13. Devem estar registadas as funções e autorizações concedidas aos sistemas de informação utilizados para o tratamento de dados pessoais.
14. As autorizações concedidas devem ser revistas periodicamente (pelo menos uma vez por ano) para garantir o seu cumprimento e validade.
15. Deve existir uma política clara de controlo e de divulgação regular entre os empregados, que forme parte das atividades de sensibilização levadas a cabo pela organização.
16. Os computadores e postos de trabalho do Encarregado do Tratamento com acesso aos sistemas de informação que tratam dados pessoais devem dispor de um protetor de ecrã protegido por palavra-passe, ativado automaticamente após um período de inatividade não superior a quinze (15) minutos.
17. Os empregados e terceiros que utilizem os computadores e estações de trabalho do Encarregado do Tratamento devem estar obrigados a bloquear os seus monitores quando deixam os seus escritórios ou estações de trabalho.

III. Medidas relativas ao controlo de transferência, armazenamento e portabilidade

1. Todas as transferências eletrónicas de dados pessoais devem estar encriptadas, quando aplicável.
2. Os dados pessoais tratados de forma automatizada deverão ser armazenados de forma encriptada, quando aplicável.
3. Um registo das transmissões de dados pessoais através de um suporte físico deve ser formalizado e guardado (por exemplo, memórias amovíveis, fitas de backup, CD, discos rígidos, etc.).
4. A administração remota dos sistemas de informação que tratam dados pessoais deve ser realizada através de um canal de comunicação seguro (SSH, IPSec, TLS /SSL, VPN, etc.).
5. O Encarregado do Tratamento incorporará medidas técnicas nos sistemas de informação para evitar a possibilidade de exportação não autorizada de dados pessoais (por exemplo, a restrição das características funcionais para descarregar, imprimir e armazenar dados nos sistemas de informação que tratam dados pessoais).
6. O suporte físico utilizado para a transmissão dos dados pessoais deve estar encriptado.
7. Antes de eliminar os meios eletrónicos (USB, discos rígidos, etc.) que tratam dados pessoais sensíveis, estes meios devem ser apagados de forma segura (tornando os dados irre recuperáveis).

IV. Controlo de gestão de incidentes de segurança

1. Os computadores e periféricos (por exemplo, plataformas de correio eletrónico, sistemas de acesso à Internet) terão uma aplicação para detetar e proteger contra software malicioso (por exemplo, vírus, trojans, etc.), que deve ser atualizada periodicamente.
2. O Encarregado do Tratamento deve dispor de um procedimento de gestão de eventos de segurança que estabeleça os critérios para classificar, priorizar e escalar os incidentes de segurança.
3. O Encarregado do Tratamento deve avaliar periodicamente a disponibilidade das atualizações de segurança para os sistemas de IT e para os seus componentes (incluindo clientes, componentes de rede, servidores, etc.) que tratam dados pessoais. As atualizações de segurança são instaladas regularmente através de um processo formal.
4. Os sistemas de informação que tratam dados pessoais devem ser analisados regularmente para detetar vulnerabilidades conhecidas. As vulnerabilidades detetadas devem ser classificadas com base na sua criticidade e impacto na segurança, e corrigidas em conformidade.
5. O Encarregado do Tratamento deve contar com uma equipa de resposta a eventos de segurança para responder aos eventos de segurança e contribuir para a coordenação da resolução destes eventos de segurança.

V. Controlo de resiliência operacional

1. O Encarregado do Tratamento deve definir, documentar e implementar planos de continuidade de IT que abranjam os sistemas e componentes de IT críticos.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 43
------------	--	---

2. O Encarregado do Tratamento deve ter ferramentas para detetar e prevenir intrusões e ciberataques (por exemplo, firewalls, IPS, IDS, ferramentas para detetar e prevenir ataques direcionados, etc.).
3. O Encarregado do Tratamento deve ter ferramentas ou serviços para detetar e limitar o impacto de ataques de recusa de serviço (por exemplo, DoS, DDoS, etc.).
4. O Encarregado do Tratamento deve executar regularmente simulações de ataques informáticos (por exemplo, testes de intrusão/penetração). Os desvios detetados devem ser avaliados e corrigidos regularmente, de acordo com um procedimento definido.
5. Os componentes e dispositivos que tratam dados pessoais devem ser protegidos através da aplicação das medidas técnicas e organizacionais correspondentes, contra desastres causados por elementos naturais (por exemplo, incêndios, inundações, tornados, etc.).
6. As redes de telecomunicações do Encarregado do Tratamento devem ser segmentadas, através da implementação de firewalls para poder limitar o seu impacto em caso de um evento de segurança.
7. Existe uma política de cópias de segurança para os dados tratados por sistemas informáticos. A política deve estabelecer o alcance dos sistemas de IT, a frequência das cópias de segurança, o período de armazenamento, a localização física das cópias e as medidas de segurança para garantir a confidencialidade e integridade (por exemplo, encriptação). A política também considera requisitos regulamentares e legais.
8. As cópias de segurança regulares dos sistemas informáticos (incluindo dados de configuração do sistema) que tratam dados pessoais devem ser realizadas de acordo com a política estabelecida.

VI. Controlo de desenvolvimento e operações de aplicações de IT

1. O Encarregado do Tratamento deve incluir a segurança como elemento integrado no seu ciclo de vida de desenvolvimento de software, através da adoção de padrões reconhecidos internacionalmente para o desenvolvimento de aplicações seguras. O Encarregado do Tratamento deve identificar e implementar requisitos legais e de segurança durante as fases iniciais de desenvolvimento.
2. Deve ser mantido um registo para utilizadores e administradores na medida em que as atividades estejam relacionadas com o acesso à aplicação (login/logout, tentativas bem-sucedidas/falhas, etc.). O registo permite identificar pelo menos quem realizou a ação, quando foi realizada, e o tipo (por exemplo, início de sessão, tentativa de acesso, etc.).
3. Os dados de registo devem ser armazenados de forma segura e o acesso aos mesmos deve ser restrito ao pessoal autorizado. Os registos que devem ser armazenados tendo em conta o seu conteúdo e/ou requisitos legais devem ser eliminados após o cumprimento do seu propósito.
4. O Encarregado do Tratamento deve realizar testes (estáticos/dinâmicos) sobre o código-fonte que ele ou um terceiro está a desenvolver, antes da implantação no ambiente de produção.
5. Os ambientes que não são de produção (p. ex., desenvolvimento, testes, consolidação) devem ser completamente separados do ambiente de produção.

SISTEMA 3P	<p>Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.</p>	<p>Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 44</p>
------------	---	--

VII. Controlo de segurança e cumprimento

1. O Encarregado do Tratamento deverá realizar periodicamente (pelo menos uma vez por ano) e de forma independente revisões de segurança dos sistemas informáticos que tratam dados pessoais, para garantir o cumprimento e a eficácia dos controlos técnicos, organizacionais e legais estabelecidos. Deve ser mantido um registo dos testes (e dos resultados dos testes). Os desvios são avaliados, priorizados e corrigidos.
2. Realizar simulações e testes periódicos dos planos de continuidade do serviço de IT estabelecidos (pelo menos anualmente). Deve ser mantido um registo dos testes (e dos resultados dos testes). Os desvios serão avaliados, priorizados e corrigidos.
3. O Encarregado do Tratamento deverá realizar revisões periódicas (pelo menos uma vez por ano) sobre a segurança dos controlos de segurança física e ambiental implementados para garantir a sua eficácia. Deve ser mantido um registo dos testes (e dos resultados dos testes). Os desvios são avaliados, priorizados e corrigidos.
4. O Encarregado do Tratamento deve realizar testes periódicos das cópias de segurança efetuadas e dos procedimentos de restauração definidos para garantir a integridade e disponibilidade das cópias. Deve ser mantido um registo dos testes (e dos resultados dos testes). Os desvios devem ser avaliados, priorizados e corrigidos.
5. O Encarregado do Tratamento deve rever periódica e independentemente os seus processos de gestão da segurança da informação. O âmbito das revisões deve pelo menos incluir controlos que possam afetar a segurança dos dados pessoais do responsável pelo tratamento dos dados.
6. O Encarregado do Tratamento deve dispor de processos, procedimentos operacionais e instruções para garantir o cumprimento dos requisitos legais e regulamentares, bem como os regulamentos aplicáveis à natureza do serviço.

APÊNDICE II.- INTELIGÊNCIA ARTIFICIAL RESPONSÁVEL

A solução de Inteligência Artificial proposta pelo FORNECEDOR deve cumprir os seguintes princípios:

Respeito da autonomia humana

O respeito pela liberdade e autonomia humana deve ser garantido. O sistema de IA proposto deve ser concebido de tal forma que as habilidades cognitivas, sociais e culturais dos indivíduos sejam melhoradas; a supervisão e o controlo humano sobre os processos de trabalho do sistema de IA proposto deve ser garantido.

Princípio da prevenção de danos

Deve ser garantido que o sistema de IA não causará quaisquer danos aos seres humanos, protegendo a dignidade humana, bem como a integridade física e mental.

O sistemas e o ambiente de IA são tecnicamente seguros e robustos e não serão utilizados de forma maliciosa em nenhuma circunstância.

Deve também ser dada especial atenção aos possíveis efeitos adversos de um sistema de IA e devem ser estabelecidas medidas específicas de mitigação para evitar possíveis danos.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04. 23/06/2023 Página 45
------------	--	--

Princípio da equidade

Deve garantir que o desenvolvimento, implantação e utilização do sistema de IA seja equitativo, com o compromisso de assegurar uma distribuição justa e igualitária dos benefícios e custos, e assegurar que indivíduos e grupos não sofram preconceitos, sejam discriminados ou estigmatizados injustamente.

O FORNECEDOR deverá evitar preconceitos injustos, e pode estabelecer medidas específicas para aumentar a equidade social através da utilização de sistemas de IA.

Para além, a utilização do sistemas de IA proposto respeitará o princípio da equidade, entendido como a capacidade de oferecer a possibilidade de oposição às decisões adotadas pelos sistemas de IA, bem como de transmitir a sua oposição às pessoas que as administram, e a proporcionalidade entre meios e fins, pelo que analisará cuidadosamente a forma de encontrar um equilíbrio entre diferentes interesses e objetivos concorrentes.

Princípio da explicabilidade

A explicabilidade do sistema de IA proposto deve-se ao facto de todos os processos que envolvem o desenvolvimento de IA serem transparentes, sendo as capacidades e o objetivo do sistema de IA clara e concisamente comunicados às partes envolvidas.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 46
------------	--	---

Requisitos para soluções de IA Responsável

Os requisitos principais que a solução do sistema de IA deve garantir para ser uma IA Responsável são os seguintes, que devem ser continuamente avaliados e tratados ao longo de todo o ciclo de vida dos sistemas de IA:

Ação e supervisão humana

Os sistemas de IA devem apoiar a autonomia e a tomada de decisões das pessoas, apoiando a ação humana e promovendo os direitos fundamentais, além de permitir a supervisão humana.

O FORNECEDOR garantirá, na medida do possível, um mínimo de intervenção humana na tomada de decisão automatizada dos sistemas de IA, com o objetivo principal de preservar a adoção de decisões éticas e não discriminatórias que garantam os direitos e liberdades das pessoas cujas informações são tratadas.

Solidez técnica e segurança

A solidez técnica exige que o sistema de IA seja desenvolvido com uma abordagem preventiva dos riscos, para que se comportem sempre como esperado e minimizem os danos não intencionais e imprevistos, e evitem causar danos inaceitáveis, e devem garantir a integridade física e mental dos seres humanos.

Para este efeito, o FORNECEDOR deve assegurar que o sistema de IA é robusto e cumpre as medidas de segurança adequadas para garantir a confidencialidade, integridade e disponibilidade das informações neles armazenadas e tratadas.

Para o efeito, deve realizar testes e avaliações de segurança rigorosos para garantir que o sistema de IA responde adequadamente a incidentes de segurança que possam causar a destruição, perda, alteração accidental ou ilegal, ou divulgação ou acesso não autorizado às referidas informações.

Privacidade e governação dos dados

O sistema de IA deverá respeitar a prevenção de danos à privacidade, o que implica uma gestão adequada dos dados, incluindo a qualidade e integridade dos dados. Consequentemente, o sistema de IA, o seu protocolo de acesso e a sua capacidade de tratar dados deve ser desenvolvido sem violar a privacidade.

No caso da solução de Inteligência Artificial fornecida pelo FORNECEDOR tratar dados pessoais, o FORNECEDOR, enquanto responsável pelo sistema de IA, deverá implementar medidas de segurança legais, organizacionais e técnicas adequadas para garantir a proteção das liberdades e direitos fundamentais dos interessados que possam ser afetados, no estrito cumprimento do Regulamento Geral de Proteção de Dados, REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 (doravante, RGPD) e dos regulamentos locais aplicáveis. Garante também que apenas serão tratados os dados estritamente necessários para cada um dos fins previstos, limitando a sua conservação ao período de tempo.

Transparência

Para que um sistema de IA seja transparente, deve dispor de (i) rastreabilidade: que as decisões do sistema de IA sejam registadas para poder identificar os motivos de uma decisão errada do sistema, o

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 47
------------	--	---

que ajuda a evitar erros futuros, (ii) explicabilidade: que as decisões adotadas por um sistema de IA sejam compreensíveis para os seres humanos e que tenham a possibilidade de as rastrear e (ii) comunicação: que as pessoas estejam cientes de que estão a interagir com um sistema de IA, o sistema de IA deve ser identificado como tal, bem como, quando necessário, seja facultada ao utilizador a opção de decidir se prefere interagir com um sistema de IA ou com outra pessoa, a fim de garantir o cumprimento dos direitos fundamentais.

Diversidade, não discriminação e equidade

Para que um sistema de IA Responsável seja de confiança, deve garantir a inclusão, diversidade, igualdade de acesso, através de processos de conceção inclusivos, bem como a igualdade de tratamento em todo o seu ciclo de vida.

