Cibersegurança - Cláusulas Aplicáveis

Este documento estabelece as cláusulas de cibersegurança que o grupo Naturgy adota ao contratar serviços ou produtos de terceiros, garantindo a segurança cibernética da cadeia de suprimentos.

Quando o serviço ou produto contratado incluir cláusulas específicas de cibersegurança, as quais deverão, em qualquer caso, ter sido negociadas com a área de Cibersegurança do grupo Naturgy, prevalecerá o que for estipulado no contrato ou acordo firmado.

Em caso de dúvidas sobre este documento, o fornecedor pode entrar em contato com seu representante no grupo Naturgy, que, se necessário, envolverá a área de Cibersegurança pertinente a cada situação.

As cláusulas estão organizadas em quatro grupos, de acordo com os tipos de serviços ou produtos contratados. Dependendo da natureza do serviço ou produto, o fornecedor deverá cumprir as cláusulas de um ou mais grupos.

1) Cláusulas gerais

Estas cláusulas são obrigatórias para qualquer serviço ou produto contratado, incluindo aqueles que, por sua natureza, não envolvem o uso de ativos tecnológicos do grupo Naturgy ou o manuseio de informações não públicas do grupo.

Essas medidas visam garantir uma governança eficaz da cibersegurança na cadeia de suprimentos e facilitar a comunicação entre as partes em caso de incidentes.

2) Cláusulas aplicáveis a informações privadas do grupo Naturgy

Estas cláusulas são obrigatórias quando o serviço envolve o tratamento, acesso ou armazenamento de informações da Naturgy que não são de domínio público, incluindo dados pessoais, mesmo que não haja acesso a redes de informação ou infraestrutura tecnológica do grupo. Exemplos não excludentes dessa categoria podem ser: consultorias, assessorias ou serviços SaaS.

Essas medidas visam proteger a disponibilidade, confidencialidade e integridade das informações privadas do grupo Naturgy que são acessadas ou tratadas pelo fornecedor, minimizando o risco de vazamentos de dados.

Se o serviço se enquadrar nesta categoria, será obrigatória a observância das cláusulas do grupo 1).

3) Cláusulas aplicáveis em caso de acesso a redes, sistemas ou infraestrutura tecnológica do grupo Naturgy

Estas cláusulas são obrigatórias para todos os produtos e/ou serviços que exijam e-mail ou usuário do grupo Naturgy, ou acesso a sistemas, redes de informação ou processos industriais, CPDs ou infraestruturas em nuvem do grupo. Exemplos não excludentes deste grupo de clausulas podem ser: serviços de contact center, atendimento de emergências, tecnólogos com acesso a redes industriais, gestão de obras ou operação e manutenção de sistemas de informação e comunicações.

Estas medidas buscam reduzir o risco de que um ciberincidente na cadeia de suprimentos seja propagado para as infraestruturas e sistemas do grupo Naturgy.

Se o serviço se enquadrar neste grupo, será obrigatória a observância das cláusulas dos grupos 1) e 2).

4) Cláusulas aplicáveis em caso de entrega de produtos ou desenvolvimento

Estas cláusulas se aplicam a todos os produtos e/ou serviços em que o fornecedor gera, desenvolve ou fornece produtos específicos, com foco em termos de entrega, qualidade e cumprimento de especificações. Exemplos não excludentes dessa categoria podem ser: fornecedores que desenvolvem software ou equipamentos industriais dentro ou fora das instalações da Naturgy.

Estas medidas visam garantir a cibersegurança na entrega de produtos ao grupo Naturgy.

Se o serviço se enquadrar neste grupo, será obrigatória a observância das cláusulas do grupo 1) e das condições dos grupos 2) e 3), se também forem aplicáveis.

1) Cláusulas gerais

ID	Cláusula
Governo e Regulamentação	
GR_01	O FORNECEDOR se compromete a garantir o cumprimento contínuo de todos os requisitos legais, regulatórios e contratuais aplicáveis à cibersegurança, com especial ênfase às normas relacionadas a infraestruturas críticas, serviços essenciais e proteção de dados. Este compromisso se estende a todas as localizações e infraestruturas onde informações do grupo Naturgy sejam armazenadas, processadas ou transmitidas. Como exemplo, e sem limitar o que foi mencionado anteriormente, o FORNECEDOR deverá cumprir, quando aplicável, as disposições estabelecidas na Diretiva europeia NIS 2 (e sua transposição a nível local), a Lei europeia de Resiliência Cibernética, além de qualquer outra legislação ou norma pertinente à cibersegurança.
GR_02	O FORNECEDOR deve garantir que todas as ferramentas utilizadas para prestar serviços ao grupo Naturgy não violem direitos de propriedade intelectual ou contratual de terceiros.
GR_03	No início do contrato, o FORNECEDOR deverá apontar um responsável por riscos tecnológicos, que será o único ponto de contato com o grupo Naturgy em questões de cibersegurança e se encarregará de zelar pela integridade, confiabilidade e disponibilidade dos sistemas envolvidos no serviço.
GR_04	O FORNECEDOR deverá identificar os potenciais riscos e impactos relacionados ao serviço e implementar as medidas compensatórias necessárias para eliminar ou mitigar esses riscos. As exceções de responsabilidade em cibersegurança deverão ser documentadas no contrato.
GR_05	Se o FORNECEDOR possuir um certificado de padrão de cibersegurança, este deverá ser renovado conforme os prazos estipulados pela certificação e, em caso de perda, o grupo Naturgy deverá ser informado o mais rápido possível.
Treinamento	
FO_01	O FORNECEDOR deverá manter um programa contínuo e atualizado de treinamento e conscientização em cibersegurança, que ajude a mitigar os riscos que possam afetar o serviço prestado ao grupo Naturgy.

