PROSEGUR

Documento de Suporte 3P às Condições Gerais de Compra

ÁREA DE CONTROLE 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

5. DEFINIÇÕES

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

- Prosegur: Empresa do Grupo que age como compradora e/ou Contratado em cada Compra e/ou Contrato.

- Filial refere-se a uma entidade ou conjunto de entidades registradas ou não sob controle comum. Conforme utilizado nesta definição, "controle" (e as variantes utilizadas) significa o poder, direta ou indiretamente, de dirigir os interesses de outra entidade, seja por propriedade, contrato ou de outra forma.

- Compra: Operação em que o valor corresponde principalmente a aquisições de bens.

- Contratação: Operação na qual o valor corresponde principalmente a aquisição de obras e/ou serviços e, portanto, de mão de obra. Tanto uma compra quanto uma contratação podem ter componentes de obras, bens e serviços. No desenvolvimento dessas Condições, os termos de compra e contrato serão considerados termos equivalentes.

- Pedido: Documento de natureza vinculante para as partes emitido pela Prosegur ao fornecedor, no qual são definidos 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 concedido. Às vezes, este documento tem o status de um contrato e um pedido de fornecimento.

- Contrato: Acordo vinculante entre as partes, no qual são definidos preços, prazos e condições para a realização de uma obra, subcontratação ou prestação de um serviço.

- Condições Gerais: Documento no qual são estabelecidas as bases do processo de Compra de bens e/ou de Contratação de obras e/ou serviços, que são aplicáveis a todo o Grupo Prosegur.

- Fornecedor: A entidade que recebeu um Pedido.

- Contratado: A entidade que recebeu um Contrato.

- Condições Especiais: Também chamado de Pedido de Oferta. Qualquer documento contendo todos os requisitos, de qualquer tipo, necessários para que o Fornecedor forneça os bens ou realize as obras e serviços da forma e qualidade exigidas.

6. CONDIÇÕES GERAIS DE COMPRA E CONTRATAÇÃO

6.1. Validade e prioridade da documentação contratual

6.1.1. As Condições Gerais serão levadas ao conhecimento dos Fornecedores/Contratados no processo de gestão da Compra/Contratação e que integrarão a documentação contratual estabelecida no Pedido/Contrato, em todos os seus termos e condições.

6.1.2. Estas Condições Gerais podem ser complementadas por Condições Especiais e/ou Pedidos/Contratos correspondentes que são gerados. Em caso de discrepância entre os documentos que constituem uma Compra/Contrato, o especial prevalecerá sobre o geral, sendo o pedido de prioridade o seguinte:

- Quaisquer modificações no Pedido/Contrato, expressamente acordadas por escrito e após sua data de assinatura ou emissão.
- O Pedido/Contrato e sua documentação anexa.
- Quaisquer modificações nas especificações técnicas solicitadas
- As especificações técnicas solicitadas.
- Modificações nas Condições Especiais e/ou Gerais.
- As Condições Especiais.
- As Condições Gerais
- Os esclarecimentos feitos por escrito pelo Fornecedor/Contratado, após sua oferta que foram aceitos pela Prosegur.

6.1.3. Outras Condições Gerais propostas pelo Fornecedor/Contratado diferentes das estabelecidas neste documento não serão aceitas, a menos que expressamente aceitas no todo ou em parte pela Prosegur.

6.1.4. As condições e especificações inseridas pelo Fornecedor/Contratado em suas notas de entrega, 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 permanecerão em vigor durante a execução das obras, de acordo com as disposições da documentação contratual. Se uma data de validade tiver sido predeterminada e a duração de tal trabalho exceder essa data, o Contrato será tacitamente prorrogado por períodos mensais sucessivos, a menos que qualquer das partes notifique a rescisão por escrito, pelo menos quinze dias antes de tal data de validade ou de qualquer prorrogação.

No entanto, o Contrato pode incluir as cláusulas que serão aplicáveis ao cumprimento dos prazos de execução e suas prorrogações.

6.2. Sistema de avaliação e homologação de Fornecedores

6.2.1. A Prosegur utiliza uma plataforma online gerida por um fornecedor externo à Prosegur (GoSupply Advanced Applications, S.L., doravante "GoSupply"), para a pré-qualificação, avaliação e homologação preliminar de seus Fornecedores/Empreiteiros. Para a qualificação e homologação definitiva de um Fornecedor/Empreiteiro, é obrigatório o registro e participação do Fornecedor/Empreiteiro no processo de análise de risco de Fornecedores, que a Prosegur implementou através da referida plataforma.

6.2.2. O Fornecedor/Empreiteiro deve ser qualificado como adequado no processo de análise da Prosegur antes do início de qualquer fornecimento de serviços, bens e/ou materiais objeto destas Condições Gerais e/ou do Contrato/Pedido correspondente. Da mesma forma, o Fornecedor/Empreiteiro garante e se compromete a manter as condições aprovadas na referida análise durante todo o prazo em vigor destas Condições Geais e/ou Contrato/Pedido correspondente e, para isso, se compromete a entregar à Prosegur as informações e/ou documentação atualizada solicitada de acordo com os critérios estabelecidos pela Prosegur.

6.2.3. O Fornecedor/Empreiteiro é informado e assume que a Prosegur não está envolvida nos serviços prestados pela "GoSupply", sendo responsabilidade do fornecedor desta plataforma os serviços de acesso e outras circunstâncias associadas ao registro na mesma. A Prosegur é apenas a destinatária da informação que o Fornecedor/Empreiteiro 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/Empreiteiros, focado na melhoria constante de seus Fornecedores/Empreiteiros para melhorar a sustentabilidade e a qualidade dos bens e serviços comercializados à Prosegur. Este serviço de pré-qualificação, avaliação e homologação preliminar, de contratação direta entre Fornecedores e Prosegur é obrigatório e envolve o pagamento à Prosegur de uma taxa anual, que será designada em função do nível de faturamento anual do Fornecedor/Empreiteiro e das categorias de produtos e serviços aos quais dedica sua atividade. Em qualquer caso, a Prosegur determinará a categoria atribuída ao Fornecedor/Empreiteiro e a taxa anual correspondente, que consiste em:

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

Estas taxas e/ou a categoria inicialmente atribuída ao Fornecedor/Empreiteiro podem ser revisadas e atualizadas pela Prosegur a qualquer momento e a seu exclusivo critério, e o Fornecedor/Empreiteiro se compromete a aceitar as novas taxas e/ou a nova categoria atribuída assim que comunicada pela Prosegur.

6.2.5. O Fornecedor/Empreiteiro aceita que o pagamento das taxas anuais pelo serviço de pré-qualificação, avaliação e homologação preliminar de Fornecedor seja feito à Prosegur, através de débito direto na mesma conta bancária que o Fornecedor/Empreiteiro 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. Da mesma forma, no caso de reembolso ou impossibilidade de efetuar o pagamento de acordo com o acima exposto, a Prosegur terá o direito de deduzir e/ou compensar o valor correspondente a tais prestações das faturas pendentes de pagamento ao Fornecedor/Empreiteiro.

6.3. Obrigações e responsabilidades do Fornecedor/Contratado

6.3.1. O Fornecedor/Contratado se compromete a realizar as obras, serviços e fornecimento de bens, de acordo com o estabelecido no Pedido/Contrato e/ou seus anexos e a cumprir todas as obrigações de natureza técnica, administrativa, fiscal, de trabalho, jurídica e qualquer outra relacionada à relação contratual.

6.3.2. O Fornecedor/Contratado deverá entregar toda a documentação exigida pela Prosegur no Pedido/Contrato, tanto em termos de prazo e quantidade, como quaisquer outras informações ou documentos de qualquer tipo que possam ser exigidos pelas leis, regras ou regulamentos aplicáveis ao fornecimento, trabalho ou serviço.

6.3.3. O Fornecedor/Contratado, a pedido da Prosegur, deve apresentar prova documental do cumprimento das obrigações referidas nas seções anteriores. A não apresentação ou apresentação insuficiente de tal documentação constituirá uma grave violação de suas obrigações.

6.3.4. De acordo com a natureza do Pedido/Contrato, o Fornecedor/Contratado nomeará os responsáveis, de sua organização, pelo fornecimento de bens e/ou contratação de obras e/ou serviços que estejam estabelecidos nas Condições Especiais, e comunicará tal nomeação ao respectivo Coordenador da Prosegur.

6.3.5. O Fornecedor/Contratado e, se for o caso, seus subcontratados são responsáveis pelo pagamento pontual de salários, previdência social e qualquer outra compensação ou indenização por trabalho ou de qualquer outra natureza que, por qualquer razão, seus funcionários devem receber e manterão a Prosegur isenta de qualquer reclamação decorrente do não cumprimento desta obrigação.

6.3.6. O Fornecedor/Contratado e, se for aplicável, seus subcontratados, deverão cumprir as normas legais em vigor e outras regulamentações, tais como as das Convenções Fundamentais da Organização Internacional do Trabalho relativas aos direitos no trabalho e previdência social.

O Fornecedor/Contratado e, se for o caso, seus subcontratados, devem cumprir todas as disposições referentes ao Meio Ambiente, Prevenção de Riscos no Trabalho, Segurança e Saúde em vigor e aplicáveis ao Pedido/Contrato, devem seguir as políticas e procedimentos da Prosegur e, em qualquer caso, devem respeitar o Código de Ética e Conduta da Prosegur que está
publicado em espanhol e inglês nos seguintes links contidos no site da Prosegur:

- Código Ético y de Conducta Prosegur - ES
- Code of Ethics and Conduct Prosegur – EN
- Código de Ética e Conduta da Prosegur - BR

6.3.7. O Fornecedor/Contratado e, se for aplicável, seus subcontratados serão responsáveis e deverão indenizar e isentar a Prosegur e o restante do Grupo Prosegur de reclamações por danos diretos, indiretos e/ou consequentes, incluindo perda de negócios, danos à imagem ou perda de lucro, perda ou destruição de propriedade do primeiro e/ou de terceiros ou por morte, doença ou lesão do pessoal do primeiro e/ou de terceiros decorrentes do desempenho pelo Fornecedor/Contratado e/ou, se for aplicável, seus subcontratados de suas obrigações contratuais ou legais. Essa responsabilidade incluirá honorários e custos legais, e os valores do Seguro contratado nos termos da Cláusula 2.10 não constituirão um limite a sua responsabilidade.

6.3.8. O Fornecedor/Contratado e, se for caso, seus subcontratados serão responsáveis perante a Prosegur e as demais Empresas do Grupo Prosegur, por quaisquer danos diretos, indiretos e/ou consequentes, incluindo perda de negócios, danos à imagem e lucros cessantes, que ele/ela ou as pessoas pelas quais são legal ou contratualmente responsáveis, possam causar à Prosegur ou às empresas do Grupo Prosegur por danos, perda ou destruição de suas propriedades ou por morte, doença ou lesão a seu pessoal, e que sejam causados por um ato ou omissão no cumprimento das obrigações derivadas do Pedido/Contrato pelo Fornecedor/Contratado e, se for o caso, por seus subcontratados ou seu pessoal. Essa responsabilidade incluirá honorários e custos legais, e os valores do Seguro contratado nos termos da Cláusula 2.10. não constituirão um limite a sua responsabilidade.

6.3.9. O Fornecedor/Contratado garante a indenização da Prosegur contra possíveis reclamações dos funcionários do Contratado envolvidos no cumprimento do Pedido/Contrato ou seus subcontratados, que serão defendidos ou negociados pelo Fornecedor/Contratado, que também assumirá os custos de defesa e os valores ou declarações objeto de liquidação ou contidos em uma condenação final.

6.3.10. Da mesma forma, o Fornecedor/Contratado garante a indenização da Prosegur contra qualquer sanção administrativa ou qualquer outra que possa ser imposta como resultado, direta ou indiretamente, da execução do Pedido/Contrato.

6.3.11. Em caso de não cumprimento pelo Fornecedor/Contratado das obrigações indicadas nos parágrafos anteriores, a Prosegur terá o direito de deduzir das seguintes certificações/faturas a serem pagas pela Prosegur os valores de tais reclamações ou sanções não cumpridas pelo Fornecedor/Contratado, bem como as despesas de defesa incorridas pela Prosegur como resultado de tal não cumprimento.

6.3.12. O regime de responsabilidade legal referido neste documento não se aplica às responsabilidades pelas quais cada uma das Partes pode ser responsabilizada de acordo com a lei de prevenção de riscos no trabalho ou os regulamentos aplicáveis nesta área e seus regulamentos de implementação, caso em que se aplicará o regime legal e regulamentar estabelecido para tal responsabilidade.

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

6.3.14. Nos casos em que a condição de Fornecedor/Contratado for detida por uma joint venture temporária, ou qualquer entidade sem personalidade jurídica própria que não seja a de seus componentes, a responsabilidade que possa ter derivada deste Pedido/Contrato em relação à Prosegur será solidária para todas as pessoas ou empresas que fazem parte das empresas em questão.

6.3.15. Como consequência do acima 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 pessoa física ou jurídica que integram 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 responsável, em nenhuma hipótese e sob nenhuma circunstância, por quaisquer danos diretos, indiretos e/ou consequentes que o Fornecedor/Contratado possa sofrer, derivados direta ou indiretamente do Pedido/Contrato, incluindo, mas não se limitando à perda de uso, lucros e interrupções de negócios.

6.3.17. A Prosegur incentiva a contratação de fornecedores que atendem aos critérios de sustentabilidade e responsabilidade social corporativa, que fomentam e estão de acordo com os

objetivos de desenvolvimento sustentável das Nações Unidas, e que possuem certificado de ASG, seja por pertencerem a Índices sustentáveis ou através de certificados nesse campo. A Prosegur fomenta e incentiva os fornecedores e associados com os quais trabalha a aceitarem os seguintes princípios:

- Respeitar as leis aplicáveis de todas as jurisdições nas quais o Grupo Prosegur opera
- Operar como empregador socialmente responsável que tenha o compromisso de:
    - pagar aos seus funcionários um salário digno que esteja sempre acima do salário mínimo interprofissional
    - respeitar a proibição do trabalho infantil e do trabalho forçado,
    - respeitar a não discriminação e a igualdade de oportunidades,
    - respeitar a liberdade de associação, o direito a negociação coletiva e a eliminação de horas de trabalho excessivas.
- Oferecer um ambiente de trabalho seguro de acordo com todas as normas de segurança e saúde ocupacional.
- Usar métodos de trabalho sustentáveis que respeitem o meio ambiente, exigindo de seus fornecedores o compromisso de:
    - Usar energias renováveis
    - Tomar medidas voltadas à redução de emissões e de agentes contaminantes que evitem a mudança climática
    - Respeito pela biodiversidade
  - Uso sustentável de recursos naturais
  - Redução de resíduos
- Respeitar o Código Ético e de Conduta da Prosegur.

6.4. Obrigações e responsabilidades da Prosegur

6.4.1. Pagamento de bens, obras e/ou serviços a preços e condições estipulados no pedido/contrato conforme estipulado nas cláusulas 2.6 e 2.7.

6.5. Cessão do Pedido/Contrato e subcontratação

6.5.1. As obras, bens e serviços objeto do Pedido/Contrato não podem ser delegadas ou subcontratadas, no todo ou em parte, sem autorização prévia por escrito da Prosegur, caso em que o subcontratado será expressamente subrogado em todas as condições deste documento.

6.5.2. Para obter autorização prévia para subcontratação, o Fornecedor/Contratado exigirá da Subcontratada toda a documentação prevista no Pedido de Oferta e nestas Condições Gerais, bem como seu compromisso por escrito de cumprir todas e cada uma das cláusulas do Pedido/Contrato e sua documentação anexa, e deverá entregar imediatamente tudo à Prosegur.

6.5.3. Em caso de utilização de subcontratados, o Fornecedor/Contratado permanecerá principalmente responsável perante a Prosegur pelo cumprimento das obrigações previstas no Pedido/Contrato, mesmo no caso de bens, obras e/ou serviços diretamente fornecidos/prestados pelo subcontratado autorizado. Sem prejuízo disso, a Prosegur pode a qualquer momento inspecionar e monitorar o trabalho do subcontratado e o cumprimento de suas obrigações.

6.6. Condições econômicas e impostos

6.6.1. Os preços incluídos no Pedido/Contrato e/ou seus anexos, serão entendidos como fixos e não revisáveis até a conclusão total e correta do Pedido/Contrato, a menos que expressamente declarado

de outra forma, e incluirão todos os impostos, tarifas, imposições, taxas e direitos presentes ou futuros, exceto o Imposto sobre Valor Agregado ou impostos similares, que deverão aparecer separadamente como um item independente.

6.6.2. Como exceção adicional ao parágrafo anterior e caso o imposto retido na fonte seja aplicado de acordo com a Legislação aplicável, o valor do imposto retido na fonte não deve ser entendido como incluído no preço. Portanto, o Fornecedor deverá pagar o valor total da fatura ao Cliente e, adicionalmente, pagar o imposto retido na fonte correspondente à Administração Fiscal do Fornecedor. Em caso de redução do imposto retido na fonte devido à aplicação de um Acordo para Evitar a dupla tributação entre os dois países, o Cliente deverá, a pedido do Fornecedor, entregar ao Fornecedor, antes de qualquer pagamento, um certificado de residência fiscal de acordo com o Acordo, para que o Fornecedor possa pagar o imposto retido na fonte de acordo com o referido Acordo. O Fornecedor, depois de pagar o imposto retido na fonte, deverá fornecer ao Cliente um certificado de pagamento do imposto retido.

6.6.3. Bens, obras e/ou serviços não incluídos no Pedido/Contrato não serão pagos se sua execução não tiver sido previamente oferecida pelo Fornecedor/Contratado, por escrito, e aceita, também por escrito, pela Prosegur, a correspondente modificação do Pedido/Contrato.

6.6.4. O pagamento de adiantamentos por conta será feito, conforme o caso, com a apresentação da garantia bancária correspondente pelo mesmo valor a ser pago, 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 contemplado no Pedido/Contrato correspondente.

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

6.6.6. O Fornecedor/Contratado será responsável por qualquer diferença no frete, transporte, impostos ou quaisquer outras despesas decorrentes do não cumprimento das instruções de envio ou quaisquer outras condições estabelecidas ou aplicáveis ao Pedido/Contrato.

6.6.7. Todos os impostos cobrados sobre as operações comerciais a que estas Condições Gerais se referem, serão assumidos pelas partes de acordo com a lei. O contribuinte do imposto é responsável, em cada caso, pela correta tributação de suas obrigações fiscais.

6.7. Forma de pagamento

6.7.1. Todos os pagamentos devem ser feitos 60 dias corridos após a data da fatura, a menos que um período diferente tenha sido acordado entre as partes ou que outro período de pagamento tenha sido estabelecido por lei. As faturas apenas serão pagas se a Prosegur tiver documentos que demonstrem o recebimento dos serviços realizados de acordo com o Pedido/Contrato. No caso de fornecimento de bens, serão aplicáveis os Incoterms e/ou condições de entrega incluídos no Pedido.

A transferência bancária ou confirmação é estabelecida como forma de pagamento habitual.

6.7.2. Todas as outras formas de pagamento devem ser claramente definidas nas Condições Especiais e no Pedido/Contrato.

6.8. Aceitação do Pedido/Contrato

6.8.1. Aceitação do Contrato: A assinatura do Contrato pelas Partes será considerada como sua aceitação plena.

6.8.2. Aceitação do Pedido: A assinatura ou confirmação de recebimento como sinal de aceitação do Pedido pelo Fornecedor/Contratado à Prosegur. Em qualquer caso, a simples execução do Pedido pelo Fornecedor implica a aceitação implícita do mesmo por ele e exclui qualquer exceção não aceita por escrito pela Prosegur.

6.9. Prazos de entrega e execução

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

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

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

6.10. Garantias

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

Garantia de cumprimento fiel e dos bens, obras e/ou serviços para a finalidade requerida. Será estabelecido pelo Fornecedor/Contratado para garantir o cumprimento de todas suas obrigações contratuais nos termos do Pedido/Contrato, a partir do momento de aceitação/assinatura do Pedido/Contrato, até a admissão definitiva pela Prosegur dos bens, obras e/ou serviços requeridos. A exigência ou não de tal Garantia será estabelecida no Pedido de Orçamento e/ou no Pedido/Contrato correspondente.

Esta Garantia será estabelecida através do Modelo de Garantia do Anexo II (emitido por um banco com uma classificação mínima BBB- da Standard & Poor ou aprovado pelo Departamento de Tesouraria da Prosegur) ou por um seguro de garantia (emitido por uma seguradora com uma classificação mínima 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 fornecimento de bens, estes são de sua propriedade, adequados à finalidade, e de primeira qualidade e primeiro uso, e que cumprem os requisitos de segurança e qualidade especificados no Pedido. O Contratado garante que a realização de obras e/ou serviços cumpre os requisitos de segurança e qualidade especificados no Contrato. Da mesma forma, o Fornecedor/Contratado garante o cumprimento da legislação correspondente em vigor, bem como os regulamentos da Prosegur, e que cumprirá os programas de trabalho/execução estabelecidos.

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

6.10.4. Retenções como Garantia: A retenção como garantia será estabelecida no Pedido/Contrato.

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

Para bens, 12 meses a partir da data de comissionamento ou 24 meses a partir da data de recebimento no destino ou disponibilização, de acordo com o Incoterm aplicável, o que ocorrer antes, se o Fornecedor tiver condições de maior duração, estas serão respeitadas.

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

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

6.10.6. Durante o período de garantia, o Fornecedor/Contratado será responsável por todas as violações e/ou danos, sem prejuízo das disposições da Cláusula 6.3.16 e seguintes, decorrentes do não cumprimento ou cumprimento defeituoso ou inadequado pelo Fornecedor/Contratado das condições contratuais aplicáveis ao fornecimento, obra ou serviço, se aplicável, devido a defeitos na qualidade dos materiais utilizados.

O período de garantia será interrompido pelo tempo utilizado nos respectivos reparos ou substituições, os quais, por sua vez, serão garantidos, após a rescisão, pelo mesmo período de tempo do período inicial da garantia.

6.10.7. Tal não conformidade ou desempenho deficiente ou inadequado do fornecimento, obra e/ou serviço, ou defeito de qualidade em questão, quando o Fornecedor/Contratado não tiver realizado as ações corretivas pertinentes, ou quando não demonstrar diligência adequada na resolução dos problemas apresentados, pode dar origem a: Retenção pela Prosegur dos pagamentos pendentes; à execução da garantia econômica e/ou bancária e mesmo à rejeição total ou parcial do fornecimento, obra ou serviço realizado, com exigência neste caso da restituição dos valores pagos sem que essa circunstância seja causa de qualquer reclamação por parte do Fornecedor/Contratado.

6.10.8. A Prosegur deverá, se aplicável, deduzir qualquer sanção aplicável das faturas pendentes de pagamento ao Fornecedor/Contratado.

Da mesma forma, a fim de se compensar por suas próprias despesas ou pelas despesas e custos derivados da contratação com terceiros para o reparo ou execução do não cumprimento ou desempenho defeituoso pelo Fornecedor/Contratado, e por qualquer outra dívida que o Fornecedor/Contratado mantenha com a Prosegur, poderá deduzir tais valores das faturas pendentes de pagamento ao Fornecedor/Contratado.

O pagamento ou dedução de tais sanções e despesas não isentará o Fornecedor/Contratado de quaisquer de suas outras obrigações e responsabilidades decorrentes do Pedido/Contrato.

6.10.9. A dívida do Proenecedor/Contratado com a Prosegur é automaticamente considerada como qualquer quantia que seja reclamada de Prosegur, devido a saques a descoberto ou não cumprimento pelo Fornecedor/Contratado em relação a salários, previdência social, obrigações fiscais e quaisquer outras que possam ser reclamadas da Prosegur de acordo com as normas legais ou regulamentares.

6.10.10. As possíveis deduções feitas, de acordo com as seções anteriores, serão totalmente independentes do valor depositado como Garantia, se houver.

6.10.11. Caso o Fornecedor pretenda interromper a fabricação do produto coberto pela Ordem de Compra, deverá enviar notificação por escrito com aviso de recebimento dirigido ao Departamento de Compras da Prosegur com seis meses de antecedência à data em que pretende interromper a fabricação do produto. Essa notificação deve conter, pelo menos, (i) identificação do produto; (ii) identificação das Ordens de Compra afetadas; (iii) lista dos países afetados; e (iv) data em que se pretende completar a fabricação do produto.

A partir da emissão da Ordem de Compra, o Fornecedor garante o serviço técnico adequado e a existência de peças de reposição pelo período mínimo de dez (10) anos em todos os países envolvidos e a partir da data em que o produto deixa de ser fabricado. O preço das peças de reposição ou produtos e serviços será oferecido à Prosegur a um preço máximo equivalente ao preço contratual dos produtos substituídos; e com o mesmo nível de cumprimento das exigências técnicas solicitadas pela Prosegur para que o produto seja reparado ou substituído.

Como garantia deste compromisso, a Prosegur se reserva o direito de exigir que o Fornecedor forneça uma garantia bancária na primeira demanda, de acordo com o modelo de Garantia no Anexo II deste documento.

O não cumprimento de tal garantia ou a capacidade de cumrpi-la por parte do Fornecedor terá os seguintes efeitos:

- A retenção de qualquer pagamento pendente por parte da Prosegur
- A execução da garantia bancária
- O cancelamento total ou parcial das Ordens de Compra em andamento, sem que isso implique qualquer indenização em favor do fornecedor.
- O direito da Prosegur de poder reivindicar todos os danos, perdas, custos e despesas incorridas (incluindo taxas legais) incorridos para cumprir suas obrigações não cumpridas do Fornecedor por seus próprios meios ou através de terceiros.