Para além, no desenvolvimento interno e/ou aquisição de soluções de IA, o FORNECEDOR garantirá, em qualquer caso, a igualdade e não discriminação das pessoas que possam ser afetadas pela sua utilização e, em particular a discriminação por razão da raça, cor, origem étnica ou social, sexo, orientação sexual, idade, características genéticas, língua, religião ou convicções políticas ou qualquer outra.

Bem-estar ambiental e societal

O FORNECEDOR promoverá a sustentabilidade e a responsabilidade ecológica através de sistemas de IA, e promoverá a investigação de soluções de Inteligência Artificial para abordar questões como o Desenvolvimento Sustentável.

Responsabilização

O FORNECEDOR implementará mecanismos para garantir a responsabilidade e responsabilização pelo sistema de IA e pelos seus resultados, tanto antes como depois da implementação.

A este respeito, o FORNECEDOR é responsável pelas ações e decisões tomadas por um sistema de IA, especialmente à medida que se avança para sistemas mais autónomos capazes de tomar decisões automatizadas e, em particular, quando tais decisões têm efeitos legais sobre o interessado.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 48
------------	--	---

7.5. ANEXO IV: Requisitos de Risco Tecnológico e Cibersegurança.

7.5.1. Requisitos de Risco Tecnológico e Cibersegurança.

7.5.1.1 Considerações prévias

O tratamento de informações e dados pessoais sob a responsabilidade do Grupo Prosegur nas instalações do Fornecedor está expressamente autorizado para os fins previstos no contrato referido neste anexo. Do mesmo modo, é dada autorização explícita para a remoção de suportes e documentação contendo informações do Grupo Prosegur, se aplicável, para a prestação dos serviços contratados. Para a transferência de suportes e documentos, o Fornecedor aplicará, em todos os casos as medidas de segurança estabelecidas para cumprir este documento ou os regulamentos em vigor.

O Fornecedor utilizará os recursos de informação e/ou dados de propriedade do Grupo Prosegur no âmbito do desenvolvimento da prestação dos serviços confiados e para os fins previamente estabelecidos.

7.5.1.1.1 Obrigação de guardar reserva

Todo o pessoal do Fornecedor que, como resultado da prestação do Serviço, ou por qualquer outra circunstância, tenha conhecimento de informações relacionadas com o GRUPO PROSEGUR será obrigado a mantê-las secretas ou confidenciais e não as poderá comunicar a terceiros em qualquer altura, seja antes, durante ou após a prestação do Serviço.

O Fornecedor e o seu pessoal somente poderão utilizar as informações para os fins previstos no objeto deste Contrato, sendo responsáveis para com o GRUPO PROSEGUR por quaisquer danos que possam surgir para o GRUPO PROSEGUR em consequência do não cumprimento.

No caso do Fornecedor subcontratar, por sua vez, um terceiro, este último é responsável por respeitar e cumprir os mesmos critérios de confidencialidade e regras sobre informações relacionadas com o GRUPO PROSEGUR, tal como descrito nas cláusulas anteriores.

O Fornecedor, bem como o seu pessoal envolvido na prestação do serviço ao GRUPO PROSEGUR, deve impedir qualquer ação ou omissão que possa resultar na divulgação não autorizada ou na utilização indevida dos Ativos de Informação envolvidos no desenvolvimento do serviço.

7.5.1.1.2 Confidencialidade das informações

O Fornecedor deve, como regra geral, tratar as informações do GRUPO PROSEGUR como informação sensível e tomar as medidas adequadas para tal classificação.

O tratamento da informação deve permitir a rastreabilidade, entendida como a capacidade de saber que pessoas e quando acederam e trataram as informações do GRUPO PROSEGUR. Entende-se por tratamento qualquer atividade realizada sobre a informação, tal como, entre outras, a leitura, escrita, alteração, cópia, transmissão, gravação ou armazenamento da mesma por meios manuais ou com aplicações de software.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 49
------------	--	---

7.5.1.2 Conformidade com a legislação

O Fornecedor deve cumprir todas as leis aplicáveis que afetam o seu âmbito de aplicação, em termos de segurança e privacidade da informação, bem como os regulamentos associados ao sector ao qual o Cliente presta a atividade, requisitos regulamentares, reguladores e estatutários.

7.5.1.2.1 Proteção de dados pessoais

O Fornecedor tem a obrigação de cumprir rigorosamente as disposições da legislação em vigor relativas aos dados pessoais tratados no decurso da prestação dos Serviços objeto deste Contrato.

O Fornecedor deve tratar os Dados com absoluta confidencialidade e de acordo com as instruções recebidas do GRUPO PROSEGUR em relação à finalidade, conteúdo e utilização do tratamento, aplicando a privacidade por defeito e desde a conceção, as medidas técnicas e organizacionais adequadas, e especificamente, com o que é indicado nos acordos de privacidade e nos contratos de cessão de tratamento assinados.

O Fornecedor deve realizar análises de risco regulamentares e de segurança que afetem os dados pessoais e realizar avaliações de impacto da proteção de dados para os tratamentos que sejam necessários de acordo com as disposições da legislação no domínio de aplicação correspondente.

7.5.1.3 Quadro regulamentar de segurança da informação

O Fornecedor deve estabelecer um quadro regulamentar de segurança TI que garanta a correta implementação das medidas de segurança indicadas neste anexo, e que esteja alinhado com os critérios do GRUPO PROSEGUR em relação à segurança aplicável às informações tratadas.

O Fornecedor deve atualizar convenientemente o referido quadro regulamentar de segurança de forma adequada, de acordo com as alterações de serviço e com novas leis, regulamentos ou normas de referência internacionais e nacionais que possam surgir em termos de segurança tecnológica e proteção de informações e dados pessoais, tais como o NIST Cybersecurity Framework, as normas ISO 27000 e 22300 e/ou outras de natureza semelhante.

Este quadro regulamentar deve conter, pelo menos, documentação relacionada com:

- Gestão de utilizadores
- Controlo de acesso e gestão de *logs* de atividade
- Gestão do pessoal
- Formação e sensibilização
- Gestão de incidentes
- Gestão da continuidade do serviço
- Gestão das operações
- Procedimentos de tratamento e destruição das informações

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 50
------------	--	---

- Gestão da mudança
- Desenvolvimento de software e novas aquisições de sistemas
- Política de palavras-passe
- Procedimentos de divulgação e armazenamento das informações
- Modelo de relação e comunicação com o GRUPO PROSEGUR

Cada um dos documentos indicados pode ser solicitado pelo GRUPO PROSEGUR para que possa verificar e comprovar que os requisitos mínimos e garantias acordadas com o Fornecedor são cumpridos.

O Fornecedor deve garantir que os processos de atribuição, distribuição e armazenamento das palavras-passe foram formalizados por escrito, sem exceções para além das que podem ser incluídas nos procedimentos acima mencionados.

O Fornecedor deve comunicar aos seus empregados encarregados da prestação de serviços ao GRUPO PROSEGUR o marco regulamentar, registando a sua aceitação.

7.5.1.3.1 Gestão do risco

O Fornecedor compromete-se a realizar uma análise de risco para determinar as medidas técnicas e organizacionais mais adequadas para garantir e poder demonstrar que o tratamento da informação é realizado de forma responsável, segura, respeitando as dimensões de segurança, bem como como a privacidade e os direitos das pessoas interessadas. Estas medidas devem adotar uma abordagem preventiva em vez de corretiva e ser revistas regularmente, para garantir que são mantidas atualizadas.

O Fornecedor, periodicamente e quando ocorram alterações relevantes no ambiente tecnológico, deve realizar um processo de análise de risco contemplando especificamente os envolvidos no Serviço prestado ao GRUPO PROSEGUR.

O Fornecedor deve ter em vigor um Plano de Tratamento de Riscos para abordar os riscos identificados nas análises que precisam ser tratados. A eficácia das ações definidas para o tratamento de riscos deve ser controlada.

7.5.1.3.2 Esquema de controlo

O Fornecedor compromete-se a cumprir todas as políticas, procedimentos e documentos de segurança específicos elaborados pelo GRUPO PROSEGUR que sejam considerados aplicáveis para as atividades a realizar e que sejam disponibilizados ao Fornecedor assim que os serviços contratados comecem a ser prestados.

Caso o Serviço trate de informações sujeitas a certificações de segurança, o Fornecedor deverá submeter ao GRUPO PROSEGUR, através de solicitação, as certificações correspondentes.

O Fornecedor aceita e compromete-se a cumprir o esquema de controlo aplicável ao serviço prestado, de acordo com a classificação resultante da avaliação realizada pelo GRUPO PROSEGUR, cujo resultado será disponibilizado ao Fornecedor.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 51
------------	--	---

O Fornecedor deve estabelecer os controlos de segurança adequados para reduzir o risco de acesso não autorizado e modificação das informações relevantes contidas nos sistemas (aplicações, sistemas operacionais e bases de dados) que apoiam o serviço e evitam a perda, roubo, indisponibilidade e tratamento não autorizado dos ativos de informação do GRUPO PROSEGUR.

Os requisitos de segurança indicados devem ser aplicados pelo Fornecedor. Caso o Fornecedor subcontrate, por sua vez, a um terceiro, o Fornecedor é responsável por garantir que os requisitos de segurança também são cumpridos por este terceiro.

O GRUPO PROSEGUR reserva-se o direito de modificar os requisitos de segurança contidos neste contrato e nos seus anexos em qualquer altura, notificando o Fornecedor, indicando as datas da sua entrada em vigor.

7.5.1.4 Organização da segurança

7.5.1.4.1 Identificação de responsabilidades

O Fornecedor deve ter estabelecido formalmente Gestores de Risco Tecnológico e de Segurança da Informação para assegurar o cumprimento das políticas de segurança e a monitorização dos controlos para garantir a integridade, confidencialidade e disponibilidade, autenticidade e rastreabilidade dos dados e sistemas, bem como o cumprimento de todos os regulamentos aplicáveis, prestando especial atenção aos relativos à proteção de dados pessoais.

O Gestor de Risco Tecnológico e Segurança deve controlar e coordenar as medidas de segurança aplicadas pelo Fornecedor, especialmente as destinadas à proteção do tratamento de dados pessoais sujeitos à prestação do serviço e realizar revisões periódicas para verificar a conformidade com os aspetos estabelecidos na Documentação de Segurança.

O Fornecedor deve designar um Coordenador encarregado da gestão dos aspetos de segurança com o GRUPO PROSEGUR. Este Coordenador de Fornecedores assite ao Comité de Coordenação composto pelo Fornecedor e pelo GRUPO PROSEGUR, caso seja convocado pelo GRUPO PROSEGUR, para realizar um acompanhamento atempado do serviço e definir os planos de ação necessários para garantir o correto desempenho dos serviços.

O Fornecedor deve estabelecer uma adequada segregação de funções, que estabeleça medidas suficientes e necessárias para garantir que os direitos de acesso (funções e perfis) para cada utilizador do serviço sejam atribuídos de acordo com as necessidades funcionais de cada utilizador e que essas necessidades funcionais não ponham em risco os ativos de informação que fazem parte do serviço subcontratado.

O Fornecedor deve comunicar a existência e as pessoas que desempenham as funções do Security Officer e do DPO (Data Privacy Officer) se tivessem a necessidade ou a obrigação de contar com eles para estabelecer as comunicações adequadas.

O Fornecedor deve comunicar através dos canais estabelecidos com o GRUPO PROSEGUR, qualquer alteração que possa ocorrer em relação à designação inicial dos responsáveis pelo serviço, bem como comunicar, no prazo máximo de 24 horas, qualquer cancelamento de um utilizador participante na prestação do serviço ao GRUPO PROSEGUR.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 52
------------	--	---

7.5.1.4.2 Planos de formação/consciencialização

O Fornecedor deverá implementar planos de formação e consciencialização para a segurança da informação, incluindo todos os empregados que prestam serviços ao GRUPO PROSEGUR.

O Fornecedor deve desenvolver explicitamente um plano de consciencialização sobre a importância da segurança da informação, dos dados pessoais e da sua confidencialidade.

O Fornecedor deve implementar explicitamente um plano de formação sobre a importância do desenvolvimento seguro do código.

7.5.1.4.3 Notificação

O Fornecedor deve comunicar o GRUPO PROSEGUR de qualquer evento diferente do acordo contratual celebrado com o GRUPO PROSEGUR no prazo máximo de 24 horas.

O Fornecedor deve notificar o GRUPO PROSEGUR de qualquer alteração ocorrida durante a prestação do serviço, seja na forma como é prestado (alteração no processo) ou nos sistemas utilizados para prestar o serviço (alteração na infraestrutura), bem como o pessoal envolvido, no período máximo de 24 horas.

7.5.1.5 Medidas tecnológicas

7.5.1.5.1 Classificação e gestão de ativos

O Fornecedor deve ter um inventário dos ativos de informação identificando o tipo de informação contida em cada ativo, a propriedade do ativo, a conservação e o grau de sensibilidade das informações tratadas.

O fornecedor deve estabelecer um processo de Classificação das informações e categorização dos ativos, atribuindo-lhes um nível de segurança em relação aos riscos inerentes e à criticidade dos sistemas e informações suportadas.

O Fornecedor deve manter e atualizar regularmente este inventário, tendo em conta quaisquer alterações aos bens que fazem parte da prestação do serviço.

A identificação dos suportes deve ser realizada com um sistema de rotulagem que só pode ser compreendido pelos utilizadores autorizados.

O Fornecedor deve encriptar dados na distribuição de suportes e em dispositivos portáteis, evitando o processamento em dispositivos portáteis que não permitam encriptação, tomando medidas que tenham em conta os riscos em ambientes desprotegidos.

Garantir o armazenamento seguro dos suportes contendo informações do GRUPO PROSEGUR, num local com acesso restrito ao pessoal autorizado.

O Fornecedor deve implementar mecanismos suficientes para garantir a conservação segura dos suportes com informações do GRUPO PROSEGUR, quando estes não são armazenados em locais seguros.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 53
------------	--	---

O Fornecedor deve ter um Procedimento de Gestão de Suportes que defina os métodos de conservação dos suportes de informação e os responsáveis pela autorização de acesso aos mesmos.