ID	Cláusula
FO_02	O FORNECEDOR deverá verificar, antes da contratação, as competências em cibersegurança dos funcionários e prestadores externos para o desempenho de suas funções, fornecendo evidências disso ao grupo Naturgy, caso solicitado.
FO_03	A critério do grupo Naturgy, poderá ser solicitada a participação do FORNECEDOR em treinamentos ou capacitações de cibersegurança, incluindo, mas não se limitando, à participação em exercícios cibernéticos internos que envolvam o serviço contratado.
Segregação de Funções	
SD_01	As informações do grupo Naturgy devem ser acessíveis apenas ao pessoal autorizado para o desempenho de suas funções. O FORNECEDOR deverá manter o acesso às informações da Naturgy (tanto digitais quanto físicas) atualizados e monitorados. Este pessoal, mesmo que subcontratado, deverá estar identificado nominalmente. Os acessos devem ser atribuídos e concedidos com base no princípio do privilégio mínimo (PoLP), utilizando grupos ou funções que definam perfis coletivos, evitando atribuir privilégios diretamente a usuários específicos.
SD_02	O FORNECEDOR deverá ter um procedimento de revisão periódica das permissões e controles de acesso às informações do grupo Naturgy, assegurando que sejam atualizados conforme necessário, com especial atenção à revogação quando não forem mais necessários (por exemplo, em casos de mudança de responsabilidades ou desligamentos).
SD_03	O FORNECEDOR deverá segmentar as redes de sua organização e manter os níveis de segurança adequados em cada um dos segmentos, garantindo que os usuários tenham a conexão mínima necessária para desempenhar suas funções.
Integridade e Confidencialidade	
IC_01	O FORNECEDOR somente acessará as informações do grupo Naturgy quando seja estritamente necessário para a execução do serviço e se compromete a manter a segurança e a confidencialidade absoluta das informações compartilhadas no âmbito da prestação do serviço. Esse acesso deverá ser restrito aos limites de sua finalidade autorizada.
IC_02	O FORNECEDOR apenas armazenará as informações permitidas e se abstém de realizar qualquer armazenamento de informações sem o conhecimento e autorização expressa do grupo Naturgy.

ID	Cláusula
	Adicionalmente, o FORNECEDOR deverá implementar um procedimento para gerenciar a saída de ativos de informação de suas instalações no contexto do serviço do grupo Naturgy, implementando mecanismos para impedir a saída de informações dos dispositivos que processam dados do grupo Naturgy. Caso a operação exija a saída de informações dos sistemas, estas deverão estar devidamente criptografadas.
IC_03	Especificamente, o FORNECEDOR garantirá que as informações do grupo Naturgy não serão transmitidas a terceiros ou a ativos tecnológicos desconhecidos sem a prévia e expressa autorização do grupo Naturgy.
IC_04	O FORNECEDOR deverá garantir o armazenamento e a transmissão criptografados das senhas do serviço oferecido ao grupo Naturgy de forma segura.
IC_05	O FORNECEDOR deverá implementar e manter medidas de segurança adequadas para assegurar a integridade e a imutabilidade dos logs e das cópias de segurança.
IC_06	O FORNECEDOR deverá estabelecer mecanismos que permitam a dissociação, anonimização, ofuscação ou tokenização dos dados ou informações que estão sujeitos a normas e/ou regulamentos pertencentes ao grupo Naturgy.
Segurança Física	
SF_01	O FORNECEDOR deverá estabelecer medidas de segurança adequadas para o armazenamento de informações do grupo Naturgy em formato físico, garantindo um nível de proteção equivalente ao do formato digital.
SF_02	O FORNECEDOR deverá implementar as medidas físicas de segurança necessárias para proteger os ativos de informação, com especial atenção a servidores de bancos de dados e arquivos, a fim de prevenir danos físicos e acessos não autorizados às informações lógicas relacionadas ao serviço prestado ao grupo Naturgy.
SF_03	Ao término do serviço, ou quando necessário em outras circunstâncias, o FORNECEDOR deverá garantir o uso de mecanismos adequados para a destruição ou reciclagem de meios, bem como a eliminação segura das informações relacionadas ao serviço prestado ao grupo Naturgy, tanto em formato físico quanto lógico, para garantir que as transações e outros dados não possam ser recuperados por pessoas não autorizadas.