Além disso, o Fornecedor, ao seu próprio custo, deverá disponibilizar para a Prosegur todos os desenvolvimentos de software personalizados, incluindo código-fonte, código-objeto, manuais e quaisquer outras informações relevantes.

6.11. Seguros

6.11.1. Sem prejuízo de sua responsabilidade nos termos do Pedido/Contratol, e sem que esta cláusula a limite, o Fornecedor/Contratado deverá contratar e manter em vigor, por sua conta, durante todo o período de validade do Pedido/Contrato, e com empresas de reconhecida solvência financeira, os seguros descritos abaixo. As coberturas e valores cobertos por esse seguro nunca devem ser inferiores aos obrigatórios nos termos das leis em vigor. Sua manutenção não deve variar as obrigações de manter a Prosegur isenta, estabelecidas pelo Pedido/Contrato.

6.11.1.1 Contratos de Obras e/ou Serviços

a) Seguro de doença e acidente de trabalho de todos os funcionários designados aos Trabalhos, de acordo com a lei aplicável, incluindo as leis do estado de origem dos funcionários expatriados.

b) Seguro de construção/edificação, montagem e danos para equipamentos de construção alugados, contratados ou de propriedade do Empreiteiro, com um limite não inferior ao seu valor de substituição. No caso de seguro de construção, será necessário contratar a cobertura adicional para pessoas

adjacentes e pré-existentes. No caso de acidente, e independentemente da causa, o Contratado renuncia expressamente ao direito de recurso contra a Prosegur por qualquer dano ou perda sofrida por tais bens, assumindo o compromisso de notificar por escrito suas seguradoras sobre esta renúncia de recurso.

c) Seguro de responsabilidade empresarial, incluindo, entre outros, responsabilidade do empregador, profissional, remoção de produtos, pós-trabalhos e poluição e contaminação com uma cobertura igual ao valor das obras/serviços contratados nas Condições Especiais de cada Contrato e que, pelo menos, será a dos valores standard indicados no Anexo I.

No caso de apólices de responsabilidade civil, se forem contratadas sob o escopo temporário de cobertura por ocorrência, o Contratado deverá manter tais apólices em vigor até o vencimento do período de garantia ou responsabilidade legal. Se as apólices forem contratadas sob o escopo temporário da cobertura de sinistros, o Contratado deverá manter as apólices em vigor, pelo menos, dois (2) anos após o vencimento da garantia ou do período de responsabilidade legal.

Esse seguro incluirá a Prosegur como um segurado adicional, sem perder sua condição de terceiro.

d) Se o uso de automóveis, máquinas automotoras, máquinas industriais, aeronaves ou embarcações for necessário para a realização da obra, seguro de responsabilidade civil, com um limite que será fixado por sinistro nas Condições Especiais de cada Contrato e que, pelo menos, será o dos valores standard indicados no Anexo I.

Se for necessário alugar embarcações, será necessária uma cobertura de proteção e indenização (proprietário/fretador) com um clube do Grupo Internacional.

Não obstante o acima exposto, o Contratado pode contratar o seguro adicional que julgar necessário para a cobertura completa de suas responsabilidades nos termos do Contrato.

6.11.1.2 Pedidos de Bens

a) Seguro de doença e acidente de trabalho de todos os funcionários designados aos trabalhos, de acordo com a lei aplicável, incluindo as leis do estado de origem dos funcionários expatriados.

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

c) Seguro de responsabilidade empresarial, incluindo, entre outros, responsabilidade do empregador, profissional, produtos, remoção de produtos, pós-trabalho, poluição e contaminação com uma cobertura igual ao valor dos bens adquiridos que, pelo menos, será o valor determinado nas Condições Especiais de cada Pedido.

No caso de apólices de responsabilidade civil, se forem contratadas sob o escopo temporário de cobertura por ocorrência, o Fornecedor deverá manter tais apólices em vigor até o vencimento do período de garantia ou responsabilidade legal. Se as apólices forem contratadas sob o escopo temporário de cobertura por reclamação, o Fornecedor deverá manter as apólices em vigor, pelo menos, dois (2) anos após o vencimento da garantia ou período de responsabilidade legal.

Esse seguro incluirá a Prosegur como um segurado adicional, sem perder sua condição de terceiro.

Não obstante o acima exposto, o Fornecedor poderá contratar o seguro adicional que julgar necessário para a cobertura completa de suas responsabilidades nos termos do Pedido.

6.11.2. Antes da entrega dos bens ou do início de obras/serviços, o Fornecedor/Contratado deverá entregar à Prosegur um certificado dos seguros contratados. Este certificado será incorporado ao Contrato/Pedido como Anexo. A não entrega do certificado dará à Prosegur o direito de rescindir o Contrato/Pedido por razões atribuíveis ao Fornecedor/Contratado.

6.11.3. A Prosegur pode, a qualquer momento, solicitar ao Fornecedor/Contratado a entrega das apólices originais, ou cópias autenticadas das apólices de seguro que contratou, bem como recibos ou comprovantes de estar em dia com o pagamento dos prêmios correspondentes. O Fornecedor/Contratado é obrigado a entregar todos os documentos acima em um prazo não superior a sete (7) dias.

6.11.4. O Fornecedor/Contratado é obrigado a 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 nos termos e condições das apólices do Fornecedor/Contratado.

6.11.6. Todos os seguros referidos na cláusula 2.10.1. devem incluir uma declaração isentando a seguradora de responsabilidade e não repetição contra a Prosegur.

6.11.7. O Fornecedor/Contratado deverá, sob sua exclusiva responsabilidade, exigir, caso aplicável, que os subcontratados mantenham a mesma política de responsabilidades e seguros exigida ao FornecedorContratado. Isto não isentará o Fornecedor/Contratado de sua responsabilidade para com a Prosegur.

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

- Solicitar limites por reclamação superiores aos estabelecidos no Anexo I,
- Solicitar coberturas ou seguros adicionais não incluídos na seção 2.10.1

6.12. Sanções por não cumprimento

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

6.12.2. Caso não sejam especificadas nas condições especiais do Pedido/Contrato, as seguintes sanções serão aplicadas no caso de não cumprimento objetivo das obrigações do Fornecedor/Contratado:

- Entrega de Materiais: Multa de até 10% por semana

- Atraso na execução de obras ou prestação de serviços: Multa de até 5% por semana.

6.13. Cessão de direitos e créditos

6.13.1. Os Pedidos/Contratos e créditos e/ou faturas decorrentes dessas relações jurídicas não podem ser cedidos, total ou parcialmente, ou prometidos, sem a autorização prévia e expressa da Prosegur, por escrito de acordo com a forma a ser estabelecida.

6.13.2. A Prosegur pode ceder, sem o consentimento prévio do Fornecedor/Contratado, parte ou todos os seus direitos e obrigações nos termos do Pedido/Contrato em favor de qualquer empresa do Grupo Prosegur ou como consequência de qualquer operação societária que envolva uma sucessão, total ou parcial, dos direitos e obrigações correspondentes.

6.14. Inspeções/Ativações

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

Para agilizar os preparativos para o cumprimento do prazo de entrega, o Fornecedor deve ter um sistema de controle para monitorar seus fornecedores de materiais, componentes e serviços que afetam os bens objeto do Pedido.

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

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

Para isso, a PROSEGUR nomeará inspetores que terão livre acesso às oficinas e processos de fabricação, sem que essa inspeção diminua a responsabilidade do Fornecedor.

6.14.3. O Fornecedor/Contratado realizará revisões semestrais dessas instalações ou oficinas temporárias nas instalações da Prosegur ou de seus clientes. Do resultado dessas inspeções e revisões, o Fornecedor/Contratado informará à Prosegur.

6.14.4. Quando o Pedido/Contrato exigir a entrega à Prosegur de documentação (planos, especificações, etc.) deve ser previamente assinado pelo Fornecedor/Contratado como aprovação. A Prosegur se reserva o direito de verificar a veracidade da documentação e das informações fornecidas pelo Fornecedor/Contratado onde está localizada ou onde a Prosegur indicar ou solicitar. Para isso, a Prosegur poderá nomear inspetores que terão livre acesso à documentação de suporte sem que essa inspeção diminua a responsabilidade do Fornecedor/Contratado.

6.15. Entrega e envio de bens

6.15.1. Todos os bens fornecidos devem ser devidamente embalados para evitar danos. A Prosegur não aceitará nenhum custo de embalagem se não tiver sido previamente acordado. Os bens de diferentes Pedidos/Contratos não serão embalados juntos.

6.15.2. Todos os envios serão acompanhados de uma nota de entrega ou comprovante de entrega indicando a quantidade, descrição do produto, número do Pedido/Contrato, referência do Fornecedor/Contratado, e lista de pacotes, fazendo a distribuição do documento conforme 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 correspondente do Pedido/Contrato, bem como indicações de manuseio ou precauções a adotar nos casos necessários.

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

a) Cada pacote deve ser identificado com o número do lote, fabricação e data
b) Os bens correspondentes a mais de dois lotes não serão incluídos na mesma entrega, exceto previamente notificado pelo Fornecedor à Prosegur, e aceita por escrito por esta última.
c) O Fornecedor notificará as limitações de expiração do bem, caso existirem, indicando ba embalagem a data de expiração do uso dos bens.
d) Regras para identificação, marcação, transporte e manuseio estabelecidas na ficha de segurança e aquelas específicas para mercadorias perigosas.

6.15.5. Para bens que por sua natureza são entregues em tanques, o Fornecedor deverá cumprir e fazer o seguinte:

a) As obrigações e responsabilidades do transportador e do expedidor, tanto na contratação quanto nas operações de carga, seguem as disposições da legislação aplicável (Lei de Gestão do Transporte Terrestre, Acordo ADR, etc.).
b) A transportadora assume a execução das operações de carga de materiais nas instalações da Prosegur.
c) O transportador é obrigado a cumprir rigorosamente as regras do centro de carga (tanto operacionais quanto de segurança).
d) O Fornecedor será sempre responsável perante a Prosegur e terceiros por quaisquer danos que possam ser causados durante as operações de carga no centro de carga (ação negligente ou inadequada).
e) Antes de facilitar o acesso ao transporte às instalações, o Fornecedor deve justificar à Prosegur no local de entrega que os transportes do MP possuem a seguinte documentação em vigor:

- Seguro(s)
- ITV
- Carteira de Motorista e ADR
- Certificado ADR de trator e petroleiro
- EPI do motorista
- Painéis laranja e etiquetas de perigo.
- Carta de expedição ADR
- EPI a ser usado pelo motorista de acordo com os regulamentos atuais.

6.15.6. O simples recebimento pela Prosegur de um envio ou expedição de mercadorias do Fornecedor não será considerado como aceitação final do mesmo, que estará sujeito a revisão subsequente. A Prosegur tem o direito de reclamar por defeitos e/ou imperfeições de qualidade ou quantidade, etc. e o Fornecedor deve tomar as medidas necessárias para atender tais reivindicações.

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

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

6.16. Recepção de obras, bens e/ou serviços

6.16.1. Recepção Provisória: Uma vez que as obras e/ou serviços tenham sido finalizados, toda a documentação exigida entregue, se a execução tiver sido correta, com todos os testes e provas de instalação realizados com sucesso, a Prosegur elaborará um certificado de recepção provisória indicando a conformidade ou não com as condições estabelecidas no Pedido/Contrato em relação às obras efetivamente executadas, datas de disponibilidade, qualidade, funcionamento correto e quaisquer outras observações. A partir da data de assinatura deste documento provisório, o período de garantia estabelecido começará a ser contado. Este documento provisório será assinado em aceitação pelo Contratado.

6.16.2. Se as obras e/ou serviços realizados apresentarem algum defeito, a Prosegur dará ao Contratado um prazo para correção. Caso isso não for realizado no prazo indicado, a Prosegur poderá realizar por si ou por terceiros, cobrado do valor retido como garantia, ou cobrado ao Contratado pelo valor das obras e/ou serviços não cobertos pela garantia retida.

6.16.3. Recepção final: Uma vez expirado o prazo de garantia estabelecido para as obras e/ou serviços e desde que não haja reclamações da Prosegur pendentes de resolução pelo Contratado, a aceitação final das obras e/ou serviços terá lugar. A Prosegur é obrigada a reembolsar ao Contratado o valor, se houver, da garantia de reparação não designado para pagamentos às suas custas.

6.16.4. O Contratado deverá refazer, por sua própria conta, as obras defeituosas devido a erros ou omissões do Contratado. Além disso, as despesas de reparação, modificação ou substituição de materiais necessários para corrigir tais erros ou omissões serão por sua conta.

6.16.5. A entrega de bens, obras e serviços e o fornecimento do documento ou nota de entrega correspondente não implica que a Prosegur tenha aceito 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 corridos para verificar a qualidade das obras, bens e/ou serviços entregues e proceder a sua devolução, por conta do Fornecedor/Contratado, caso não cumpram as especificações de qualidade ou técnicas exigidas de acordo com o 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/Contratado o preço das obras, bens e/ou serviços que foram corretamente entregues e aceitos pela Prosegur. Isso sem prejuízo do direito da Prosegur de exigir o cumprimento pelo Fornecedor/Contratado de sua obrigação de entregar as demais obras, bens e/ou serviços ou o cancelamento do Pedido/Contrato correspondentes, e, em qualquer caso, ser indenizada pelos danos sofridos.

6.17. Rescisão do Pedido/Contrato

6.17.1. O Pedido/Contrato será finalizado por rescisão ou expiração.

6.17.2. Rescisão do Pedido/Contrato devido ao Fornecedor/Contratado.

6.17.2.1 Além dos legalmente estabelecidos, a Prosegur se reserva o direito de rescindir o Pedido/Contrato pelos motivos que, por exemplo e não por limitação, são indicados abaixo:

a) A venda ou transferência inter vivos ou mortis causa da empresa do Fornecedor/Contratado ou sua transformação em outra pessoa jurídica, pelos meios legalmente estabelecidos, sem a aprovação por escrito da Prosegur.

b) O não cumprimento pelo Fornecedor/Contratado de qualquer uma das cláusulas ou obrigações contidas nestas Condições Gerais, do Pedido/Contrato ou de qualquer um dos documentos contratuais assinados pelas partes.

c) As sanções máximas aplicáveis, conforme estabelecido no Pedido/Contrato, foram alcançadas.

d) O não cumprimento da legislação em vigor pelo Fornecedor/Contratado.

e) A existência de embargos e retenções de créditos decretados por órgãos judiciais ou administrativos de natureza executória (Agência do Estado, Tributária, Previdência Social, etc.) ou a dissolução da empresa do Fornecedor/Contratado.

f) Estar pendente de execução/entrega, mais de 20% das obras, bens e serviços, quando o prazo estabelecido no Pedido/Contrato expirar.

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

h) Existência de graves imprecisões nas informações disponibilizadas pelo Fornecedor/Contratado, especialmente em relação à qualidade, prevenção de riscos no trabalho, segurança e saúde, sistemas de gestão ambiental, condições e cumprimento das exigências de trabalho.

i) Não cumprimento dos princípios éticos e de conduta da Prosegur.

j) O não cumprimento das obrigações de confidencialidade.

k) Quando detectado um caso de conflito de interesses entre o Fornecedor/Contratado e um funcionário da Prosegur e tal situação não tenha sido previamente comunicada e expressamente autorizada.

l) Quando o Fornecedor/Contratado, seus acionistas ou seus diretores, estiverem envolvidos em casos de fraude, corrupção ou na prática de qualquer outro tipo de crime.

6.17.2.2 Quando ocorrer alguma das causas acima, o Pedido/Contrato será rescindido e sem efeito a partir da data em que a Prosegur comunicar sua decisão a este respeito ao Fornecedor/Contratado ou, quando for o caso, aos seus sucessores.

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

a) Suspender os pagamentos pendentes

b) Executar as garantias que o Fornecedor/Contratado constituiu.

c) Manter em penhor os bens e elementos do Fornecedor/Contratado que estão na posse da PROSEGUR.

6.17.3. Rescisão do Pedido/Contrato por vontade da Prosegur

6.17.3.1 A Prosegur se reserva o direito de cancelar o Pedido/Contrato unilateralmente a qualquer momento, justificando e comunicando por escrito sua decisão ao Fornecedor/Contratado, pelo menos, 30 (trinta) dias antes da data em que a resolução deva entrar em vigor.

6.17.4. O pedido de declaração de falência, quebra, suspensão de pagamentos ou início de qualquer processo de insolvência, do Fornecedor/Contratado, de acordo com as leis ou regulamentos aplicáveis,

dará à Prosegur, no prazo de 30 (trinta) dias após tomar conhecimento da existência do referido pedido, exigir que o Fornecedor/Contratado acredite no prazo de 10 (dez) dias após receber o pedido feito para este fim pela Prosegur os seguintes pontos:

- Que tenha os meios materiais e pessoais necessários e suficientes para continuar executando os trabalhos contratados (pessoal, meios técnicos, etc.).

- Que possui os meios econômicos necessários para executar até a conclusão dos trabalhos contratados, apresentará à Prosegur uma garantia bancária conjunta, a pedido inicialmente e com renúncia expressa dos benefícios de execução e divisão, pelo valor total dos trabalhos contratados pendentes de execução aumentado 25% do referido valor, para garantir o cumprimento pelo Fornecedor/Contratado com todas as suas obrigações contratuais.

Se no prazo de dez (10) dias, o Fornecedor/Contratado não comprovar todos os pontos referidos nesta seção, a Prosegur terá direito a rescindir o Pedido/Contrato, com direito a indenização pelo Fornecedor/Contratado por todos os danos que tal rescisão do contrato possa causar.

6.18. Força Maior

6.18.1. Nenhuma das partes será responsabilizada pelo não cumprimento de suas obrigações decorrentes do Pedido/Contrato, desde que a execução do mesmo seja adiada ou impossibilitada em decorrência de Força Maior.

Para essa finalidade, serão considerados de Força Maior os fenômenos naturais, acidentes inevitáveis, pandemias, incêndio, revoltas populares, 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 similar imprevisível ou que seja previsível, inevitável, irresistível ou independente da vontade das partes e fora de seu controle.

No entanto, as disposições do parágrafo anterior não podem ser invocadas como causa de Força Maior a suspensão das obrigações contratuais causadas pelo pessoal do Fornecedor/Contratado ou de seus Subcontratados.

6.18.2. A suspensão das obrigações contratuais durará enquanto a causa que originou a força maior permanecer. A parte que sofrer a suspensão deverá informar imediatamente a outra parte e fazer esforços razoáveis para resolver a causa da suspensão no menor tempo possível.

Se a causa de força maior durar mais de um mês, a Prosegur se reserva o direito de cancelar o Pedido/Contrato com o pagamento ao Fornecedor/Contratado dos valores devidos para a realização dos trabalhos, prestação de serviços ou entrega dos bens que até o momento da rescisão foram realizados pelo Fornecedor/Contratado, sem esta rescisão do direito à cobrança de qualquer valor adicional ou multa ou compensação em favor do Fornecedor/Contratado.

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 Direitos de Propriedade Intelectual e Industrial, ou similares, de terceiros e que não há qualquer reivindicação, demanda ou litígio; (ii) que está suficientemente autorizada para o fornecimento de serviços, produtos, entregas e desenvolvimentos Ad Hoc para a Prosegur, e que não possui acordo com terceiros que a 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 assegurar a exploração plena e pacífica pela Prosegur. Em conformidade com a garantia acima, o Fornecedor isenta a Prosegur de qualquer responsabilidade por infrações relacionadas à exploração e uso dos serviços, produtos, entregas e desenvolvimentos Ad Hoc para a Prosegur fornecidos pelo Provedor, 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 a Prosegur e é obrigado a fornecer prova documental à Prosegur e, se necessário, que possui os Direitos de Propriedade Intelectual e Industrial necessários para a execução do que é objeto deste 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.

2.19.2. Indenização.

Se eventualmente se interponha 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 dos seus administradores, agentes ou funcionários, em relação ao cumprimento das obrigações referidas, o Fornecedor isenta a Prosegur de qualquer responsabilidade e indenizará a Prosegur pelos danos e prejuízos sofridos, comprometendo-se a isentar seus conselheiros, diretores e funcionários de qualquer perda, responsabilidade, danos, prejuízos, gastos e custos (incluindo custos legais) incorridos

pela Prosegur, bem como quaisquer danos causados a terceiros, garantindo à Prosegur o uso dos Direitos de Propriedade Intelectual e Industrial que deram origem à reclamação ou disponibilizando outros diferentes que permitam a continuidade dos serviços, produtos ou do contrato.

2.19.3. Direitos de Propriedade Intelectual e Industrial da Prosegur.

2.19.3.1. Entende-se por Direitos de Propriedade Intelectual e Industrial 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. 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 neste documento é uma transferência, cessão ou licença sobre tais 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, sendo obrigado a respeitar as instruções da Prosegur.

2.19.3.2. Em particular, o Fornecedor não poderá utilizar a denominação, nome comercial, logotipo ou marcas registradas da Prosegur, nem utilizá-los ou utilizar a aceitação de qualquer oferta, nem a assinatura ou execução deste Contrato, nem a prestação dos serviços nele referidos, como referência para a aquisição 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 que, como resultado da relação entre as partes, o Fornecedor deva 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 como resultado da relação aqui regulada.

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 deste 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 todos e para qualquer tipo de exploração, ainda que não seja o setor habitual de atividade da Prosegur. Consequentemente, a Prosegur poderá exercer livremente e da forma que considerar, os Direitos de Propriedade Intelectual e Industrial dos Desenvolvimentos Ad Hoc, incluindo a sua exploração, transmissão, cessão, licença a terceiros e tudo nos termos e condições que considerar.

2.19.4.2. O Fornecedor compromete-se a colaborar com a Prosegur para dar cumprimento às suas obrigações e, em particular, (i) a colaborar na obtenção dos registros 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 por ele assumidos nesta cláusula, renunciando a reclamar por eles.

2.19.5. Software.

2.19.5.1. Na hipótese do Fornecedor licenciar o Software Padrão (aquele desenvolvido genericamente para o mesmo uso por muitas pessoas) à Prosegur para a execução deste contrato, a referida licença será exclusiva, irrevogável, sublicenciável para uso (inclusive em favor do Grupo Prosegur), em todo o mundo e pelo prazo máximo de vigência de tais direitos.

2.19.5.2. O Fornecedor garante que não utilizará software de código aberto (sob licença de código aberto) para a execução deste contrato sem o consentimento prévio por escrito da Prosegur. Para este fim, informará a Prosegur dos termos e condições da licença aplicável, confirmará que o programa de computador como um todo não pode ser considerado como software de código aberto e que seu uso não restringe o uso dos serviços, produtos, Entregas e Desenvolvimentos Ad Hoc para a Prosegur. Em caso de uso autorizado, o Fornecedor se compromete e garante o cumprimento dos termos e condições da licença aplicável.

2.20. Confidencialidade de informações e documentos

2.20.1. As informações confidenciais serão consideradas 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 após a data do Pedido/Contrato por parte da Prosegur ou seus administradores, funcionários, representantes, subsidiárias ou seus consultores, advogados, auditores ou Fornecedores externos, ou processados no âmbito das atividades objeto do Pedido/Contrato e todas as informações a que o Fornecedor/Contratado acesse ou tenha conhecimento durante a prestação dos serviços objeto do Pedido/Contrato e, em qualquer caso, todos os dados relacionados ou associados a uma pessoa física específica ou determinável, sejam informações ou materiais relacionados à Prosegur ou a terceiros (quer sejam, sem limitação, informações ou dados relacionados a clientes, fornecedores, funcionários ou qualquer outro terceiro que mantenha qualquer vínculo com a Prosegur ou qualquer uma 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/Contratado, a existência de qualquer oferta de bens, obras e/ou serviços, de qualquer documento de aceitação de qualquer oferta de bens, obras e/ou serviços, ou de qualquer outro acordo, contrato ou documento relativo ou destinado à prestação de bens, obras e/ou serviços pelo Fornecedor/Contratado à Prosegur, bem como o conteúdo de tais conversas, negociações, oferta de bens, obras e/ou serviços, carta, contrato, acordos, contratos ou documentos.

c) a título de exemplo e sem limitação, o termo Informações Confidenciais inclui a forma como o Grupo Prosegur opera, segredos comerciais, segredos de negócios, 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, quaisquer informações científicas ou técnicas, invenção, design, processo, procedimento, fórmula, melhoria, tecnologia ou método; quaisquer conceitos, amostras, relatórios, dados, know-how, trabalhos em andamento, projetos, desenhos, fotografias, ferramentas de desenvolvimento, especificações, programas de computador, código fonte, código de objeto, gráficos organizacionais e bancos de dados, independentemente de as informações estarem por escrito, ou em outro formato documental, oral, visual, eletrônico ou legível por máquina, amostras, modelos ou de outra forma. As Partes concordam que as Informações Confidenciais não são obrigadas a serem novas, únicas, patenteáveis, protegidas por direitos autorais ou um segredo comercial para que sejam classificadas como Informações Confidenciais e, portanto, protegidas.

A partir de agora, qualquer das informações referidas em a), b) e c) serão referidas como "Informações Confidenciais".