Garantir que qualquer tipo de receção ou entrega de suportes é realizado exclusivamente por pessoal autorizado, quer o destinatário seja uma empresa do GRUPO PROSEGUR ou uma empresa externa.

Ao realizar a transferência da documentação contida num ficheiro, devem ser tomadas medidas para impedir o acesso ou a manipulação das informações contidas

O Fornecedor deve manter um registo da entrada e saída dos suportes que permita conhecer o tipo de suporte ou documento, a data e hora, o remetente e/ou recetor, o tipo de informação, a forma como foi enviada e a pessoa responsável por ela.

O Fornecedor deve tomar medidas para evitar o acesso indevido às informações no caso de suportes descartados.

7.5.1.5.2 Controlo de acesso

O Fornecedor deve estabelecer controlos suficientes e necessários para garantir que o acesso físico e lógico aos sistemas com informações relevantes seja controlado de acordo com os requisitos estabelecidos pelo GRUPO PROSEGUR no quadro regulamentar indicado neste anexo.

O Fornecedor, ao conceder um nível de acesso à informação, aplicações e sistemas envolvidos neste serviço, deve fazê-lo através de um sistema de gestão de identidade, baseado em papéis e funções, tendo em conta o princípio do "menor privilégio", garantindo que apenas o nível mínimo de acesso necessário para uma posição específica é concedido aos seus colaboradores envolvidos no serviço prestado ao GRUPO PROSEGUR.

O Fornecedor deve estabelecer as medidas suficientes e necessárias para garantir que sejam realizadas revisões periódicas das permissões de acesso e controlos de acesso configurados nos sistemas utilizados no serviço.

7.5.1.5.2.1 Controlar o acesso a aplicações e sistemas

O Fornecedor deve implementar os mecanismos necessários para evitar a existência de utilizadores genéricos, exceto os exigidos pelas tecnologias utilizadas. Caso necessário para o desenvolvimento do serviço, estes utilizadores devem ser aprovados e validados pelo GRUPO PROSEGUR.

O Fornecedor deve implementar os mecanismos necessários que permitam identificar inequivocamente os seus utilizadores com acesso aos sistemas que fazem parte do serviço prestado ao GRUPO PROSEGUR. Os códigos de utilizador e palavras-passe não devem ser partilhados entre pessoas. Em qualquer altura, os códigos de utilizador de acesso às aplicações devem permitir ao Fornecedor identificar inequivocamente a pessoa que acede.

O Fornecedor deve registar os dados de cada tentativa de acesso, incluindo informações sobre o utilizador, data e hora, ficheiro acedido, tipo de acesso e se o acesso foi autorizado ou negado. Caso tenha sido autorizado, o registo acedido será guardado.

O Fornecedor deve realizar uma verificação periódica do controlo de acesso, indicando os dados das tentativas de acesso válidas ou não válidas. Estes registos devem ser mantidos durante pelo menos 2 anos para efeitos de busca de provas de eventos de segurança.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04. 23/06/2023 Página 54
------------	--	--

O Responsável de Segurança do Fornecedor deve ter controlo direto sobre o acesso aos mecanismos de controlo de registo de acesso.

O Fornecedor deve implementar os mecanismos necessários para manter um registo atualizado dos utilizadores. O Fornecedor deve manter um registo atualizado para cada sistema ou aplicação envolvida no serviço prestado ao GRUPO PROSEGUR. O registo deve incluir a associação de cada código de utilizador com a pessoa a ele atribuída, o seu perfil e acessos autorizados.

O registo deve indicar todas as alterações no mapeamento: inscrições, anulações e possíveis alterações.

O Fornecedor deve garantir que os seus utilizadores ligados à prestação do serviço que apresentem ausência ou as contas que sejam detetadas como inativas por mais de sessenta (60) dias devem ter as suas contas de utilizador desativadas. Estas contas de utilizador podem ser reativadas se necessário, caso contrário, se a inatividade continuar com o tempo, estas contas serão permanentemente bloqueadas.

O Fornecedor deve garantir que os seus utilizadores ligados à prestação do serviço que alterem as suas responsabilidades profissionais tenham os seus níveis de acesso revistos para determinar se é necessário alterar o perfil atribuído, a fim de garantir que não tenham acesso aos ativos de informação para os quais não têm necessidade comercial válida.

O Fornecedor deve implementar os mecanismos necessários para permitir o processamento imediato das anulações dos utilizadores. As anulações dos utilizadores devem ser realizadas imediatamente, através das ferramentas de administração da aplicação, desativando o acesso à aplicação com o código de utilizador anulado. A anulação de um utilizador significa o seu bloqueio temporário, antes de proceder à sua eliminação definitiva.

O Fornecedor deve implementar os mecanismos necessários para a disponibilidade de mecanismos de registo da atividade dos utilizadores.

O Fornecedor deve implementar os mecanismos necessários para restringir o acesso à Internet ou a qualquer ligação que possa permitir o vazamento de informações sobre os dados tratados.

O Fornecedor deve definir uma Política de Controlo de Acesso/Palavra-passe que estabeleça um quadro regulamentar para o controlo de acesso com base nos requisitos de serviço e de Segurança da Informação.

O Fornecedor deve implementar esses controlos, para garantir que todos os elementos com os quais prestará o Serviço sejam geridos e explorados de forma segura. Estes controlos devem ser disponibilizados ao GRUPO PROSEGUR quando solicitados.

Os controlos indicados no ponto anterior devem incluir:

- Políticas de utilizador/palavra-passe dos operadores e administradores de sistemas ou produtos, incluindo expressamente os gestores de bases de dados.
- Acesso a sistemas com ferramentas que protegem a confidencialidade das palavras-passe dos administradores, por exemplo, SSH no UNIX.
- Proteção de sistemas de servidores contra o acesso não autorizado.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 55
------------	--	---

- Nos casos de acesso a informações confidenciais, o Serviço deverá fornecer mecanismos de autenticação multifator.

O Fornecedor deve incluir na sua Política de Palavras-passe pelo menos os seguintes aspetos:

- Um procedimento de distribuição de palavras-passe que garante que estas sejam conhecidas apenas pelo utilizador.
- Um procedimento para controlar a expiração das palavras-passe e o armazenamento de palavras-passe ininteligíveis.
- Robustez adequada, de acordo com as seguintes regras, na medida do possível: a) mínimo de oito (8) caracteres de comprimento, b) ser maiúsculas, c) minúsculas, d) números e e) caracteres especiais (por exemplo, !, \$, @)
- Expiração da palavra-passe (recomendável 60 dias e não mais que 90), com um procedimento de alteração que não leve a uma interrupção do serviço.
- Armazenamento codificado obrigatório de palavras-passe para os sistemas e aplicações que fazem parte da subcontratação.

O Fornecedor deve implementar os mecanismos necessários para conceder permissões de acesso aos sistemas que prestam serviços ao GRUPO PROSEGUR, apenas ao pessoal autorizado no Documento de Segurança e nas listas de utilizadores de cada um dos sistemas.

O Fornecedor deve estabelecer um mecanismo para limitar o número de tentativas repetidas de acesso não autorizado.

O Fornecedor deve estabelecer controlos suficientes e necessários para garantir que o acesso lógico aos sistemas que detêm informações relevantes seja controlado de acordo com os requisitos estabelecidos pelo GRUPO PROSEGUR.

O Fornecedor deve garantir que os empregados que são obrigados a utilizar ligações remotas para a prestação do serviço cumpram as diretrizes das regras de Acesso Remoto do Grupo Prosegur previstas para a prestação do serviço, uma vez iniciadas as atividades correspondentes e contratadas. Especialmente que:

- Todos os acessos remotos devem ser previamente autorizados pelo Grupo Prosegur.
- As credenciais devem ter um identificador único associado a um utilizador e devem ser intransferíveis.
- No caso de um empregado partilhar as suas credenciais ou partilhar a sua sessão aberta com outros utilizadores:
 - Deve ser considerado como um incidente de segurança
 - O utilizador será imediatamente removido dos sistemas do Grupo Prosegur
 - O empregado e, portanto o fornecedor, será diretamente responsável pelas ações (ou omissões) do utilizador que o representa, e pode estar sujeito às sanções estipuladas por utilização indevida.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04 23/06/2023 Página 56
------------	--	---

O Fornecedor deve estabelecer mecanismos para identificar os acessos efetuados para documentos com acesso de vários utilizadores.

O Fornecedor deve estabelecer medidas suficientes e necessárias para garantir que sejam realizadas revisões periódicas das permissões de acesso e controlos de acesso configurados nos sistemas envolvidos no serviço.

O Fornecedor deve estabelecer medidas suficientes e necessárias para garantir que o acesso remoto ao ambiente tecnológico seja controlado e monitorizado.

O Fornecedor deve assegurar que as informações relacionadas com o Serviço prestado não sejam transmitidas a terceiros sem a autorização prévia do GRUPO PROSEGUR e no quadro legal da lei.

7.5.1.5.2.2 Controlar o acesso às instalações e CPD

O Fornecedor deve assegurar o controlo de acesso às salas onde estão os bens envolvidos no serviço prestado ao GRUPO PROSEGUR, com as devidas garantias administrativas, lógicas e físicas, incluindo, em função da criticidade dos sistemas, mas não limitadas:

- Bloqueio das portas de acesso
- Destruição segura de ativos de informação, de forma atempada.
- Acesso às instalações e centros de tratamento de dados do Fornecedor;
- Dispositivos de armazenamento seguro;
- Pessoal de segurança física
- Áreas de videovigilância

O Fornecedor deve garantir que a entrada não autorizada seja impedida, detetada e comunicada imediatamente ao pessoal apropriado do Fornecedor. Todos os pontos de entrada e saída devem ser protegidos, registados e monitorizados para garantir que apenas o pessoal autorizado possa aceder aos edifícios e áreas seguras do Fornecedor.

No caso do Fornecedor utilizar cartões de identificação ou tokens similares para os seus empregados que fazem parte do serviço prestado ao GRUPO PROSEGUR, deve haver um processo documentado, juntamente com procedimentos de apoio, para garantir que as credenciais e tokens perdidos sejam desativados imediatamente após a notificação de perda.

O Fornecedor deve dispor de procedimentos e mecanismos suficientes para assegurar que, caso um empregado que faça parte do serviço prestado ao GRUPO PROSEGUR cesse a sua relação de trabalho com o Fornecedor, as credenciais de identificação sejam imediatamente desativadas.

O Fornecedor deve assegurar que todos os ativos de informação do GRUPO PROSEGUR que fazem parte do serviço subcontratado, na posse do Fornecedor, estejam fisicamente seguros em uma área de acesso controlado, sala fechada ou contentor de armazenamento seguro ou armário de arquivo.

O Fornecedor deve informar o GRUPO PROSEGUR de qualquer movimento ou eliminação de qualquer sistema de informação, que não pode ser realizado sem o consentimento escrito do GRUPO PROSEGUR.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 57
------------	--	---

7.5.1.5.2.3 Controlos físicos e ambientais

O Fornecedor será responsável pela implementação de medidas de segurança física para a proteção dos sistemas de informação localizados nas suas instalações contra o acesso não autorizado e danos físicos.

Os controlos físicos e ambientais devem incluir:

- Medidas de proteção contra incêndios
- Medidas de proteção contra inundações
- Controlos do fornecimento de energia
- Outros controlos aplicáveis de acordo com a legislação e regulamentação.

O Fornecedor deve estabelecer controlos suficientes e necessários para garantir o acesso físico às instalações onde estão localizados os sistemas de informação que possuem informações relevantes. Para além, a base de dados do pessoal com acesso autorizado deve ser mantida atualizada e controlada, de acordo com os requisitos estabelecidos pelo GRUPO PROSEGUR.

7.5.1.5.2.4 Autorização e autenticação

O Fornecedor deve implementar medidas de segurança necessárias e suficientes para garantir que o acesso dos administradores aos sistemas de informação seja realizado utilizando canais encriptados e uma forte autenticação.

No caso do Serviço ser para servir clientes, o Fornecedor deve implementar medidas de segurança necessárias e suficientes para garantir que a autenticação dos referidos clientes seja realizada através de mecanismos de duplo fator, pelo menos para a execução de operações ou consulta de informações confidenciais.

O Fornecedor deve garantir o armazenamento encriptado de palavras-passe nos sistemas de processamento de informações.

O Fornecedor deve implementar mecanismos necessários para identificar inequivocamente os acessos de cada um dos utilizadores, permitindo apenas o acesso aos dados e recursos necessários para o desenvolvimento das suas funções.

O Fornecedor deve implementar mecanismos necessários para impedir que os utilizadores sejam administradores locais dos seus postos, a menos que expressamente solicitado e validado pelo GRUPO PROSEGUR.

7.5.1.5.3 Encriptação

O Fornecedor deve utilizar algoritmos de encriptação padrão com um comprimento de chave baseado em práticas e padrões internacionalmente reconhecidos para proteger a confidencialidade e integridade dos dados sensíveis do GRUPO PROSEGUR.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 58
------------	--	---

O Fornecedor deve proteger as chaves de encriptação com mecanismos de segurança durante todo o seu ciclo de vida, desde a sua geração, passando pelo seu armazenamento, distribuição, renovação, arquivamento e terminando com a sua eliminação.

O Fornecedor deverá fornecer ao Grupo Prosegur a documentação relativa à gestão de chaves de encriptação para verificar que os requisitos mínimos de segurança para chaves criptográficas são cumpridos. No caso de ser necessário o acesso aos sistemas do Grupo Prosegur, as regras e procedimentos que o Fornecedor e o seu pessoal necessitam conhecer relativamente à gestão e utilização de chaves de encriptação devem ser fornecidas no momento do início da atividade.

O Fornecedor deve garantir que os dispositivos que processam dados críticos ou sensíveis sejam encriptados. Especialmente os dispositivos que são removíveis ou móveis, tais como laptops ou dispositivos amovíveis.