ID	Cláusula
SF_04	Caso o FORNECEDOR precise de acesso físico às instalações do grupo Naturgy, deverá cumprir com a normativa do grupo Naturgy referente ao acesso físico às suas instalações.
Gestão de Ativos e Operações	
GO_01	O FORNECEDOR deverá identificar seus ativos de informação envolvidos no serviço prestado ao grupo Naturgy, assim como os dados que serão gerenciados e os responsáveis por sua gestão, garantindo sua adequada proteção e registro.
GO_02	O FORNECEDOR terá a responsabilidade de desenvolver e/ou implementar mecanismos de segurança, baseados nas últimas versões de melhores práticas e padrões internacionais, que assegurem o funcionamento ótimo de todos os ativos de informação, incluindo dispositivos móveis e portáteis, e também qualquer nova aquisição ou desenvolvimento de aplicações ou sistemas que sejam usados no serviço contratado pelo grupo Naturgy ou para comunicações com o grupo Naturgy. De maneira singular, mas não excludente, o FORNECEDOR deverá contar com um processo de gestão de vulnerabilidades em seus componentes de hardware ou software, de modo que esses componentes estejam atualizados em relação às versões e, especificamente, que qualquer fraqueza ou vulnerabilidade crítica seja tratada de forma urgente. Essas atualizações de segurança, ou qualquer outra necessária, devem ser testadas em ambientes prévios para avaliar sua efetividade e os potenciais efeitos colaterais sobre o serviço prestado ao grupo Naturgy antes de sua instalação em ambientes produtivos.
GO_03	O FORNECEDOR deverá contar com proteção de antivírus ou EDR permanentemente atualizado em sistemas e equipamentos de usuários envolvidos no serviço prestado ao grupo Naturgy. O acesso à administração dessa ferramenta deverá ser restrito ao pessoal necessário.
GO_04	O FORNECEDOR deverá implementar mecanismos de autenticação que garantam a comunicação inequívoca com o grupo Naturgy.
GO_05	O FORNECEDOR deverá estabelecer mecanismos robustos que assegurem a identidade do remetente nas comunicações com o grupo Naturgy.
GO_06	O FORNECEDOR deverá garantir o correto registro das informações por meio da sincronização horária (NTP) entre todos os componentes do serviço, assim como entre os diferentes elementos de rede e os sistemas associados a eles.

ID	Cláusula
GO_07	O FORNECEDOR deverá realizar tarefas de manutenção na infraestrutura tecnológica utilizada no serviço oferecido ao grupo Naturgy, com o propósito de evitar possíveis danos ou falhas.
Resposta a Incidentes de Cibersegurança	
RI_01	O FORNECEDOR deverá notificar o grupo Naturgy sobre os incidentes de cibersegurança que afetem seus dados e/ou serviços assim que forem detectados. A notificação deverá ser feita de forma a permitir que o grupo Naturgy cumpra os prazos estabelecidos na legislação vigente a cada momento. Especificamente, e de forma não excludente, o FORNECEDOR deverá notificar imediatamente o grupo Naturgy caso detecte ou tenha uma suspeita fundamentada de que os sistemas, suportes ou dados tenham sido comprometidos ou utilizados sem autorização durante a prestação do serviço, assim como qualquer exposição ou vazamento de informações do grupo Naturgy. A notificação deverá ser realizada por e-mail ao SOC do grupo Naturgy (soc@naturgy.com). Caso o e-mail do FORNECEDOR não esteja disponível, deverá entrar em contato por outros meios com seu ponto de contato no grupo Naturgy. Em caso de vazamento de dados, este deverá ser comunicado em paralelo ao seu interlocutor no grupo Naturgy. Na notificação de incidentes de segurança, o FORNECEDOR deverá fornecer todas as informações e evidências que forem requeridas pelo grupo Naturgy em relação ao incidente.
RI_02	Da mesma forma, em caso de um incidente de segurança no grupo Naturgy relacionado ao serviço prestado pelo FORNECEDOR, este deverá oferecer suporte e ajuda em tudo o que for necessário.
RI_03	Para tudo o que foi mencionado anteriormente, o FORNECEDOR deverá dispor de um procedimento de gestão e reporte de incidentes de segurança, que deverá ser revisado e testado periodicamente pelo fornecedor.
Subcontratação ou Quarta Parte	
SC_01	Caso o FORNECEDOR subcontrate uma empresa para a prestação de serviços relacionados a este acordo, o FORNECEDOR se compromete a garantir que tal