2.20.2. Obrigação de confidencialidade:

a) As Informações Confidenciais serão tratadas confidencialmente pelo Fornecedor/Contratado e não serão divulgadas, total ou parcialmente, direta ou indiretamente (através de seus funcionários, colaboradores externos e internos, subcontratados, auditores ou outras entidades relacionadas) a terceiros, sob qualquer circunstância, exceto com o consentimento prévio por escrito da Prosegur. Em particular, o Fornecedor/Contratado se compromete a tomar as medidas necessárias para impedir o acesso de terceiros não autorizados às Informações Confidenciais e a limitar o acesso às mesmas a funcionários autorizados que precisem ter acesso para a realização dos bens, obras e/ou serviços, transferindo a eles a mesma obrigação de confidencialidade.

b) O Fornecedor/Contratado garante que as Informações Confidenciais não serão utilizadas ou exploradas, para seu próprio benefício ou de terceiros, para usos ou finalidades que não sejam a prestação dos bens, obras e/ou serviços.

c) O Fornecedor/Contratado se compromete a não copiar, divulgar, comunicar, emprestar ou de outra forma reproduzir, divulgar ou difundir as Informações Confidenciais a terceiros, publicá-las ou de qualquer outra forma disponibilizá-las a terceiros, seja diretamente ou através de terceiros ou empresas, sem o consentimento prévio por escrito da Prosegur.

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

e) As obrigações estabelecidas para o Fornecedor/Contratado no Pedido/Contrato também serão vinculantes aos seus funcionários, colaboradores externos ou internos, subcontratados, advogados e auditores, pelo qual o Fornecedor/Contratado será responsabilizado pela Prosegur se tais obrigações não são cumpridas por tais funcionários, colaboradores, subcontratados, advogados e auditores. O Fornecedor/Contratado se compromete a obter de seus colaboradores externos ou subcontratados autorizados pela Prosegur um compromisso escrito em termos idênticos aos estipulados nesta cláusula em relação às Informações Confidenciais em sua posse.

2.20.3. Exceções à obrigação de confidencialidade. Auditorias:

a) A obrigação de confidencialidade não se aplica e, portanto, as Informações Confidenciais que são ou se tornam acessíveis ao público por razões que não sejam o não cumprimento da obrigação de confidencialidade pelo Fornecedor/Contratado; que tenham sido publicadas antes da data do Pedido/Contrato que já estejam na posse legítima do Fornecedor/Contratado e não estejam sujeitas a um acordo de confidencialidade entre as partes, desde que este fato seja divulgado à outra parte antes do momento da divulgação; que sejam recebidas através de terceiros sem restrições e sem implicar uma violação de qualquer obrigação legal ou contratual de terceiros; ou que sejam desenvolvidas independentemente pelo Fornecedor/Contratado para outros fins que não os bens, obras e/ou serviços a serem prestados à Prosegur e que tenha sido desenvolvido sem o uso ou assistência de Informações Confidenciais.

b) A divulgação de Informações Confidenciais a fim de cumprir uma ordem judicial ou administrativa não estará sujeita à obrigação de confidencialidade desde que o Fornecedor/Contratado que tenha recebido a ordem correspondente informe com antecedência por escrito a Prosegur sobre a obrigação de proceder com tal divulgação.

c) A Prosegur está autorizada a supervisionar o desenvolvimento dos bens, obras e/ou serviços contratados, a fim de garantir que estejam de acordo com as instruções emitidas e as normas pertinentes, e pode solicitar ao Fornecedor/Contratado quaisquer informações que considere relevantes, acessar o local físico onde os serviços são desenvolvidos e realizar, diretamente ou através de terceiros, quaisquer auditorias e verificações que considere de interesse.

2.20.4. Devolução de Informações Confidenciais: Após a conclusão da obra ou entrega de bens e/ou prestação do serviço objeto do Pedido/Contrato, ou antes dessa data, se assim solicitado pela Prosegur e não é necessário que o Fornecedor/Contratado disponha deles para prestar os serviços a Prosegur, o Fornecedor/Contratado, deve devolver à Prosegur quaisquer Informações Confidenciais que esteja na posse do Fornecedor/Contratado.

2.20.5. Propriedade das Informações Confidenciais: Não se reconhece a favor do Fornecedor/Contratado qualquer direito de propriedade ou outro direito sobre as Informações Confidenciais, exceto os direitos de uso estabelecidos no Pedido/Contrato e com as limitações nele estabelecidas.

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

2.20.7. Não cumprimento: O Fornecedor/Contratado é responsável e indenizará a Prosegur por todos os danos causados como resultado do não cumprimento de qualquer uma das obrigações de confidencialidade estabelecidas.

2.20.8 Em qualquer caso, a prestação dos serviços sujeitos a qualquer oferta de serviço do Fornecedor, ou através de subcontratados autorizados pelo Cliente, não deverá prejudicar os poderes de inspeção do Banco de Espanha e/ou outros órgãos reguladores da atividade do Cliente. O Fornecedor se compromete a permitir ao Banco de Espanha e a outros órgãos reguladores acesso direto e irrestrito às informações do Cliente em poder do Fornecedor ou de seus subcontratados autorizados pelo Cliente, para que o Banco de Espanha ou outros órgãos reguladores possam realizar as verificações relevantes em relação a tais informações, incluindo a verificação da adequação dos sistemas e aplicativos utilizados. O Fornecedor se compromete a obter de seus subcontratados autorizados pelo Cliente um compromisso por escrito em termos idênticos aos estipulados nesta cláusula em relação às informações em seu poder, acesso às suas instalações e verificação da adequação dos sistemas e aplicativos utilizados.

6.21. Proteção de dados pessoais

6.21.1. Caso o Fornecedor tenha que acessar dados pessoais de propriedade da Prosegur, será necessário assinar o contrato de Responsável pelo Processamento, previsto no Anexo III.

6.21.2. Em qualquer caso, o Fornecedor que tem que ter acesso aos dados pessoais de propriedade da Prosegur (a partir de agora, "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 sobre proteção das pessoas físicas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE -Regulamento Geral de Proteção de Dados- (a partir de agora, "RGPD"), bem como na Lei Orgânica 3/2018, de 5 de dezembro, sobre Proteção de Dados Pessoais e garantia dos direitos digitais (LOPDGDD).

Em geral, em conformidade com as disposições das normas aplicáveis de proteção de dados, o Fornecedor que tem acesso a dados pessoais manifesta-se expressamente e compromete-se a:

a. Utilizar e processar os Dados com o único e exclusivo propósito de cumprir este Contrato e em qualquer caso seguindo as instruções recebidas da Prosegur. O Fornecedor deve abster-se expressamente de utilizar os Dados para qualquer outro uso diferente do acordado e, em particular, deverá abster-se de modificar, utilizar para seu próprio interesse comercial ou comunicá-los ou permitir que terceiros tenham acesso a eles, mesmo para armazenamento.

b. Observar a máxima confidencialidade e reserva em relação aos dados pessoais fornecidos pela Prosegur em relação ao desenvolvimento do tema deste Contrato, comprometendo-se a não divulgar a terceiros esses dados, bem como quaisquer outras informações que teriam sido fornecidas a ele em relação à Prosegur.

c. Devolver a Prosegur, ao finalizar a prestação de serviços objeto deste Contrato, todos os documentos e arquivos nos quais todos ou quaisquer dos Dados, qualquer que seja seu suporte ou formato, bem como cópias dos mesmos.

d. Restringir o acesso e o uso dos Dados aos funcionários, agentes e colaboradores que sejam absolutamente essenciais para que tenham acesso e conhecimento para o desenvolvimento do objeto deste Contrato, se comprometendo a impor a eles as obrigações de confidencialidade e proibição de uso em relação aos Dados, nos mesmos termos previstos neste Contrato, e se comprometendo a ser responsável por qualquer violação dessas obrigações por qualquer de seus funcionários, agentes e colaboradores mencionados acima.

e. Adotar, implementar e exigir as medidas de segurança técnicas e organizacionais necessárias para garantir a segurança adequada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perdas, destruição ou danos acidentais, através da aplicação de medidas técnicas ou organizacionais apropriadas ("integridade e confidencialidade") e para atualizar as medidas de segurança de acordo com os requisitos legalmente supervenientes durante a duração deste Contrato e quaisquer outras medidas que estejam sujeitas a notificação pela Prosegur.

   Especificamente, de acordo com o artigo 32 do RGPD, o Fornecedor implementará as medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, levando em conta o nível de sensibilidade das atividades de dados e processamento realizadas, incluindo, mas não se limitando a, o seguinte:

- a pseudonimização e criptografia de dados pessoais, quando apropriado;
- a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento de dados;
- a capacidade de recuperar a disponibilidade e o acesso aos dados pessoais com rapidez em caso de incidente físico ou técnico;
- um processo de verificação, avaliação e valorização periódico da eficácia das medidas técnicas e organizacionais para garantir a segurança do tratamento de dados.

f. O Fornecedor não pode subcontratar nenhum dos serviços que fazem parte do tema deste Contrato em apoio ao processamento de dados pessoais, a menos que expressamente autorizado por escrito pela Prosegur.

   Se for necessário subcontratar qualquer processamento, este fato deve ser comunicado com antecedência e por escrito à Prosegur, indicando os tratamentos que se destinam a ser subcontratados e identificando de forma clara e inequívoca a empresa subcontratada e seus detalhes de contato.

   Em caso de autorização, o subcontratado, que também terá o status de processador, também será obrigado a cumprir as obrigações estabelecidas neste Contrato para o Fornecedor e as instruções dadas pela Prosegur. Cabe ao Fornecedor inicial regular a nova relação de acordo com o artigo 28 do RGPD, de modo que o novo processador esteja sujeito às mesmas condições (instruções, obrigações, medidas de segurança...) e com os mesmos requisitos formais que ele, no que diz respeito ao processamento adequado de dados pessoais e à garantia dos direitos das pessoas em causa.

   Em caso de descumprimento pelo subprocessador, o Fornecedor inicial permanecerá plenamente responsável pela Prosegur no que diz respeito ao cumprimento das obrigações.

g. Quando as pessoas afetadas exercem seus direitos de acesso, retificação, eliminação, oposição, não estar sujeitas a decisões individualizadas automatizadas, limitação de processamento e portabilidade de dados perante o Fornecedor, este último deve comunicar por e-mail ao endereço indicado pela Prosegur. A comunicação deverá ser feita imediatamente e em nenhum caso depois do dia útil após o recebimento do pedido, juntamente, se for o caso, com outras informações que possam ser relevantes para a solução do pedido.

h. No caso de qualquer violação da segurança dos Dados Pessoais, o Fornecedor deverá notificar tal violação sem demora indevida, e em qualquer caso, no prazo máximo de vinte e quatro (24) horas através de qualquer endereço de contato, físico ou eletrônico, 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. Isentar a Prosegur de qualquer reclamação que possa ser movida contra a Prosegur com a Autoridade de Controle correspondente, que seja causada pela violação do Fornecedor e/ou de seus subcontratados das disposições deste acordo e da legislação atual sobre o assunto de proteção de dados pessoais, e compromete-se a pagar o valor a que a Prosegur possa ser condenada a título de multa, indenização, danos e juros, incluindo honorários advocatícios, em virtude da referida violação.

6.22. Segurança em tecnologias da informação

O Fornecedor se compromete a ter um sistema operacional em suporte, com as últimas atualizações de segurança, pelo menos as dos últimos três meses. Também garante que possui um software antivírus atualizado instalado com atualização automática ativada.

O Fornecedor não se conectará de uma máquina não pertencente à Prosegur para realizar tarefas administrativas nos servidores da Prosegur.

Em caso de não cumprimento destas obrigações, a Prosegur está isenta, em toda a extensão permitida pela legislação aplicável, de qualquer responsabilidade por danos de qualquer tipo, diretos e indiretos, incluindo, perda de lucro ou perdas de clientes, lucro ou exploração, que possam ser devidos a uma violação da segurança de equipamentos/sistemas de computador ou redes de comunicação do Fornecedor, incluindo situações de vazamento de informações ou adulteração de informações, intervenção ilegal ou intrusão de sistemas, comunicação e/ou software por malware (vírus, Trojans, worms) e outras rotinas de programação prejudiciais de terceiros, sem que esta lista seja limitada de outras formas que possam modificar e/ou afetar o computador ou os sistemas de comunicação da Prosegur.

O Fornecedor será responsável sem limite por danos de qualquer natureza, direta e indireta, entre outros, à perda de lucro ou perda de clientes, lucro ou exploração, por qualquer interrupção, perturbação ou falha do serviço prestado à Prosegur, causada por atos ou omissões de terceiros decorrentes do não cumprimento dessas obrigações.

Caso o Fornecedor identifique uma violação de segurança de seus sistemas, deverá informar o gerente de projeto da Prosegur, por qualquer meio que deixe um registro e no prazo de 24 horas após tomar conhecimento disso. O cumprimento desta obrigação não isenta o Fornecedor de responsabilidade por não cumprimento das obrigações acima.

O Fornecedor deve cumprir o disposto no Anexo V Uso de Recursos e Sistemas de TI, bem como assinar o anexo "*DECLARAÇÃO DO USUÁRIO SOBRE O USO DE RECURSOS E SISTEMAS DE TI",* do qual faz parte.

Qualquer Fornecedor que requer acesso às tecnologias de informação do Grupo Prosegur, fornece serviços/produtos tecnológicos e/ou digitais, bem como serviços não tecnológicos que tenham capacidade de acessar a tecnologias da informação e/ou informações do Grupo, deve devem cumprir as disposições do Anexo IV. Caso o fornecedor preste serviços que não exijam acesso a tecnologias da Informação do Grupo Prosegur, serão aplicadas as seções 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 fazer auditorias técnicas e revisar o status de conformidade do fornecedor com o Esquema de Controle por ele estabelecido.

Em relação às auditorias técnicas, os custos e despesas associados à intervenção da Prosegur serão por sua conta. Em caso de detecção de vulnerabilidades, o Fornecedor será responsável por corrigi-las segundo os procedimentos técnicos de gerenciamento de vulnerabilidades do Grupo Prosegur e os seguintes tempos de resolução:

- Crítica: 10 dias.

- Alta: 20 dias.
- Médias: 90 dias.
- Demissões: 180 dias.

Em caso de descumprimento dos prazos, uma penalização de 5% será aplicada sobre a faturação anual total, que será compensada em faturas futuras associadas ao serviço.

6.23. Solução de controvérsias e litígios

6.23.1. A legislação aplicável ao Pedido/Contrato será a do local de seu cumprimento. O local de execução é o lugar onde, de acordo com o Pedido/Contrato, os bens devem ser entregues ou a obra executada e/ou os serviços prestados.

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

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

6.24. Arquivos

6.24.1. O Fornecedor/Contratado deverá manter atualizado um registro completo do bem fornecido e/ou obras e/ou serviços realizados sob o Pedido/Contrato, bem como todas as transações relacionadas a ele. O Fornecedor/Contratado deverá manter todos esses registros por um período de pelo menos três anos após depois da conclusão do Pedido/Contrato. Esses registros estarão disponíveis para possível auditoria por parte da Prosegur. A auditoria, se houver, não se aplicará às Patentes do Fornecedor/Contratado ou a quaisquer informações adicionais relacionadas a elas.

6.24.2. A Prosegur reserva-se o direito de rever as políticas ambientais, trabalhistas e de governança corporativa dos seus principais fornecedores, visando aumentar o nível de exigência em relação aos seus fornecedores no que diz respeito à sustentabilidade.

7. ANEXOS

7.1. Documentos Associados:

Código	Nome
DS-GLO-EF-COM-02	Anexo I: Lista de limites exigidos nos seguros de acordo com produtos ou serviços

MD-GLO-EF-COM-02	Anexo II: Modelo de garantia bancária de cumprimento fiel e garantia de bens, obras e/ou serviços
MD-GLO-LEG-07	Anexo III: Contrato de Processador de Dados
	Anexo IV: Requisitos de Risco Tecnológico e Segurança Digital
	Anexo V: Uso de Recursos e Sistemas de TI da Prosegur

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

VALORES A PAGAR NOS SEGUROS DE PRODUTOS OU SERVIÇOS (POR SINISTRO)

ATIVIDADE	PMEs	MULTINACIONAL
TODOS		
Seguros de Acidentes:	Mínimo legal	Mínimo legal
Seguro de Responsabilidade Civil exploração da atividade de trabalho	3.000.000 €	6 000 000 €
Responsabilidade Civil do Produto, Recall de Produtos, Pós-Trabalho, Vínculo e Mistura, Poluição e Poluição	3.000.000 €	6 000 000 €
Seguro de Responsabilidade Civil do Empregador	300.000 €	600.000 €
Responsabilidade Civil de automóveis, máquinas autopropulsionadas, aeronaves, barcos:	Mínimo legal	Mínimo legal
Seguro adaptado ao local de benefício		
CONSTRUÇÃO		
Seguro de construção/construção e montagem:	Orçamento obra	Orçamento obra
Responsabilidade Civil do Produto, Recall de Produtos, Pós-Trabalho, Vínculo e Mistura, Poluição e Poluição	3.000.000 €	6.000.000 €
Máquinas industriais de responsabilidade civil:	3.000.000 €	6.000.000 €
Danos próprios aos equipamentos de construção; alugado ou de propriedade do Contratado:	Valor de reposição	Valor de reposição
Seguro decenal:	Mínimo legal	Mínimo legal
SERVIÇOS PROFISSIONAIS		
Responsabilidade Civil Profissional Atividade profissional fornecida	3.000.000 €	6.000.000 €
	3.000.000 €	6.000.000 €
SERVIÇOS DE TECNOLOGIA PROFISSIONAL		
Responsabilidade Civil Profissional Tech PL	3.000.000 €	6.000.000 €
Riscos cibernéticos e proteção de dados	3.000.000 €	6.000.000 €
TECNOLOGIA		
Responsabilidade Civil Profissional Tech PL	3.000.000 €	6.000.000 €
Responsabilidade Civil do Produto, Recall de Produtos, Pós-Trabalho, Vínculo e Mistura, Poluição e Poluição	3.000.000 €	6.000.000 €
Ciberriscos e proteção de dados	3.000.000 €	6.000.000 €
TRANSPORTE DE BENS COMPRADOS		
Cobertura de transporte porta a porta	Valor transportado	Valor transportado
Transporte carga e descarga		
ARMAZENAMENTO DE ESTOQUE EM ARMAZÉNS DE		
Cobertura de todos os riscos de armazém	Valor transportado	Valor transportado
GARANTIA DE PRODUTO E SERVIÇOS		
Garantia do produto	Mínimo legal	Mínimo legal
Recall de produtos		
Garantia de quebra 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 [•] (a partir de agora, o "BANCO"), com CIF [•] residente em [•], e em seu nome e representação o Sr. [•] e o Sr. [•] com poderes suficientes para vinculá-lo neste ato em conformidade com a procuração concedida pelo Notário de [•], Sr. [•], em [•] de [•] de [•], com o número [•] de protocolo

ENDOSSA

Incondicional, irrevogável e solidariamente, renunciando expressamente aos benefícios de divisão, excusão e ordem, até os limites indicados e sob as condições expressas abaixo, para [ ] (a partir de agora o [FORNECEDOR]), com sede social em [ ] e com NIF [ ], para garantir o pagamento pelo FORNECEDOR a PROSEGUR COMPAÑÍA DE SEGURIDAD, S.A. (a partir de agora, "PROSEGUR") de todas as obrigações assumidas pelo FORNECEDOR no contrato de [ ] datado de [ ] (a partir de agora, o "CONTRATO") sob o qual o FORNECEDOR [ ] a PROSEGUR (a partir de agora os [BENS] [OBRAS] [SERVIÇOS]) e, especialmente, ser responsável pelo pagamento de quaisquer perdas, reinvindicações por danos, reclamações, causas de ação, responsabilidades, sanções, custos e, ou despesas quantificadas e determinadas de qualquer natureza incorridas pelo FORNECEDOR contra a PROSEGUR ou imputadas a esta última, por responsabilidade do FORNECEDOR agora ou no futuro, como resultado de quaisquer declarações enganosas ou imprecisas, não cumprimento, contingência e/ou reclamações de terceiros decorrentes da execução do CONTRATO.

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

O BANCO se compromete a efetuar o pagamento do valor requerido até os valores máximos (individuais e conjuntos) previamente previstos, no prazo não prolongado de três (3) dias a partir do recebimento de tal comunicação, e na conta indicada para tais fins pela PROSEGUR.

SEGUNDO. - RENÚNCIA DE EXCEÇÕES. Esta Garantia é irrevogável e é concedida de forma abstrata e, o primeiro pedido, o BANCO não pode se opor ou alegar contra a PROSEGUR qualquer tipo de exceção e, em particular, as exceções pessoais que o FORNECEDOR possa conceder contra a PROSEGUR. Assim, uma vez apresentado o pedido descrito na seção anterior, o BANCO não pode, de forma alguma questionar a validade da reivindicação da PROSEGUR ao BANCO.

TERCEIRO: - PRAZO DE VALIDADE. Esta garantia entrará em vigor hoje e será válida durante [...] ([...]) anos a partir de hoje. Nessa data, se o BANCO não tiver recebido comunicação confiável de qualquer pagamento do valor feito pelo FORNECEDOR, ele expirará e será automaticamente extinto.

QUARTO. - CESSÃO. A PROSEGUR pode ceder esta garantia a qualquer terceiro. Para que tal cessão seja válida em relação ao BANCO, basta que seja comunicada ao BANCO pela PROSEGUR. Neste caso, todas as referências à PROSEGUR contidas nesta garantia devem ser interpretadas como referência ao cessionário desta garantia.

QUINTO. - DESPESAS. Quaisquer custos e despesas relacionadas a esta garantia bancária serão pagos e suportados exclusivamente pelo FORNECEDOR.

Essa garantia foi registrada nesta mesma data no Registro Especial de Garantias com o n mero [•].

[*AUTENTICADA POR NOTÁRIO PÚBLICO*]

7.4. ANEXO III. CONTRATO DE RESPONSÁVEL PELO PROCESSAMENTO DE DADOS

REUNIDOS

De um lado, a PROSEGUR (de um lado, o "Controlador de Dados"), e de outro lado, o Fornecedor (doravante o "Processador"), que serão coletivamente referidos como "**Partes**" e, individualmente, cada um deles como a "**Parte**"

EXPÕEM

I. Que, em consequência da prestação dos serviços detalhados no Contrato de Compra ou Fornecimento, o Processador poderá ter acesso aos dados pessoais que estão sob a responsabilidade, guarda e proteção da **PROSEGUR**; para esses fins, o Fornecedor tendo o status legal de Processador de Dados com relação a eles.

II. Que, consequentemente e para cumprir na íntegra o estabelecido nas diretrizes nacionais e comunitárias aplicáveis, as Partes têm a intenção de reunir no presente Acordo as condições de tratamento de dados pelo Fornecedor em conformidade com o previsto na legislação espanhola.

III. Que, não obstante o acima exposto, as Partes também desejam cumprir as exigências relativas à regulamentação da relação do Processador de dados conforme estabelecido pelo artigo 28 do Regulamento do Parlamento Europeu e do Conselho (UE) 2016/679, de 27 de abril de 2016; para isso assinam as seguintes

CLÁUSULAS

Primeira - Tratamento de dados pessoais

A prestação de serviços poderia envolver o acesso do Processador de dados a informações confidenciais e dados pessoais de responsabilidade da PROSEGUR. esse sentido, o Fornecedor será considerado como Processador de Dados, e seu processamento da responsabilidade de dados pessoais da PROSEGUR consistirá única e exclusivamente de acesso e, se for o caso, armazenando os dados pessoais estritamente necessários para a prestação dos serviços referidos no Contrato de Compra ou Fornecimento.

Segunda - Confidencialidade e dever de sigilo

Exceto se acordado o contrário pelas Partes, estas e as demais empresas pertencentes ao seu Grupo ou que estejam vinculadas a elas, manterão segredo absoluto em relação a esse acordo, seu negócio e as informações e a documentação referente à outra Parte, que tenha chegado ao seu conhecimento como resultado do cumprimento do acordo. O Encarregado do tratamento de dados se compromete, do mesmo modo, especificamente, a tratar como confidencial todas as informações às quais possa ter acesso, e que sejam de responsabilidade do responsável ou de terceiros, a fim de prestar seus serviços, comprometendo-se a fazer com que tais dados permaneçam secretos.

O Encarregado do tratamento de dados se compromete, para essa finalidade, a tomar as medidas necessárias em relação aos seus funcionários ou colaboradores para que sejam informados sobre a necessidade de cumprir as obrigações que lhe compete como Encarregado do tratamento de

dados e que devem respeitar, consequentemente, bem como garantir que os dados pessoais dos quais tenham conhecimento com resultado do presente acordo permanecem secretos mesmo depois que o presente acordo seja finalizado por qualquer motivo que for. Para isso, o Processador cumprirá todas as advertências (por meio de treinamento, mensagens de conscientização, etc.) e assinará os documentos necessários com seus funcionários ou colaboradores, a fim de garantir o cumprimento de tais obrigações. Estes deverão estar informados, de forma compreensível, sobre a existência do presente acordo, as normas de segurança que afetam o desempenho das suas funções, as consequências em caso de não cumprimento e o caráter de confidencialidade das informações e do dever de manter segredo dos dados pessoais, sendo que a obrigação de confidencialidade e de segredo subsistirá mesmo que a relação com o Encarregado do tratamento de dados seja finalizada.

Tal obrigação de informação para os funcionários e colaboradores do Encarregado de tratamento de dados deverá ser realizada de tal forma que seja possível documentar o cumprimento dessa obrigação e colocar à disposição da PROSEGUR.

Adicionalmente, as informações e a documentação confidencial não poderão ser utilizadas para finalidades diferentes do cumprimento da finalidade do acordo, exceto se essa informação for de conhecimento geral e salvo no que diz respeito às informações necessárias devido às Leis ou a qualquer outra regulamentação aplicável e obrigatória.

Depois que finalizado este acordo, a obrigação de confidencialidade e o dever de manter sigilo previsto nesta cláusula serão mantidas indefinidamente, mesmo depois de finalizada a relação com o Responsável pelo processamento, por qualquer razão.

