Segurança cibernética - Cláusulas aplicáveis

Este documento estabelece as cláusulas de cibersegurança aplicáveis pelo grupo Naturgy na contratação de serviços ou produtos de terceiros, de forma a garantir a cibersegurança da sua cadeia de abastecimento.

Este conjunto de cláusulas está estruturado em quatro blocos de acordo com as tipologias dos serviços ou produtos contratados. Dependendo do tipo de serviço ou produto, o fornecedor deve cumprir as cláusulas de um ou mais blocos.

1) Cláusulas Gerais

Cumprimento obrigatório de qualquer serviço ou produto contratado, incluindo aqueles que, por sua natureza, não envolvam o uso de ativos tecnológicos do grupo Naturgy ou o tratamento de informações não públicas do grupo Naturgy.

Essas medidas visam garantir a governança da segurança cibernética na cadeia de suprimentos que garanta a continuidade do serviço prestado ao grupo Naturgy e a comunicação entre ambas as partes em caso de possíveis incidentes de segurança cibernética.

2) Cláusulas aplicáveis ao lidar com informações privadas do grupo Naturgy

Conformidade quando o serviço processa, acessa ou armazena informações da Naturgy que não são acessíveis ao público, incluindo informações pessoais, mesmo que as redes de informações ou infraestrutura tecnológica do grupo Naturgy não sejam acessadas. Exemplos, mas não exclusivos, desta categoria podem ser: assessorias, consultorias ou serviços SaaS

Estas medidas destinam-se a salvaguardar a disponibilidade, confidencialidade e integridade das informações privadas do grupo Naturgy acessíveis ou geridas pelo fornecedor, minimizando o risco de fugas de informação.

3) Cláusulas aplicáveis ao acesso a redes, sistemas ou infraestrutura tecnológica do grupo Naturgy

Conformidade para todos os produtos e/ou serviços que exijam um endereço de e-mail ou usuário do grupo Naturgy ou acesso a sistemas, redes de informação ou processos industriais, data centers ou infraestruturas em nuvem do grupo Naturgy. Exemplos, mas não exclusivos, desta categoria podem ser: serviços de contact center, atendimento de emergência, tecnólogos com acesso a redes industriais, gerenciamento de construção, operação e manutenção de sistemas de informação e comunicação, etc.

Essas medidas visam minimizar o risco de um incidente cibernético na cadeia de suprimentos ser transmitido às infraestruturas e sistemas do grupo Naturgy

Caso o serviço corresponda a este grupo, as cláusulas do grupo 2 também devem ser cumpridas.

4) Cláusulas aplicáveis à entrega de um produto ou desenvolvimento

De aplicação geral para 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 das especificações. Exemplos, mas não exclusivos, desta categoria podem ser: fornecedores que geram desenvolvimentos de software ou equipamentos industriais dentro ou fora das instalações da Naturgy,

Essas medidas buscam garantir a segurança cibernética básica na entrega de produtos ao grupo Naturgy.

Se o serviço satisfizer as condições deste grupo, deve cumprir as condições dos grupos 2 e 3, se também lhe forem aplicáveis.

Caso o serviço ou produto contratado tenha uma cláusula específica, que deve em qualquer caso ter sido acordada com a Cibersegurança do grupo Naturgy, prevalecerão as disposições do contrato ou acordo contratual.

Para qualquer dúvida sobre este documento, o fornecedor pode entrar em contato com sua pessoa de contato no grupo Naturgy, que envolverá a função de Cibersegurança do grupo Naturgy aplicável em cada caso, se necessário.

1) Cláusulas Gerais:

ID	Cláusula
Legislação e Regulamentação	
CU_01	O FORNECEDOR deve manter sempre o cumprimento dos requisitos legais, regulamentares ou contratuais relacionados com a cibersegurança, com especial enfoque nos que se referem a infraestruturas críticas ou serviços essenciais, e proteção de dados, incluindo os de natureza pessoal, em todos os locais e infraestruturas onde a sua informação é armazenada e tratada.
CU_02	O FORNECEDOR deve garantir que todas as ferramentas utilizadas para fornecer o serviço ao grupo Naturgy não violem a propriedade intelectual ou qualquer regulamento, contrato, direito ou interesse na propriedade de terceiros.
Governança (GO)	
GO_01	No início do contrato, o FORNECEDOR deverá nomear um gerente de risco tecnológico, que será o único interlocutor com o grupo Naturgy em matéria de segurança cibernética e será responsável por garantir a integridade, confiabilidade e disponibilidade dos sistemas envolvidos no serviço.
GO_02	O FORNECEDOR deve identificar os possíveis riscos e impactos que possam existir no serviço, auxiliando na validação das medidas compensatórias adotadas para eliminar ou mitigar o risco. Qualquer excepcionalidade de responsabilidade em segurança cibernética deve ser incluída e detalhada no contrato.
Formação (FO)	
FO_01	O FORNECEDOR deve ter um programa de treinamento/conscientização sobre segurança da informação regularmente, que permita que seus funcionários e/ou subcontratados saibam a ação correta em qualquer suspeita de violação da segurança da informação. Também garante que a equipe envolvida na prestação do atendimento ao cliente conheça e siga os regulamentos internos de segurança cibernética aplicáveis ao processamento correto das informações do grupo Naturgy que eles tratam no serviço.
FO_02	O FORNECEDOR deve verificar, antes da contratação, o treinamento em segurança cibernética dos funcionários/partes externas e fornecer evidências disso ao grupo Naturgy.
FO_03	A critério do grupo Naturgy, poderá ser solicitada a participação do FORNECEDOR em treinamentos de cibersegurança, incluindo, mas não se limitando, à participação em exercícios cibernéticos internos envolvendo o serviço contratado.
Custódia de informações (CI)	
CI_01	O FORNECEDOR apenas terá acesso às informações do grupo Naturgy para a prestação do serviço e compromete-se a manter a segurança das informações transferidas no contexto da prestação do serviço.

ID	Cláusula
CI_02	O FORNECEDOR armazenará apenas as informações permitidas e se absterá de armazenar qualquer informação sem o conhecimento e autorização expressa do grupo Naturgy. Além disso, o fornecedor deve implementar um procedimento para gerenciar a saída de ativos de informação de suas instalações dentro do serviço do grupo Naturgy. Devem ser implementados mecanismos para evitar a saída de informações dos dispositivos que processam as informações do grupo Naturgy. Caso a operação exija a saída de informações dos sistemas, ela deve ser criptografada.
CI_03	O FORNECEDOR deve tratar os dados e informações do grupo Naturgy com absoluta confidencialidade e cumprir sempre as instruções recebidas pelo grupo Naturgy em relação à sua finalidade, conteúdo, uso e processamento.
CI_04	Especificamente, o FORNECEDOR garantirá que as informações do grupo Naturgy não serão transmitidas a terceiros ou ativos tecnológicos desconhecidos sem a autorização prévia e expressa do grupo Naturgy.
Segurança física (SF)	
SF_01	O FORNECEDOR deve estabelecer medidas de segurança adequadas para o armazenamento das informações do grupo Naturgy em formato físico, garantindo um nível de proteção equivalente ao do formato digital.
SF_02	O FORNECEDOR deve implementar as medidas de segurança física necessárias para proteger os ativos de informação, a fim de evitar danos físicos e acesso não autorizado a informações lógicas relacionadas ao serviço oferecido ao grupo Naturgy.
SF_03	O FORNECEDOR deve garantir a utilização de mecanismos adequados para a destruição ou reciclagem de suportes, bem como a eliminação segura da informação relacionada com o serviço prestado ao grupo Naturgy.
SF_04	O FORNECEDOR deve remover e destruir de forma adequada e segura todas as instâncias de quaisquer informações ou dados do grupo Naturgy e material impresso relacionado para garantir que as transações e outros dados não possam ser recuperados por pessoas não autorizadas.
SF_05	Caso o FORNECEDOR necessite de acesso físico às instalações do grupo Naturgy, deverá cumprir os regulamentos do grupo Naturgy relativos ao acesso físico às suas instalações.
Medidas técnicas (MT)	
MT_01	O FORNECEDOR deve identificar os seus ativos de informação envolvidos no serviço ao Grupo Naturgy, os dados que serão geridos e os responsáveis pela sua gestão.