ID	Cláusula
	subcontratado cumpra, no mínimo, com os mesmos requisitos de cibersegurança estabelecidos neste documento. Em caso de qualquer descumprimento por parte de um subcontratado, o FORNECEDOR assumirá plena responsabilidade e tomará as medidas corretivas necessárias para sanear qualquer incidente de cibersegurança.
SC_02	O grupo Naturgy se reserva o direito de revisar e aprovar previamente qualquer subcontratado proposto pelo FORNECEDOR. O grupo Naturgy pode, a seu critério, rejeitar a utilização de qualquer subcontratado se determinar que tal subcontratado não cumpre com os requisitos de cibersegurança especificados neste documento, ou se sua participação representar um risco inaceitável para a segurança das informações do grupo Naturgy.
Avaliações de Cibersegurança	
EC_01	O FORNECEDOR poderá ser objeto de revisão para verificar o correto cumprimento das cláusulas incluídas neste contrato e deverá fornecer as evidências e informações necessárias para garantir esse cumprimento. Em caso de descumprimento de alguma das cláusulas deste contrato, o FORNECEDOR deverá aplicar as medidas corretivas necessárias para eliminar ou mitigar o risco detectado.
EC_02	O FORNECEDOR deverá facilitar o cumprimento das obrigações de inspeção, supervisão e revisão do grupo Naturgy, a cargo de: (a) qualquer regulador competente na matéria, (b) a unidade de revisão interna do grupo Naturgy ou qualquer uma de suas unidades locais, seja diretamente ou através de um terceiro designado para tal, e (c) seus auditores no exercício de suas responsabilidades. Isso inclui todos os aspectos dos serviços prestados ao grupo Naturgy e qualquer tipo de informação relacionada. Os responsáveis pela inspeção ou revisão terão acesso livre às instalações, equipamentos, sistemas e documentos do FORNECEDOR, desde que estejam relacionados aos serviços prestados ao grupo Naturgy. As informações obtidas serão confidenciais e tratadas como tal por ambas as partes.
EC_03	As revisões e inspeções realizadas pelo FORNECEDOR ou por seus subcontratados, que envolvam informações do grupo Naturgy, poderão ocorrer durante o horário normal de trabalho, com um aviso prévio mínimo de quinze (15) dias. Esse aviso deve especificar o objetivo e a justificativa da inspeção, a fim

ID	Cláusula
	de minimizar interrupções nos processos de negócios. O FORNECEDOR se compromete a fornecer os recursos necessários para a análise e correção de incidentes, permitindo que o grupo Naturgy investigue os logs de sistemas e outros elementos de segurança, garantindo sua integridade por pelo menos sete (7) dias após a notificação do incidente, além de preservar qualquer evidência que possa ser útil para uma possível análise forense. Caso o grupo Naturgy indique um terceiro para realizar a revisão de cibersegurança, o FORNECEDOR poderá se opor se houver conflito de interesses, e o grupo Naturgy designará outro terceiro com experiência comprovada. Antes da verificação, o FORNECEDOR poderá solicitar um acordo de confidencialidade em termos habituais.
EC_04	Se o serviço ou produto contratado for um SaaS com certificação SOC1, SOC2 do tipo 2 ou ENS (Esquema Espanhol de Segurança) de nível Alto, as partes poderão, de comum acordo, substituir as revisões de cibersegurança pela entrega anual dos relatórios de renovação de certificação.
Inteligência Artificial	
IA_01	Caso o FORNECEDOR deseje utilizar ferramentas que contenham soluções, modelos, sistemas ou componentes de inteligência artificial (doravante denominados "Sistemas de IA"), deverá informar previamente ao Grupo Naturgy antes de iniciar o uso desses Sistemas de IA, estando tal uso condicionado à autorização prévia por escrito do Grupo Naturgy.
IA_02	Quando o FORNECEDOR utilizar, desenvolver ou implementar Sistemas de IA no âmbito da prestação do Serviço, deverá garantir por padrão a aplicação do princípio da minimização dos dados pessoais, de forma que apenas os dados estritamente necessários e indispensáveis sejam tratados, devendo aplicar as técnicas de pseudonimização e anonimização que forem necessárias para assegurar o cumprimento efetivo desse princípio.
IA_03	Em nenhuma hipótese o FORNECEDOR poderá utilizar os dados pessoais de titularidade do Grupo Naturgy para treinar, configurar, melhorar, escalar, desenvolver ou otimizar tais Sistemas de IA.