Em caso de detecção de qualquer tipo de atuação indevida de qualquer pessoa que desempenhe funções profissionais para o Encarregado do tratamento de dados (acesso a informações que não correspondam às suas funções, utilização indevida de nome de usuário e senhas, um usuário com mais autorizações do que as necessárias, ou qualquer outra), caberá ao Encarregado do tratamento de dados a responsabilidade e a obrigação específicas de informar a PROSEGUR imediatamente juntamente com um relatório dos fatos.

Terceira - Instruções do Responsável do processamento

O Processador de dados se compromete a processar os dados pessoais aos quais tenha acesso apenas de acordo com as instruções por escrito indicadas para essa finalidade pelo Responsável do processamento de dados, observando sempre, pelo menos, a mesma política de proteção de dados pessoais e com a política de medidas de segurança para sua conservação, como as empregadas para isso pela PROSEGUR. Esse compromisso também se estenderá em relação às transferências internacionais de dados pessoais a outro país ou a uma organização internacional.

Consequentemente, os dados que sejam conhecidos ou obtidos como resultado do presente acordo:

- não poderão ser usados para nenhuma finalidade diferente da execução desse, serão confidenciais e não serão publicados ou divulgados a terceiros sem a autorização prévia por escrito do Responsável pelo tratamento de dados. Os dados não deverão ser tratados, em caso algum para fins próprios.
- não serão comunicados a terceiros sem a autorização prévia por escrito da PROSEGUR. Neste sentido, o Encarregado do tratamento de dados identificará por escrito, antes que a PROSEGUR autorize sua divulgação, a entidade ou as entidades às quais irá comunicar os dados, quais

dados ou categoria de dados pessoais serão submetidos a comunicação e as medidas de segurança a serem aplicadas para realizar tal comunicação.

Neste sentido, o Encarregado do tratamento de dados se compromete a informar imediatamente o Responsável pelo tratamento de dados caso uma instrução encaminhada por este venha a infringir as disposições que sejam aplicáveis no que diz respeito à proteção de dados nas regulamentações comunitárias ou dos Estados-Membros.

Caso o Encarregado do tratamento de dados os destine a uma finalidade diferente, comunique ou utilize em contravenção das estipulações do presente acordo, também será considerado Responsável pelo tratamento de dados, respondendo pessoalmente pelas infrações que possa ter causado, bem como pelos danos e prejuízos que possam ser causados, neste caso, à PROSEGUR.

Quarta - Subcontratação de serviços

O Processador de Dados não pode subcontratar nenhum dos serviços que fazem parte do tema do Contrato em apoio ao processamento de dados pessoais, a menos que expressamente autorizado por escrito pela Prosegur.

Se for necessário subcontratar qualquer processamento, este fato deve ser comunicado com antecedência e por escrito à Prosegur, indicando os tratamentos que se destinam a ser subcontratados e identificando de forma clara e inequívoca a empresa subcontratada e seus detalhes de contato.

Em caso de autorização, o subcontratado, que também terá o status de processador, também será obrigado a cumprir as obrigações estabelecidas no presente Contrato de Processamento de Dados e as instruções dadas pela Prosegur. Cabe ao Processador de Dados inicial regular a nova relação de acordo com o artigo 28 do RGPD, de modo que o novo processador esteja sujeito às mesmas condições (instruções, obrigações, medidas de segurança...) e com os mesmos requisitos formais que ele, no que diz respeito ao processamento adequado de dados pessoais e à garantia dos direitos das pessoas em causa.

Em caso de descumprimento pelo subprocessador, o Processador de Dados inicial permanecerá plenamente responsável pela Prosegur no que diz respeito ao cumprimento das obrigações.

Quinta - Medidas de segurança

O Encarregado do tratamento de dados se compromete a cumprir as medidas de segurança técnicas e organizacionais que sejam apropriadas para assegurar um nível de segurança adequado ao risco que possa ser resultante do tratamento de dados, a fim de garantir a segurança e integridade dos dados pessoais e evitar que sejam alterados, perdidos, tratados ou acessados sem autorização, levando em consideração o status da tecnologia, os custos de aplicação, a natureza dos dados armazenados, o alcance do tratamento de dados, bem como os riscos aos quais estejam expostos, e o impacto que esses poderiam exercer sobre os direitos e as liberdadesdas pessoas físicas, sejam eles provenientes de ação humana ou do meio físico ou natural, cumprindo assim com o exigido pela diretriz em vigor.

O Encarregado do tratamento de dados estará sujeito a medidas de segurança que serão adequadas para a proteção dos dados pessoais e demais informações a serem realizadas pelo Encarregado do tratamento de dados e de acordo com o resultado da avaliação de riscos realizada pela PROSEGUR, levando em consideração o status da tecnologia, os custos de aplicação, a

natureza dos dados armazenados, o alcance e as finalidades dos tratamentos de dados e os riscos aos quais estejam expostos. Neste sentido, o Encarregado do tratamento de dados deverá proporcionar à PROSEGUR as informações necessárias, se a análise de risco realizada por aquela ou pelo Encarregado do tratamento de dados chegar à conclusão que o tratamento de dados envolve alto risco.

Em consequência, o Processador deverá aplicar aos dados pessoais objeto das operações de processamento, pelo menos, as medidas especificadas no APÊNDICE I deste Contrato.

Sexta - Notificação de lacunas de segurança

O Encarregado do tratamento de dados terá a obrigação de garantir a implementação dos requisitos de segurança estabelecidos neste acordo e de comunicar à PROSEGUR qualquer incidente que afetar direta ou indiretamente as informações, documentação e os dados pessoais de responsabilidade da PROSEGUR.

Quando o Processador de dados ou qualquer pessoa nos serviços detectar uma ocorrência que resulte em roubo, perda ou danos de informações, que uma pessoa tenha acessado a estas informações sem ter autorização ou se as informações forem utilizadas de modo inadequado, o Processador de dados deverá comunicar imediatamente à PROSEGUR informando os detalhes da ocorrência e, em qualquer caso, antes do prazo de vinte e quatro (24) horas, através do e-mail dpo@prosegur.com, anexando todas as informações relevantes para a documentação e comunicação da ocorrência e, pelo menos, as seguintes informações (desde que disponíveis):

1. Descrição da natureza da violação da segurança dos dados pessoais, inclusive, quando for possível, as categorias e o número aproximado de interessados atingidos e as categorias e o número aproximado de registros de dados pessoais afetados.
2. O nome e os dados de contato do encarregado da proteção de dados ou de outro ponto de contato do qual seja possível obter informações.
3. Descrição das possíveis consequências.
4. Descrição das medidas adotadas ou propostas para remediar a lacuna de segurança dos dados pessoais, incluindo, se for o caso, medidas para paliar os possíveis efeitos negativos.

Caso não seja possível fornecer as informações simultaneamente e, na medida em que não o seja, as informações serão disponibilizadas gradualmente, sem adiamentos indevidos.

Caberá ao Encarregado do tratamento de dados a responsabilidade de realizar as ações de contenção e resolução da ocorrência que sejam necessárias.

A PROSEGUR realizará um acompanhamento periódico do status da resolução da ocorrência, sendo que o Encarregado do tratamento de dados se comprometerá a responder com os relatórios que sejam solicitados.

Sétima - Registro das categorias de tratamento de dados

O Encarregado do tratamento de dados deverá manter um registro por escrito, naqueles casos em que seja determinado pelo Regulamento Geral de Proteção de Dados, e a legislação aplicável restante sobre o assunto, referente a todas as categorias de tratamentos de dados realizados em nome da PROSEGUR, devendo constar:

1. Os dados de contato da PROSEGUR e do Processador, bem como, se for o caso, os de seus representantes e responsáveis pela proteção de dados.
2. As categorias de tratamentos realizados em nome da PROSEGUR.

3. Se for o caso, as possíveis transferências internacionais de dados que possam ser geradas no escopo do tratamento de dados em si.
4. Uma descrição geral das medidas técnicas e organizacionais que sejam aplicáveis.

Oitava - Transferências Internacionais

De modo geral, o Encarregado do tratamento de dados não poderá realizar transferências internacionais de dados que sejam de responsabilidade do Responsável pelo tratamento de dados fora do Espaço Econômico Europeu, exceto se este tiver dado sua autorização prévia por escrito.

Se o Encarregado do tratamento de dados precisar transferir dados pessoais a outro país ou a uma organização internacional devido ao Direito da União ou dos Estados-Membros que lhe seja aplicável, ele deverá informar o responsável por essa exigência legal com antecedência, exceto se isto for vedado por tal Direito por questões relevantes de interesse público.

Caso o Responsável pelo tratamento de dados autorize as transferências internacionais de dados mencionadas, e estes sejam transferidos para um país que não tenha um nível de proteção adequado ou equivalente, deverão ser assinadas cláusulas em contrato do tipo estabelecido pela Comissão Europeia para essa finalidade. Neste sentido, o Encarregado do tratamento de dados deverá facilitar esses trâmites ao Responsável pelo tratamento de dados antes da realização da transferência internacional de dados.

Nona - Direitos Interessados

O Processador ajudará o Responsável do processamento de dados por meio da aplicação daquelas medidas técnicas e organizacionais que sejam apropriadas e estejam em conformidade com a natureza dos dados processados em relação com as solicitações que tenham como finalidade exercer os direitos dos interessados e, especificamente, seus direitos de acesso, retificação, eliminação (“direito ao esquecimento”), objeção ao processamento de seus dados, pedido de portabilidade de seus dados pessoais, limitação ao tratamento, bem como o direito de não ser submetido a uma decisão individual automatizada, incluindo a elaboração de perfis.

Caso as pessoas afetadas exerçam os direitos mencionados na seção acima perante o Processador de dados, deve comunicar através do e-mail protecciondedatos@prosegur.com. O comunicado deverá ser realizado em caráter imediato não devendo exceder, em caso algum, o dia útil após o recebimento da solicitação, juntamente, se for o caso, com qualquer outra informação que possa ser relevante para solucionar a solicitação.

Décima - Devolução ou destruição dos dados

Uma vez cumprida a prestação contratual, o Processador compromete-se a devolver à Prosegur os dados pessoais e, se for o caso, os meios de comunicação onde estão incluídos, uma vez que o serviço tenha sido cumprido. A devolução deve incluir a exclusão total dos dados existentes nos equipamentos computadorizados utilizados pelo Encarregado do tratamento de dados.

Do mesmo modo, o Encarregado do tratamento de dados deverá garantir que, ao finalizar a relação contratual com qualquer pessoa com a qual desempenhe uma função profissional:

- a pessoa devolva e não conserve, de forma alguma as informações e meios da PROSEGUR.
- o mencionado no parágrafo anterior deve ser confirmado por escrito ou por qualquer meio similar permitido no escopo legal vigente.
- o cancelamento imediato das autorizações para os processos de informação.

Não obstante o anterior, o Processador de dados pode manter uma cópia, com os dados devidamente bloqueados, durante o tempo em que houver responsabilidades decorrentes da execução dos serviços.

Décima primeira – Auditoria

A PROSEGUR poderá realizar por sua conta, em cumprimento da sua capacidade de controle, revisões para verificar que as políticas e medidas de segurança exigidas no presente acordo são cumpridas, para proteger as informações e os dados pessoais. As revisões poderão estar nos sistemas de informação e em instalações de tratamento de dados do Encarregado do tratamento de dados ou por meio da coleta de informações que confirmem o cumprimento pelo Encarregado do tratamento de dados.

O Encarre gado do tratamento de dados deverá manter à disposição da PROSEGUR a documentação (em mídia física ou eletrônica) que certifique que suas obrigações são cumpridas em conformidade com o acordo.

O Encarregado do tratamento de dados deverá comprovar, do mesmo modo, que realizou a análise de riscos correspondente e, se for indicado pela PROSEGUR, as avaliações do impacto exercido na proteção dos dados pertinentes.

Para poder facilitar ou inclusive evitar a revisão pela PROSEGUR, o Encarregado do tratamento de dados poderá fornecer as certificações apropriadas e cujos âmbitos de aplicação incluam serviços e pessoal colocados à disposição da PROSEGUR. Se o Encarregado do tratamento de dados decidir proporcionar as certificações mencionadas, também deverá fornecer a documentação pertinente, os certificados, o âmbito de aplicação e apresentar os relatórios das auditorias às quais estiver submetida de acordo com a certificação. Se a PROSEGUR encontrar não cumprimentos da segurança, que estejam em incompatibilidade com a prestação de serviços de acordo com a análise de riscos realizada, dependendo da sua gravidade, poderá exigir ao Encarregado do tratamento de dados que os problemas detectados sejam resolvidos imediatamente por meio da elaboração de um plano de ações corretivas detalhado.

O acima exposto não impede a possibilidade de realizar qualquer outra auditoria ou revisão para verificar outras obrigações contidas neste acordo.

Décima segunda- Dever de diligência

O Processador se compromete a facilitar ao Responsável do processamento de dados todas aquelas informações necessárias para demonstrar o cumprimento de suas obrigações, e informará o Responsável do processamento de dados sobre sua adesão a um código de conduta aprovado ou sua filiação a qualquer meio de certificação que possa garantir o cumprimento de suas obrigações em relação ao processamento de dados pessoais.

As pessoas que desempenham funções profissionais para o Encarregado do tratamento de dados devem estar cientes da importância das informações da PROSEGUR, tratá-las com segurança e estar devidamente treinadas e qualificadas em cada fase do processo de informação para todas aquelas funções que desempenharem. Deverão também observar toda a diligência possível e as medidas adequadas para proteger o processo de informação em cumprimento do seu dever de fidedignidade à qual estão obrigadas por contrato.

Décima terceira - Dever de Informação

Os dados pessoais dos contatos do Encarregado do tratamento de dados serão tratados, por sua vez, pela PROSEGUR, com sede social no endereço Calle Pajaritos, 24, Madri, na qualidade de Responsável pelo tratamento de dados, a fim de administrar a relação que mantém com o primeiro em sua condição de prestador de serviços e com base na execução da prestação de serviços, podendo o primeiro exercer seus direitos de acesso, retificação, eliminação, objeção, limitação do tratamento, portabilidade, e de não ser objeto de decisões individualizadas automatizadas, enviando um e-mail ao endereço protecciondedatos@prosegur.com, e anexando cópia do seu documento de identidade ou outro equivalente. O interessado também terá direito de apresentar uma reclamação relacionada com a proteção de dados perante a Agência Espanhola de Proteção de Dados. A Prosegur tratará esses dados enquanto a relação contratual perdurar, após o qual serão bloqueados durante os prazos prescritos das ações legais aplicáveis.

Décima Quarta – Inteligência Artificial

Caso a prestação de serviços envolva o uso soluções de Inteligência Artificial pelo Gerente de processamento, este garantirá que a solução de Inteligência Artificial cumpra os princípios e requisitos descritos no **APÊNDICE II** do presente Contrato.

Da mesma forma, o Gerente de processamento garante o cumprimento dos requisitos exigidos pela normativa vigente pertinente ao caso concreto.

A este respeito, o Gerente de processamento implementará as medidas necessárias para garantir e demonstrar o cumprimento das obrigações estabelecidas no parágrafo anterior.

A PROSEGUR poderá realizar por sua conta, em cumprimento da sua capacidade de controle, revisões para verificar que as políticas e medidas de segurança exigidas no presente contrato para a implementação de soluções de Inteligência Artificial sejam cumpridas. O Gerente de processamento compromete-se a participar do processo de avaliação e a implantar as medidas solicitadas pelo PROSEGUR para o cumprimento de sua Política de Inteligência Artificial Responsável.

Décima quinta - Indenidade

O Processador de dados se compromete a isentar a Prosegur de qualquer reclamação que possa ser movida contra a Prosegur com a Autoridade de Controle correspondente, que seja causada pela violação do Processador de dados e/ou de seus subcontratados das disposições deste acordo e da legislação atual sobre o assunto de proteção de dados pessoais, e compromete-se a pagar o valor a que a Prosegur possa ser condenada a título de multa, indenização, danos e juros, incluindo honorários advocatícios, em virtude da referida violação.

Décima sexta - Jurisdição

Este acordo será regido e interpretado em conformidade com as leis da Espanha, renunciando a qualquer outra jurisdição que possa corresponder, e se submetem à jurisdição exclusiva dos Tribunais e Cortes da cidade de Madri.

APÊNDICE I. MEDIDAS DE SEGURANÇA

Em conformidade com os artigos 28 e 29 do RGPD, esta seção se refere às medidas de segurança que o Processador de dados deve tomar para garantir o nível de segurança adequado ao risco.

O Processador deve implementar as medidas técnicas e organizacionais de segurança a seguir, visando que a segurança adequada dos dados pessoais seja garantida, incluindo a proteção contra seu processamento não autorizado ou ilícito, e contra a perda, destruição ou danos.

1. Medidas organizacionais

O Processador será obrigado a cumprir as medidas relacionadas ao pessoal ao qual dará acesso aos dados pessoais:

I. Medidas organizacionais genéricas

1. O Processador deverá garantir a existência e publicação de uma política de Segurança da Informação e de Proteção de Dados, para assegurar que o Processador implementou as medidas necessárias para garantir um nível de segurança adequado ao risco, e a proteção dos dados pessoais seja realizada de acordo com a legislação em vigor aplicável.
2. O Processador deverá garantir a existência de uma estrutura (departamento/cargo) responsável pela segurança da informação e da proteção dos dados pessoais (dados internos e externos de outros clientes).
3. Realizar um inventário dos recursos de TI (servidores, computadores, aplicativos de software, backups) contendo dados pessoais.

II. Adesão e conformidade com as Políticas Corporativas da PROSEGUR

1. O Processador de dados 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), à versão mais recente dos mesmos A este respeito, serão aplicáveis as disposições dos mencionados documentos e todas as medidas de segurança definidas ou referidas nos mesmos.

III. Medidas genéricas de pessoal

1. O Processador deve elaborar e aplicar uma Política de Segurança da Informação em conformidade com as melhores práticas de segurança e que inclua as obrigações referentes ao pessoal.
2. O Processador deve garantir que o pessoal designado para o serviço tenhahabilidades e competências adequadas para desempenhar suas funções.
3. O Processador deverá garantir a elaboração de um programa de treinamento e conscientização para fornecedores, terceiros e funcionários da organização que processam dados pessoais. Todos os usuários que acessam dados pessoais devem ter feito um curso de treinamento adequado às funções a realizar.
4. Os contratos de trabalho devem incluir cláusulas específicas de adesão às políticas de segurança e privacidade da organização, e devem ser assinados pelos funcionários recém-admitidos antes que estes recebam direitos de acesso a ativos, recursos ou instalações para o processamento de dados pessoais.

IV. Dever de sigilo e confidencialidade

1. A fim de impedir o acesso a dados pessoais por pessoaL não autorizado, o Processador deve garantir a adoção de medidas para evitar que os dados pessoais sejam expostos a terceiros (telas eletrônicas não assistidas, documentos impressos deixados em áreas de acesso público, mídia contendo dados pessoais, etc.) Isso inclui as telas utilizadas para ver as imagens do sistema de vigilância por vídeo, se houver. Os funcionários terão de bloquear a tela ou finalizar a sessão ativa toda vez que deixarem a sua sala ou estação de trabalho.
2. O Processador deve assegurar que os documentos impressos e as mídias eletrônicas sejam armazenados em local seguro (arquivos ou estantes de acesso restrito), 24 horas por dia, e sob custódia, quando estiverem fora dos seus dispositivos de armazenamento ou salas de arquivo correspondentes.
3. Os documentos impressos (papel) ou eletrônicos (CD, pen drive, disco rígido, etc.) que contenham dados pessoais não poderão ser descartados, exceto se for possível assegurar a sua destruição para que a informação neles contidos seja irrecuperável.
4. Os dados pessoais, ou qualquer outro tipo de informação pessoal, não poderão ser revelados a terceiros, com cuidado especial para não revelar dados pessoais protegidos em conversas telefônicas, e-mails, etc.
5. O dever de sigilo confidencialidade persiste inclusive após a finalização da relação laboral ou da prestação de serviços.

V. Direitos dos interessados

1. O Processador deve dispor de um protocolo de ação para atender os interessados que exercerem seus direitos, a fim de assegurar uma resposta rápida e eficaz no exercício dos mesmos.
2. O Processador deve tratar os pedidos para exercer os direitos de proteção de dados, incluindo, mas não limitando, acesso, retificação e apagamento.
3. O Processador deve informar o Responsável do Processamento de tais pedidos e ajudar o Responsável do Processamento a solucioná-los.

VI. Violação da segurança de dados pessoais

1. O Processador deve dispor de um procedimento para gerenciar e notificar eventos (ocorrências, vulnerabilidades, problemas, etc), em função do qual os eventos devem ser gerenciados de forma adequada e comunicados ao Responsável pelo Processamento.
2. Em caso de violação dos dados pessoais, como roubo ou acesso não autorizado aos dados pessoais, o Responsável pelo Processamento dos dados será imediatamente informado da violação, incluindo todas as informações necessárias para esclarecer os fatos e acontecimentos que possam ter levado ao acesso não autorizado aos dados pessoais. Da mesma forma, se prestará ajuda ao Responsável pelo Tratamento para que notifique à Autoridade de Controle e, conforme o caso, aos interessados afetados, sobre a violação dos dados pessoais, levando em consideração a informação disponível do Processador de dados.
3. O Processador deve manter um registro de todas as tarefas de manutenção e/ou suporte dos sistemas do Responsável pelo Processamento.

2. Medidas Técnicas.

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

1. As instalações deverão contar com medidas de segurança perimetral (muros, cercas, portas de acesso, barreiras, vigilância por vídeo, mecanismos de autenticação de acesso às instalações, recepção para visitantes, etc.) para proteger os sistemas de informação e os dados pessoais contra-acesso físico ou manuseio não autorizados.
2. Os acessos às salas e escritórios onde os dados pessoais são processados deverão contar com medidas técnicas e organizacionais de proteção contra-acesso não autorizado (controle de acesso eletrônico, vigilância por vídeo, janelas equipadas com sistemas de detecção de quebras/modificações, processos de pedido de acesso a salas ou escritórios, identificação pessoal, sistema de alarmes de detecção de intrusões).
3. Deverá ser autorizada com antecedência a retirada das instalações de dispositivos de suporte de armazenamento (discos rígidos, dispositivos extraíveis, fitas de cópia de segurança) que contenham dados pessoais.
4. As entradas e saídas das áreas de segurança das instalações deverão ser restringidas e estar supervisionadas por meio de mecanismos de controle de acesso e vigilância por vídeo para garantir que somente pessoas autorizadas possam acessar essas áreas.
5. O Processador deverá garantir a implementação das medidas técnicas e organizacionais para proteger os dados contra ameaças imediatas, tais como vazamentos de água, incêndios no centro de tratamento de dados, pane elétrica, vandalismo, etc.

II. Medidas relativas ao controle de acesso lógico

1. O Processador deverá definir, documentar e estabelecer um processo padronizado de gerenciamento de contas para o acesso aos sistemas de informação que tratam dados pessoais [solicitações de autorização, criação, edição e exclusão].
2. Somente será possível conceder acesso a dados pessoais ou aos sistemas de processamento de dados pessoais a usuários que contem com as autorizações correspondentes (de acordo com o processo predefinido).
3. O Processador deve documentar e implementar um processo para garantir que as contas de acesso ao sistema são modificadas corretamente após mudanças organizacionais (por exemplo, mudanças de funções, licenças, demissões, etc.).
4. O Processador deve garantir que cada conta de usuário tenha um ID único e inequívoco.
5. As modificações realizadas nas contas dos usuários devem ser rastreáveis (criação, edição, cancelamento) e deve ser mantido um registro dessas modificações (por exemplo, em documentos ou registros em sistemas de informação).
6. O Processador deverá garantir a revogação das autorizações dos usuários, imediatamente após a finalização da relação contratual (incluindo subcontratação).
7. As contas de acesso privilegiado para os sistemas de processamento de dados pessoais devem ser restringidas exclusivamente ao pessoal autorizado e ter um número limitado.
8. As contas privilegiadas devem ser concedidas apenas a pessoal tecnicamente qualificado que tenha participado previamente de um curso de treinamento e conscientização específico para o gerenciamento e utilização de contas privilegiadas.

9. Os usuários que precisam realizar atividades privilegiadas com dados pessoais devem ter duas contas no sistema: uma conta padrão para realizar tarefas e operações de rotina, e uma conta privilegiada para realizar tarefas que exijam permissões privilegiadas.
10. As senhas padrão das contas de usuários devem cumprir, pelo menos, os seguintes requisitos de complexidade e segurança:
    - Devem ser armazenados criptografados nos sistemas de informação.
    - As senhas não devem ser exibidas durante o processo de inserção da senha pelo usuário.
    - A senha deve ser alterada obrigatoriamente depois da inserção inicial de acesso ao sistema.
    - A senha deve ter no máximo noventa (90) dias de validade. Após o prazo máximo de validade,o sistema deverá forçar a alteração obrigatória da senha.
    - A senha deve ter no mínimo oito (8) caracteres de comprimento (incluindo 2 números ou caracteres especiais).
    - O histórico de senhas deve ser de, no mínimo, três (3).
    - O número de tentativas com falhas consecutivas ao inserir a senha antes de a conta ser bloqueada deve ser de, no máximo, três (3).
    - Caso a senha tenha sido inserida de modo errado repetidamente, a conta permanecerá bloqueada, no mínimo, por 15 minutos.
    - Deve-se evitar inserir senhas simples ou fáceis de serem adivinhadas.
11. O controle do acesso aos dados e aos sistemas de informação que processam dados pessoais deve estar baseado em um conceito de funções e autorizações formalmente documentados.
12. A atribuição das autorizações/funções deve ser válida por tempo limitado e realizada levando em consideração os princípios de segregação de funções (SoD) e princípio do privilégio mínimo.
13. As funções e autorizações concedidas aos sistema de informação utilizados para o processamento de dados pessoais devem estar registradas.
14. As autorizações concedidas devem ser revisadas periodicamente (pelo menos, uma vez por ano), para garantir seu cumprimento e validade.
15. Deve existir uma política clara de controle e publicidade periódica entre os funcionários, que deverá fazer parte das atividades de conscientização e sensibilização realizadas pela organização.
16. Os computadores e postos de trabalho do Processador de dados com acesso aos sistemas de informação que processam dados pessoais, devem contar com um protetor de tela protegido por senha que seja ativado automaticamente após um período de inatividade de, no máximo, quinze (15) minutos.
17. Os funcionários e terceiros que utilizam computadores e postos de trabalho do Processador de dados devem estar obrigados a bloquear sua tela quando deixam seu escritório ou posto de trabalho.