A perda de confidencialidade de qualquer chave criptográfica que afete os sistemas do Grupo Prosegur é um incidente de segurança e deve ser comunicada sem demora, para implementar mecanismos apropriados.

7.5.1.5.4 Segurança perimetral e de infraestrutura

O Fornecedor deverá informar o GRUPO PROSEGUR da infraestrutura tecnológica utilizada para prestar o Serviço, com o nível de detalhe exigido pelo GRUPO PROSEGUR para permitir a realização das tarefas de supervisão/monitorização estabelecidas pelo GRUPO PROSEGUR.

O Fornecedor deve desenvolver uma infraestrutura tecnológica para a prestação do serviço, de forma a facilitar a migração modular para outro local ou uma migração tecnológica.

O Fornecedor não deve ligar hardware ou software não pertencente ao GRUPO PROSEGUR à rede interna do GRUPO PROSEGUR sem:

- Uma avaliação de risco com o alcance necessário, incluindo a identificação dos controlos existentes e compensatórios com base nos requisitos deste anexo;
- Verificação da implementação dos controlos identificados na avaliação dos riscos;
- Aprovação escrita pelo Responsável de Segurança do Cliente (CISO)

O Fornecedor deve proteger ou desativar as portas de rede não vigiadas quando não estiverem a ser utilizadas. Se os requisitos comerciais justificarem a necessidade de ativá-las, as portas de rede podem permanecer ativas, desde que a gestão do Fornecedor tenha analisado a necessidade comercial e haja aprovação documentada. Exemplos dessa necessidade incluem portas de rede em salas de conferência, áreas de trabalho partilhadas, etc.

7.5.1.5.4.1 Segregação de ambientes (No caso do Fornecedor gerir a infraestrutura para a prestação do Serviço)

O ambiente de produção do Fornecedor deve ser segregado física ou logicamente dos ambientes não produtivos, para que haja controlo sobre a troca de informações entre eles.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04 23/06/2023 Página 59
------------	--	---

A rede de utilizadores do Fornecedor deve ser segregada da rede de sistemas centrais, permitindo a ligação mínima necessária para o acesso dos utilizadores aos sistemas de que necessitam para desempenhar as suas funções.

Em qualquer caso, a segmentação dos ambientes de funcionamento, desenvolvimento e teste deve ser implementada para reduzir os riscos de acessos não autorizados ou alterações, bem como para garantir que não haja impactos nos sistemas de produção.

7.5.1.5.4.2 Segurança do servidor (No caso do Fornecedor gerir a infraestrutura para a prestação do Serviço)

O Fornecedor deve ter documentação ou diretrizes para fortificação de servidores, gestão de patch, versões e vulnerabilidades para garantir a segurança e disponibilidade do sistema. O software instalado nos servidores deve ser apenas o indispensável para a prestação correta do serviço e deve ter uma proteção antivírus atualizada.

Os servidores devem ser colocados em plataforma de acordo com as boas práticas reconhecidas e ter apenas ativos os serviços necessários.

Os servidores necessários para a prestação do serviço, se possível, ser segmentados logicamente, por exemplo, dedicando uma VLAN para o serviço prestado ao GRUPO PROSEGUR.

A proteção de dados deve ser garantida e deve-se assegurar que não sejam visíveis, exceto para o GRUPO PROSEGUR. Os dados, quer residam em bases de dados ou em sistemas de ficheiros, apenas devem ser acessíveis a partir das aplicações que os processam, e nunca devem ser acessíveis ao público a partir de redes externas.

O Servidor da base de dados deve ser instanciado num sistema diferente daquele em que a aplicação está a funcionar, permitindo apenas a comunicação com o servidor onde a aplicação está alojada; ou seja, não deve ser diretamente acessível a partir da Internet.

Os servidores devem ser devidamente fechados/selados, para que qualquer adulteração possa ser detetada visualmente.

7.5.1.5.4.3 Segurança perimetral

O servidor que aloja a aplicação deve ser protegido do acesso de terceiros por uma Firewall.

Se houver aplicações expostas à Internet, o acesso às mesmas deve ser protegido por um dispositivo que funcione como proxy invertido, localizado numa DMZ protegida por uma barreira dupla Firewall. Não deve haver exposição direta à Internet, a menos que expressamente autorizada pelo GRUPO PROSEGUR.

O Fornecedor deve garantir que, no caso de integração de novo software em dispositivos com licenças de ligação nos sistemas de informação do GRUPO PROSEGUR, este deve ser precedido de uma avaliação de risco e incorporar procedimentos formais de controlo de alterações para determinar e proteger o impacto na rede do GRUPO PROSEGUR.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 60
------------	--	---

7.5.1.5.4.4 Rede sem fios

O Fornecedor deve configurar pontos de acesso à rede sem fios para garantir que apenas os dispositivos autorizados pelo Fornecedor podem estabelecer uma ligação à rede interna do Fornecedor onde a informação do GRUPO PROSEGUR é visualizada, alojada, armazenada, processada, transmitida, impressa, com backup ou destruída. Para além, as ligações de rede sem fios estabelecidas devem utilizar as melhores práticas do setor para a encriptação e outras proteções apropriadas concebidas para proteger contra o acesso e utilização não autorizados.

7.5.1.5.4.5 Segurança de Endpoints

O Fornecedor deve implementar uma solução de proteção de endpoints que inclua:

- Aplicações antimalware como parte de configurações seguras comuns para sistemas, equipamentos e componentes. Detecção e atualização de vulnerabilidades, não permitindo alterações pelos utilizadores e execução de varreduras frequentes.
- Firewalls pessoais fornecem restrições de portas e serviços, controlo contra a execução de malware, controlo de dispositivos amovíveis, tais como dispositivos USB, e recursos de auditoria e registo.
- Ferramentas IDPS para identificar e parar qualquer atividade suspeita, monitorizando o tráfego de rede e os dispositivos de ligação.
- Restrições à utilização de código móvel para impedir a execução de código malicioso nos equipamentos.

7.5.1.5.5 Gestão do pessoal

O Fornecedor deve implementar práticas de gestão de recursos humanos para contratar, reter e despedir empregados, contratantes e outros pessoal que trabalhe em nome da organização.

O Fornecedor deve comprometer-se a implementar critérios de seleção adequados para posições que afetam os sistemas do Grupo Prosegur.

O Fornecedor deve garantir que a gestão de recursos humanos esteja vinculada à gestão de riscos. Portanto, deve garantir a existência de processos de registo, alteração e cessação de emprego que definam que, quando houver alteração do seu registo, sejam imediatamente tomadas medidas adequadas, tais como a cessação dos sistemas ou a retirada das autorizações de acesso, para proteger a segurança das informações e dos sistemas.

O Fornecedor deve garantir que o seu pessoal e/ou subcontratados e/ou colaboradores que devem ter acesso aos sistemas, ativos e informações do Grupo Prosegur conheçam e cumpram as Políticas, regras e procedimentos fornecidos pelo Grupo Prosegur, uma vez formalizado o contrato e iniciados os serviços, especialmente no que diz respeito aos seus deveres e obrigações relativamente à utilização dos sistemas, redes e outros recursos do Grupo Prosegur, bem como as consequências e sanções por não cumprimento.

Em particular, o Fornecedor deve garantir que os seus empregados não o façam, exceto com a autorização escrita da Prosegur:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 61
------------	--	---

- A instalação de software ou dispositivos no ambiente Prosegur que não tenham sido aprovados pela Prosegur.
- O carregamento de dados ou softwares obscenos, ofensivos ou inadequados, em violação da sua política de licenças no ambiente Prosegur.
- A utilização do ambiente Prosegur para interceptar, analisar ou monitorizar de outra forma o tráfego nas redes Prosegur.

O Fornecedor deve garantir formação adequada e sensibilização dos seus empregados sobre questões de cibersegurança e privacidade, tendo em vigor Planos de Formação e Sensibilização do pessoal geridos entre a equipa de gestão de riscos e o departamento de RH. O Grupo Prosegur pode solicitar o acesso ao conteúdo dos Planos de Formação e Sensibilização dos empregados para verificar a sua adequação.

O Fornecedor deve garantir que seja dada formação específica aos utilizadores privilegiados com funções de segurança específicas para garantir que compreendam as suas funções e responsabilidades exclusivas.

O Fornecedor deve garantir que o pessoal subcontratado cumpre os mesmos requisitos de formação e sensibilização que o outro pessoal.

7.5.1.5.6 Gestão das operações

O Fornecedor deve estabelecer controlos de segurança adequados para garantir que as operações realizadas nas aplicações e sistemas envolvidos no serviço são autorizadas e programadas de acordo com os requisitos acordados entre o GRUPO PROSEGUR e o Fornecedor. Especificamente, as operações a considerar no serviço referem-se à geração de cópias de segurança e à gestão de incidentes de segurança tecnológica.

O Fornecedor deve ter em vigor um conjunto de políticas que especifiquem as medidas a tomar para os backups, incluindo os procedimentos a seguir para a recuperação dos sistemas.

O Fornecedor deve ter estabelecido uma série de medidas especificando as ações a realizar para a correta gestão (detecção, resolução e comunicação ao GRUPO PROSEGUR) dos incidentes de segurança tecnológica que ocorram durante a prestação do serviço.

7.5.1.5.6.1 Configuração dos sistemas

O Fornecedor deve garantir que existem processos de gestão da configuração e proteção dos sistemas que cumpram as normas internacionais e que permitam a aplicação dos requisitos de segurança estabelecidos pelo Grupo Prosegur para os sistemas.

A gestão da configuração deve ser centralizada para todos os sistemas operacionais, aplicações, servidores e outras tecnologias que possam ser configuradas.

O Fornecedor deve manter um registo das configurações históricas no caso de serem necessárias para a resolução de problemas ou para fins forenses.

As alterações de configuração não autorizadas detetadas que afetem os ativos do Grupo Prosegur devem ser tratadas como incidentes de segurança e comunicadas ao Grupo Prosegur.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 62
------------	--	---

O Fornecedor deve instalar proteção antivírus nos sistemas utilizados para prestar o serviço ao GRUPO PROSEGUR, os quais devem estar sempre operacionais e atualizados.

O Fornecedor deve implementar controlos para restringir dispositivos de saída, tais como USB, unidade/gravador de CD/DVD ou outros, que permitam a extração de dados.

7.5.1.5.6.2 Manutenção de sistemas (caso o Fornecedor utilize os seus próprios sistemas para a prestação do Serviço ao GRUPO PROSEGUR)

O Fornecedor deve implementar um processo de monitorização de vulnerabilidades para a infraestrutura tecnológica do Serviço, identificando e tratando as vulnerabilidades de forma atempada sem expor as informações do GRUPO PROSEGUR a tais riscos. Para além, realizará periodicamente uma avaliação da segurança da rede interna e perimetral, quer com os seus próprios recursos, quer por um terceiro independente.

O Fornecedor poderá propor proativamente a instalação de atualizações e patches de segurança. As referidas atualizações e patches serão comunicadas e autorizadas pelo GRUPO PROSEGUR. O GRUPO PROSEGUR também solicitará a instalação de atualizações e patches se considerar necessário.

De qualquer modo, a implantação de patches deve ser testada em ambientes anteriores, para evitar possíveis impactos sobre o Serviço.

Independentemente do software de base que suporta a plataforma e as suas versões (sistemas operacionais, base de dados, servidor web, etc.), deve existir uma política de monitorização de alertas de segurança e de atualização de patches de segurança publicados pelos fabricantes.

Os tempos de ação não devem exceder 24 horas nos casos de falhas de segurança classificadas pelo fabricante como graves/altas.

O Fornecedor deve estabelecer controlos de segurança adequados em relação a quaisquer alterações que possam ser necessárias às aplicações, ou sistemas envolvidos no Serviço. Estes controlos devem, no mínimo, abranger pedidos de alteração de cobertura, análise de impacto, aprovações, testes de utilizadores finais e separação adequada entre os ambientes de montante e de produção.

A execução de qualquer alteração nos sistemas de informação associados ao Serviço deve ser previamente aprovada pelo GRUPO PROSEGUR e deve ser realizada garantindo a integridade, confidencialidade e disponibilidade da informação e do Serviço.

O Fornecedor deve estabelecer os mecanismos necessários para realizar a administração e o funcionamento dos dispositivos de segurança, desde que o GRUPO PROSEGUR delegue expressamente tais funções.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 63
------------	--	---

7.5.1.5.6.3 Localização dos dados (caso o Fornecedor deva armazenar informações relacionadas com a prestação do Serviço ao GRUPO PROSEGUR nos seus próprios sistemas).

O Fornecedor deve informar o GRUPO PROSEGUR da localização dos dados a serem armazenados antes da contratação do Serviço. Durante o período de duração do Serviço, qualquer alteração na localização dos dados deve ser comunicada ao GRUPO PROSEGUR com antecedência e as alterações não podem ser realizadas até receberem a autorização do GRUPO PROSEGUR.

O Fornecedor deve implementar mecanismos de controlo de alterações nos ficheiros armazenados no Serviço, registando todas as informações necessárias que permitam a rastreabilidade dos eventos.

7.5.1.5.6.4 Ficheiros temporários

O Fornecedor, no caso de utilizar ficheiros temporários ou auxiliares para a prestação do serviço, deve proteger estes ficheiros com as mesmas medidas de segurança utilizadas para os ficheiros principais, e deve apagá-los, eliminá-los ou destruí-los de forma segura quando deixarem de ser necessários para os fins para que foram criados, garantindo que não possam ser recuperados numa data posterior.

Os responsáveis pelos sistemas de informação, designados para o efeito, devem verificar periodicamente a eventual existência de ficheiros temporários criados automaticamente em resultado de falhas no sistema.

A menos que o serviço o exija, deve ser evitada a impressão de dados pessoais em papel a partir de aplicações de gestão de dados pessoais.