2) Cláusulas aplicáveis a informações privadas do grupo Naturgy

ID	Cláusula
	Governo e Regulamentação
GR_06	O FORNECEDOR deve estar ciente e cumprir as normas do grupo Naturgy, especialmente as políticas relacionadas à gestão de acesso lógico à informação. É responsabilidade do FORNECEDOR manter-se informado sobre quaisquer mudanças ou atualizações nessas políticas. O FORNECEDOR deve assegurar que todos os subcontratados compreendam e sigam as políticas, procedimentos e controles de cibersegurança estabelecidos pelo grupo Naturgy. De maneira geral, o FORNECEDOR se adaptará, em primeiro lugar, às medidas de proteção já existentes no grupo Naturgy. Se houver algum impedimento para a adoção dessas medidas, o FORNECEDOR deverá justificar ao grupo Naturgy, oferecendo proteção alternativa equivalente ou superior e facilitando os meios para acompanhamento e monitoramento, com as mesmas garantias e abrangências das medidas internas de cibersegurança do grupo Naturgy.
GR_07	Se um serviço ou produto SaaS for contratado do FORNECEDOR, este deve estar devidamente protegido e criptografado, possuindo uma certificação SOC 2 Tipo 2 ou ENS (Esquema Espanhol de Segurança) de nível Alto sobre o serviço contratado. A certificação não será obrigatória caso o serviço ou produto SaaS suporte processos de negócio da Naturgy com BIA (Análise de Impacto nos Negócios) classificado como 'Baixo', embora seja recomendável que tenha ENS de nível médio. Em qualquer caso, sempre que o site for acessado por clientes do grupo Naturgy, deverá contar com um certificado de Extended Validation.
GR_08	Se um serviço ou produto SaaS relevante para o controle interno sobre a informação financeira do grupo Naturgy for contratado, esse serviço ou produto deverá ter uma certificação SOC 1 Tipo 2 sobre o serviço contratado.
	Controle de Acessos
CA_01	O FORNECEDOR deve implementar e comunicar as medidas de segurança lógica perimetral adequadas para proteger as informações dos serviços contratados pelo grupo Naturgy.

ID	Cláusula
CA_02	O FORNECEDOR deve estabelecer e manter um procedimento abrangente de gestão de senhas para os sistemas envolvidos no serviço à Naturgy. Este procedimento deve incluir, entre outros aspectos: 1. Troca obrigatória da senha inicial, 2. Requisitos mínimos de comprimento e complexidade das senhas, 3. Expiração das senhas, 4. Restrições sobre a reutilização de senhas anteriores. Além disso, o FORNECEDOR deve incluir em sua política de gestão de senhas um procedimento de distribuição que garanta que estas sejam conhecidas apenas pelo usuário, para a prestação do serviço oferecido à Naturgy.
CA_03	A infraestrutura tecnológica do FORNECEDOR que armazena ou processa informações do grupo Naturgy deve ter medidas que permitam a separação lógica das informações em caso de infraestruturas compartilhadas com outros clientes ou serviços com múltiplos clientes. Isso garante o isolamento de cada serviço/cliente, evitando a propagação de ataques entre eles.
CA_04	Se o serviço ou produto contratado pelo grupo Naturgy incluir bancos de dados hospedados na infraestrutura do FORNECEDOR, estes devem estar localizados em sistemas distintos dos que executam as aplicações associadas. Além disso, não deve haver comunicação direta da internet para esses bancos de dados, devendo ser utilizado algum componente tecnológico intermediário que gerencie esse acesso.
CA_05	As funções críticas, como administração, do FORNECEDOR devem estar claramente identificadas e separadas das funções não críticas, como operações habituais.
CA_06	O FORNECEDOR deve estabelecer medidas adequadas para garantir que o acesso às ferramentas de administração dos sistemas do serviço oferecido à Naturgy seja estritamente reservado ao pessoal necessário. Dependendo da criticidade da atividade, a Naturgy concordará com o FORNECEDOR sobre a necessidade de empregar uma autenticação robusta, tanto em nível de gestão de senhas quanto em nível de autenticação de dois fatores, para o acesso do pessoal no desempenho de suas funções. Além disso, o FORNECEDOR deve implementar os mecanismos necessários para garantir que o acesso dos administradores aos sistemas de informação que prestam serviço ao grupo Naturgy seja realizado utilizando canais criptografados e autenticação forte.

ID	Cláusula
CA_07	O FORNECEDOR deve implementar mecanismos que garantam o controle e monitoramento contínuo dos acessos remotos ao ambiente tecnológico do serviço oferecido ao grupo Naturgy, a fim de prevenir acessos não autorizados e garantir a segurança da informação.
CA_08	O FORNECEDOR deve monitorar e registrar toda atividade de acesso à informação de propriedade do grupo Naturgy, armazenando os dados dessas atividades de forma adequada por um período mínimo de quinze (15) meses. Essas medidas são especialmente relevantes em caso de acesso a informações identificativas e sensíveis de clientes do grupo Naturgy.
CA_09	O FORNECEDOR deve acordar com o grupo Naturgy um procedimento para a finalização do serviço que inclua aspectos referentes à segurança da informação. Este procedimento deverá incluir pelo menos: 1. A devolução de todos os ativos e informações de propriedade do grupo Naturgy em condições que permitam sua reintegração aos sistemas da Naturgy. 2. A custódia segura dos registros e logs relevantes relacionados ao serviço. 3. A exclusão segura de toda informação do grupo Naturgy armazenada nos sistemas do FORNECEDOR, garantindo que esta não possa ser recuperada ou utilizada posteriormente.
CA_10	O FORNECEDOR garantirá, dentro de seu processo interno de gestão de acessos, que qualquer acesso à informação da Naturgy seja revogado assim que não for mais necessário (por exemplo, em casos de mudança de responsabilidades ou desligamentos no serviço).
CA_11	O FORNECEDOR deve garantir que todos os recursos utilizados para a prestação do serviço possuam autenticação multifator (MFA).
Integridade e Confidencialidade	
IC_07	O envio de informações sensíveis nunca deve ser realizado por e-mail, mas sim através de gateways de comunicação destinados a esse fim entre os sistemas do grupo Naturgy e do FORNECEDOR.
IC_08	O FORNECEDOR deve implementar os controles necessários para assegurar a integridade das informações privadas do grupo Naturgy, ou seja, controles voltados a evitar modificações não autorizadas sobre as informações. Além disso, o FORNECEDOR deve realizar processos de verificação desses controles.