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

1. Todas as transferências eletrônicas de dados pessoais devem ser feitas de forma criptografada, quando necessário.
2. Os dados pessoais processados automaticamente devem ser armazenados de forma criptografada, quando necessário.
3. Deve ser formalizado e conservado um registro de transmissões de dados pessoais através de um meio físico [por exemplo, memórias removíveis, fitas de backup, CDs, discos rígidos, etc.].
4. A administração remota de sistemas de informação que processam dados pessoais deve ser realizada por meio de um canal de comunicação seguro (SSH, IPSec, TLS /SSL, VPN, etc.).
5. O Processador incorporará medidas técnicas nos sistemas de informação para evitar a possibilidade de que dados pessoais possam ser exportados de modo não autorizado (por exemplo, restrição das característica funcionais para download, imprimir e armazenar dados nos sistemas de informação que processam dados pessoais).
6. A mídia física utilizada para a transmissão dos dados pessoais deverá estar criptografada.
7. Antes de eliminar as mídias de computação (USB, discos rígidos, etc.) que processam dados pessoais sensíveis, os mesmos deverão ser apagados com segurança (o que faz os dados serem irrecuperáveis).

IV. Controle de gerenciamento de incidentes de segurança

1. Os computadores e periféricos (por exemplo, plataformas de e-mail, sistemas de acesso à Internet) contarão com um aplicativo para detectar e se proteger de software mal-intencionado (por exemplo, vírus, cavalos de Troia, etc.), o qual deverá ser atualizado periodicamente.
2. O Processador deve contar com um procedimento de gerenciamento de eventos de segurança que estabeleça os critérios para classificar, priorizar e escalonar os incidentes de segurança.
3. O Processador de dados deve avaliar regularmente a disponibilidade de atualizações de segurança para os sistemas de TI e seus componentes (incluindo clientes, componentes de rede, servidores, etc.) que processam dados pessoais. As atualizações de segurança são realizadas periodicamente por meio de um procedimento formal.
4. Os sistemas de informação que processam dados pessoais devem ser analisados regularmente para detectar vulnerabilidades conhecidas. As vulnerabilidades detectadas devem ser classificadas com base na sua criticidade e impacto na segurança, e consequentemente, corrigidas.
5. O Processador deve contar com uma equipe de resposta a eventos para responder a incidentes de segurança e contribuir para coordenar a resolução dos incidentes de segurança.

V. Controle de resiliência operacional

1. O Processador deve definir, documentar e implementar planos de continuidade de TI que abranjam sistemas e componentes críticos de TI.

2. O Processador deve possuir ferramenta de detecção e prevenção de invasões e ataques cibernéticos (por exemplo, firewalls, IPS, IDS, ferramentas para detectar e prevenir ataques direcionados, etc.).

3. O Processador deve possuir ferramentas ou serviço para detectar e limitar o impacto dos ataques de denegação do serviço (por exemplo, DoS, DDoS, etc.).

4. O Processador de dados deve realizar, regularmente, simulações de ataques aos computadores (por exemplo, teste de invasão/penetração). Os desvios detectados devem ser avaliados e corrigidos periodicamente de acordo com um procedimento predefinido.

5. Os componentes e os dispositivos que processam dados pessoais devem estar protegidos pela implementação de medidas técnicas e organizacionais correspondentes contra desastres causados por elementos naturais (por exemplo, incêndio, enchentes, furacões, etc).

6. As redes de telecomunicações do Processador, devem estar segmentadas por meio da implementação de firewalls para poder limitar o seu impacto em caso de incidente de segurança.

7. Existe uma política de backup para os dados processados por sistemas de computador. A política deve estabelecer o alcance dos sistemas de TI, a frequência das backups de segurança, o período de armazenamento, a localização física das cópias e as medidas de segurança para salvaguardar a confidencialidade e integridade (por exemplo, criptografia). A política também deve levar em consideração requisitos regulatórios e jurídicos.

8. Devem ser realizadas cópias periódicas de segurança dos sistemas computadorizados (incluindo os dados de configuração do sistema) que processam dados pessoais de acordo com a política estabelecida.

VI. Controle de desenvolvimento e operações de aplicativos de TI

1. O Processador de dados deve incluir a segurança como um elemento integrado em seu ciclo de vida de desenvolvimento de software, adotando normas internacionalmente reconhecidas para desenvolver aplicativos seguros. O Processador deve identificar e implementar os requisitos de segurança e jurídicos durante as primeiras etapas de desenvolvimento.

2. Deve ser mantido um registro para usuários e administradores na medida em que as atividades estejam relativas ao acesso ao aplicativo (login, logout, tentativas bem-sucedidas/falhas, etc.). O registro permite a identificação de, pelo menos, quem realizou a ação, quando ela foi realizada e o tipo de atividade realizada (por exemplo, login, tentativa de acesso, etc.).

3. Os dados de registro devem ser armazenados com segurança e o acesso aos mesmos deve ser restrito ao pessoal autorizado. Os registros que devem ser armazenados levando em consideração seu conteúdo e/ou os requisitos jurídicos devem ser excluídos depois que sua finalidade tiver sido cumprida.

4. O Processador realizará testes (estáticos/dinâmicos) no código-fonte que ele ou um terceiro estiver desenvolvendo, antes de implantá-lo no ambiente de produção.

5. Os ambientes que não forem de produção (por exemplo, desenvolvimento, testes, consolidação) devem estar totalmente separados do ambiente de produção.

VII. Controle de garantia e cumprimento

1. O Processador de dados deverá regularmente realizar revisões de segurança dos sistemas de TI que processam dados pessoais, a fim de garantir a conformidade e eficácia dos controles técnicos, organizacionais e jurídicos estabelecidos. É obrigatório manter um registro dos testes (e seus resultados). Os desvios são avaliados, priorizados e corrigidos.
2. Realizar simulações e testes regulares dos planos de continuidade do serviço de TI estabelecidos (pelo menos uma vez por ano). É obrigatório manter um registro dos testes (e seus resultados). Os desvios serão avaliados, priorizados e corrigidos.
3. O Processador de dados deverá realizar revisões de segurança regularmente (pelo menos uma vez por ano) dos controles de segurança física e ambiental em vigor para garantir sua eficácia. É obrigatório manter um registro dos testes (e seus resultados). Os desvios são avaliados, priorizados e corrigidos.
4. O Processador de dados deve regularmente realizar testes de backups e dos procedimentos de restauração definidos, para garantir a integridade e a disponibilidade das cópias. É obrigatório manter um registro dos testes (e seus resultados). Os desvios devem ser avaliados, priorizados e corrigidos.
5. O Processador de dados deve revisar regular e independentemente seus processos de gerenciamento de segurança da informação. O escopo das revisões deve incluir, no mínimo, controles que possam afetar a segurança dos dados pessoais do processador de dados.
6. O Processador deve contar com processos, procedimentos operacionais e instruções para garantir o cumprimento dos requisitos legais e regulatórios e dos regulamentos aplicáveis à natureza do serviço.

APÊNDICE II - INTELIGÊNCIA ARTIFICIAL RESPONSÁVEL

A solução de Inteligência Artificial proposta pelo FORNECEDOR deve seguir estes princípios:

Respeito à autonomia humana

O respeito pela liberdade e autonomia do ser humano deve ser garantido. O sistema de IA proposto deve ter sido projetado de forma que as habilidades cognitivas, sociais e culturais dos indivíduos sejam favorecidas; é obrigatório garantir supervisão humana e controle sobre os processos de trabalho do sistema de IA proposto.

Princípio de Prevenção de Danos

É obrigatório garantir que o sistema de IA não cause danos nem prejudique seres humanos de qualquer outra forma, protegendo a dignidade humana, bem como a integridade física e mental.

O sistema e o ambiente de IA sejam seguros e robustos do ponto de vista técnico e, em nenhum caso, serão usados com más intenções.

Da mesma forma, é obrigatório prestar atenção especial aos possíveis efeitos adversos que possam ser causados por um sistema de IA, estabelecendo medidas específicas para sua mitigação, a fim de evitar possíveis danos.

Princípio de equidade

É obrigatório garantir que o desenvolvimento, implantação e uso do sistema de IA seja equitativo, comprometendo-se a assegurar uma distribuição justa e igualitária dos custos e benefícios, e que indivíduos e grupos estejam livres de injustiças, preconceitos, discriminação e estigmatização.

O FORNECEDOR tentará evitar a ocorrência de preconceitos e injustiças, podendo estabelecer medidas específicas para aumentar a equidade social por meio do uso de sistemas de IA.

Da mesma forma, o uso do sistema de IA proposto respeitará o princípio da equidade, entendido como a capacidade de oferecer a possibilidade de se opor às decisões adotadas pelo sistema de IA, bem como demonstrar oposição às pessoas que os administram, e proporcionalidade entre meios e fins, para o qual estudará cuidadosamente como alcançar um equilíbrio entre os diferentes interesses e objetivos conflitantes.

Princípio da explicabilidade

É preciso haja clareza em relação ao sistema de IA proposto. Para isso, todos os processos que envolvem um desenvolvimento de IA devem ser transparentes, devem comunicar às partes envolvidas de forma clara e concisa os recursos e as finalidades do sistema de IA.

Requisitos para soluções de IA Responsável

Seguem abaixo os principais requisitos que a solução do sistema de IA deve cumprir para ser uma IA Responsável, que devem ser continuamente avaliados e abordados ao longo do ciclo de vida dos sistemas de IA:

Ação e supervisão humana

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

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

Solidez técnica e segurança

A solidez técnica requer que o sistema de IA seja desenvolvido com uma abordagem preventiva em relação aos riscos, para que sempre se comportem da forma esperada e minimizem danos involuntários e imprevistos, evitando também causar danos inaceitáveis, e devem garantir a integridade física e mental dos seres humanos.

Nesse sentido, o FORNECEDOR observará que o sistema de IA seja robusto e cumpra as devidas medidas de segurança que garantam a confidencialidade, integridade e disponibilidade das informações neles armazenadas e processadas.

Para isso, deverão ser realizados testes e avaliações de segurança rigorosos para garantir que o sistema de IA responda adequadamente a incidentes de segurança que possam causar a destruição, perda, alteração acidental ou ilícita, ou comunicação ou acesso não autorizado a tais informações.

Gerenciamento da privacidade e dos dados

O sistema de IA observará a prevenção de danos à privacidade, o que significar gerenciar adequadamente os dados, que engloba sua qualidade e integridade. Consequentemente, o sistema de IA, seu protocolo de acesso e sua capacidade de processar dados devem ser desenvolvidos sem violar a privacidade.

Caso a solução de inteligência artificial entregue pelo FORNECEDOR processe dados pessoais, o FORNECEDOR, como responsável pelo sistema de IA, implementará medidas adequadas de segurança de natureza legal, organizacional e técnica, de modo a garantir a proteção de liberdades e direitos fundamentais das partes interessadas que possam ser afetadas, cumprindo rigorosamente o Regulamento Geral de Proteção de Dados, REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 (doravante, o RGPD) e as normas locais pertinentes. Da mesma forma, garante que somente os dados estritamente necessários para cada uma das finalidades pretendidas sejam objeto de processamento, limitando também a sua conservação ao período estabelecido.

Transparência

Para que um sistema de IA seja transparente, ele deve ser (i) rastreável: que as decisões do sistema de IA sejam registradas para poder identificar os motivos de uma decisão incorreta do sistema, o que ajuda a evitar erros futuros, (ii) explicável: que as decisões adotadas por um sistema de IA sejam compreensíveis para os seres humanos e que tenham a possibilidade de rastreá-las e (ii) comunicáveis: que as pessoas saibam que estão interagindo com um sistema de IA; o sistema de IA deve ser identificado como tal e, quando necessário, deve ser oferecida ao usuário a opção de decidir se prefere interagir com um sistema de IA ou com outro ser humano, de forma a garantir o cumprimento dos direitos fundamentais.

Diversidade, não discriminação e equidade

Para que um sistema de IA Responsável seja confiável, ele deve garantir inclusão, diversidade, igualdade de acesso, por meio de processos de design exclusivos, bem como tratamento igualitário ao longo do seu ciclo de vida.

Além disso, no desenvolvimento interno e/ou na aquisição de soluções de IA, o FORNECEDOR garantirá, em todos os casos, a igualdade e não discriminação das pessoas que possam ser afetadas na sua utilização, especialmente por motivos de raça, cor, origens étnicas ou sociais, sexo, orientação sexual, idade, características genéticas, idioma, religião ou convicções, opinião política ou qualquer outra.

Bem-estar ambiental e social

O FORNECEDOR promoverá a sustentabilidade e a responsabilidade ecológica por meio de sistemas de IA e promoverá a pesquisa de soluções de Inteligência Artificial para abordar questões como o Desenvolvimento Sustentável.

Prestação de contas

O FORNECEDOR implementará mecanismos para garantir a responsabilidade e prestação de contas pelo sistema de IA e seus resultados, tanto antes quanto depois da implementação.

Nesse sentido, o FORNECEDOR será responsável pelas ações e decisões adotadas por um sistema de IA, especialmente à medida que avança para sistemas mais autônomos capazes de tomar decisões automatizadas e, principalmente, quando essas decisões produzirem efeitos jurídicos sobre o interessado.

7.5. ANEXO IV: Requerimentos de Risco Tecnológico e Segurança Digital

7.5.1. Requisitos de Risco Tecnológico e Cibersegurança

7.5.1.1 Considerações preliminares

O tratamento de informações e dados pessoais é expressamente autorizado pelo Grupo Prosegur, nas dependências do Prestador para fins contidos no contrato de referência a este anexo. Da mesma forma, a divulgação de mídias e documentos contendo informações do Grupo Prosegur é explicitamente autorizada, se for o caso, para a prestação dos serviços contratados. Para o transporte de mídias e documentos, o Prestador aplicará, em qualquer caso, as medidas de segurança estabelecidas de acordo com este documento ou com as normas vigentes.

O Prestador utilizará os recursos de informações e/ou dados de propriedade do Grupo Prosegur no âmbito do desenvolvimento da prestação de serviços contratados e com a finalidade previamente estabelecida.

7.5.1.1.1 Obrigação de guardar reserva

Todos os funcionários do Prestador que, por ocasião da prestação do Serviço, ou por qualquer outra circunstância, tenham conhecimento das informações relacionadas ao GRUPO PROSEGUR terão a obrigação de manter o assunto em sigilo, não podendo comunicá-lo a terceiros a qualquer momento, seja antes, durante ou após a prestação do Serviço.

O Prestador e seus funcionários só poderão utilizar as informações com a finalidade prevista no objeto deste Contrato, respondendo ao Grupo PROSEGUR por quaisquer danos e prejuízos que possam ser causados ao GRUPO PROSEGUR decorrentes de seu não cumprimento.

Caso o Prestador, por sua vez, subcontrate um Prestador terceirizado, este último é responsável por respeitar e cumprir os mesmos critérios de confidencialidade e regras sobre informações relacionadas ao GRUPO PROSEGUR, descritas nas cláusulas anteriores.

O Prestador, bem como seus funcionários envolvidos na prestação de serviços ao GRUPO PROSEGUR, evitará qualquer tipo de ação ou omissão que possa resultar na divulgação não autorizada ou no uso indevido dos Ativos de Informação relacionados à realização do serviço.

7.5.1.1.2 Confidencialidade das informações

O Prestador deve, em geral, tratar as informações do Grupo Prosegur como confidenciais e tomar as medidas cabíveis para tal classificação.

O tratamento das informações deve permitir a rastreabilidade, definida como a capacidade de saber quando e quais pessoas acessaram e trataram as informações do GRUPO PROSEGUR. Será entendido como tratamento qualquer operação realizada com as informações, tais como, mas não exclusivamente, sua leitura, escrita, modificação, cópia, transmissão, gravação ou arquivamento por meios manuais ou uso de aplicações informáticas.

7.5.1.2 Conformidade com a legislação

O Prestador deve obedecer a todas as leis vigentes que o afetam em seu escopo de atuação, como questões de segurança e privacidade da informação, assim como às regulamentações associadas ao setor no qual o Cliente oferece seus serviços, requisitos regulamentares, judiciários e estatutários.

7.5.1.2.1 Proteção de dados pessoais

O Prestador é obrigado a cumprir rigorosamente com o estipulado pela legislação vigente relativa aos dados pessoais tratados durantes a prestação dos Serviços abrangidos por este Contrato.

O Prestador deve tratar os Dados com absoluta confidencialidade e de acordo com as instruções recebidas do GRUPO PROSEGUR em relação à finalidade, conteúdo e tratamento, aplicando a privacidade padrão desde o início, as medidas técnicas e organizacionais adequadas, e em particular, o que está indicado nos acordos de privacidade e contratos de ordem de tratamento assinados.

O Prestador deve realizar análises dos riscos regulamentares e de segurança que afetam os dados pessoais e realizar avaliações do impacto da proteção de dados nos tratamentos que requerem conformidade com o determinado pela legislação acerca do escopo de atuação correspondente.

7.5.1.3 Quadro regulamentar de segurança da informação

O Prestador deve estabelecer um quadro regulamentar de segurança nas tecnologias da informação que garanta a implementação adequada 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 Prestador deve atualizar este quadro regulamentar de maneira apropriada, de acordo com as modificações do serviço e com as novas leis, regulamentos ou padrões de referência internacional e por países que possam surgir em termos de segurança tecnológica e proteção de informações e dados pessoais, como o Cybersecurity Framework do NIST, as normas ISO 27000 e 22300 e/ou outros de natureza semelhante.

Este quadro regulamentar deve conter, no mínimo, documentação relativa a:

- Gerenciamento de usuários
- Controle de acesso e gerenciamento de *logs* de atividade
- Gerenciamento de funcionários
- Treinamento e conscientização
- Gerenciamento de ocorrências
- Gerenciamento da continuidade do serviço
- Gerenciamento de operações
- Procedimentos de tratamento e destruição de informações

- Gerenciar as mudanças
- Desenvolvimento de software e novas aquisições de sistemas
- Política de senhas:
- Procedimentos de divulgação e armazenamento de informações
- Modelo de relatório e relacionamento com o GRUPO PROSEGUR

Cada um dos documentos indicados pode ser solicitado pelo GRUPO PROSEGUR para que possa comprovar e verificar se os requisitos e garantias essenciais definidos com o Prestador estão sendo cumpridos.

O Prestador deve garantir que os processos de atribuição, distribuição e armazenamento de senhas tenham sido formalizados por escrito, sem que haja exceções diferentes daquelas que podem ser incluídas nos procedimentos acima mencionados.

O Prestador deve comunicar aos seus colaboradores responsáveis pela prestação do serviço ao GRUPO PROSEGUR, o marco regulatório, registrando a aceitação de sua parte.

7.5.1.3.1 Gestão do risco

O Prestador compromete-se a realizar uma análise de risco que lhe permita determinar as medidas técnicas e organizacionais mais adequadas para garantir e demonstrar que o tratamento das informações é realizado de forma responsável, segura, respeitando as dimensões de segurança, bem como a privacidade e os direitos das partes interessadas. Essas medidas devem ter uma abordagem preventiva e não corretiva e devem ser revistas periodicamente para garantir que continuem atualizadas.

O Prestador deve realizar um processo de análise de risco que contemple especificamente os envolvidos no Serviço prestado ao GRUPO PROSEGUR de maneira periódica e quando houver mudanças significativas no ambiente tecnológico.

O Prestador deve ter um Plano de Tratamento de Riscos em vigor para tratar daqueles que são determinados nas análises como requerentes de tratamento. A efetividade das ações definidas para o tratamento dos riscos deve ser monitorada.

7.5.1.3.2 Esquema de controle

O Prestador compromete-se a cumprir com todas essas políticas, procedimentos e documentos de segurança específicos realizados pelo GRUPO PROSEGUR que sejam considerados aplicáveis às atividades que são realizadas e disponibilizadas ao Prestador assim que os serviços contratados começam a ser prestados.

Caso o Serviço trate informações sujeitas a certificações de segurança, o Prestador deverá apresentar as certificações correspondentes ao GRUPO PROSEGUR, a seu pedido.

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

O Prestador deve estabelecer os controles de segurança adequados a fim de reduzir o risco de acesso e modificação não autorizados às informações relevantes contidas nos sistemas (aplicativos, sistemas operacionais e bancos de dados) suportados pelo serviço e evitar a perda, roubo, indisponibilidade e tratamento não autorizado dos ativos de informação do GRUPO PROSEGUR.

Os requisitos de segurança determinados devem ser implementados pelo Prestador. Caso um terceiro seja subcontratado pelo Prestador, por sua vez, ele próprio é responsável por garantir que os requisitos de segurança sejam cumpridos também por este terceiro.

O GRUPO PROSEGUR reserva-se o direito de modificar a qualquer momento os requisitos de segurança contidos neste contrato e seus anexos, comunicando o Prestador e indicando as datas para sua entrada em vigor.

7.5.1.4 Organização da segurança

7.5.1.4.1 Identificação de responsabilidades

O Prestador deve dispor de Responsáveis pelo Risco Tecnológico e Segurança da Informação formalmente estabelecidos, a fim de garantir o cumprimento das políticas de segurança e monitoramento dos controles para garantir a integridade, confidencialidade, disponibilidade, autenticidade e rastreabilidade de dados e sistemas, bem como o cumprimento de todas as regulamentações aplicáveis, principalmente a relacionada à proteção de dados pessoais.

O Responsável pelo Risco Tecnológico e Segurança deve realizar o controle e a coordenação das medidas de segurança executadas pelo Prestador, especialmente aquelas destinadas à proteção no tratamento de dados pessoais objeto da prestação de serviços, e realizar revisões periódicas para verificar o cumprimento dos aspectos estabelecidos na Documentação de Segurança.

O Prestador deve nomear um Coordenador responsável pela gestão dos aspectos de segurança junto ao GRUPO PROSEGUR. Este Coordenador de Prestadores deverá auxiliar o Comitê de Coordenação composto pelo Prestador e pelo GRUPO PROSEGUR, caso seja convocado pelo GRUPO PROSEGUR, a fim de realizar um acompanhamento oportuno do serviço e definir os planos de ação necessários para garantir o desempenho correto dos serviços.

O Prestador deve determinar uma divisão adequada das funções, que estabeleça medidas suficientes e necessárias para garantir que os direitos de acesso (funções e perfis) para cada usuário do serviço sejam atribuídos de acordo com as necessidades funcionais de cada um, e que essas necessidades funcionais não coloquem em risco os ativos de informação que fazem parte do serviço contratado.

O Prestador deve comunicar a existência e as pessoas que atuam como Oficial de Segurança e do DPO (Data Privacy Officer) caso tenha a necessidade ou obrigação de contar com eles para estabelecer as comunicações apropriadas.

O Prestador deve comunicar, através dos canais estabelecidos com o GRUPO PROSEGUR, qualquer modificação que ocorra em relação à designação inicial do responsável pelo serviço, bem como deve comunicar, no prazo máximo de 24 horas, qualquer retirada de um usuário participante da prestação do serviço ao Grupo PROSEGUR.

7.5.1.4.2 Planos de treinamento/conscientização

O Prestador implementará planos de treinamento e conscientização na área de segurança da informação que incluam todos os funcionários que prestam serviço ao GRUPO PROSEGUR.

O Prestador deve desenvolver de forma clara um plano de conscientização sobre a importância da segurança das informações, dados pessoais e confidencialidade sobre eles.

O Prestador deve implementar de forma clara um plano de treinamento sobre a importância do desenvolvimento seguro do código.

7.5.1.4.3 Notificação

O Prestador deve notificar o GRUPO PROSEGUR de qualquer evento que saia do acordo contratual firmado com o GRUPO PROSEGUR no prazo máximo de 24 horas.

O Prestador deve notificar o GRUPO PROSEGUR de qualquer modificação ocorrida durante a prestação do serviço, seja na forma em como ele é prestado (modificação no processo) ou nos sistemas utilizados para a prestação do serviço (modificação na infraestrutura), bem como nos funcionários envolvido neles, com um prazo máximo de 24 horas.

7.5.1.5 Medidas tecnológicas

7.5.1.5.1 Classificação e gerenciamento de ativos

O Prestador deve ter um inventário de ativos de informação nos quais são identificados o tipo de informação contida em cada um deles, a propriedade do ativo, a custódia e o grau de sensibilidade das informações tratadas.

O Prestador 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 que eles suportam.

O Prestador deve manter e atualizar este inventário periodicamente, tendo em vista quaisquer alterações ocorridas nos ativos que fazem parte da prestação do serviço.

A identificação das mídias será realizada com um sistema de rotulagem compreensível apenas para usuários autorizados.

O Prestador deve criptografar os dados na distribuição de mídias e em dispositivos portáteis, evitando o tratamento em dispositivos portáteis que não permitem criptografia, adotando medidas que levem em conta os riscos em ambientes desprotegidos.