7.5.1.5.6.5 Serviço partilhado

O Fornecedor deve implementar medidas suficientes para garantir a segurança da infraestrutura tecnológica, caso seja partilhada com outros clientes do Fornecedor. A infraestrutura tecnológica do Serviço deverá dispor de canais de comunicação codificados entre outros serviços oferecidos pelo Fornecedor e as ligações do pessoal responsável pela administração da infraestrutura. Por exemplo; SSH, VPN com IPSEC, etc.

O armazenamento de dados do Serviço prestado ao GRUPO PROSEGUR deve ser logicamente isolado de outros repositórios de armazenamento externos. O Serviço do Fornecedor deverá ter a capacidade de encriptar as informações armazenadas, utilizando algoritmos de encriptação fortes, se necessário.

7.5.1.5.7 Gestão de incidências

O Fornecedor deve dispor de um procedimento para a gestão e comunicação de incidentes de segurança e proteção de dados pessoais, e deve informar atempadamente o GRUPO PROSEGUR sobre um potencial incidente de segurança ou a ocorrência de um incidente de segurança e a forma como pode ser resolvido, se aplicável. Este procedimento deve ser divulgado para o conhecimento e sensibilização de todos os seus empregados.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 64
------------	--	---

Em relação à gestão de incidentes, o Fornecedor deve dispor de mecanismos automatizados e de gestão que cubram:

- Prevenção
- Detecção
- Análise
- Contenção
- Mitigação
- Recuperação
- Monitorização

O Fornecedor deve tomar as medidas adequadas para garantir que a anomalia que causou o incidente seja corrigida o mais rapidamente possível.

O Fornecedor deve registar para cada caso: tipo de incidente, descrição, hora da ocorrência ou deteção, pessoa que notificou o caso, pessoa a quem o caso é comunicado, efeitos, medidas aplicadas, procedimentos de recuperação de dados realizados, pessoa que realiza os procedimentos, dados restaurados e registados manualmente.

O Fornecedor deve autorizar a realização de procedimentos de recuperação de dados (se necessário) de acordo com os planos de recuperação à sua disposição.

O Fornecedor deve prestar o apoio necessário ao GRUPO PROSEGUR no caso de que decida iniciar uma avaliação independente de segurança ou uma investigação de incidentes.

O Fornecedor deve definir um meio de comunicação seguro para comunicar situações não habituais, incidentes ou de qualquer outra natureza relacionados com a confidencialidade das informações do GRUPO PROSEGUR sem atrasos indevidos.

O Fornecedor deve informar imediatamente o GRUPO PROSEGUR em caso de deteção ou suspeita de incidente de segurança, juntamente com um relatório com informações relacionadas com o incidente, os processos, ativos e informações afetados, as medidas tomadas e a sua resolução. O Grupo Prosegur pode monitorizar estes incidentes para identificar possíveis situações em que medidas específicas devem ser tomadas.

O Fornecedor deve acordar com o GRUPO PROSEGUR os critérios de notificação de um incidente de segurança, nos casos de fuga de informações, interrupção do serviço, ataques que afetem a reputação do GRUPO PROSEGUR e qualquer outro caso acordado.

A falta de notificação de um incidente crítico conhecido pode ser considerada uma violação da segurança do tratamento e pode constituir uma violação da boa-fé contratual.

O Fornecedor deve manter um registo dos incidentes de segurança, pelo menos dos sistemas e ativos que afetam o GRUPO PROSEGUR, contendo os incidentes ocorridos, o impacto, as datas e horas de deteção e resolução do incidente, as pessoas responsáveis pela sua gestão e pelas soluções e medidas implementadas para a sua resolução.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 65
------------	--	---

O GRUPO PROSEGUR, pode solicitar a consulta do inventário de incidentes que afetem os seus sistemas e ativos em qualquer altura, ou solicitar um relatório sobre a monitorização de eventos e incidentes que afetem os seus sistemas e informações. O Fornecedor deve ser capaz da sua disponibilização.

7.5.1.5.8 Comunicações

O Fornecedor deve estabelecer todos os mecanismos necessários para que as comunicações através de redes públicas ou redes de comunicações eletrónicas sem fios sejam encriptadas.

A ligação do CPD do Fornecedor com os sistemas do GRUPO PROSEGUR apenas pode ser realizada estabelecendo as medidas de controlo determinadas pelo GRUPO PROSEGUR, após uma análise detalhada das necessidades.

As comunicações com o CPD do GRUPO PROSEGUR devem ser redundantes.

O Fornecedor deve disponibilizar ao GRUPO PROSEGUR, quando solicitado, um mapa completo da rede do Fornecedor do Serviço em que todos os elementos de comunicação envolvidos, bem como os elementos de segurança, estejam perfeitamente identificados.

O Fornecedor deve ter pelo menos as seguintes medidas de segurança perimetral: Firewall, Sistemas de Detecção e Prevenção de Intrusão (IDS/IDPS), Zona Desmilitarizada (DMZ), Redes Privadas Virtuais (VPN) e Proxy.

7.5.1.5.8.1 Segurança na utilização do correio eletrónico (no caso do Fornecedor enviar correio em nome do GRUPO PROSEGUR ou com informação a ele referentes)

Quando o Fornecedor enviar correio em nome do GRUPO PROSEGUR ou com informações a ele referentes, deve cumprir as seguintes medidas:

- Os endereços web (URL) incluídos nos correios eletrónicos e os seus conteúdos devem ser previamente supervisionados pelo departamento de Segurança da Informação do GRUPO PROSEGUR.
- O departamento de Segurança da Informação do GRUPO PROSEGUR deve estar ciente dos dados do GRUPO PROSEGUR a serem incluídos nos correios eletrónicos. Estes não devem ser confidenciais ou secretos e este departamento determinará se e como devem ser protegidos.
- A Segurança da Informação do GRUPO PROSEGUR deve receber:
 - Notificação prévia do envio de correios eletrónicos.
 - Uma breve explicação sobre o conteúdo do correio eletrónico.
 - Um exemplo do correio eletrónico/SMS que os clientes irão receber.
 - Conhecer a caixa de correio de onde são enviados os correios eletrónicos que os clientes irão receber.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 66
------------	--	---

- Deve haver vestígios e provas (logs) de quando e para quem são enviados correios eletrónicos do servidor de correio utilizado para enviar os correios eletrónicos, quer seja feito na infraestrutura do GRUPO PROSEGUR ou na do Fornecedor.
- Os registos de atividade (logs) devem registar a data e hora de envio, a conta da qual o correio é enviado e os destinatários do correio.
- O correio deve incluir os avisos/recomendações acordados com o Departamento de Prevenção de Fraudes Tecnológicas.
- Os correios eletrónicos devem ser enviados com um domínio registado em nome do GRUPO PROSEGUR.
- O departamento de Mensagens (no caso do GRUPO PROSEGUR enviar a mensagem) ou o Fornecedor de Serviços deve criar mecanismos de controlo das listas negras de SPAM para garantir que os domínios do GRUPO PROSEGUR não apareçam.
- Os correios eletrónicos enviados aos clientes devem passar os controlos necessários para estarem livres de vírus. Em outras palavras, os correios eletrónicos devem ser verificados com as ferramentas antivírus existentes no GRUPO PROSEGUR ou, no caso de subcontratação, no Fornecedor de Serviços.

7.5.1.5.9 Gestão da capacidade, dimensionamento e aquisição de sistemas

O Fornecedor deve gerir a capacidade e os recursos que afetam o serviço prestado, estabelecendo processos de gestão da capacidade e dimensionamento que consistem na gestão dinâmica dos recursos do Fornecedor com base nas necessidades, obrigações contratuais e capacidade económica.

A aquisição de novos sistemas, equipamentos, componentes ou software deve ser gerida tendo em conta:

- Os riscos associados a cada atividade, serviço e sistemas
- Devem estar em conformidade com os requisitos e arquitetura de segurança estabelecidos para o serviço
- As necessidades técnicas dos recursos
- Os esforços e meios económicos da sua implementação.

O Fornecedor deve estabelecer controlos de segurança adequados em relação à aquisição e desenvolvimento de novas aplicações e/ou novos sistemas, e em relação a quaisquer alterações que possam ser necessárias às aplicações ou sistemas envolvidos na subcontratação, durante a prestação do serviço. Estes controlos devem, no mínimo, abranger autorizações de utilizadores, testes, aprovações do utilizador final e separação adequada dos meios a montante do ambiente de produção.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04. 23/06/2023 Página 67
------------	--	--

7.5.1.5.9.1 Utilização e desenvolvimento de software para a prestação do serviço

O Fornecedor deve utilizar apenas software licenciado e testado pelo GRUPO PROSEGUR e pelo Fornecedor, para o desenvolvimento do serviço subcontratado.

Todos os desenvolvimentos realizados para prestação de serviços ao GRUPO PROSEGUR serão autorizados pelo GRUPO PROSEGUR e o Fornecedor deve:

- Abster-se de armazenar dados do GRUPO PROSEGUR sem o conhecimento, autorização e/ou auditoria do GRUPO PROSEGUR.
- Realizar uma revisão de segurança do código-fonte para qualquer software que não tenha sido desenvolvido pelo GRUPO PROSEGUR, antes de colocá-lo em produção de acordo com os princípios e boas práticas de desenvolvimento seguro.
- Caso sejam realizados desenvolvimentos de software para o GRUPO PROSEGUR, o Fornecedor deve disponibilizar ao GRUPO PROSEGUR todos os desenvolvimentos de software feitos à medida, incluindo código-fonte, código objeto, manuais e qualquer outra informação relevante.
- Estar disponível para realizar uma avaliação do ambiente de controlo, hacking ético ou qualquer outra avaliação de segurança antes da produção de qualquer versão do sistema, a qualquer altura que o GRUPO PROSEGUR assim o exija.
- Os ambientes de não produção não podem conter dados reais e devem ter os mesmos controlos que o ambiente de produção.
- Assegurar que os desenvolvimentos realizados para a prestação dos Serviços ao GRUPO PROSEGUR e as ferramentas utilizadas cumprem as leis de propriedade intelectual e não violam qualquer legislação, regulamento, contrato, direito, interesse ou propriedade de terceiros.
- Estabelecer controlos de segurança adequados em relação à aquisição ou desenvolvimento de novas aplicações ou sistemas durante a prestação do Serviço. Estes controlos devem, no mínimo, abranger análises de viabilidade, autorizações, testes, aprovações do utilizador final e separação adequada dos meios a montante do ambiente de produção.
- O Fornecedor deve seguir as melhores práticas de desenvolvimento de software seguro de acordo com os requisitos da norma, evitando a introdução de vulnerabilidades conhecidas, caso o software seja desenvolvido.
- As equipas de desenvolvimento do GRUPO PROSEGUR devem estar localizadas em segmentos de rede e ambientes dedicados exclusivamente ao desenvolvimento de aplicações, sem acesso a ambientes de produção ou a dados reais do GRUPO PROSEGUR.
- O Fornecedor deve estabelecer controlos de segurança adequados em relação à validação da integridade dos desenvolvimentos nos ambientes de produção.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 68
------------	--	---

7.5.1.5.10 Revisão

7.5.1.5.10.1 Revisões realizadas pelo GRUPO PROSEGUR

O Fornecedor aceitará a realização de revisões de conformidade com o Esquema de Controlo pelo GRUPO PROSEGUR, numa base:

- Regular, como parte da avaliação da prestação do Serviço.
- Extraordinária, por razões de um incidente de segurança, ou no caso de qualquer extensão, regressão de serviços ou circunstâncias que levem o GRUPO PROSEGUR a considerar apropriada a realização.

O GRUPO PROSEGUR realizará estas revisões de acordo com o esquema de controlo, seguindo um método de avaliação, âmbito, método de monitorização e frequência estabelecidos pelo GRUPO PROSEGUR.

O Fornecedor deve prestar toda a colaboração necessária para cumprir adequadamente os requisitos da revisão que o GRUPO PROSEGUR, as pessoas ou empresas designadas pelo GRUPO PROSEGUR, podem formular e entregar ao mesmo, toda a documentação e/ou provas solicitadas para efeitos desta revisão.

Adicionalmente, o GRUPO PROSEGUR pode exercer controlo sobre os riscos tecnológicos associados ao Serviço, sendo o Fornecedor responsável por fornecer as seguintes informações quando solicitadas:

- Revisão de relatórios de auditoria e/ou certificações, por exemplo:
 - Relatórios de auditoria interna/controlo interno.
 - Relatórios emitidos por terceiros independentes (SOC 2 tipo 2, ISAE 3402, SSAE 16, etc.).
 - Certificações de segurança (ISO 27001, 22301, etc.).
 - Certificações de qualidade do Serviço (ISO 9001, ISO 2000, etc.).

Para além dos relatórios apresentados, o GRUPO PROSEGUR terá capacidade para desenvolver um plano de avaliação de controlos de risco tecnológico e executá-lo de acordo com os prazos, âmbito e procedimentos acordados com o Fornecedor. Este plano pode incluir:

- Monitorização periódica dos indicadores de segurança do Serviço:
 - Os indicadores a controlar são acordados antes da assinatura do contrato e devem ser revistos periodicamente.
 - Acesso aos painéis ou consolas de controlo pelo GRUPO PROSEGUR, que permitem o acompanhamento contínuo do risco tecnológico.
- Notificação de eventos relevantes pelo Fornecedor:
 - Incidentes de segurança.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 69
------------	--	---

- Testes de recuperação em caso de catástrofe (DRP)
- Informação sobre a infraestrutura tecnológica que suporta o GRUPO PROSEGUR (no caso do Fornecedor utilizar infraestrutura própria para prestar o Serviço):
 - Arquitetura de rede.
 - Arquitetura de segurança perimetral.
 - Servidores e bases de dados.
 - Protocolos de rede e comunicações.
 - Outros necessários para que o GRUPO PROSEGUR possa exercer adequadamente as funções de controlo.
- Informações sobre o acompanhamento realizado nos sistemas que prestam serviços ao GRUPO PROSEGUR, bem como o modelo de relacionamento estabelecido para a comunicação destas informações quando considerado necessário.

O Fornecedor deve resolver os pontos fracos de controlo identificados pelo GRUPO PROSEGUR nas revisões realizadas na sequência dos planos de ação acordados.