ID	Cláusula
IC_09	No caso específico de informações classificadas como confidenciais, o FORNECEDOR deve assinar um acordo de confidencialidade com o grupo Naturgy e garantir seu cumprimento. O FORNECEDOR deve dispor de procedimentos e mecanismos de classificação da informação, considerando os requisitos legais aplicáveis, bem como a criticidade e sensibilidade de cada tipo de informação. E ajudará na classificação de seus ativos de propriedade ou exploração pelo grupo Naturgy com base na classificação vigente do grupo Naturgy.
IC_10	Nas comunicações com clientes, o FORNECEDOR deve utilizar as ferramentas necessárias para garantir que estas ocorram de maneira a assegurar a integridade das informações enviadas pela Naturgy.
Criptografia e proteção de dados	
CP_01	O FORNECEDOR não utilizará dados ou informações reais do grupo Naturgy em ambientes que não sejam de produção ou de teste autorizados. Caso sejam necessários dados reais, o FORNECEDOR deve obter o consentimento explícito do proprietário e responsável pelos dados.
CP_02	O FORNECEDOR deve ter a capacidade de criptografar as informações do grupo Naturgy utilizando algoritmos de criptografia robustos e reconhecidos. A criptografia deve ser aplicada tanto ao armazenamento temporário quanto permanente dessas informações em seus sistemas. Além disso, o FORNECEDOR deve garantir que os mecanismos de criptografia implementados estejam em conformidade com as normas e padrões de segurança vigentes.
CP_03	O FORNECEDOR deve estabelecer a criptografia dos dados e das comunicações realizadas através de redes públicas e/ou privadas pelas quais transitem informações relativas ao serviço do grupo Naturgy, especialmente quando se tratar de dados confidenciais ou sujeitos a alguma regulamentação, protegendo as informações contra divulgação não autorizada.
Fortificação e Proteção contra ameaças	
BP_01	O FORNECEDOR deve implementar os controles, mecanismos e ferramentas de segurança necessários para a detecção e gestão de ameaças sobre todos os ativos de informação do FORNECEDOR, incluindo aqueles que armazenam ou processam informações do grupo Naturgy, com o objetivo de preveni-las, resolvê-las e alertar ao grupo Naturgy conforme necessário. Essas medidas devem ser revisadas e atualizadas periodicamente para garantir sua efetividade.

ID	Cláusula
BP_02	Concretamente, o FORNECEDOR deve instalar, em qualquer ativo de informação do FORNECEDOR que trate, armazene ou acesse informações da Naturgy, elementos com a capacidade de realizar análises de comportamento, para a detecção e resposta a ameaças desconhecidas (EDR).
Continuidade Tecnológica e de Negócios	
PC_01	O FORNECEDOR se compromete a implementar e manter um plano de continuidade de negócios que garanta a continuidade da prestação do serviço à Naturgy em caso de interrupções significativas. Esse plano deve ser revisado periodicamente para identificar e mitigar possíveis novos riscos que possam afetar a continuidade do negócio e testado regularmente para garantir sua efetividade e realizar ajustes conforme necessário. O FORNECEDOR deve fornecer ao grupo Naturgy relatórios periódicos sobre o estado e a efetividade do programa de continuidade de negócios, bem como qualquer atualização ou mudança significativa no mesmo.
PC_02	O FORNECEDOR deve realizar periodicamente cópias de segurança dos sistemas e/ou informações envolvidos na prestação do serviço ao grupo Naturgy, de forma a permitir sua recuperação em caso de desastre. O FORNECEDOR deve contar com os procedimentos necessários para a geração de cópias de segurança dos dados do serviço que presta ao grupo Naturgy. Essas cópias devem ser armazenadas em locais alternativos aos que suportam a operação habitual.
PC_03	O FORNECEDOR deve implementar as medidas necessárias, tanto físicas quanto lógicas, para assegurar a correta manipulação das cópias de segurança das informações relativas à prestação do serviço do grupo Naturgy. Essas cópias devem ser tratadas e armazenadas corretamente para que possam ser recuperadas sem que a segurança e integridade das informações tenham sido comprometidas durante a cadeia de custódia das mesmas.
PC_04	O FORNECEDOR deve contar com um Plano de Recuperação em Caso de Desastre (DRP) detalhado e atualizado para todos os sistemas envolvidos na prestação do serviço ao grupo Naturgy. Este plano deve incluir procedimentos específicos para a rápida e eficaz restauração dos sistemas críticos em caso de desastres, garantindo a continuidade do serviço. Além disso, o DRP deve contemplar testes periódicos e revisões regulares para garantir sua efetividade e estar em conformidade com as melhores práticas e normas vigentes, pessoal envolvido nos processos de