Garantir o armazenamento seguro dos meios de comunicação que contenham informações do GRUPO PROSEGUR em um local com acesso restrito aos funcionários autorizados.

O Prestador deve implementar mecanismos suficientes para garantir a custódia segura dos meios de comunicação com informações do GRUPO PROSEGUR, quando não estiverem armazenados em locais seguros.

O Prestador deve ter um Procedimento de Gerenciamento de Mídia no qual defina os métodos de custódia dos meios de comunicação e os responsáveis por autorizar o acesso a eles.

Garantir que qualquer tipo de recepção ou envio de mídia seja feito exclusivamente por funcionários autorizados, seja a destinatária uma empresa do GRUPO PROSEGUR ou uma empresa externa.

Quando a documentação contida em um arquivo for transferida, devem ser tomadas medidas para evitar o acesso ou manipulação das informações nela contidas.

O Prestador deve manter um registro de entrada e saída de mídias que permita o reconhecimento do tipo de mídia ou documento, data e a hora, remetente e/ou receptor, tipo de informação, a forma de envio e o responsável.

O Prestador deve tomar medidas para evitar o acesso indevido às informações em caso de eliminação de mídias.

7.5.1.5.2 Controle de acesso

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

O Prestador, ao conceder um nível de acesso às informações, aplicações e sistemas envolvidos neste serviço, deve fazê-lo por meio de um sistema de gerenciamento de identidade com base em papéis e funções que levam em conta o princípio do "menor privilégio", garantindo que apenas o nível mínimo de acesso necessário para um determinado cargo seja concedido aos seus funcionários envolvidos no serviço prestado ao GRUPO PROSEGUR.

O Prestador deve estabelecer medidas necessárias e suficientes para garantir a realização de revisões periódicas das permissões de acesso e controles de acesso configurados nos sistemas envolvidos no serviço.

7.5.1.5.2.1 Controlando o Acesso a Aplicações e Sistemas

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

O Prestador deve implementar os mecanismos necessários para identificar de maneira evidente seus usuários com acesso aos sistemas que fazem parte do serviço prestado ao GRUPO PROSEGUR. Os códigos de usuário e senhas não devem ser compartilhados entre pessoas. A todo momento, os códigos de usuário usados para acessar aplicativos devem permitir com que o Prestador identifique claramente a pessoa que os acessa.

O Prestador deve registrar os dados de cada tentativa de acesso, incluindo informações relativas ao usuário, data e hora, arquivo acessado, tipo de acesso e se foi autorizado ou negado. Caso tenha sido autorizado, o registro acessado será salvo.

O Prestador deve realizar uma verificação periódica do controle de acesso, indicando os dados de tentativas de acesso válidas ou não. Esses registros devem ser mantidos por um período mínimo de 2 anos para a busca de provas no caso de eventos de segurança.

O Responsável da Segurança do Prestador deve ter controle direto sobre o acesso aos mecanismos de controle dos registros de acesso.

O Prestador deve implementar os mecanismos necessários para permitir um registro atualizado dos usuários. O Prestador deve manter um registro atualizado para cada sistema ou aplicativo envolvido no serviço prestado ao GRUPO PROSEGUR. O registro deve indicar a associação de cada código de usuário com a pessoa atribuída a ele, seu perfil e os acessos autorizados.

O registro deve apontar todas as alterações no mapeamento: altas, baixas e possíveis modificações.

O Prestador deve garantir que tanto seus usuários ausentes envolvidos na prestação do serviço como as contas detectadas como inativas por mais de sessenta (60) dias devem ter suas contas de usuário desativadas. Essas contas de usuário podem ser reativadas se necessário, caso contrário, se a inatividade persistir ao longo do tempo, essas contas serão bloqueadas permanentemente.

O Prestador deve garantir que seus usuários envolvidos na prestação do serviço que tenham suas responsabilidades no trabalho modificadas devem ter seus níveis de acesso revisados para determinar se é necessário modificar o perfil atribuído, a fim de garantir que eles não tenham acesso a ativos de informação que não os dizem respeito.

O Prestador deve implementar os mecanismos necessários que permitam o tratamento imediato dos cancelamentos de usuários. O anulamento de usuário deve ser executado imediatamente usando as ferramentas de gerenciamento dos aplicativos, desativando o acesso a eles por meio do código de usuário cancelado. O cancelamento de um usuário resulta em seu bloqueio temporário antes de prosseguir para sua eliminação definitiva.

O Prestador deve implementar os mecanismos necessários para dispor de mecanismos de registro de atividade dos usuários.

O Prestador deve implementar os mecanismos necessários para restringir o acesso à Internet ou qualquer tipo de conexão que permita o vazamento de informações dos dados tratados.

O Prestador deve definir uma Política de Controle de Acesso/Senhas que estabeleça um quadro regulamentar para controle de acesso com base nos requisitos do serviço e da Segurança da Informação.

O Prestador deve implementar esses controles para garantir que todos os elementos com os quais fornecerá o Serviço sejam gerenciados e explorados com segurança. Esses controles devem estar disponíveis para o GRUPO PROSEGUR, se solicitado.

Os controles citados no ponto anterior devem incluir:

- Políticas de usuários/senhas dos operadores e administradores de sistemas ou produtos, incluindo especificamente administradores de bancos de dados.
- Acesso aos sistemas por meio de ferramentas que protegem a confidencialidade das senhas dos administradores, por exemplo, SSH no UNIX.
- Proteção dos sistemas de servidores contra acessos não autorizados.
- Em casos de acesso a informações confidenciais, o Serviço deve fornecer mecanismos de autenticação multifatorial.

O Prestador deve incluir em sua Política de Senhas pelo menos os seguintes aspectos:

- Um procedimento de distribuição de senhas que garante que a senha seja conhecida apenas pelo usuário.
- Um procedimento para controlar a expiração de senhas e o armazenamento ininteligível delas.
- Robustez adequada, de acordo com as seguintes regras, na medida do possível: a) mínimo de oito (8) caracteres de comprimento, b) ter maiúsculas, c) minúsculas, d) números e e) caracteres especiais (por exemplo. !, $, @)
- Expiração da senha (aconselhável 60 dias e não mais de 90), com um procedimento de alteração que não cause interrupção do serviço.
- Armazenamento criptografado obrigatório das senhas dos sistemas e aplicativos que fazem parte da terceirização.

O Prestador deve implementar os mecanismos necessários para conceder permissões de acesso aos sistemas que prestam serviço ao GRUPO PROSEGUR apenas aos funcionários autorizados no Documento de Segurança e nas listas de usuários de cada um dos sistemas.

O Prestador deve estabelecer um mecanismo que limite o número de tentativas repetidas de acesso não autorizado.

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

O Prestador deve garantir que os funcionários que precisam utilizar conexões remotas para a prestação do serviço cumpram as diretrizes das normas de Acesso Remoto do Grupo Prosegur que estão previstas para a prestação do serviço assim que as atividades correspondentes e contratadas começarem. Especificamente:

- Todo acesso remoto deve ser autorizado antecipadamente pelo Grupo Prosegur.
- As credenciais devem ser intransferíveis e possuir um identificador único associado a um usuário.
- No caso de um funcionário compartilhar suas credenciais ou sua sessão aberta com outros usuários:
    - Será considerado como um incidente de segurança.
    - O usuário será imediatamente removido dos sistemas do grupo Prosegur
    - O empregado, e portanto o Prestador, será diretamente responsável pelas ações (ou omissões) realizadas pelo usuário que o representa, podendo recair sobre as sanções estipuladas por uso indevido.

O Prestador deve estabelecer mecanismos para identificar os acessos feitos em documentos acessados por diversos usuários.

O Prestador deve estabelecer medidas necessárias e suficientes para garantir a realização de revisões periódicas das permissões de acesso e controles de acesso configurados nos sistemas envolvidos no Serviço.

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

O Prestador deve assegurar que as informações relacionadas ao Serviço prestado não sejam transmitidas a terceiros sem a autorização prévia do GRUPO PROSEGUR e no âmbito legal da lei.

7.5.1.5.2.2 Controlar o acesso às instalações e ao CPD

O Prestador deve garantir o controle do acesso às salas onde estão localizados os ativos envolvidos no serviço prestado ao GRUPO PROSEGUR, com as devidas salvaguardas administrativas, lógicas e físicas, inclusive, dependendo da criticidade dos sistemas, mas não só:

- Bloqueio das portas de acesso
- Destruição segura de ativos de informação em tempo hábil.
- Acesso aos escritórios e centros de processamento de dados do Prestador;
- Dispositivos de armazenamento seguro;
- Equipe de segurança física
- Áreas vigiadas por vídeo

O Prestador deve verificar se a entrada não autorizada é impedida, detectada e informada aos funcionários adequados do Prestador imediatamente. Todos os pontos de entrada e saída devem ser protegidos, registrados e monitorados para garantir que apenas os funcionários autorizados possam acessar os edifícios e áreas seguras do Prestador.

Caso o Prestador utilize cartões de identificação ou tokens similares para seus funcionários envolvidos no serviço prestado ao GRUPO PROSEGUR, é necessário realizar um processo documentado, juntamente com os procedimentos de suporte, para garantir que as credenciais e tokens perdidos sejam desativados imediatamente após a notificação da perda.

O Prestador deve dispor de procedimentos e mecanismos suficientes para garantir que, se um funcionário que faz parte do serviço prestado ao GRUPO PROSEGUR terminar seu vínculo empregatício com o prestador, as credenciais de identificação sejam imediatamente desativadas.

O Prestador deve garantir que todos os ativos de informação do GRUPO PROSEGUR que fazem parte do serviço terceirizado, na posse do Prestador, sejam fisicamente protegidos em uma área de acesso restrito, sala trancada, contêiner de armazenamento seguro ou arquivo.

O Prestador deve informar ao GRUPO PROSEGUR qualquer movimentação ou exclusão de qualquer sistema ou ativo de informação que não possa ser realizado sem o consentimento por escrito do GRUPO PROSEGUR.

7.5.1.5.2.3 Controles físicos e ambientais

O Provedor será responsável pela implementação de medidas de segurança física para a proteção dos sistemas de informação localizados em suas instalações contra acessos não autorizados e danos físicos.

Os controles físicos e ambientais devem incluir:

- Medidas de proteção contra incêndios
- Medidas de proteção contra inundações
- Controle do fornecimento de eletricidade
- Outros controles que sejam aplicáveis de acordo com a legislação e regulamentos.

O Prestador deve ter o controle necessário e suficiente para garantir que o acesso físico às instalações onde estão localizados os sistemas de informação que possuem informações relevantes. Além disso, o banco de dados pessoais deve ser mantido atualizado, com acesso autorizado e controlado de acordo com os requisitos estabelecidos pelo GRUPO PROSEGUR.

7.5.1.5.2.4 Autorização e autenticação

O Prestador deve implementar as medidas de segurança necessárias e suficientes para garantir que o acesso dos administradores aos sistemas de informação seja realizado usando canais criptografados e forte autenticação.

Caso o Serviço exija atender os clientes, o Prestador deve implementar as medidas de segurança necessárias e suficientes para garantir que a autenticação desses clientes seja realizada por meio de mecanismos de dois fatores, pelo menos para a execução de operações ou consulta de informações confidenciais.

O Prestador deve garantir o armazenamento criptografado das senhas nos sistemas de tratamento de informações.

O Prestador deve implementar os mecanismos necessários que permitam identificar visivelmente os acessos de cada um dos usuários, permitindo o acesso apenas aos dados e recursos necessários para o desenvolvimento de suas funções.

O Prestador deve implementar os mecanismos necessários para evitar que os usuários sejam administradores locais de seus cargos, abrindo exceção apenas se explicitamente exigido e validado pelo GRUPO PROSEGUR.

7.5.1.5.3 Criptografia

O Prestador deve usar algoritmos de criptografia padrão com um comprimento de chave baseado em práticas e padrões reconhecidos internacionalmente para proteger a confidencialidade e integridade dos dados confidenciais do GRUPO PROSEGUR.

O Prestador deve proteger as chaves de criptografia com mecanismos de segurança ao longo de seu ciclo de vida, desde sua geração, passando por seu armazenamento, distribuição, renovação, arquivamento e terminando em sua eliminação.

O Prestador providenciará ao Grupo Prosegur a documentação relacionada ao gerenciamento de chaves de criptografia para verificar se os requisitos mínimos de segurança para chaves criptográficas são atendidos. Caso seja necessário o acesso aos sistemas do Grupo Prosegur, as regras e procedimentos que o Prestador e seus funcionários precisam saber sobre a gestão e uso de chaves de criptográficas serão fornecidos no momento do início da atividade.

O Prestador deve garantir que os dispositivos que processam dados críticos ou confidenciais sejam criptografados. Especialmente os dispositivos que são removíveis ou móveis, como laptops ou dispositivos removíveis.

A perda de sigilo de qualquer chave criptográfica que afete os sistemas do Grupo Prosegur é um incidente de segurança, por isso deve ser comunicada sem demora para implementar os mecanismos adequados.

7.5.1.5.4 Segurança de perímetro e infraestrutura

O Prestador informará ao GRUPO PROSEGUR sobre a infraestrutura tecnológica implantada para a prestação de serviço, com o nível de detalhamento exigido pelo GRUPO PROSEGUR para que este realize a fiscalização/monitoramento estabelecida pelo GRUPO PROSEGUR.

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

O Prestador não deve conectar nem hardware nem software não pertencente aos GRUPO PROSEGUR à rede interna do GRUPO PROSEGUR sem:

- Uma avaliação de risco com o escopo necessário, incluindo a identificação de controles existentes e compensatórios com base nos requisitos deste anexo;
- A verificação da aplicação dos controles identificados na avaliação de risco;
- A aprovação por escrito do Responsável de Segurança do Cliente (CISO)

O Prestador deve proteger ou desativar portas de rede autônomas quando não estiverem em uso. Se os requisitos de negócios justificarem a necessidade de tê-los habilitados, as portas de rede podem permanecer ativas desde que a administração do Prestador tenha revisado a necessidade do negócio e haja uma aprovação documentada. Exemplos dessa necessidade incluiriam portas de rede em salas de conferência, espaços de trabalho compartilhados, etc.

7.5.1.5.4.1 Separação de ambientes (Caso o Prestador disponibilize a infraestrutura para a prestação de Serviço)

O ambiente de produção do Prestador deve ser separado física ou logicamente de ambientes não produtivos, de modo que exista um controle sobre a troca de informações entre eles.

A rede de usuários do Prestador deve ser separada da rede de sistemas centrais, permitindo a conectividade mínima necessária para que os usuários acessem os sistemas fundamentais para executar suas funções.

De qualquer forma, deve ser realizada uma separação nos ambientes operacionais, de desenvolvimento e de testes para reduzir os riscos de acessos ou alterações não autorizados e para que não haja impactos nos sistemas de produção.

7.5.1.5.4.2 Segurança dos servidores (Caso o Prestador disponibilize a infraestrutura para a prestação de Serviço)

O Prestador deve possuir uma documentação ou manual de proteção de servidores, gerenciamento de patches, versões e vulnerabilidades que garanta a segurança e a disponibilidade dos sistemas. O software instalado nos servidores deve ser apenas o indispensável para prestar o serviço corretamente e contar com uma proteção antivírus atualizada.

Os servidores devem ser plataformados de acordo com as boas práticas reconhecidas e só terão os serviços necessários ativos.

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

É necessário garantir a proteção dos dados e assegurar que estes não sejam visíveis exceto para o GRUPO PROSEGUR. Os dados, sejam residentes em bancos de dados ou sistemas de arquivos, devem ser acessíveis apenas a partir dos aplicativos que os processam, impossibilitando acessos públicos a partir de redes externas.

O Servidor do banco de dados deve ser instanciado em um sistema diferente daquele que executa o aplicativo, permitindo a comunicação apenas com o servidor onde o aplicativo está armazenado; ou seja, não deve ser diretamente acessível a partir da Internet.

Os servidores serão devidamente fechados/selados para que qualquer manipulação possa ser detectada visualmente.

7.5.1.5.4.3 Segurança perimetral:

O servidor que hospeda o aplicativo deve ser protegido contra o acesso de terceiros através de um Firewall.

Caso haja aplicativos expostos à Internet, o acesso a eles deve ser protegido por um dispositivo que funciona como um proxy reverso, localizado em um DMZ protegido por uma barreira de Firewall dupla. Não deve existir uma exposição direta à internet, a menos que o GRUPO PROSEGUR a autorize expressamente.

O Prestador deve garantir que, em caso de integração de novos softwares em dispositivos com permissões de conectividade nos sistemas de informação do GRUPO PROSEGUR, esta integração seja precedida por uma avaliação de risco, incorporando procedimentos formais de controle de mudanças para determinar e proteger o impacto na rede do GRUPO PROSEGUR.

7.5.1.5.4.4 Rede sem fio

O Prestador deve configurar os pontos de acesso à rede sem fio para garantir que somente dispositivos autorizados por ele possam estabelecer uma conexão com a rede interna do Prestador, na qual as informações do GRUPO PROSEGUR são exibidas, alojadas, armazenadas, processadas, transmitidas, preparadas, apoiadas ou destruídas. Além disso, as conexões de rede sem fio estabelecidas devem dispor das melhores práticas de criptografia da área e de outras garantias adequadas e projetadas para barrar o acesso e uso não autorizados.

7.5.1.5.4.5 Segurança dos Endpoints

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

- Aplicativos anti-malware como parte das configurações seguras comuns a sistemas, computadores e componentes. Que detectem e atualizem as vulnerabilidades, executando varreduras com frequência e não permitindo modificações por parte dos usuários.

- Firewalls pessoais fornecem restrições em portas e serviços, controle contra a execução de malware, controle de dispositivos removíveis, como dispositivos USB, e capacidade de auditoria e registro.

- Ferramentas IDPS para identificar e impedir atividades suspeitas monitorando o tráfego de rede e os dispositivos que se conectam a ela.

- Restrições ao uso de código móvel para evitar que códigos maliciosos sejam executados em computadores.

7.5.1.5.5 Gerenciamento de funcionários

O provedor deve implementar práticas de gestão de recursos humanos para contratar, manter e demitir funcionários, empreiteiros e outros funcionários que trabalham em nome da organização.

O Prestador deve se comprometer a implementar critérios adequados de seleção para cargos que afetem os sistemas do Grupo Prosegur.

O Prestador deve garantir que o gerenciamento de recursos humanos esteja vinculado ao gerenciamento de riscos. Portanto, é de suma importância garantir a presença de processos de registro, modificação e cancelamento de funcionários que defina que as medidas cabíveis serão tomadas imediatamente frente a algum tipo de mudança, como a retirada dos sistemas ou permissões de acesso que possibilitam a preservação da segurança das informações e dos sistemas.

O Prestador deve garantir que seus funcionários e/ou subcontratados e/ou funcionários de subcontratados tenham acesso aos sistemas, ativos e informações do Grupo Prosegur, estejam cientes e cumpram as Políticas, regras e procedimentos que o Grupo Prosegur exige a partir do momento em que o contrato é formalizado e os serviços são iniciados, especialmente no que diz respeito a seus deveres e obrigações quanto ao uso dos sistemas, redes e outros recursos do Grupo Prosegur, bem como as consequências e penalidades de seu não cumprimento.

Em particular, o Prestador deve garantir que seus funcionários não realizem, exceto com a permissão por escrito da Prosegur:

- A instalação de softwares ou dispositivos no ambiente Prosegur que não tenham sido aprovados pela Prosegur.

- O upload de dados ou softwares obscenos, ofensivos ou inadequados, violando a política de licenciamento no ambiente Prosegur.

- O uso do ambiente Prosegur para interceptar, analisar ou fazer qualquer outro tipo de monitoramento de tráfego das redes da Prosegur.

O provedor deve garantir o treinamento correto e a conscientização de seus funcionários acerca de cibersegurança e privacidade, tendo Planos de Treinamento e Conscientização para os funcionários gerenciados entre a equipe de gerenciamento de riscos e o RH. O grupo Prosegur pode solicitar acesso ao conteúdo dos Planos de Formação e Conscientização dos Funcionários para verificar sua adequação.

O provedor deve garantir que o treinamento específico seja fornecido aos usuários com privilégios e funções de segurança específicas para garantir que eles entendam suas funções e responsabilidades únicas.

O Prestador deve garantir que os funcionários subcontratados atendam aos mesmos requisitos de treinamento e conscientização que o resto da equipe.

7.5.1.5.6 Gerenciamento de operações

O Prestador deve estabelecer os controles de segurança adequados para garantir que as operações realizadas nos aplicativos e sistemas envolvidos no serviço sejam autorizadas e programadas de acordo com os requisitos acordados entre o GRUPO PROSEGUR e o Prestador. Especificamente, as operações a serem consideradas no serviço referem-se à realização de backups e ao gerenciamento de incidentes de segurança tecnológica.

O Prestador deve ter estabelecida uma série de políticas especificando as medidas a serem tomadas para a realização de backups, incluindo os procedimentos a serem seguidos para a recuperação dos sistemas.

O Prestador deve ter estabelecida uma série de medidas especificando as ações a serem realizadas em prol de um gerenciamento correto (detecção, resolução e comunicação ao GRUPO PROSEGUR) dos incidentes de segurança tecnológica ocorridos durante a prestação do serviço.

7.5.1.5.6.1 Configuração dos sistemas

O Prestador deve garantir que existam processos de gerenciamento da configuração e bastionado dos sistemas que estejam em conformidade com as normas internacionais e que permitam aplicar os requisitos de segurança estabelecidos pelo Grupo Prosegur para os sistemas.

O gerenciamento de configuração deve ser centralizado para todos os sistemas operacionais, aplicativos, servidores e outras tecnologias que possam ser configuradas.

O Prestador deve manter um registro do histórico de configurações caso seja necessário para a solução de problemas ou razões forenses.

Alterações de configuração não autorizadas que afetem os ativos do Grupo Prosegur, ao serem detectadas, devem ser tratadas como incidentes de segurança e comunicadas ao Grupo Prosegur.

O Prestador deve instalar nos sistemas utilizados para a prestação de serviços ao GRUPO PROSEGUR uma proteção antivírus que seja mantida operacional e atualizada o tempo todo.

O Prestador deve implementar controles para restringir dispositivos de saída, como USB, CD/DVD ou outros, que permitem a extração de dados a partir deles.

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

O Prestador deve implementar um processo de monitoramento de vulnerabilidades na infraestrutura tecnológica do Serviço, identificando e tratando vulnerabilidades em tempo hábil sem expor as informações do GRUPO PROSEGUR a tais riscos. Além disso, deve ser realizada periodicamente uma avaliação de segurança da rede interna e do perímetro, seja com recursos próprios ou por um terceiro independente.

O Prestador pode propor proativamente a instalação de atualizações de segurança e patches. Essas atualizações e patches serão comunicadas e autorizadas pelo GRUPO PROSEGUR. Ademais, o GRUPO PROSEGUR solicitará a instalação de atualizações e patches, caso considere necessário.

De qualquer maneira, a implantação de patches deve ser testada em ambientes anteriores para evitar possíveis impactos no Serviço.

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

Os períodos de atuação não devem exceder 24 horas em casos de falhas de segurança classificadas pelo fabricante como graves/altas.

O Prestador deve estabelecer controles de segurança adequados em relação a quaisquer alterações que possam ser feitas aos aplicativos ou sistemas envolvidos no Serviço. Esses controles devem cobrir pelo menos solicitações de alterações, análises de impacto, autorizações, testes, aprovações de usuários finais e uma separação adequada de ambientes anteriores do ambiente de produção.

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

O Prestador deve estabelecer os mecanismos necessários para a realização de uma administração e operação dos dispositivos de segurança, desde que o GRUPO PROSEGUR faça uma delegação expressa de tais funções.

7.5.1.5.6.3 Localização dos dados (caso o Prestador precise armazenar informações relacionadas à prestação do Serviço ao GRUPO PROSEGUR em seus próprios sistemas)

O Prestador deve informar ao GRUPO PROSEGUR a localização dos dados que serão armazenados antes da contratação do Serviço. Durante a duração do Serviço, qualquer alteração na localização dos dados deve ser comunicada antecipadamente ao GRUPO PROSEGUR e realizada apenas após o recebimento da autorização do GRUPO PROSEGUR.

O Prestador deve implementar mecanismos de controle de alteração nos arquivos armazenados no Serviço, registrando todas as informações necessárias que permitam a rastreabilidade dos eventos.

7.5.1.5.6.4 Arquivos temporários

O Prestador, ao utilizar arquivos temporários ou auxiliares para a prestação do serviço, deve proteger esses arquivos com as mesmas medidas de segurança usadas para os arquivos principais, e deve apagá-los, excluí-los ou destruí-los com segurança ao deixarem de ser necessários para os propósitos que motivaram sua criação, garantindo que sua recuperação subsequente não seja permitida.

Os responsáveis pelos sistemas de informação, designados para este fim, devem verificar periodicamente a possível existência de arquivos temporários criados automaticamente como resultado do mau funcionamento dos sistemas.

A menos que o serviço assim exija, a impressão em papel de dados pessoais dos aplicativos de gerenciamento será evitada.

7.5.1.5.6.5 Serviço compartilhado

O Prestador deve implementar medidas suficientes para garantir a segurança da infraestrutura tecnológica caso esta seja compartilhada com outros clientes do Prestador. A infraestrutura tecnológica do Serviço deve ter canais de comunicação criptografados entre outros serviços oferecidos pelo Provedor e as conexões do funcionários responsáveis pela administração da infraestrutura. Por exemplo: SSH, VPN com IPSEC, etc.

O armazenamento de dados do Serviço prestado ao GRUPO PROSEGUR deve ser coerentemente isolado de outros repositórios de armazenamento externos. O Serviço do Provedor deve ter a capacidade de criptografar informações armazenadas usando algoritmos de criptografia fortes, se necessário.