7.5.1.5.10.2 Controlo interno do Fornecedor

O Fornecedor deve ter uma função de controlo interno que garanta o cumprimento de todos os controlos exigidos pelo GRUPO PROSEGUR.

O Fornecedor deve descrever e disponibilizar ao GRUPO PROSEGUR, quando solicitado, os procedimentos e controlos que irá articular internamente para garantir que os requisitos declarados são cumpridos.

O Fornecedor deve realizar todas as auditorias legalmente exigidas, internas e externas, nos sistemas envolvidos no serviço prestado ao GRUPO PROSEGUR, disponibilizando ao GRUPO PROSEGUR os relatórios de auditoria gerados.

O Fornecedor deve realizar revisões de segurança dos seus sistemas quando feitas alterações substanciais nos sistemas de informação, disponibilizando o relatório da referida revisão ao GRUPO PROSEGUR e deve propor medidas corretivas.

7.5.1.5.10.3 Controlos coordenados com o GRUPO PROSEGUR

O GRUPO PROSEGUR e o Fornecedor acordarão os procedimentos para que qualquer incidente de segurança seja prontamente comunicado ao GRUPO PROSEGUR. Serão definidos protocolos de comunicação específicos para os casos em que seja necessária uma ação imediata por parte do GRUPO PROSEGUR, para mitigar o impacto dos incidentes de segurança.

O GRUPO PROSEGUR poderá verificar o cumprimento dos requisitos técnicos em qualquer altura, tanto através de visita às instalações do Fornecedor como através da utilização de meios seguros de acesso remoto aos sistemas envolvidos, a acordar com o Fornecedor.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 70
------------	--	---

Os aspetos observados nestas revisões e que o GRUPO PROSEGUR considerar como uma violação desta ou que possam colocar em risco os sistemas do GRUPO PROSEGUR serão comunicados ao Fornecedor, ao qual será dado um período de tempo para a sua resolução com o consequente compromisso contratual de que o Fornecedor cumprirá os aspetos observados, conforme acordado com o GRUPO PROSEGUR.

7.5.1.5.10.4 Devolução do Serviço

O GRUPO PROSEGUR e o Fornecedor devem definir e acordar procedimentos para a devolução do serviço de modo a garantir o armazenamento seguro dos suportes e, quando apropriado, a destruição segura das informações utilizadas pelo Fornecedor durante a prestação do Serviço.

O Fornecedor deve garantir que são utilizados mecanismos de eliminação segura de informações. Estes incluirão casos de reciclagem de suportes e fim de Serviço.

Se a destruição da informação for realizada por terceiros, o GRUPO PROSEGUR deve ser notificado e ter um certificado de destruição segura.

O Fornecedor deve cumprir, nos aspetos aplicáveis ao serviço subcontratado, as orientações fornecidas nas normas e práticas internacionais aplicáveis.

Para registos que cumpram os requisitos legais de retenção, os períodos de retenção devem ser estabelecidos e devidamente mantidos pelo Fornecedor. Para além, o GRUPO PROSEGUR pode fornecer requisitos específicos de retenção que o Fornecedor aplicará, incluindo, mas não limitado a, retenção para fins de litígio, legais ou regulamentares.

O Fornecedor deve garantir que a destruição dos sistemas e ativos do GRUPO PROSEGUR que fazem parte do serviço seja realizada de acordo com o programa de gestão de registos do Fornecedor. Antes de um posto de trabalho ou servidor ser reutilizado, desativado ou devolvido ao fornecedor de aluguer, as metodologias de destruição devem ser realizadas de forma segura para que as informações não possam ser lidas ou recriadas após a eliminação.

O Fornecedor deve ter em conta o impacto da eliminação no ambiente.

7.5.1.5.11 Monitorização

O Fornecedor deve disponibilizar ao GRUPO PROSEGUR, quando solicitado, os procedimentos e controlos que irá implementar para monitorizar e alertar sobre possíveis violações da segurança do sistema.

O Fornecedor deve implementar os mecanismos necessários para monitorizar o software instalado nos equipamentos que prestam serviços ao GRUPO PROSEGUR, para que apenas o software essencial para a correta prestação do serviço possa ser instalado, quer os sistemas sejam propriedade do utilizador ou do GRUPO PROSEGUR.

7.5.1.5.11.1 Custódia e exploração dos logs de segurança.

Em relação aos eventos que geram logs, o GRUPO PROSEGUR especificará o formato e conteúdo dos registos e o período de custódia. Caso solicitado, estes logs devem estar disponíveis em tempo real, quer através de acesso direto ao sistema do Fornecedor, quer através da sua receção nos repositórios internos do GRUPO PROSEGUR. Para além, deve ser verificado que a rastreabilidade é

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04. 23/06/2023 Página 71
------------	--	--

gerada no resto dos sistemas envolvidos indiretamente no serviço ou que foram previamente analisados pelo GRUPO PROSEGUR. O Fornecedor deve gerar logs (acesso, autenticação, administração e atividade), no mínimo, dos seguintes eventos:

- Comunicações.
- Envio de ficheiros (sistemas envolvidos na transmissão, tanto na origem como no destino, e sistemas de armazenamento temporário intermédio).
- Aplicações web.
- Sistemas de virtualização (arquitetura cliente-servidor).
- Backend (servidores e aplicações).

7.5.1.5.12 Cópias de backup e recuperação (no caso do Grupo Prosegur autorizar o backup dos dados ou sistemas para a prestação do serviço ao GRUPO PROSEGUR)

O Fornecedor deve estabelecer e implementar uma política de backup que inclua segurança de backup, testes e procedimentos de recuperação. Deve dispor de controlos para garantir o correto tratamento e transporte dos meios de armazenamento de backup, atribuindo pessoal, controlos de acesso físico e lógico, cadeia de custódia e inventários periódicos, garantindo a confidencialidade das informações contidas.

O Fornecedor deve implementar controlos na sua política de backup que garantam a recuperação dos dados no estado em que se encontravam na altura de um incidente de modificação, perda ou destruição.

O Fornecedor deve estabelecer procedimentos para backups pelo menos semanais, exceto se nenhuma atualização de dados tiver sido feita durante este período.

O Fornecedor deve fazer periodicamente cópias de segurança dos seus sistemas que cumpram os Objetivos de Tempo de Recuperação e os Objetivos de Ponto de Recuperação que devem ser incluídos no Plano de Continuidade de Negócios e de Recuperação de Catástrofes e que foram acordados com o GRUPO PROSEGUR.

O Fornecedor deve localizar os procedimentos de backup e recuperação como as próprias cópias num local diferente de onde estão localizados os sistemas de informação.

O Fornecedor deve armazenar um máximo de uma (1) cópia de segurança completa e incremental de seis (6) dias subsequentes nas suas próprias instalações, todas as cópias fora deste intervalo devem ser subcontratadas.

O Fornecedor deve incluir na sua política de proteção a verificação e teste bianual da eficácia dos procedimentos de cópia pelo responsável do tratamento.

Os dados reais apenas serão utilizados se o nível de segurança correspondente ao tratamento for garantido.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 72
------------	--	---

A geração de cópias ou a reprodução dos documentos apenas pode ser realizada sob o controlo do pessoal indicado no Documento de Segurança, e as cópias descartadas devem ser destruídas de modo a tornar as suas informações inacessíveis.

7.5.1.5.13 Continuidade de negócio

O Fornecedor deve ter um Plano de Continuidade de Negócio e Recuperação de Catástrofes que lhe permita recuperar o Serviço de sistemas de informação formalmente documentado e testado periodicamente, bem como garantir a disponibilidade do serviço prestado ao GRUPO PROSEGUR.

O Fornecedor deve rever os Planos de Continuidade pelo menos uma vez por ano e sempre que se verifiquem alterações tecnológicas, organizacionais ou regulamentares relevantes.

O Fornecedor deve garantir que todo o pessoal designado para o trabalho de continuidade de negócio seja suficientemente experiente, competente e capaz de desempenhar as funções requeridas.

O Fornecedor deve realizar testes de contingência para demonstrar a eficácia dos Planos de Continuidade e Recuperação de Catástrofes. Devem também fazer parte dos testes que o GRUPO PROSEGUR solicita como parte da Continuidade dos sistemas do GRUPO PROSEGUR.

O Fornecedor deve fornecer atualizações regulares sobre o estado de continuidade do serviço que presta ao GRUPO PROSEGUR, de acordo com as instruções dadas.

Em caso de interrupção devido a um evento de segurança, o Fornecedor assume a responsabilidade de retomar os serviços prestados dentro dos prazos estabelecidos pelo Grupo Prosegur, de acordo com a criticidade dos sistemas afetados. Os sistemas de maior criticidade podem ser obrigados a retomar as atividades no prazo de 4 horas. O Fornecedor é responsável pela retoma dos serviços nos prazos acordados e o não cumprimento injustificado pode levar a consequências e sanções contratuais.

O Fornecedor será obrigado a permitir que o GRUPO PROSEGUR realize auditorias do Plano de Continuidade de Negócio (BCP) e do Plano de Recuperação de Catástrofes (DR) do Fornecedor que digam respeito ou afetem os Ativos de Informação envolvidos no serviço subcontratado, incluindo os procedimentos de BCP e DR, bem como os resultados dos testes realizados, pelo menos uma vez por ano, e após qualquer contingência ou catástrofe natural.

7.5.1.5.14 Gestão de fornecedores

O Fornecedor deve garantir a existência de mecanismos de gestão de terceiros quando os serviços prestados dependem de outros fornecedores.

O Fornecedor deve garantir que a sua equipa de gestão de risco possa realizar atividades coordenadas de resposta a incidentes envolvendo prestadores de serviços externos que possam afetar direta ou indiretamente as atividades, processos e ativos do Grupo Prosegur.

O Fornecedor deve dispor de um processo de seleção e avaliação de fornecedores que avalie os riscos da cadeia de fornecimento. Os fornecedores devem ser identificados, avaliados e hierarquizados como outros ativos da organização como parte da análise de risco e do seu tratamento.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 73
------------	--	---

O Fornecedor deve manter sempre identificadas as empresas subcontratadas envolvidas no serviço prestado ao Grupo Prosegur e deve transferir a obrigação de cumprir os requisitos tecnológicos e de segurança descritos neste documento.

O Fornecedor deve garantir que na assinatura dos seus contratos de aquisição com terceiros sejam identificados acordos de confidencialidade e acordos de nível de serviço com requisitos mínimos de segurança, bem como outros contratos com as necessidades da organização para proteger os sistemas e dados do Grupo Prosegur. Estes contratos devem ser regularmente revistos e o seu cumprimento controlado.

O Fornecedor deve assegurar que tanto os fornecedores terceiros como os utilizadores que tenham acesso a quaisquer dados pessoais e outras informações do Grupo Prosegur, no desempenho do seu trabalho para a empresa, assumam e se comprometam a cumprir as suas funções com o máxima diligência e, em particular, boa-fé na custódia e tratamento dos mesmos.

O Grupo Prosegur pode solicitar informações ou relatórios ao Fornecedor sobre as medidas e requisitos adotados com um determinado fornecedor.

O Fornecedor será responsável perante o Grupo Prosegur pelo não cumprimento, por parte das empresas subcontratadas envolvidas no serviço prestado ou serviços prestados ao Grupo Prosegur, se existirem, dos requisitos descritos neste anexo.

O Fornecedor deve determinar que sejam realizados controlos e auditorias regulares da prestação de serviços por terceiros para verificar o cumprimento dos acordos contratuais estabelecidos e, especificamente, dos requisitos estabelecidos neste documento.

O Fornecedor deve, em particular, garantir o controlo das alterações aos serviços pelos fornecedores, tendo em conta a importância das informações, sistemas e processos empresariais no âmbito do terceiro.

O não cumprimento de qualquer uma das obrigações contidas neste anexo, quer diretamente pelo Fornecedor, quer indiretamente pelos subcontratados, pode constituir motivo de rescisão do contrato ou ter outras consequências contratuais.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 74
------------	--	---

7.6. ANEXO V UTILIZAÇÃO DE RECURSOS DE IT E SISTEMAS PROSEGUR

Medidas de Proteção

No caso de equipamento informático fornecido pelo Grupo Prosegur, o utilizador deve cumprir as medidas de proteção indicadas abaixo:

Os equipamentos informáticos devem ser utilizados unicamente para fins profissionais.

É proibida a utilização de aplicações e serviços Web baseados em serviços de streaming de áudio ou vídeo, compra e venda de produtos, redes sociais, notícias, desporto e em geral websites não relacionados com a atividade profissional.

Os utilizadores devem guardar a informação e os ficheiros que tratem no desempenho das suas funções nas plataformas cloud de armazenamento habilitadas e autorizadas pela organização (p. ex., OneDrive), evitando guardá-los nos equipamentos localmente.

Os utilizadores devem garantir que o equipamento que lhes for atribuído não será utilizado por pessoas alheias ou não autorizadas para tal.

Não se deve divulgar informação sensível a terceiros não autorizados, sendo especialmente cuidadosos com a informação comunicada através do telefone e Internet.

Os utilizadores devem facilitar ao pessoal técnico autorizado pelo Grupo Prosegur o acesso aos seus equipamentos para levar a cabo as atividades de reparação, instalação ou manutenção aplicáveis.

Os utilizadores devem proceder à devolução dos recursos informáticos e/ou de comunicações que lhes tenham sido atribuídos pelo Grupo Prosegur quando cessarem a sua atividade na organização.

Da mesma forma, quando os meios informáticos ou de comunicações facultados pelo Grupo Prosegur estiverem associados ao desempenho de um determinado cargo ou função, a pessoa a quem estiverem atribuídos deve devolvê-los imediatamente à sua unidade informática quando terminar o seu vínculo a esse cargo ou função.

O utilizador deve seguir as indicações e instruções para minimizar os riscos derivados das ameaças provocadas por malware prestando especial atenção à utilização de dispositivos amovíveis, correio eletrónico e software transferido da Internet ou de origens desconhecidas e/ou ilegais.