ID	Cláusula
	recuperação, atividades e responsabilidades detalhadas para cada participante, procedimentos de notificação ao grupo Naturgy e matriz de escalonamento para a tomada de decisões. Ademais, o FORNECEDOR deve capacitar seu pessoal para a execução deste plano visando minimizar o impacto de qualquer interrupção no serviço.
PC_06	O FORNECEDOR deve implementar cópias de segurança imutáveis e offline para proteger os dados.

3) Cláusulas aplicáveis em caso de acesso a redes, sistemas ou infraestrutura tecnológica do grupo Naturgy

ID	Cláusula
	Segurança em Redes e Conectividade
RC_01	O acesso às infraestruturas e sistemas do grupo Naturgy deve ser realizado em conformidade com as políticas vigentes, incluindo, quando necessário, as diretrizes de segurança industrial baseadas na norma IEC-62443 para acessos a redes de processos industriais. A solução geral para acesso aos sistemas do grupo Naturgy que não estão disponíveis na Internet será a abordagem de Zerotrust, que o grupo Naturgy disponibilizará ao terceiro, e que este deverá utilizar.
RC_02	O FORNECEDOR, em sua área de responsabilidade, deve implementar os mecanismos necessários para assegurar que as comunicações entre sua infraestrutura e a do grupo Naturgy preservem a confidencialidade, integridade e disponibilidade das informações, limitando-se às necessidades do serviço prestado.
RC_03	Dependendo do tipo de acesso, as políticas de acesso às redes e sistemas do grupo Naturgy poderão exigir que o FORNECEDOR implemente controles adicionais de cibersegurança para os terminais de acesso utilizados na prestação do serviço. Isso inclui, mas não se limita a instalação de componentes de segurança atualizados e com características mínimas em seus dispositivos. O grupo Naturgy se reserva o direito de aplicar técnicas de análise de risco para o dispositivo e o usuário que desejam se conectar aos ativos do grupo, negando o acesso caso o risco de conexão seja considerado inaceitável pelos algoritmos de análise de risco automatizados. Essas análises serão realizadas por meio de técnicas de "acesso condicional" e "postura". Isso pode incluir, entre outras opções, a exigência de uso de MFA para acesso aos ativos, dependendo do contexto de cibersegurança e gestão de riscos que o grupo considerar adequado, sendo responsabilidade do FORNECEDOR garantir que todos os recursos envolvidos na prestação do serviço possam se autenticar utilizando múltiplos fatores.
RC_04	O FORNECEDOR deve notificar imediatamente o grupo Naturgy sobre qualquer usuário sob sua responsabilidade que deixe de prestar serviço e que tenha acesso lógico aos sistemas do grupo, para que o grupo possa realizar o processo de desativação na sua área de responsabilidade.
RC_05	Como parte dos planos de resposta a ameaças e incidentes do grupo Naturgy, os acessos do FORNECEDOR a ativos e redes poderão ser suspensos ou restringidos caso seja identificado que a situação do FORNECEDOR representa uma ameaça à segurança dos ativos do grupo.

ID	Cláusula
RC_06	Se o FORNECEDOR acessar os sistemas do grupo Naturgy, deverá colaborar, no mínimo, nas provas periódicas do DRP (Plano de Recuperação de Desastres) do grupo.