7.5.1.5.7 Gerenciamento de incidentes

O Prestador deve ter um procedimento para gerenciar e relatar incidentes de segurança e proteção de dados pessoais, devendo informar prontamente ao GRUPO PROSEGUR sobre um possível incidente de segurança ou ocorrência de um incidente de segurança e o modo de resolução, quando apropriado. Este procedimento deve ser divulgado para o conhecimento e conscientização de todos os seus colaboradores.

Em relação ao gerenciamento de incidentes, o Prestador deve ter mecanismos automatizados e de gestão que cubram:

- Prevenção
- Detecção
- Análise
- Contenção
- Mitigação
- Recuperação
- Monitoramento

O Prestador deve adotar as medidas adequadas para que, no menor tempo possível, a anomalia geradora do incidente seja corrigida.

O Prestador deve registrar cada incidente ocorrido: Tipo de incidente, descrição, tempo em que ocorreu ou foi detectado, pessoa que o notificou, pessoa a quem foi notificado, efeitos colaterais, medidas corretivas aplicadas, procedimentos realizados para a recuperação de dados, pessoa que os executa, dados restaurados e registrados manualmente.

O Prestador deve autorizar a execução dos procedimentos de recuperação de dados (se necessário) de acordo com os planos de Recuperação disponíveis.

O Prestador deve fornecer o suporte necessário ao GRUPO PROSEGUR caso este decida iniciar uma avaliação de segurança independente ou investigação de incidentes.

O Prestador deve definir um meio de comunicação seguro para comunicar situações incomuns, incidentes ou qualquer outra natureza relacionada à confidencialidade das informações do GRUPO PROSEGUR sem demora injustificada.

O Prestador deve informar imediatamente ao GRUPO PROSEGUR caso se suspeite ou seja detectado algum incidente de segurança, juntamente com um relatório com as informações relacionadas ao incidente, os processos, ativos e informações afetados, as medidas que foram tomadas e sua resolução. O Grupo Prosegur pode acompanhar esses incidentes para identificar possíveis situações em que medidas concretas devem ser tomadas.

O Prestador deve acordar com o GRUPO PROSEGUR os critérios para a notificação de um incidente de segurança em casos de vazamento de informações, interrupção do serviço, ataques que afetam a reputação do GRUPO PROSEGUR e qualquer outro caso que seja acordado.

A falta da notificação de um incidente crítico do qual se tem conhecimento pode ser considerada uma falha contra a segurança dos tratamentos e pode constituir uma violação da boa-fé contratual.

O Prestador deve manter um registro de incidentes de segurança, pelo menos dos sistemas e ativos que afetam o GRUPO PROSEGUR, contendo os incidentes ocorridos, o impacto, as datas e horários de detecção e resolução do incidente, as pessoas que foram responsáveis por seu gerenciamento e as soluções e medidas tomadas para resolvê-los.

O GRUPO PROSEGUR pode solicitar a consulta do inventário de incidentes que afetam os sistemas e ativos de sua propriedade a qualquer momento se assim achar necessário ou solicitar um relatório

do monitoramento de eventos e incidentes que afetem seus sistemas e informações. O Prestador deve ser capaz de torná-los disponíveis para você.

7.5.1.5.8 Comunicações

O Prestador deve estabelecer todos os mecanismos necessários para criptografar comunicações em redes públicas ou redes de comunicações eletrônicas sem fio.

A conexão do CPD do Prestador com os sistemas do GRUPO PROSEGUR somente pode ser realizada estabelecendo as medidas de controle determinadas pelo GRUPO PROSEGUR, após análise detalhada das necessidades.

As comunicações com o CPD do Grupo PROSEGUR devem estar redundadas.

O Prestador deve disponibilizar ao GRUPO PROSEGUR, quando solicitado, um mapa completo da rede do prestador de Serviços no qual todos os elementos de comunicação envolvidos estejam perfeitamente identificados, bem como os elementos de segurança.

O Prestador deve ter pelo menos as seguintes medidas de segurança do perímetro em ordem: Firewall, Sistemas de Detecção e Prevenção de Intrusões (IDS/IDPS), Zona Desmilitarizada (DMZ), Redes Privadas Virtuais (VPNs) e Proxy.

7.5.1.5.8.1 Segurança no uso de e-mail (Caso o Prestador envie e-mails em nome do GRUPO PROSEGUR ou com informações que se refiram a ele)

Ao enviar e-mails em nome do GRUPO PROSEGUR ou com informações que se referem a ele, o Prestador deve cumprir as seguintes medidas:

- Os endereços web (URLs) incluídos nos e-mails e o conteúdo destes devem ser previamente supervisionados pelo departamento de Segurança da Informação do GRUPO PROSEGUR.
- O Departamento de Segurança da Informação do GRUPO PROSEGUR deve conhecer os dados do GRUPO PROSEGUR incluídos nos e-mails. Estes não devem ser confidenciais ou secretos e este departamento determinará se e como eles devem ser certificados.
- A Segurança da Informação do GRUPO PROSEGUR deve receber:
    - O aviso prévio do envio de e-mails.
    - Uma breve explicação do conteúdo dos e-mails.
    - Um exemplo dos e-mails/SMSs a serem recebidos pelos clientes.
    - Conhecer a caixa de correio para onde serão enviados os e-mails direcionados aos clientes.

- Deve haver vestígios e evidências (logs) de quando e para quem os e-mails são enviados a partir do servidor de e-mail utilizado para isso, seja na infraestrutura do GRUPO PROSEGUR ou na do Prestador.

- Nos registros de atividades, a data e a hora dos envios, a conta pela qual os e-mails são enviados e seus destinatários devem ser registrados.

- Os e-mails devem incluir os avisos/recomendações acordados com o departamento de Prevenção de Fraudes Tecnológicas.

- Os e-mails devem ser enviados por um domínio registrado em nome do GRUPO PROSEGUR.

- O departamento de Mensagens (no caso do envio ser realizado pelo GRUPO PROSEGUR) ou o Prestador de Serviços devem definir mecanismos de controle sobre listas negras de spam para garantir que os domínios do GRUPO PROSEGUR não apareçam.

- Os e-mails enviados aos clientes devem passar pelos controles necessários para eliminar a presença de vírus. Ou seja, os e-mails devem ser escaneados com as ferramentas antivírus existentes do GRUPO PROSEGUR ou, em caso de terceirização, do Prestador de Serviços.

7.5.1.5.9 Gerenciamento de capacidade, dimensionamento e aquisição de sistemas

O Prestador deve gerenciar a capacidade e os recursos que afetam o serviço prestado por meio do estabelecimento de processos de gestão da capacidade e dimensionamento que consistam em uma administração dinâmica dos recursos do prestador com base na capacidade econômica, necessidades e obrigações contratuais.

A aquisição de novos sistemas, equipamentos, componentes ou softwares deve ser gerenciada levando em conta:

- Os riscos associados a cada atividade, serviço e sistemas

- A concordância com os requisitos de segurança estabelecidos para o serviço

- As necessidades técnicas dos recursos

- Os esforços e meios econômicos de sua implementação.

O Prestador deve estabelecer controles de segurança adequados em relação à aquisição e desenvolvimento de novos aplicativos e/ou novos sistemas, e em relação a quaisquer alterações que possam ser feitas aos aplicativos ou sistemas envolvidos na terceirização durante a prestação do serviço. Esses controles devem englobar pelo menos autorizações, testes, aprovações de usuários finais e uma separação adequada dos ambientes anteriores do ambiente de produção.

7.5.1.5.9.1 Uso e desenvolvimento de software para a prestação do serviço

O Prestador só deve utilizar softwares licenciados e testados pelo GRUPO PROSEGUR e pelo Prestador para a realização do serviço terceirizado.

Todos os desenvolvimentos realizados com o objetivo de prestar serviços ao GRUPO PROSEGUR devem ser autorizados pelo GRUPO PROSEGUR, fazendo com que o Prestador:

- Abstenha-se de armazenar dados do GRUPO PROSEGUR sem que o GRUPO PROSEGUR os conheça, autorize e/ou audite-os.
- Realize uma revisão de segurança do código-fonte de qualquer software que não tenha sido desenvolvido pelo GRUPO PROSEGUR antes de sua produção, de acordo com os princípios e boas práticas de desenvolvimento seguro.
- Disponibilize todos os desenvolvimentos de software feitos sob medida, incluindo código-fonte, código objeto, manuais e quaisquer outras informações relevantes, caso sejam realizados desenvolvimentos de software para o GRUPO PROSEGUR.
- Esteja em condições de realizar uma avaliação do ambiente de controle, hacking ético ou qualquer outra avaliação de segurança antes da produção de qualquer versão do sistema, a qualquer momento que o GRUPO PROSEGUR o exija.
- Garantir que ambientes que não sejam de produção não contenham dados reais e tenham os mesmos controles do ambiente de produção.
- Assegurar que os desenvolvimentos feitos para a prestação dos Serviços ao GRUPO PROSEGUR e as ferramentas utilizadas cumpram as leis de propriedade intelectual e não violem qualquer legislação, regulamento, contrato, direito, interesse ou propriedade de terceiros.
- Estabelecer controles de segurança adequados em relação à aquisição ou desenvolvimento de novas aplicações ou sistemas durante a prestação do Serviço. Esses controles devem englobar pelo menos análises de viabilidade, autorizações, testes, aprovações de usuários finais e uma separação adequada dos ambientes anteriores do ambiente de produção.
- O Prestador 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 equipes de desenvolvimento do GRUPO PROSEGUR devem estar localizadas em segmentos de rede e ambientes dedicados exclusivamente ao desenvolvimento de aplicativos, sem acesso a ambientes de produção ou dados reais do GRUPO PROSEGUR.
- O Prestador deve estabelecer controles de segurança adequados em relação à validação de integridade dos desenvolvimentos nos ambientes de produção.

7.5.1.5.10 Revisão

7.5.1.5.10.1 Avaliações realizados pelo GRUPO PROSEGUR

O Prestador deve aceitar a realização de revisões em conformidade com o Regime de Controle do GRUPO PROSEGUR, com caráter:

- Ordinário, como parte da avaliação da prestação do Serviço.
- Extraordinário, por razões de incidente de segurança ou em caso de qualquer prorrogação, regressão dos serviços ou circunstâncias que levem o GRUPO PROSEGUR a considerá-los adequados para realização.

O GRUPO PROSEGUR deve realizar essas revisões de acordo com o regime de controle, seguindo um método de avaliação, escopo, método de monitoramento e periodicidade estabelecidos pelo GRUPO PROSEGUR.

O Prestador deve fornecer quantas colaborações forem necessárias para atender adequadamente aos requisitos da revisão que o GRUPO PROSEGUR, as pessoas ou empresas designadas pelo GRUPO PROSEGUR possam formular e entregar a este, independentemente da quantidade de documentações e/ou comprovações solicitadas.

Além disso, o GRUPO PROSEGUR pode exercer controle sobre os riscos tecnológicos associados ao Serviço, sendo o Prestador responsável por fornecer as seguintes informações, quando necessário:

- Revisão de relatórios de auditoria e/ou certificações, por exemplo:
    - Relatórios de auditoria interna/controle 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 de Serviço (ISO 9001, ISO 2000, etc.).

Além dos relatórios apresentados, o GRUPO PROSEGUR deve ter a capacidade de desenvolver um plano de avaliação para controle de riscos tecnológicos e executá-lo de acordo com os prazos, escopo e procedimentos acordados com o Prestador. Este plano pode incluir:

- Monitoramento regular dos indicadores de segurança do Serviço:
    - Os indicadores a serem monitorados acordados antes da assinatura do contrato devem ser revistos periodicamente.
    - Acesso a painéis ou consoles pelo GRUPO PROSEGUR que permitam o monitoramento contínuo do risco tecnológico.
- Relatório de eventos relevantes por parte do Prestador:
    - Incidentes de segurança.

- Testes de recuperação de desastres.

- Informações sobre a infraestrutura tecnológica que dá suporte ao GRUPO PROSEGUR (caso o Prestador faça uso de infraestrutura própria para a prestação do Serviço):
  - Arquitetura de rede.
  - Arquitetura de segurança perimetral.
  - Servidores e bancos de dados.
  - Protocolos de rede e comunicações.
  - Quaisquer necessidades para que o GRUPO PROSEGUR seja capaz de exercer adequadamente as funções de controle.

- Informações sobre o monitoramento realizado nos sistemas que prestam serviço ao GRUPO PROSEGUR, bem como o modelo de relacionamento estabelecido para a comunicação dessas informações, quando julgar necessário.

O Prestador deve resolver as fragilidades de controle identificadas pelo GRUPO PROSEGUR nas revisões realizadas após os planos de ação acordados.

7.5.1.5.10.2 Controle interno do Prestador

O Prestador deve ter uma função de controle interno que garanta o cumprimento de todos os controles exigidos pelo GRUPO PROSEGUR.

O Prestador deve descrever e disponibilizar ao GRUPO PROSEGUR, quando solicitado, os procedimentos e controles a serem articulados internamente para garantir que os requisitos estabelecidos sejam atendidos.

O Prestador deve realizar todas as auditorias legalmente requeridas, interna e externamente, nos sistemas envolvidos no serviço prestado ao GRUPO PROSEGUR, deixando os relatórios de auditoria à disposição do GRUPO PROSEGUR.

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

7.5.1.5.10.3 Controles coordenados com o GRUPO PROSEGUR

O GRUPO PROSEGUR e o Prestador devem acordar os procedimentos para que qualquer incidente de segurança seja comunicado diligentemente ao GRUPO PROSEGUR. Serão definidos protocolos específicos de comunicação para os casos em que é necessária ação imediata do GRUPO PROSEGUR para mitigar o impacto dos incidentes de segurança.

O GRUPO PROSEGUR poderá verificar o cumprimento dos requisitos técnicos a qualquer momento, tanto por meio de visitas às instalações do Prestador, quanto por uso de meios seguros de acesso remoto aos sistemas envolvidos acordados com o Prestador.

Os aspectos observados nessas revisões considerados pelo GRUPO PROSEGUR como uma violação ou risco para os sistemas do GRUPO PROSEGUR serão comunicados ao Prestador, que será dado um prazo para sua resolução com o consequente compromisso contratual de cumprir com os aspectos observados conforme acordado com o GRUPO PROSEGUR.

7.5.1.5.10.4 Devolução do Serviço

O GRUPO PROSEGUR e o Prestador devem definir e acordar os procedimentos de devolução do serviço de forma a garantir um armazenamento seguro dos meios de comunicação e, se for o caso, a destruição segura das informações utilizadas pelo Prestador durante a prestação do Serviço.

O Prestador deve garantir que mecanismos seguros de eliminação de informações sejam usados. Estes incluirão casos de reciclagem de mídia e de encerramento de Serviço.

Se a destruição das informações for realizada por terceiros, o GRUPO PROSEGUR deve ser comunicado e disponibilizado um certificado de destruição segura.

O Fornecedor deve cumprir, nos aspectos aplicáveis ao serviço terceirizado, as diretrizes previstas nas normas e práticas internacionais aplicáveis.

Para registros que atendam aos requisitos legais de retenção, os períodos de retenção devem ser estabelecidos e mantidos adequadamente pelo Prestador. Além disso, o GRUPO PROSEGUR pode fornecer requisitos específicos de retenção que o Prestador deverá aplicar, incluindo, mas não se limitando, a retenção para fins contenciosos, legais ou regulatórios.

O Prestador 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 gerenciamento de registros do Prestador. Antes que uma estação de trabalho ou servidor sejam reutilizados, desmontados ou devolvidos ao fornecedor de locação, as metodologias de destruição devem ser executadas com segurança para que as informações não possam ser lidas ou recriadas após a exclusão.

O Prestador deve levar em conta o impacto do descarte no meio ambiente.

7.5.1.5.11 Monitoramento

O Prestador deve disponibilizar ao Grupo PROSEGUR, quando solicitado, os procedimentos e controles a serem implementados para monitorar e alertar sobre possíveis violações de segurança dos sistemas.

O Prestador deve implementar os mecanismos necessários para monitorar o software instalado nos equipamentos que prestam serviço ao GRUPO PROSEGUR para que apenas os softwares essenciais para a prestação adequada do serviço possam ser instalados, seja de propriedade do usuário ou de propriedade do GRUPO PROSEGUR.

7.5.1.5.11.1 Custódia e exploração de registros de segurança.

Quanto aos eventos que geram logs, o GRUPO PROSEGUR especificará o formato, conteúdo dos logs e o período de custódia. Se solicitado, esses logs devem estar disponíveis em tempo real, seja através do acesso direto ao sistema do Prestador ou por meio de sua recepção nos repositórios internos do GRUPO PROSEGUR. Além disso, deve-se garantir que a rastreabilidade seja gerada no restante dos sistemas indiretamente envolvidos no serviço ou que tenham sido previamente analisados pelo

GRUPO PROSEGUR. O Prestador deve gerar logs (acesso, autenticação, administração e atividade), no mínimo, dos seguintes eventos:

- Comunicações.
- Envio de arquivos (sistemas envolvidos na transmissão, tanto na origem quanto no destino, e sistemas intermediários de armazenamento temporário).
- Aplicativos.
- Sistemas de virtualização (arquitetura cliente-servidor).
- Backend (servidores e aplicativos).

7.5.1.5.12 Cópias de backup e recuperação (caso o Grupo Prosegur autorize o backup dos dados ou sistemas para a prestação do serviço ao GRUPO PROSEGUR)

O Prestador deve estabelecer e adotar uma política de backup que inclua a segurança das cópias e procedimentos de teste e recuperação. Tendo controles implementados para garantir o manuseio e o transporte corretos dos meios de armazenamento dos backups, atribuindo responsáveis, controles de acesso físicos e lógicos, cadeias de custódia e inventários periódicos, garantindo a confidencialidade das informações contidas.

O Prestador deve implementar controles em sua política de backup que garantam a recuperação dos dados no estado em que estavam no momento de um incidente de modificação, perda ou destruição.

O Prestador deve estabelecer procedimentos de realização de backups no mínimo semanais, a menos que nesse período não tenha havido atualização dos dados.

O Prestador deve fazer backups periódicos de seus sistemas que estejam em conformidade com as disposições dos Tempos Objetivos de Recuperação e do Ponto Objetivo de Recuperação que devem ser incluídos no Plano de Continuidade de Negócios e Recuperação de Desastres e que foram acordados com o GRUPO PROSEGUR.

O Prestador deve manter os procedimentos de backup e recuperação de dados, além das próprias cópias, em um local diferente de onde os sistemas de informação estão localizados.

O Prestador deve armazenar no máximo um (1) backup completo e incremental dos últimos seis (6) dias em suas próprias instalações, terceirizando todas as cópias que não estejam nessa margem.

O Prestador deve incluir em sua política de backup verificações e testes semestrais da eficácia dos procedimentos de backup por parte dos responsáveis.

Só será possível trabalhar com dados reais ao garantir o nível de segurança correspondente aos tratamentos.

A geração de cópias ou a reprodução dos documentos só podem ser realizadas sob o controle dos funcionários definidos no Documento de Segurança, destruindo as cópias descartadas de tal forma que suas informações sejam inacessíveis.

7.5.1.5.13 Continuidade de negócios

O Prestador deve ter um Plano de Continuidade de Negócios e Recuperação de Desastres que 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 prestador deve rever os Planos de Continuidade pelo menos uma vez por ano e sempre que houver mudanças tecnológicas, organizacionais ou regulatórias relevantes.

O Prestador deve garantir que todos os funcionários designados para tarefas de continuidade de negócios tenham experiência, competência e capacidade suficientes para desempenhar as funções necessárias.

O Prestador deve realizar testes de contingência para demonstrar a eficácia dos Planos de Continuidade e Recuperação de Desastres. Da mesma forma, deve fazer parte dos testes solicitados pelo GRUPO PROSEGUR como parte da Continuidade dos sistemas do GRUPO PROSEGUR.

O Prestador deve fornecer atualizações regularmente sobre a situação da continuidade do serviço prestado ao GRUPO PROSEGUR de acordo com as instruções disponíveis.

Caso haja uma interrupção antes de um evento de segurança, o prestador deve assumir a responsabilidade de retomar os serviços prestados dentro dos prazos definidos pelo Grupo Prosegur, dependendo da criticidade dos sistemas afetados. Para sistemas com maior criticidade, a retomada das atividades em até 4 horas pode ser requisitada. O prestador é considerado responsável pela retomada dos serviços dentro dos prazos acordados, estando sujeito às consequências contratuais e sancionadas em caso descumprimento injustificado.

O Prestador será obrigado a permitir que o GRUPO PROSEGUR realize auditorias do Plano de Continuidade de Negócios (BCP) e do Plano de Recuperação de Desastres (DR) do Prestador que pertençam ou afetem os Ativos de Informação envolvidos no serviço terceirizado, incluindo os procedimentos BCP e DR, bem como os resultados dos testes realizados, pelo menos uma vez por ano e depois de qualquer contingência ou desastre natural.

7.5.1.5.14 Gerenciamento de fornecedores

O Prestador deve garantir, quando os serviços prestados dependerem de outros provedores, que os mecanismos de gerenciamento de terceiros estejam em vigor..

O prestador deve garantir que sua equipe de gerenciamento de riscos possa executar operações coordenadas de resposta a incidentes que incluam prestadores de serviços externos que possam afetar direta ou indiretamente as atividades, processos e ativos do Grupo Prosegur.

O prestador deve ter um processo de seleção e avaliação de prestadores no qual os riscos da cadeia de suprimentos sejam avaliados. Os prestadores devem ser identificados, avaliados e priorizados como outros ativos da organização, fazendo parte das análises e tratamento de riscos.

O prestador deve manter as empresas subcontratadas envolvidas no serviço prestado ao Grupo Prosegur identificadas a todo momento, transferindo a obrigação de cumprir os requisitos tecnológicos e de segurança descritos neste documento.

O prestador deve garantir que, na assinatura de seus contratos de aquisição com terceiros, sejam identificados acordos de confidencialidade e nível de serviço com os requisitos mínimos de segurança, bem como em outros contratos que reflitam as necessidades da organização de proteção dos sistemas e dados do Grupo Prosegur. Esses contratos devem ser revistos e monitorados periodicamente.

O Prestador deve garantir que tanto os fornecedores terceirizados quanto os usuários que tenham acesso a quaisquer dados pessoais e outras informações do Grupo Prosegur, por ocasião do cumprimento de seu trabalho para a entidade, se comprometam a desenvolver suas funções observando a máxima diligência e boa-fé na custódia e tratamento destes.

O Grupo Prosegur poderá solicitar ao prestador informações ou relatórios sobre as medidas e requisitos adotados com um determinado prestador.

O prestador será responsável pelo Grupo Prosegur diante do não cumprimento por parte das empresas subcontratadas envolvidas nos serviços prestados ao Grupo Prosegur, se houver, com os requisitos descritos neste anexo.

O prestador deve garantir que as supervisões e auditorias periódicas da prestação de serviços de terceiros sejam realizadas para verificar o cumprimento dos acordos contratuais estabelecidos e especificamente com os requisitos estabelecidos neste documento.

O prestador deve especificamente garantir o controle das mudanças nos serviços por parte dos prestadores, levando em conta a importância das informações, sistemas e processos de negócios que estejam ao alcance de terceiros.

O não cumprimento de qualquer das obrigações contidas neste anexo, tanto diretamente pelo prestador quanto indiretamente pelas empresas subcontratadas pelo prestador pode constituir uma causa para rescisão do contrato ou outras consequências contratuais.

7.6. ANEXO V USO DE RECURSOS E SISTEMAS DE TI DA PROSEGUR

Medidas de proteção

No caso de equipamentos de informática fornecidos pelo Grupo Prosegur, o usuário deve cumprir as medidas de proteção indicadas abaixo:

Os equipamentos de computador devem ser utilizados apenas para fins profissionais.

É proibida a utilização de aplicativos e serviços Web baseados em serviços de streaming de áudio ou vídeo, compra e venda de produtos, redes sociais, notícias, esportes e, em geral, sites não relacionados ao trabalho profissional.

Os usuários devem salvar as informações e arquivos com os qual lidam no desempenho de suas funções em plataformas de armazenamento em nuvem habilitadas e autorizadas pela organização (por exemplo, onedrive) evitando salvá-las em computadores localmente.

Os usuários devem ser responsáveis por garantir que o equipamento atribuído a eles não seja utilizado por terceiros ou por pessoas não autorizadas.

As informações confidenciais não devem ser divulgadas a terceiros não autorizados, sendo especialmente cuidadosos com informações comunicadas por telefone e na Internet.

Os usuários devem fornecer ao pessoal técnico autorizado pelo Grupo Prosegur acesso ao seu equipamento para realizar qualquer trabalho de reparo, instalação ou manutenção que possa ocorrer.

Os usuários devem proceder à devolução dos recursos de informática e/ou comunicações que tenham sido atribuídas pelo Grupo Prosegur, quando sua atividade na organização cessar.

Da mesma forma, quando o computador ou os meios de comunicação fornecidos pelo Grupo Prosegur estiverem associados ao desempenho de um determinado cargo ou função, a pessoa com essa atribuição deverá devolvê-los imediatamente à sua unidade informática quando terminar o relacionamento com tal cargo ou função.

O usuário deve seguir as indicações e instruções para minimizar os riscos derivados de ameaças causadas por malware, prestando atenção especial ao uso de dispositivos removíveis, e-mail e software baixado da Internet ou de fontes desconhecidas e/ou ilegais.

Os sistemas nos quais o uso inadequado for detectado, ou nos quais os requisitos mínimos de segurança não forem atendidos, poderão ser bloqueados ou temporariamente suspensos pelo Grupo Prosegur, restaurando o serviço quando a causa da ameaça ou degradação desaparecer.