Os sistemas em que seja detetada uma utilização inadequada, ou em que os requisitos mínimos de segurança não sejam cumpridos, podem ser bloqueados ou temporariamente suspensos pelo Grupo Prosegur, sendo o serviço restaurado quando a causa da ameaça ou degradação desaparecer.

O utilizador não deve violar de forma alguma as permissões da sua conta, especialmente para instalar aplicações não relacionadas com as suas funções profissionais. Caso o utilizador necessite da instalação de uma aplicação específica para realizar as suas funções, deverá efetuar esse pedido à Direção de Tecnologia da Informação (doravante, DTI) através do Service Portal.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 75
------------	--	---

Não é permitida a configuração de contas pessoais no dispositivo para serviço não definidos pelo Grupo Prosegur.

Proíbe-se expressamente o acesso, o descarregamento e/ou o armazenamento em qualquer suporte de: páginas ou conteúdos ilegais inadequados ou que atentem contra a moral e os bons costumes, dos formatos de imagens, sons ou vídeo; de vírus e códigos maliciosos; em geral de todo tipo de programas e/ou plug-in sem a expressa autorização do Grupo Prosegur.

O utilizador é responsável por zelar que os equipamentos que lhe foram atribuídos se mantêm atualizados e com os patches de segurança correspondentes.

O Grupo Prosegur tem o direito de monitorizar a atividade nos equipamentos informáticos para verificar a correta utilização dos mesmos, bem como para prevenir e detetar incidentes de segurança.

É proibida a utilização de dispositivos de armazenamento amovíveis sem autorização prévia.

Por predefinição, as entradas USB estão desativadas. Caso seja necessário utilizá-las, deve pedir-se à área de Segurança da Informação e DTI, que avaliarão a justificação desse pedido.

Em caso de autorização, o utilizador é responsável pelas ações executadas com as informações extraídas ou introduzidas nos recursos informáticos do Grupo Prosegur.

Os suportes de armazenamento disponíveis estão destinados a uma utilização meramente profissional.

A perda ou subtração destes suportes deve ser tratada como um incidente de segurança e ser notificada sem demora.

Os suportes que sejam reutilizados devem passar primeiro por um processo de eliminação segura em conformidade com as normas do Grupo Prosegur.

Os suportes que não devem ser reutilizados devem ser destruídos por métodos seguros, de acordo com os padrões do Grupo Prosegur.

Devolução de equipamentos, dispositivos e suportes.

Em caso de:

- Conclusão do serviço para o qual foram utilizados.
- Cessação da relação contratual do utilizador com o Grupo Prosegur.
- Obsolescência dos equipamentos, dispositivos e/ou suportes.
- Avarias nos equipamentos, dispositivos e/ou suportes.

Deve proceder-se à sua devolução, enviando o dispositivo para a área local correspondente de microinformática através dos meios para o efeito com um pedido a indicar os motivos da devolução:

Em caso de conclusão do projeto: Deve abrir-se um pedido de serviço não catalogado no Service Portal indicando, pelo menos, alguns dos seguintes dados:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 76
------------	--	---

- Número de série
- Hostname do equipamento
- Último utilizador que utilizou: Por exemplo: ES00605432.

Uma vez aberto o ticket, deve esperar-se por instruções do departamento de Microinformática local para a devolução e recolha do equipamento. Neste caso, a reutilização do equipamento do utilizador cessante para o entregar à nova incorporação deve também ser validada por DTI por razões de segurança.

Em caso de obsolescência ou avaria: Deve abrir-se um ticket no Service Portal e seguir as instruções de devolução do equipamento indicadas pelo departamento de Microinformática local.

Os equipamentos NÃO devem ficar, em caso algum, em dependências departamentais do negócio sem controlos de segurança física e lógica nem serem utilizados depois de estarem desligados da rede durante um grande período de tempo, uma vez que põem em perigo a segurança da empresa por possíveis vulnerabilidades nos mesmos.

Mesa limpa e posto de trabalho organizado

É obrigação dos utilizadores realizar as seguintes medidas:

- Manter o posto de trabalho limpo e organizado, sem mais material na mesa do que o necessário para a atividade a ser realizada em qualquer altura.
- Ao concluir uma tarefa ou função, o material deve ser removido para uma área segura num local fechado; para o qual o Grupo Prosegur pode atribuir armários e gavetas com fechadura.
- Trancar documentação e dispositivos de armazenamento com informações confidenciais durante ausências prolongadas e no final do dia de trabalho.
- As chaves não devem ser deixadas em gavetas ou armários onde guardadas informações confidenciais.
- Cuidado com as informações apresentadas nos ecrãs do equipamento, sempre que exista pessoal não autorizado perto e possa visualizar essas informações.
- Evitar trabalhar com informações em papel. As palavras-passe e outra informação de interesse não devem estar à vista anotadas em papel ou post-its.
- Verificar se a documentação de apoio para reuniões, apresentações e outros eventos realizados nas salas destinadas para estes fins não permanecem nas salas, quando finalizado qualquer evento.
- Imprimir sempre com a opção "Impressão protegida" ativada, e deve ser introduzida uma palavra-passe para tal efeito.
- Para todas as impressoras com mecanismos de impressão segura com palavra-passe, o empregado deve sempre assegurar-se de sair da sessão.
- Remover imediatamente a informação sensível das impressoras, copiadoras e aparelhos de fax, assegurando que não é deixada qualquer documentação na bandeja de saída ou na fila de impressão.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04. 23/06/2023 Página 77
------------	--	--

- Destruir todos os documentos descartados de forma que a informação sensível não possa ser lida ou facilmente recuperada. Para esses efeitos, utilizar a trituradora de papel ou depósitos colocados à disposição.
- Os cartões criptográficos não devem ser deixados sem vigilância e à vista, o que poderia levar a que pessoas não autorizadas tivessem acesso a informações e recursos do Grupo Prosegur.

Bloqueio do posto de trabalho e das sessões.

Os utilizadores dos sistemas têm o dever de:

- Ativar o protetor de ecrã e o bloqueio do equipamento quando o posto de trabalho for deixado sem vigilância.
- Bloquear o equipamento durante qualquer ausência Utilizar dispositivos que protejam fisicamente os equipamentos portáteis, tais como cadeados, quando disponíveis.
- Verificar se os equipamentos estão desligados no final do dia de trabalho.
- As imagens visualizadas após o bloqueio do ecrã não devem incluir ou revelar informações confidenciais.
- Quando o posto de trabalho fique sem vigilância durante ausências prolongadas, as sessões de aplicações e do sistema devem ser encerradas sempre que o seu funcionamento contínuo não seja necessário para a sua funcionalidade.
- Não alterar a configuração estabelecida para bloqueio automático do equipamento ou logout automático por qualquer método sem autorização prévia.

Acesso aos sistemas de informação.

Credenciais de acesso.

Os utilizadores são responsáveis pela custódia das credenciais de acesso, identificação eletrónica e certificados de assinatura, bem como software ou outros meios atribuídos (por exemplo, cartões criptográficos, tokens), para acesso autorizado aos recursos e sistemas do Grupo Prosegur.

Os autenticadores são únicos para cada pessoa, intransferíveis e independentes do recurso informático a partir do qual se efetua o acesso.

Utilização de Palavras-passe.

- As palavras-passe devem ser difíceis de adivinhar.
- Não devem ser utilizadas:
 - Palavras do dicionário, gírias ou dialetos.
 - Palavras referentes ao contexto da organização ou das funções dos utilizadores.
 - Palavras contendo informações pessoais como data de nascimento, nomes de familiares, pessoas à sua volta, números de telefones, etc...

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 78
------------	--	---

- Os utilizadores são responsáveis pela custódia e utilização das palavras-passe.
- As palavras-passe devem apenas ser do conhecimento do utilizador que as utiliza. Não devem ser comunicadas a terceiros, nem sequer da organização. Todas as palavras-passe devem ser tratadas como informação confidencial e de utilização exclusiva pelo utilizador atribuído. Não se devem revelar as palavras-passe por telefone mesmo que falem em nome da DTI ou de um superior hierárquico.
- As palavras-passe não devem ser transmitidas por correio eletrónico ou outros meios eletrónicos de comunicação.
- A palavra-passe não deve ser escrita ou mostrada num papel ou documento onde seja registada. Da mesma forma, não se devem guardar em documentos de texto ou notas dentro do próprio computador ou dispositivos móveis.
- É proibido utilizar as palavras-passe utilizadas para as contas de recursos e serviços do Grupo Prosegur em contas que não pertencem à empresa e vice-versa.
- O utilizador é obrigado a alterar as palavras-passe quando o sistema o notifica da necessidade de alteração antes da sua expiração.
- A palavra-passe deve ser alterada imediatamente se houver qualquer indicação de que foi violada e comunicada de acordo com o processo estabelecido de comunicação de incidentes, para: seguridad.informacion@prosegur.com
- É proibida a utilização de lembretes das palavras-passe. Caso se pretenda utilizar ferramentas, como por exemplo gestores de palavras-passe, é necessária homologação e validação prévia por parte da Segurança da Informação e da DTI.
- A palavra-passe não deve ser comunicada a ninguém durante as férias ou durante períodos de ausência prolongada.
- Caso o utilizador precisar alterar a palavra-passe e o sistema já não o permitir ou a conta tiver sido suspensa, isto deve ser comunicado como um incidente ao CAU através do Service Portal e um administrador restaurará a palavra-passe verificando previamente a identidade.

Acesso Remoto.

O acesso através de VPN permite que os utilizadores que se encontram fora das instalações próprias do Grupo Prosegur acessem aos recursos de informação e de rede estabelecendo uma ligação criptografada via Internet.

Em conformidade com o anterior, estabelecem-se as diretrizes seguintes:

- O acesso remoto é concedido com base nas necessidades das funções de cada utilizador e pode ser retirado a qualquer altura, caso considerado apropriado.
- O acesso remoto é concedido previamente pelo Grupo Prosegur aos utilizadores atribuídos ou que justifiquem a necessidade de trabalhar desta forma.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 79
------------	--	---

- É proibida a utilização de outras ferramentas de acesso remoto para além das aprovadas pelo Grupo Prosegur.
- Os utilizadores são responsáveis por proteger as suas credenciais de acesso remoto, impedir a sua divulgação e garantir a sua privacidade.
- O utilizador que utilize o acesso remoto deve zelar pela segurança física onde o irá efetuar, seja em casa, em instalações de terceiros, locais de acesso público, etc.
- Os utilizadores são os únicos responsáveis pelas ações realizadas nos recursos acedidos durante a sessão VPN.
- O acesso VPN à rede e aos recursos associados é puramente para fins profissionais, qualquer outra utilização é considerada imprópria e a responsabilidade total recai sobre o utilizador.
- Os utilizadores com acesso remoto que realizam tarefas de apoio técnico, administração de equipamentos ou desenvolvimento não devem exceder os seus privilégios.
- O pessoal colaborador e terceiros autorizados a utilizar a ligação remota têm um acesso limitado para o desenvolvimento das suas funções.
- É proibido divulgar a terceiros ou externalizar o conteúdo de qualquer informação secreta, confidencial ou interna do Grupo Prosegur a que se tenha acesso utilizando o serviço VPN.
- As ligações paralelas não são permitidas quando ligadas através de acesso remoto.
- Na sessão de acesso remoto, o acesso à Internet apenas é permitido através do proxy do Grupo Prosegur.
- Os utilizadores são proibidos de se ligarem a redes públicas WI-FI para a ligação à Internet necessária para o acesso remoto. Este tipo de rede não conta com os mecanismos suficientes para garantir a confidencialidade na navegação pelo website; ainda que o fluxo de informação através da VPN se realize de forma criptografada.
- O utilizador deve fechar as sessões VPN remotas quando estas deixarem de ser utilizadas para a função realizada ou quando estiver ausente do posto de trabalho.
- O Grupo Prosegur pode monitorizar os acessos através de ligação remota para prevenir ataques e detetar utilizações indevidas.

Acesso e Utilização da Internet.