4) Cláusulas aplicáveis em caso de entrega de produtos ou desenvolvimento

ID	Cláusula
Produto ou Desenvolvimento Seguro	
	En caso de que o escopo dos trabalhos do FORNECEDOR inclua o desenvolvimento de software, este será realizado conforme as melhores práticas de segurança estabelecidas em frameworks reconhecidos internacionalmente e acordados entre ambas as partes, garantindo a implementação de medidas de segurança desde as fases iniciais do ciclo de vida do desenvolvimento de software, incluindo a validação e sanitização de dados, a autenticação e autorização seguras, e a proteção de dados sensíveis por meio de criptografia.
PD_01	O FORNECEDOR deve fornecer informações técnicas sobre os recursos que disponibilizará ao grupo Naturgy, visando a realização de testes de compatibilidade de aplicações antes da implementação. Em caso de modificações substanciais (atualizações, melhorias, patches...) nas certificações ou medidas de segurança aplicáveis ao serviço prestado, o FORNECEDOR deve fornecer as informações necessárias para que o grupo possa resolver possíveis incidentes decorrentes dessas modificações. Em especial, o FORNECEDOR deve garantir a compatibilidade de atualizações, patches e configurações com o restante do sistema, por meio de validações de fabricantes ou apresentando evidências de compatibilidade em ambientes não produtivos.
PD_02	O FORNECEDOR deve comunicar imediatamente qualquer mudança ou perda nas certificações ou aprovações de cibersegurança e proteção de dados, sendo responsável pelos danos que isso possa causar ao grupo Naturgy. Além disso, o FORNECEDOR deve apresentar o alinhamento de seu produto e serviço com qualquer certificação internacional e/ou nacional que seja recomendável ou necessária para a implementação do produto em um ambiente industrial ou de TI pertencente ao grupo.
PD_03	O FORNECEDOR deve estabelecer controles de segurança em relação à aquisição ou desenvolvimento de novas aplicações ou sistemas para a prestação do serviço ao grupo Naturgy. Deve haver segmentação entre os ambientes de desenvolvimento, testes e produção para os aplicativos do serviço. Qualquer revisão de segurança, desenvolvimento, atualização ou compra de componentes do sistema incorporado ao serviço deve ser realizada em ambientes distintos ao de produção.
PD_04	Caso o FORNECEDOR realize desenvolvimentos de software, deverá aplicar técnicas e padrões alinhados com as melhores práticas de desenvolvimento seguro

ID	Cláusula
	estabelecidas em frameworks reconhecidos internacionalmente, garantindo a implementação de medidas de segurança desde as fases iniciais do ciclo de vida de desenvolvimento de software, incluindo validação e higienização de dados, autenticação e autorização seguras, e proteger dados confidenciais por meio de criptografia
PD_05	No caso de o FORNECEDOR fornecer produtos ou projetos de caráter industrial, estes devem estar alinhados com as arquiteturas de cibersegurança industrial do grupo e com padrões industriais de cibersegurança, especificamente com a norma IEC 62443, incluindo, mas não se limitando a: 1. Segmentação entre redes. 2. Acessos remotos para operação e manutenção. 3. Gestão de antivírus, robustez e/ou patching. 4. Ciclo de vida. Essas medidas devem ser revisadas e atualizadas prioritariamente e periodicamente para garantir sua eficácia. O FORNECEDOR deve indicar os riscos e contramedidas relacionadas ao produto e sua integração com as infraestruturas da Naturgy. Do ponto de vista da cibersegurança, deve responder explicitamente às seguintes perguntas: 1. Quais são os riscos do produto e/ou solução? 2. Quais riscos podem surgir ao integrar o produto com as infraestruturas da Naturgy? 3. Quais medidas são aplicadas para proteger tanto o produto quanto a infraestrutura dos riscos identificados anteriormente?
PD_06	Todo software desenvolvido ou entregue pelo FORNECEDOR deve passar por análises de vulnerabilidades com ferramentas reconhecidas como SAST e DAST antes de sua entrega à Naturgy para implementação em ambientes produtivos.
PD_07	O FORNECEDOR validará a segurança das integrações com as infraestruturas do grupo Naturgy, garantindo que não comprometam a operação nem a cibersegurança dos sistemas existentes.

Glossário de termos e abreviações

- **AES-256:** Padrão de Criptografia Avançada.
- **DAST:** Teste Dinâmico de Segurança de Aplicações.
- **DRP:** (Disaster Recovery Plan) Plano de Recuperação de Desastres.
- **ENS:** Esquema Nacional de Segurança espanhol.
- **EDR:** Detecção e Resposta em Endpoints.
- **GDPR:** Regulamento Geral sobre a Proteção de Dados.
- **IEC-62443:** Padrão global para a segurança cibernética em sistemas industriais.
- **MFA:** Autenticação Multifatorial.
- **NTP:** Protocolo de Tempo de Rede.
- **PoLP:** Princípio do Mínimo Privilégio.
- **Postura:** Conformidade de um dispositivo com os controles de cibersegurança estabelecidos, avaliada para verificar se atende aos requisitos mínimos para acessar uma rede ou sistema.
- **SaaS:** Software como Serviço.
- **SAST:** Teste Estático de Segurança de Aplicações.
- **SOC:** Centro de Operações de Segurança.
- **SOC 1:** Relatório que analisa os controles internos de uma organização relacionados à elaboração de relatórios financeiros.
- **SOC 2 Tipo 2:** Relatório que examina os controles internos de uma organização sobre segurança, disponibilidade, integridade, confidencialidade e privacidade.
- **TLS 1.2:** Transport Layer Security 1.2.
- **Zero trust:** Modelo de segurança que elimina a confiança implícita, exigindo verificação contínua da identidade e permissões de todos os usuários e dispositivos.