ID	Cláusula
MT_02	Em geral, o FORNECEDOR adaptar-se-á em primeira instância às medidas de proteção existentes no grupo Naturgy, caso se verifique algum impedimento que não permita a sua adoção, o FORNECEDOR deverá justificá-lo ao grupo Naturgy e fornecer a mesma ou maior proteção e fornecer os meios para o seu acompanhamento e monitorização com as mesmas garantias e alcance das medidas internas de cibersegurança do grupo Naturgy.
MT_03	O FORNECEDOR será responsável por desenvolver e/ou implementar mecanismos de segurança, baseados nas últimas versões das melhores práticas e padrões internacionais, que garantam o funcionamento ideal de todos os ativos de informação, incluindo dispositivos móveis e portáteis, e também incluindo qualquer nova aquisição ou desenvolvimento de aplicativos ou sistemas que sejam utilizados no serviço contratado por, ou para comunicações com o Grupo Naturgy. Singularmente, mas não exclusivamente, o FORNECEDOR deve ter um processo de gerenciamento de vulnerabilidades em seus componentes de hardware ou software, para que esses componentes sejam atualizados em termos de versões e, especificamente, qualquer fraqueza ou vulnerabilidade crítica neles seja tratada com urgência Tais atualizações de segurança, ou quaisquer outras atualizações necessárias, antes de serem instaladas em ambientes de produção, devem ser testadas em ambientes anteriores para avaliar sua eficácia e potenciais efeitos colaterais no serviço prestado ao grupo Naturgy.
MT_04	O FORNECEDOR deve ter proteção antivírus ou EDR (end point detection & response) permanentemente atualizada nos sistemas e equipamentos do usuário envolvidos no serviço prestado ao grupo Naturgy. O acesso à administração desta ferramenta deve ser restrito ao pessoal-chave.
MT_05	O FORNECEDOR deve implementar mecanismos de autenticação que garantam uma comunicação inequívoca com o grupo Naturgy.
MT_06	O FORNECEDOR deve estabelecer mecanismos que garantam a identidade do remetente nas comunicações com o grupo Naturgy.
MT_07	As informações do grupo Naturgy só devem ser acessíveis por pessoal autorizado para o desempenho de suas funções. O FORNECEDOR deve manter-se atualizado e monitorar as permissões de acesso às informações da Naturgy (em formato digital ou físico). Este pessoal, mesmo que tenha sido subcontratado, deve ser identificado pelo nome. As permissões devem ser atribuídas/concedidas de acordo com o princípio do menor privilégio (PoLP, também conhecido como Princípio do Menor Privilégio ou Princípio da Menor Autoridade). Os privilégios devem ser atribuídos/concedidos por meio do uso de grupos ou funções (ou seja, perfis que identificam grupos e não privilégios atribuídos a um usuário específico). O FORNECEDOR assegurará, no âmbito do seu processo interno de gestão de acessos, que qualquer acesso às informações da Naturgy é revogado quando não for mais necessário (por exemplo, em casos de mudança de responsabilidades ou cancelamentos de serviço)

ID	Cláusula
	Os mecanismos de vigilância e garantia devem medir e monitorar o processo para garantir que os requisitos legais, estatutários, regulamentares ou contratuais relacionados à segurança cibernética e proteção de dados sejam cumpridos, incluindo aqueles de natureza pessoal
MT_08	O FORNECEDOR deve ter um procedimento de revisão periódica sobre as permissões e controles de acesso configurados nos sistemas que atendem ao grupo Naturgy.
MT_09	O FORNECEDOR deve garantir o armazenamento seguro e a transmissão criptografada das senhas do serviço oferecido ao grupo Naturgy.
MT_10	O FORNECEDOR deve garantir o correto registo da informação através da sincronização temporal (NTP) entre todos os componentes do serviço, bem como entre os diferentes elementos da rede e os sistemas a ela associados.
MT_11	O FORNECEDOR deve ter segmentado as redes da sua organização e manter os níveis de segurança necessários em cada um dos segmentos de rede. Os usuários devem ter uma conexão mínima necessária permitida para realizar suas próprias funções.
MT_12	O FORNECEDOR deve estabelecer mecanismos que permitam a dissociação, anonimização, ofuscação ou tokenização de dados ou informações que estejam sujeitos a regras e/ou regulamentos pertencentes ao grupo Naturgy.
MT_13	O FORNECEDOR deve realizar tarefas de manutenção na infraestrutura tecnológica utilizada no serviço oferecido ao grupo Naturgy, a fim de evitar possíveis danos ou avarias.
MT_14	O FORNECEDOR deve implementar e manter medidas de segurança apropriadas para garantir a integridade e imutabilidade dos logs e backups.
Resposta a incidentes cibernéticos (GI)	
GI_01	O FORNECEDOR deve notificar o grupo Naturgy sobre incidentes de segurança cibernética que afetem seus dados e/ou serviços, assim que forem detectados. A notificação será feita de forma a permitir que o grupo Naturgy cumpra os prazos estabelecidos na legislação em vigor em todos os momentos. Especificamente, e sem limitação, o FORNECEDOR deve notificar imediatamente o grupo Naturgy no caso de detectar ou ter uma suspeita fundada de que os sistemas, mídias ou dados foram comprometidos ou usados sem autorização na prestação do serviço, bem como qualquer exposição ou vazamento de informações do grupo Naturgy Esta notificação será feita por e-mail para o SOC do grupo Naturgy (soc@naturgy.com). Caso o e-mail do FORNECEDOR não esteja disponível, você deve entrar em contato com o ponto de contato do grupo Naturgy por outros meios. Em caso de vazamento de dados, você precisará se comunicar em paralelo com seu interlocutor no grupo Naturgy.