- Deve ser feita uma utilização estritamente profissional da Internet. A utilização para fins pessoais ou recreativos é proibida.
- O acesso à Internet é concedido de acordo com as necessidades das funções desempenhadas por cada empregado, e a qualquer altura pode ser retirado se o Grupo Prosegur considerar apropriado.
- Os utilizadores comprometem-se a utilizar corretamente a Internet e são responsáveis pelas sessões iniciadas na Internet através de qualquer dispositivo.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GL0/GdM/COM/01 Ed. 04 23/06/2023 Página 80
------------	--	---

- É proibido armazenar, divulgar a terceiros ou externalizar o conteúdo de qualquer informação propriedade do Grupo Prosegur, através de qualquer meio de acesso público ou privado na Internet, sem o consentimento expresso da empresa. O Grupo Prosegur pode filtrar o conteúdo ao qual se pode aceder através da Internet. Se um utilizador justificar a necessidade do acesso a um determinado endereço, deve solicitá-lo através do seu responsável para que este o peça à Direção de IT (doravante, DTI).
- O Grupo Prosegur pode monitorizar a atividade dos utilizadores na Internet, bem como registar os acessos realizados.
- O utilizador não deve visitar páginas não confiáveis ou suspeitas de conterem conteúdo malicioso.
- Em nenhuma circunstância é permitido alterar a configuração dos navegadores (opções de Internet) dos equipamentos ou a ativação de servidores ou portas sem a autorização da DTI.
- É expressamente proibido descarregar e/ou armazenar em qualquer suporte, páginas com conteúdos ilegais, prejudiciais, inadequados ou que violem a moral e os bons costumes e, em geral, qualquer tipo de conteúdo que viole o código de ética do Grupo Prosegur.
- A utilização e a descarga de ficheiros P2P ou similares não é permitida em nenhuma circunstância.
- Antes de utilizar uma informação obtida na Internet, os utilizadores devem verificar em que medida está sujeita aos direitos de Propriedade Intelectual ou Industrial, e/ou que possa violar a legislação de aplicação em matéria de proteção de dados pessoais.
- Quando realizados intercâmbios de informação ou transações, deve-se aceder às páginas web escrevendo e verificando o endereço na barra de endereço do navegador e não através de ligações externas. Quando a página Web estiver autenticada por certificado digital, o utilizador deve verificar a sua autenticidade.
- A segurança da ligação deve ser verificada assegurando a sua encriptação, entre outras, verificando a utilização do protocolo HTTPS na comunicação.
- O utilizador deve eliminar periodicamente a informação armazenada nos navegadores: cookies, histórico, palavras-passe, etc.
- É proibida a instalação de plug-ins não previamente autorizados pelo Grupo Prosegur.
- É proibida a utilização de ferramentas de qualquer tipo na nuvem não tenham sido previamente autorizadas pelo Grupo Prosegur, por exemplo, para armazenar ou partilhar informações.
- É proibida a utilização do acesso à Internet para participar em debates em tempo real (canais de chat/IRC), quer através de sítios Web que prestam o serviço, quer por aplicações instaladas nos equipamentos (por exemplo: MS Messenger, TOM, Yahoo, ICQ ou similares).
- Não é permitida a utilização de qualquer outro meio de acesso à Internet (por exemplo, modems) que não tenham sido autorizados pela área de DTI.
- É proibida a utilização da Internet para fins que possam influenciar negativamente a imagem do Grupo Prosegur, dos seus representantes ou de terceiros com os quais tenha uma relação.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 81
------------	--	---

Utilização do Correio Eletrónico

O correio eletrónico é uma ferramenta que o Grupo Prosegur disponibiliza para aquelas comunicações requeridas como consequência do desenvolvimento da atividade própria da empresa com outras entidades ou com outros utilizadores. Relativamente à utilização do correio eletrónico, estabelecem-se as diretrizes seguintes:

- O acesso e utilização destes serviços pelos utilizadores, bem como os privilégios associados a tal acesso, devem ser limitados aos estabelecidos pelas suas obrigações profissionais.
- Todas as contas de correio eletrónico que existem no serviço de correio são de propriedade do Grupo Prosegur.
- Os utilizadores devem apenas utilizar as ferramentas e programas de correio eletrónico fornecidos, instalados e configurados pelo Grupo Prosegur.
- No caso de pessoal externo, a utilização de endereços externos deve ser previamente aprovada pelo Grupo Prosegur.
- A conta de correio eletrónico é pessoal e intransferível.
- Os utilizadores são os únicos responsáveis por todas as atividades realizadas através das suas contas de correio eletrónico.
- Os utilizadores são responsáveis de proteger as suas credenciais de acesso ao correio.
- A forma e o conteúdo dos correios enviados pelo utilizador devem estar em conformidade com o código de conduta do Grupo Prosegur; e em nenhum caso devem ser enviados correios ofensivos, ameaçadores ou de mau gosto.
- Quando houver necessidade de enviar correios eletrónicos a mais de destinatário, o campo "Bcc" deve ser utilizado para manter a privacidade dos correios eletrónicos dos destinatários.
- A caixa de correio eletrónico tem uma capacidade limitada. O sistema informa ao utilizador quando a cota atribuída for alcançada, e este deverá liberar espaço eliminando aqueles correios que não são mais necessários para o desempenho das suas funções.
- O utilizador deve esvaziar diariamente o contentor de lixo reciclável, uma vez que os correios que contém estão incluídos na quota atribuída a cada caixa de correio.
- O utilizador deve manter todas as suas caixas de correio e pastas organizadas e classificadas. Os correios inutilizáveis devem ser eliminados permanentemente.
- Os anexos de elevado tamanho de bytes devem ser comprimidos antes de serem enviados.
- Verificar a barra de endereços antes de enviar uma mensagem e responder apenas à pessoa apropriada.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 82
------------	--	---

- Sempre que possível, em vez de partilhar documentos por correio eletrónico, deve ser indicado um link para o recurso.
- Ao enviar informação crítica ou sensível, a mensagem deve ser encriptada. Caso a ligação seja efetuada através da Web, ao finalizar a atividade a sessão deve ser encerrada.
- O correio eletrónico é um dos principais meios de entrada de programas maliciosos em computadores e sistemas. Para isso são estabelecidas as seguintes normas:
 - Nunca clicar em links de correio ou abrir anexos, a menos que a autenticidade e fiabilidade do correio e do conteúdo sejam verificadas.
 - Não responder ao correio não solicitado ou de origem desconhecida, especialmente se houver anexos. Esse tipo de mensagens devem ser eliminadas imediatamente.
 - Os correios com anexos com extensões não permitidas (.exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta) ou com extensões aceitáveis que ocultam as não permitidas, devem ser eliminados imediatamente. Os correios que contenham esse tipo de arquivos anexos não devem ser abertos, em nenhum caso.
 - É proibido o registo em serviços de páginas da Internet com as contas de correio profissional, exceto em serviços autorizados.
 - Ao responder ou reenviar um correio eletrónico, eliminar todas as informações irrelevantes, tal como endereços, assinaturas, cabeçalhos, etc.
 - Deve ser desativada a pré-visualização para a caixa de entrada.
- Todas as contas de correio genéricas e listas de distribuição têm um responsável associado que deve cumprir as seguintes normas:
 - Utilizar a caixa de correio ou a lista de distribuição exclusivamente para os fins para os quais foi criada (serviço ao cliente, resposta a pedidos, etc.).
 - É recomendável incluir uma assinatura corporativa ao enviar correos eletrónicos de tais contas.
 - Autorizar de forma responsável o acesso e utilização destas contas.
 - Proteger a reputação e a imagem do Grupo Prosegur, mantendo um tom cordial nas suas respostas.
 - Verificar pelo menos 2 vezes por ano se as pessoas que foram autorizadas ainda são válidas.
- Qualquer evento suspeito deve ser notificado à área de Segurança da Informação Empresarial para que sejam tomadas as medidas necessárias. O Grupo Prosegur criou um botão nas aplicações de correio “Comunicar correio eletrónico” para facilitar esta tarefa.
- O Grupo Prosegur pode controlar as contas de correio disponibilizadas aos seus empregados, sem notificação prévia, a fim de assegurar a correta utilização e exploração deste recurso, bem como para detetar possíveis incidentes de segurança.

Utilizações Proibidas

- Utilizar o correio eletrónico para fins comerciais externos à empresa. Participar na propagação de “cadeias de cartas”, esquemas em pirâmide, etc.
- Criar listas de distribuição sem o consentimento da DTI.
- Distribuição maciça de mensagens com conteúdo inadequado que prejudicam o bom funcionamento dos serviços da Internet.
- Enviar ou reenviar mensagens com conteúdo difamatório, ofensivo ou obsceno.
- Utilizar mecanismos e sistemas que tentam esconder ou fazer-se passar pela identidade do remetente do correio.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 83
------------	--	---

- Envio de correios SPAM de qualquer tipo (correios SPAM são aqueles não relacionados com os processos de trabalho).
- Não é permitido enviar anexos com extensão .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, porque estes anexos podem esconder vírus e são frequentemente utilizados para espalhar vírus.
- A divulgação de conteúdo ilegal; por exemplo, ameaças, código malicioso, defesa do terrorismo, pornografia infantil, software ilegal ou de qualquer outra natureza criminosa.

Armazenamento Partilhado

Os recursos de armazenamento partilhado são espaços dedicados para conter e partilhar os documentos e arquivos desenvolvidos como resultado da atividade profissional entre os membros de um grupo de trabalho.

Todos os utilizadores com acesso a recursos de armazenamento partilhado devem cumprir as normas estabelecidas a seguir:

- O acesso e a utilização dos recursos de armazenamento partilhado pelos utilizadores, bem como os privilégios associados a esse acesso, devem ser limitados aos necessários para realizar as suas funções (numa base de “necessidade de saber”).
- Em nenhum caso, é permitido o armazenamento de informações pessoais nos recursos de armazenamento partilhado.
- É proibido o armazenamento de ficheiros executáveis ou instaláveis (.exe) nos recursos de armazenamento partilhado sem o controlo da DTI.
- Não é permitido solicitar um recurso de armazenamento partilhado para a utilização exclusiva de uma pessoa.
- O backup e recuperação da informação contida nos recursos de armazenamento partilhado é tarefa exclusiva da DTI.
- Todos os recursos de armazenamento partilhado têm um responsável atribuído que é a pessoa com autorização de acesso. Este responsável deve rever, no mínimo semestralmente, as autorizações de acesso a esse recurso de armazenamento partilhado. A utilização do espaço atribuído no recurso de armazenamento é responsabilidade de todas as pessoas autorizadas.
- No caso da informação histórica necessitar de ser mantida, a DTI pode fornecer um meio de armazenamento alternativo e assegurar que a informação seja arquivada.
- Para o armazenamento de dados pessoais nos recursos de armazenamento partilhado, devem ser utilizadas medidas técnicas e de controlo necessário para garantir o cumprimento da legislação aplicável nesta matéria.

Utilização de certificados e assinatura eletrónica.

- É possível que, como parte das atividades no Grupo Prosegur, o utilizador utilize certificados e assinatura eletrónica. O utilizador deve:

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 84
------------	--	---

- Conhecer e cumprir as condições de utilização dos certificados previstas nos regulamentos do Grupo Prosegur, bem como as limitações da sua utilização em conformidade com a legislação aplicável.
 - Agir com diligência relativamente à custódia e conservação dos dados de assinatura ou certificado ou qualquer outra informação sensível, como chaves, códigos de pedido do certificado, palavras-passe, etc., incluindo os suportes dos certificados ou os equipamentos em que se encontram.
 - Os dados acima mencionados NÃO devem ser divulgados em circunstância alguma.
 - Solicitar a revogação do certificado em caso de suspeita de perda da confidencialidade, divulgação ou utilização não autorizada dos dados através da notificação da Segurança da Informação pelos métodos estabelecidos.
- Em qualquer caso, o utilizador é responsável pela utilização que possa ser feita destes certificados e pela sua custódia segura, caso contrário poderia levar à ativação do processo de sanção aplicável.

Gestão de Incidentes de Segurança.

Quando um utilizador deteta qualquer tipo de anomalia ou incidente de segurança que possa comprometer a segurança, utilização e/ou funcionamento dos recursos informáticos ou sistemas de informação a quem tem acesso, bem como as informações e dados pessoais neles contidos, é obrigado a informar imediatamente a Área de Segurança da Informação para que possam ser tomadas as medidas necessárias, documentando a notificação com as provas e documentos disponíveis.

- A notificação deve ser realizada através dos seguintes meios:
 - Por correio eletrónico para o departamento de Segurança da Informação: seguridad.informacion@prosegur.com
- O utilizador é obrigado a cooperar com o Grupo Prosegur na investigação e mitigação do incidente e, se necessário, para o efeito, deve entregar o recurso informático afetado ou, se necessário, deve permitir o acesso de forma remota para que o pessoal técnico do Grupo Prosegur possa efetuar as verificações relevantes e verificar se o recurso pode continuar a ser utilizado com segurança.

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 85
------------	--	---

DECLARAÇÃO DO UTILIZADOR SOBRE A UTILIZAÇÃO DOS SISTEMAS E RECURSOS DA PROSEGUR

O utilizador declara:

- Que é da responsabilidade do utilizador proteger e utilizar os recursos e ferramentas atribuídas de uma forma responsável e tendo sempre em conta os objetivos profissionais estabelecidos.
- Que é da responsabilidade do utilizador fazer bom uso dos recursos e dispositivos propriedade do Grupo Prosegur, utilizando-os para as funções as quais foram atribuídos, respeitando a sua integridade e sendo utilizados apenas pela pessoa designada como responsável por eles.
- Que é da responsabilidade do utilizador ler, compreender e agir em conformidade com todos os outros regulamentos e documentos de Segurança da Informação, bem como qualquer outro disponibilizado pela Direção-geral do Grupo Prosegur.
- Que o utilizador deve informar a Área de Segurança da Informação Empresarial de qualquer incidente, anomalia ou suspeita, do ponto de vista da segurança da informação, que considere relevante e que possa afetar o Grupo Prosegur.
- Que as informações armazenadas nos dispositivos e equipamentos são propriedade do Grupo Prosegur, e estão sujeitas a auditoria. Os equipamentos devem ser devolvidos ao Grupo Prosegur a seu pedido em qualquer altura.
- Que, no desenvolvimento das suas funções, quando o utilizador gere os recursos de um Cliente, pode também estar sujeito à Política de Segurança e às normas de segurança aprovadas pelo Cliente se este o exigir, sem prejuízo da obrigação de continuar a cumprir as disposições das normas do Grupo Prosegur.
- Que o não cumprimento das normas e diretrizes acima referidas dá origem às medidas legais a que o Grupo Prosegur pode recorrer para a preservação dos seus direitos, em conformidade com a legislação e acordos aplicáveis.

DECLARO TER LIDO O PRESENTE E TER CONHECIMENTO SOBRE AS NORMAS DE UTILIZAÇÃO DOS RECURSOS INFORMÁTICOS DA PROSEGUR AQUI ESTABELECIDAS.

_____, _____ de _____ de _____

Nome

Documento de Identidade

Assinatura

SISTEMA 3P	Todos os conteúdos (entendendo por este a título meramente enunciativo, informação, marcas, nomes comerciais, sinais distintivos, textos, fotografias, gráficos, imagens, ícones, tecnologia, links e demais conteúdos audiovisuais ou sonoros, bem como o seu design gráfico) deste documento, são propriedade intelectual do Grupo Prosegur ou de terceiros, sem que nenhum dos direitos de exploração reconhecidos pela legislação em vigor em matéria de propriedade intelectual e industrial sobre os mesmos possa ser entendido como cedido ao destinatário, exceto os que forem estritamente necessários para a consulta do documento facultado. A Prosegur não assume qualquer compromisso para verificar a veracidade, exatidão e atualidade das informações fornecidas através do documento.	Classificação - Interno DS/GLO/GdM/COM/01 Ed. 04 23/06/2023 Página 86
------------	--	---