O usuário não deve vulnerar, de forma alguma, as permissões da sua conta, principalmente para instalar aplicativos que não estejam relacionados com o desempenho do seu trabalho. Caso o usuário exija a instalação de um aplicativo específico para realizar suas funções, deverá fazer tal solicitação à Diretoria de Tecnologia da Informação (doravante DTI) através do Service Portal.

Não é permitido configurar no dispositivo contas pessoais de serviços não definidos pelo Grupo Prosegur.

É expressamente proibido acessar, baixar e/ou armazenar, em qualquer suporte: sites ou conteúdos ilegais, inadequados ou que representem um ataque à moral e aos bons costumes; formatos de imagens, áudio ou vídeo mencionados na regra anterior; vírus e códigos maliciosos; de modo geral, qualquer tipo de programa e/ou plug-ins sem a autorização expressa do Grupo Prosegur.

O usuário é responsável por garantir que os equipamentos que lhe são atribuídos sejam mantidos atualizados e com os patches de segurança correspondentes.

O Grupo Prosegur tem o poder de monitorar a atividade nos equipamentos informáticos para verificar o uso adequado dos mesmos, bem como prevenir e detectar incidentes de segurança.

É proibido o uso de dispositivos de armazenamento removíveis sem autorização prévia.

As portas USB são desativadas por padrão e, caso seu uso seja necessário, deverá ser solicitado à área de Segurança da Informação e DTI, que deve avaliar a justificativa de tal solicitação.

Se autorizado, o usuário será responsável pelas ações realizadas com as informações extraídas ou inseridas nos recursos informáticos do Grupo Prosegur.

As mídias de armazenamento disponíveis destinam-se apenas a uso profissional.

A perda ou roubo de tal mídia deve ser tratada como um incidente de segurança e comunicada sem demora.

As mídias que serão reutilizadas devem passar previamente por um processo de exclusão seguro de acordo com os regulamentos do Grupo Prosegur.

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

Devolução de equipamentos, dispositivos e mídia

No caso de:

• Conclusão do serviço a que se destinam
• Rescisão do vínculo contratual do usuário com o Grupo Prosegur.
• Obsolescência de equipamentos, dispositivos e/ou mídia
• Avarias em equipamentos, dispositivos e/ou mídia

Deve ser devolvido, enviando o dispositivo para a área de microcomputação local correspondente através dos canais que lhe são disponibilizados com um pedido indicando os motivos da devolução:

Em caso de conclusão do projeto: Uma solicitação de serviço não catalogada deve ser aberta no Service Portal indicando, pelo menos, algumas das seguintes informações:

o Número de série
o Nome do host do equipamento
o Ou último usuário que usou: Por exemplo: ES00605432.

Uma vez aberto o tíquete, deve-se aguardar as instruções do departamento de microinformática local para a devolução e retirada do equipamento. Neste caso, a reutilização do equipamento do usuário que causa o cancelamento para entregá-lo à nova incorporação, também deve ser validado pelo DTI por razões de segurança.

Em caso de obsolescência ou avaria: Você deve abrir um tíquete no Service Portal e seguir as instruções para devolução do equipamento indicadas pelo departamento de microinformática local.

De qualquer forma, o equipamento NÃO deve permanecer em dependências departamentais do negócio sem controles de segurança físicos e lógicos e não deve ser utilizado após ficar desconectado da rede por um longo período de tempo, pois isso coloca em risco a segurança na empresa devido a possíveis vulnerabilidades.

Mesa limpa e estação de trabalho organizada

É obrigação dos usuários colocar em prática as seguintes medidas:

• Manter o local de trabalho limpo e organizado, não havendo mais material sobre a mesa do que o necessário para a atividade realizada em determinado momento.

• No momento em que uma tarefa ou função é concluída, o material deve ser removido para uma área segura em local fechado, para isso, o Grupo Prosegur pode atribuir armários e gavetas com chave.

• Armazenar documentação e dispositivos de armazenamento de informações confidenciais trancados durante períodos de ausência prolongada e no término do dia de trabalho.

• As chaves não devem ser deixadas em gavetas ou armários onde as informações confidenciais são armazenadas.

• Deve-se ter cuidado com as informações exibidas nas telas do computador sempre que estiver perto do pessoal não autorizado a visualizar tais informações.

• Evite trabalhar com informações em papel. Senhas e outras informações de interesse não devem ser visíveis escritas em papel ou post-its.

• Conferir se a documentação de suporte para reuniões, apresentações e outras ocasiões, realizadas nas salas previstas para essa finalidade, não é deixada nas salas após o término dos eventos.

• Imprimir sempre com a opção "Impressão protegida" ativada, que exija inserir uma senha para poder ser realizada.

• Em todas as impressoras que possuem mecanismos de impressão seguros com senha, o funcionário deve sempre certificar-se de fechar a sessão.

• Remover imediatamente todas as informações sigilosas de impressoras, máquinas de fotocópia e de fax, certificando-se de que nenhuma documentação permaneça na bandeja de saída ou na fila de impressão.

• Destruir todos os documentos descartados, de forma que as informações sigilosas fiquem ilegíveis ou não possam ser recuperadas com facilidade. Para isso, usar as fragmentadoras de papel ou contêineres destinados especificamente a essa finalidade.

• Os cartões criptográficos não devem ser deixados sem vigilância e visíveis, pois podem fazer com que pessoas não autorizadas acessem as informações e recursos do Grupo Prosegur.

Bloqueio de estação de trabalho e logins

Os usuários do sistema têm o dever de:

• Ativar o protetor de tela e o bloqueio do computador quando deixar a estação de trabalho sem supervisão.

• Bloquear os equipamentos durante qualquer ausência Usar dispositivos que protejam fisicamente os equipamentos portáteis, como cadeados, sempre que disponíveis.

• Conferir se os equipamentos estão desligados no fim do período de trabalho.

• As imagens exibidas após o bloqueio de tela não podem incluir ou revelar informações confidenciais.

• Quando a estação de trabalho for deixada sem vigilância durante ausências prolongadas, os aplicativos e sessões do sistema devem ser fechados sempre que sua operação contínua não seja necessária devido à sua funcionalidade.

• Não modificar as configurações estabelecidas para bloqueio automático do computador ou logout automático por qualquer método sem autorização prévia.

Acesso aos sistemas de informação

Credenciais de acesso

Os usuários são responsáveis pela custódia das credenciais de acesso, identificação eletrônica e certificados de assinatura, bem como do software ou outras mídias atribuídas (como cartões criptográficos, tokens), para acesso autorizado a recursos e sistemas do Grupo Prosegur.

Os autenticadores são únicos para cada pessoa, intransferíveis e independentes do recurso de computação a partir do qual é feito o acesso.

Utilização de senhas

• As senhas devem ser difíceis de adivinhar.

• Não devem ser usados:
o Palavras do dicionário, gíria ou dialeto.
o Palavras referentes ao contexto da organização ou às funções dos usuários.
o Palavras que contenham informações pessoais, como data de nascimento, nomes de familiares, pessoas do mesmo ambiente, números de telefone, etc.

• Os usuários são responsáveis pela custódia e uso das senhas.

• Somente os usuários que usam as senhas devem conhecê-las. Não devem ser comunicadas a terceiros, nem mesmo à organização. Todas as senhas devem ser tratadas como informação confidencial e utilizadas exclusivamente pelo usuário ao qual foram designadas. As senhas não devem ser informadas por telefone, mesmo que falem com você em nome da DTI ou de um superior sênior.

• As senhas jamais devem ser transmitidas por e-mail nem por nenhum outro meio de comunicação eletrônica.

• As senhas não devem ser escritas em um papel ou documento onde possam permanecer registradas. Também não devem ser salvas em documentos de texto ou em notas no próprio computador ou em dispositivos móveis.

• É proibido utilizar senhas empregadas para contas de recursos e serviços do Grupo Prosegur em contas alheias à empresa, e vice-versa.

• O usuário tem a obrigação de alterar as senhas quando o sistema o notificar da necessidade da alteração antes do vencimento.

• A senha deve ser alterada imediatamente se houver algum indício de que tenha sido violada, e isso deve ser notificado de acordo com o processo predefinido de comunicação de incidentes à administração pelo e-mail seguridad.informacion@prosegur.com

• É proibido usar mecanismos para lembrar senhas. A utilização de ferramentas, como os administradores de senhas, exige a aprovação e validação preliminar da área de Segurança da Informação e da DTI.

• A senha jamais deve ser informada a nenhuma pessoa que esteja em períodos de férias ou de ausência prolongada.

• Se o usuário precisar alterar a senha e o sistema não permitir mais ou a conta tiver sido suspensa, ele deve informar esse fato como um incidente ao CAU através do Service Portal. A conta será recuperada por um administrador após verificar a identidade do usuário.

Acesso Remoto

O acesso via VPN permite que os usuários, que estão fora das instalações do Grupo Prosegur, acessem os recursos de informações e de rede fazendo uma conexão criptografada pela Internet.

De acordo com o exposto, são estabelecidas as seguintes diretrizes:

• O acesso remoto é concedido em base naquilo que as funções desempenhadas pelos usuários exijam, e poderá ser cancelado quando for considerado adequado.

• O acesso remoto é concedido antecipadamente pelo Grupo Prosegur aos usuários atribuídos ou que justifiquem a necessidade de trabalhar por meio deste canal.

• É proibido o uso de ferramentas de acesso remoto que não as aprovadas pelo Grupo Prosegur.

• Os usuários são responsáveis por proteger suas credenciais de acesso remoto, evitar que sejam divulgadas e garantir sua privacidade.

O usuário que utilizar medidas para acesso remoto deve garantir a segurança física onde utilizará o acesso, como residência, instalações de terceiros, locais de acesso público, etc.

• Os usuários são os únicos responsáveis pelas ações realizadas em relação aos recursos que são acessados durante a sessão via VPN.

• O acesso à rede e aos recursos associados via VPN deve ser usado apenas para fins profissionais. Qualquer outro tipo de utilização é considerado indevido e cabe ao usuário a responsabilidade completa sobre isto.

• Os usuários com acesso remoto que executarem tarefas de suporte técnico, administração de equipamentos ou de desenvolvimento não devem ultrapassar a aplicação dos seus privilégios.

• O pessoal colaborador e terceiros autorizados a usar a conexão remota têm acesso limitado para o desenvolvimento de suas funções.

• É proibido revelar a terceiros ou externamente o conteúdo de qualquer informação secreta, confidencial ou interna do Grupo Prosegur acessada por meio do serviço de VPN.

• Durante a conexão via acesso remoto, as conexões paralelas não são permitidas.

• O acesso à Internet durante a sessão remota é permitido apenas por meio do proxy do Grupo Prosegur.

• Os usuários ficam proibidos de se conectar a redes Wi-Fi públicas para a conexão à Internet necessária para o acesso remoto. Embora o fluxo de informações via VPN seja feito cifrado, este tipo de redes não possui mecanismos suficientes para garantir a confidencialidade da navegação na Web.

• O usuário deve fechar as sessões remotas de VPN quando não forem mais usadas para a função executada ou estiverem ausentes de seu local de trabalho.

• O Grupo Prosegur pode monitorar o acesso via conexão remota para prevenir ataques e detectar uso indevido.

Acesso e uso da Internet

• Deve ser feito um uso estritamente profissional da Internet. É proibido o uso para fins pessoais ou recreativos.

• O acesso à Internet é concedido de acordo com os requisitos das funções desempenhadas pelos funcionários individualmente, e pode ser tirado em qualquer momento, caso seja considerado conveniente pelo Grupo Prosegur.

• Os usuários comprometem-se a fazer bom uso da Internet e são responsáveis pelas sessões iniciadas na Internet a partir de qualquer dispositivo.

• É proibido armazenar, divulgar a terceiros ou terceirizar o conteúdo de qualquer informação de propriedade do Grupo Prosegur, por meio de qualquer meio na Internet de acesso público ou privado sem o consentimento expresso da empresa. O Grupo Prosegur pode filtrar o conteúdo que pode ser acessado pela Internet. Caso um usuário justifique a necessidade de acessar um endereço específico, deverá solicitá-lo através de seu gerente para que ele solicite à Gerência de TI (doravante DTI).

• O Grupo Prosegur pode monitorar a atividade dos usuários na Internet, bem como registrar os acessos realizados.

• Páginas não confiáveis ou suspeitas de conter conteúdo malicioso não devem ser visitadas.

• Não é permitido, em hipótese alguma, alterar a configuração dos navegadores (opções da Internet) nos equipamentos nem ativar servidores ou portas sem a devida autorização da DTI.

• Fica expressamente proibido o download e/ou armazenamento em qualquer meio de páginas com conteúdo ilegal, nocivo, inapropriado ou que viole a moral e os bons costumes e, em geral, de qualquer tipo de conteúdo que viole o código de ética do Grupo.

• Não é permitido, de forma alguma, utilizar ou baixar arquivos P2P ou semelhantes.

• Antes de utilizar as informações obtidas na Internet, os usuários devem verificar em que medida estão sujeitas aos direitos derivados da Propriedade Intelectual ou Industrial e/ou podem violar as normas aplicáveis em matéria de proteção de dados pessoais.

• Quando são feitas trocas de informações ou transações, as páginas Web devem ser acessadas digitando e verificando o endereço na barra de endereços do navegador e não por meio de links externos. Quando a página Web é autenticada por meio de certificado digital, o usuário deve verificar sua autenticidade.

• A segurança da conexão deve ser verificada, certificando-se de sua criptografia, entre outros, verificando se o protocolo HTTPS é utilizado na comunicação.

• O usuário deve excluir periodicamente as informações armazenadas nos navegadores: cookies, histórico, senhas, etc.

• É proibida a instalação de complementos e plug-ins não autorizados previamente pelo Grupo Prosegur.

• É proibido o uso de ferramentas de qualquer tipo na nuvem não autorizadas previamente pelo Grupo Prosegur, como armazenar ou compartilhar informações.

• A utilização do acesso à Internet para participar de debates em tempo real (canais de chat/IRC) é expressamente vedada, seja através de websites que preste esses serviços ou de aplicativos instalados em equipamentos (como MS Messenger, TOM, Yahoo, ICQ ou semelhantes).

• Não é permitido utilizar nenhum outro meio de acesso à Internet (por exemplo, modens) que não tenha sido devidamente autorizado pela área de DTI.

• É proibido o uso da Internet para fins que possam influenciar negativamente a imagem do Grupo Prosegur, seus representantes ou terceiros com os quais mantenha relacionamento.

Utilização do e-mail

O e-mail é uma ferramenta que o Grupo Prosegur habilita para as comunicações necessárias como resultado das interações próprias da empresa com outras entidades ou outros usuários. As seguintes diretrizes são estabelecidas em relação ao uso de e-mail:

• O acesso e a utilização destes serviços pelos usuários, bem como os privilégios associados ao acesso a eles, devem se limitar àqueles definidos pelas suas obrigações profissionais.

• Todas as contas de e-mail existentes nos serviços de e-mail da Prosegur pertencem ao Grupo Prosegur.

• Os usuários devem usar apenas as ferramentas e programas de e-mail fornecidos, instalados e configurados pelo Grupo Prosegur.

• No caso de pessoal externo, o uso de endereços externos deve ser previamente aprovado pelo Grupo Prosegur.

• A conta de e-mail é pessoal e intransferível.

• Os usuários são os únicos responsáveis pelas ações realizadas nas suas próprias contas de e-mail.

• Os usuários são responsáveis por proteger suas credenciais de acesso a e-mail.

• A forma e o teor dos e-mails enviados pelos usuários devem corresponder ao código de conduta do o Grupo Prosegur, e não devem ser enviados, em caso algum, e-mails contendo ofensas, ameaças ou assunto de mau gosto.

• Caso seja necessário enviar e-mails para mais de um destinatário, deve-se usar o campo "Com Cópia Oculta (CCO)", de forma a manter a privacidade dos endereços de e-mail dos destinatários.

• A capacidade da caixa de entrada de e-mail é limitada. Quando a cota atribuída for atingida, o sistema informa o usuário sobre esta situação e caberá ao usuário liberar espaço excluindo os e-mails que não sejam necessários para desempenhar suas funções.

• O usuário deverá esvaziar a lixeira diariamente, tendo em vista que os e-mails estão incluídos dentro da cota designada a cada caixa.

• O usuário deve manter todas as suas caixas e pastas organizadas e classificadas. Os e-mails que não tiverem mais utilidade deverão ser excluídos permanentemente.

• Os arquivos anexos com grande número de bytes devem ser compactados antes da remessa.

• Verifique a barra de endereços antes de enviar uma mensagem e responda apenas a quem ela corresponde.

• Sempre que possível, em vez de compartilhar documentos por e-mail, deve ser fornecido um link para o recurso.

• Quando informações críticas ou confidenciais são enviadas, a mensagem deve ser criptografada. Se você se conectar via Web, no final da atividade você fazer logout.

• O e-mail é um dos principais meios de entrada de malware em computadores e sistemas. Por isso, são definidas as regras a seguir:

o Jamais deve-se clicar em links em e-mails ou abrir anexos, a menos que verifique a autenticidade e confiabilidade do e-mail e do conteúdo.
o Não é permitido responder a e-mails não solicitados ou e-mails de origem desconhecida, principalmente se tiver arquivos anexos. Esse tipo de e-mail deve ser eliminado imediatamente.
o Os e-mails que contém arquivos anexos com extensão não permitida (.exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta), ou com extensões aceitáveis que mascarem as não aceitas, devem ser eliminados imediatamente. E-mails contendo arquivos anexos desse tipo não devem ser abertos sob nenhuma circunstância.
o É proibido o registro em serviços e páginas de Internet com contas de e-mail profissionais, exceto em serviços autorizados.
o Ao encaminhar ou responder a um e-mail, todas as informações irrelevantes, como endereços, assinaturas, cabeçalhos, etc. devem ser removidas.
o A visualização da caixa de entrada deve ser desativada.

• Todas as contas de e-mail genéricas e as listas de distribuição estão subordinadas a uma pessoa responsável, que deverá observar as regras a seguir:

o Usar a caixa de correio ou lista de distribuição exclusivamente para o propósito para o qual foi criado (atendimento ao cliente, resposta a solicitações, etc.).
o Recomenda-se incluir uma assinatura corporativa ao enviar e-mails desses tipos de contas.
o O acesso e a utilização dessas contas devem ser autorizados de modo responsável.
o A reputação e a imagem do Grupo Prosegur devem ser protegidas, respondendo às mensagens com cordialidade.
o A validez da autorização outorgada aos usuários deve ser verificada no mínimo 2 vezes por ano.

• Qualquer fato suspeito deve ser comunicado à área de Segurança da Informação Corporativa para que sejam tomadas as providências necessárias. O Grupo Prosegur estabeleceu um botão "Denunciar e-mail" nos aplicativos de e-mail para facilitar esta tarefa.
• O Grupo Prosegur pode monitorar as contas de e-mail que coloca a serviço de seus funcionários, sem notificação prévia, a fim de garantir o uso correto e exploração desse recurso, bem como detectar possíveis incidentes de segurança.

Usos proibidos

• Usar o e-mail para fins comerciais alheios à empresa. Participar da propagação de “correntes”, esquemas piramidais, etc.

• Criar listas de distribuição sem o consentimento da DTI.

• Realizar a distribuição em massa de e-mails com teor inadequado que sejam contrários ao funcionamento correto dos serviços na Internet.

• Enviar ou reenviar mensagens contendo difamações, ofensas ou obscenidades.

• Usar mecanismos e sistemas de phishing ou que ocultem a identidade do emissor do e-mail.

• Enviar qualquer tipo de e-mail de SPAM (são considerados e-mails SPAM aqueles que não estão relacionados aos processos de trabalho).

• Arquivos anexos com extensão .exe, .pif, .scr, .vbs, .cmd, .com, .bat não devem ser enviados, tendo em vista que arquivos desse tipo permitem mascarar vírus e normalmente são usados para propagá-los.

• Divulgar conteúdo ilegal, como, por exemplo ameaças, malware, apologia de terrorismo, pornografia infantil, software ilegal, ou qualquer outro item de natureza criminosa.

Armazenamento compartilhado

Os recursos de armazenamento compartilhado são espaços reservados para a guarda e compartilhamento de documentos e arquivos produzidos como resultado das atividades realizadas profissionalmente pelos membros de um grupo de trabalho.

Todos os usuários que tenham acesso a recursos de armazenamento compartilhado devem observar às regras definidas a seguir:

• O acesso e a utilização, pelos usuários, dos recursos de armazenamento compartilhados, bem como os privilégios relacionados a esse acesso, devem ser limitados àqueles que sejam necessários para o desempenho das suas funções (obedecendo à regra de "necessidade de conhecimento").

• É expressamente proibido armazenar informações pessoais nos recursos de armazenamento compartilhado.

• É proibido armazenar arquivos executáveis ou instaláveis (.exe) em recursos de armazenamento compartilhado sem o devido controle da DTI.

• Não é permitido solicitar um recurso de armazenamento compartilhado para ser usado por uma única pessoa.

• Cabe exclusivamente à DTI prestar suporte e realizar a recuperação de informações contidas nos recursos de armazenamento compartilhado.

• Todos os recursos de armazenamento compartilhado têm com uma pessoa responsável devidamente designada, à qual a autorização de acesso a esses recursos é delegada. Este responsável deve revisar pelo menos a cada 6 meses as permissões de acesso a tal recurso de armazenamento compartilhado. A utilização do espaço atribuído no recurso de armazenamento é de responsabilidade de todas as pessoas autorizadas.

• Se houver a necessidade de conservar informações de histórico, a DTI pode providenciar um meio de armazenamento alternativo que garanta que as informações serão arquivadas.

• Para armazenar dados pessoais nos recursos de armazenamento compartilhado, as medidas técnicas e controles necessários devem ser implantados para garantir o cumprimento da legislação aplicável nesta área.

Uso de certificados e assinatura eletrônica

• É possível que, como parte das atividades do Grupo Prosegur, o usuário utilize certificados e assinaturas eletrônicas. O usuário deve:
o Conhecer e cumprir as condições de uso dos certificados previstos na regulamentação do Grupo Prosegur, bem como as limitações de seu uso de acordo com a legislação aplicável.
o Agir com diligência em relação à custódia e conservação dos dados de assinatura ou certificado ou quaisquer outras informações confidenciais, como chaves, códigos de solicitação de certificado, senhas, etc. incluindo os suportes dos certificados ou do equipamento em que estão localizados.
o NÃO deve-se revelar em nenhuma circunstância os dados mencionados.
o Solicitar a revogação do certificado em caso de suspeita de perda de confidencialidade, divulgação ou uso não autorizado dos dados, notificando a Segurança da Informação pelos métodos estabelecidos.

• Em qualquer caso, o usuário é responsável pelo uso que pode ser dado a tais certificados e sua custódia segura, caso contrário, pode levar à ativação do processo sancionatório aplicável.

Gerenciamento de Incidentes de Segurança

Quando um usuário detecta qualquer tipo de anomalia ou incidente de segurança que possa comprometer a segurança, o uso adequado e/ou o funcionamento dos recursos do computador ou sistemas de informação aos quais ele tenha acesso, bem como as informações e dados pessoais nele contidos, ele é obrigado a informar a Área de Segurança da Informação imediatamente para que sejam tomadas as medidas necessárias documentando a notificação com evidências e documentos disponíveis.

• Deve ser comunicado através dos seguintes canais:
o Por e-mail para o departamento de Segurança da Informação:
seguridad.informacion@prosegur.com

• O usuário 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 for o caso, deve permitir o acesso a ele remotamente para que o pessoal técnico do Grupo Prosegur realize as verificações pertinentes e verifique se pode continuar a usar o recurso com segurança.

DECLARAÇÃO DO USUÁRIO SOBRE O USO DE RECURSOS E SISTEMAS INFORMÁTICOS DA PROSEGUR

O usuário declara:

• Que é responsabilidade do usuário proteger e utilizar os recursos e ferramentas atribuídos de forma responsável, levando sempre em consideração os presentes objetivos profissionais estabelecidos.

• Que é responsabilidade do usuário fazer bom uso dos recursos e dispositivos de propriedade do Grupo Prosegur, utilizando-os para as funções para as quais foram atribuídos, respeitando sua integridade e utilizando-os apenas pela pessoa designada como responsável por eles.

• Que é responsabilidade do usuário ler, entender e agir de acordo com todas as outras regras e documentos de Segurança da Informação, bem como qualquer outro disponibilizado a eles pela Diretoria Geral do Grupo Prosegur.

• Que o usuário deve informar a Área Corporativa de Segurança da Informação 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 de propriedade do Grupo Prosegur, e estão sujeitas a auditoria. Os equipamentos devem ser devolvidos ao Grupo Prosegur a qualquer momento, a pedido deste.

• Que, no desenvolvimento de suas funções, quando o usuário gerencia os recursos de um Cliente, também poderá estar sujeito à Política de Segurança e às normas de segurança que o Cliente teria aprovado se assim exigir, sem prejuízo da obrigação de continuar cumprindo as disposições das regras do Grupo Prosegur.

• O não cumprimento das normas e diretrizes acima mencionadas dá origem às medidas legais a que o Grupo Prosegur poderá recorrer para a preservação de seus direitos com base na legislação e nos acordos pertinentes.

DECLARO QUE LI A PRESENTE E TOMEI CONHECIMENTO DAS NORMAS DE UTILIZAÇÃO DE RECURSOS DE COMPUTAÇÃO DA PROSEGUR, AQUI ESTABELECIDAS.
_____, _____ de _____ de _____

Nome

Documento de Identidade

Assinatura