ID	Cláusula
	O FORNECEDOR deve fornecer todas as informações e evidências exigidas pelo grupo Naturgy em relação ao incidente. Para isso, o FORNECEDOR normalmente terá um procedimento de gerenciamento e reporte de incidentes de segurança, que deve ser revisado e testado pelo fornecedor periodicamente.
GI_02	Da mesma forma, em caso de incidente de segurança no grupo Naturgy relacionado ao serviço prestado pelo FORNECEDOR, este deve prestar apoio e ajuda em tudo o que for necessário.
Gestão e Terceirização de Terceiros (GT)	
GT_01	Caso o FORNECEDOR contrate uma empresa subcontratada para a prestação de serviços relacionados a este contrato, o FORNECEDOR se compromete a garantir que tal subcontratado cumpra, no mínimo, os mesmos requisitos de segurança cibernética aqui estabelecidos. O FORNECEDOR deve garantir que todos os subcontratados entendam e cumpram as políticas, procedimentos e controles de segurança cibernética especificados pelo grupo Naturgy. Em caso de violação por parte de um subcontratado, o FORNECEDOR assumirá total responsabilidade e tomará as medidas corretivas necessárias para resolver qualquer incidente de segurança cibernética.
GT_02	O grupo Naturgy reserva-se o direito de revisar e aprovar antecipadamente qualquer subcontratado proposto pelo FORNECEDOR. O grupo Naturgy pode, a seu exclusivo critério, recusar o uso de qualquer subcontratado se determinar que tal subcontratado não cumpre os requisitos de segurança cibernética especificados neste documento, ou se sua participação representar um risco inaceitável para a segurança da informação do grupo Naturgy.
Revisões e auditorias de segurança cibernética (AU)	
AU_01	O FORNECEDOR poderá ser sujeito a auditorias nas quais se verifique o correto cumprimento das cláusulas incluídas neste contrato e deverá fornecer as provas e informações necessárias para garantir tal cumprimento das mesmas. Em caso de incumprimento de alguma das cláusulas incluídas no presente contrato, o FORNECEDOR deverá aplicar as medidas corretivas necessárias para eliminar ou mitigar o risco detectado.
AU_02	O FORNECEDOR facilitará o cumprimento das obrigações de inspeção, supervisão e auditoria do grupo Naturgy, através do seguinte: (a) qualquer regulador competente na matéria, (b) a unidade de auditoria interna do grupo Naturgy ou qualquer uma de suas unidades locais, diretamente ou por meio de um terceiro designado para esse fim, e (c) seus auditores no exercício de suas responsabilidades. Esta obrigação abrange todos os aspectos dos serviços prestados ao grupo Naturgy, incluindo qualquer tipo de ativo de informação. Isso inclui todos os aspectos dos serviços prestados ao grupo Naturgy e qualquer informação relacionada. Os responsáveis pela inspeção ou auditoria terão livre acesso às instalações, equipamentos, sistemas e documentos do FORNECEDOR, desde que relacionados aos serviços do grupo Naturgy. As informações obtidas serão confidenciais e tratadas como tal por ambas as partes.

ID	Cláusula
AU_03	As auditorias e inspeções ao FORNECEDOR ou aos seus subcontratados, onde são tratadas informações do grupo Naturgy, podem ser realizadas durante o horário normal de trabalho e com um pré-aviso mínimo de 15 (quinze) dias, especificando a finalidade e a justificativa, para minimizar as interrupções nos processos de negócio. O FORNECEDOR deverá fornecer os recursos necessários para a análise e correção de incidentes, permitindo ao grupo Naturgy investigar os logs dos sistemas e outros elementos de segurança, garantindo sua integridade por pelo menos 7 (sete) dias a partir da notificação do incidente, e salvaguardará qualquer evidência útil para uma possível cópia forense. Se o grupo Naturgy nomear um terceiro para a revisão da segurança cibernética, o FORNECEDOR poderá se opor em caso de conflito de interesses, e o grupo Naturgy nomeará outro terceiro com experiência credenciada. Antes da verificação, o FORNECEDOR pode exigir um acordo de confidencialidade nos termos habituais.
AU_04	Caso o FORNECEDOR seja auditado, o relatório final será enviado a ele pelo grupo Naturgy. O FORNECEDOR deve corrigir as deficiências de controle identificadas no referido relatório, seguindo os planos de ação acordados entre ambas as partes.
AU_05	Caso o serviço ou produto contratado seja um SaaS que possua certificação SOC1 ou SOC2 tipo 2, de comum acordo entre as partes, as auditorias poderão ser substituídas pela entrega anual de relatórios de renovação da certificação

2) Cláusulas aplicáveis ao lidar com informações privadas do grupo Naturgy:

ID	Cláusula
Segmentação lógica e acesso às informações da Naturgy	
CA_01	O FORNECEDOR deve estar ciente e cumprir a regulamentação de segurança cibernética estabelecido no grupo Naturgy para a prestação do serviço, em particular, e não exclusivamente, no que diz respeito ao gerenciamento de acesso lógico. É responsabilidade do FORNECEDOR manter-se atualizado sobre quaisquer alterações ou atualizações em tais regulamentos internos de segurança cibernética. De uma forma muito única, mas não exclusiva, será necessária a instalação, em qualquer ativo que trate ou armazene informação da Naturgy, elementos com capacidade para realizar análises comportamentais, para a deteção e resposta a ameaças desconhecidas (EDR)
CA_02	Caso um serviço ou produto SaaS seja contratado do FORNECEDOR, ele deverá estar devidamente protegido e criptografado, com certificação SOC 2 Tipo 2 sobre o serviço contratado. Sempre que este website for acedido por clientes do grupo Naturgy, deverá ter um certificado de Validação Alargada.
CA_03	Caso seja contratado um serviço ou produto SaaS relevante para o controle interno das informações financeiras do grupo Naturgy, além disso, o referido serviço ou produto deve ter uma certificação SOC 1 tipo 2 sobre o serviço contratado.
CA_04	O FORNECEDOR deve implementar e comunicar as medidas de segurança lógicas perimetrais adequadas para proteger as informações dos serviços contratados pelo grupo Naturgy.
CA_05	O FORNECEDOR deve estabelecer um procedimento de gerenciamento de senhas para os sistemas envolvidos no serviço à Naturgy. Este procedimento deve exigir, entre outros aspectos, a alteração da senha inicial, um comprimento mínimo, nível de complexidade das chaves e que defina a expiração das senhas ou o número de registros para evitar a reutilização. Além disso, o FORNECEDOR deve incluir em sua política de gerenciamento de senhas um procedimento de distribuição de senhas, que garanta que elas sejam conhecidas apenas pelo usuário, para a prestação do serviço oferecido à Naturgy.
CA_06	A infraestrutura tecnológica do FORNECEDOR que armazena ou processa informações do grupo Naturgy deve ter medidas que permitam a separação lógica das informações no caso de infraestruturas compartilhadas com outros clientes ou serviços com vários clientes. Além disso, garantindo o isolamento de cada serviço/cliente para evitar a propagação de ataques entre clientes.
CA_07	Caso o serviço ou produto contratado necessite de um banco de dados hospedado na infraestrutura do FORNECEDOR, deve-se levar em consideração que esse banco de dados deve estar localizado em um sistema diferente daquele em que o aplicativo é executado. Além

ID	Cláusula
	disso, não deve haver comunicação direta da internet com essa(s) base(s) de dados e deve fazer uso de qualquer componente tecnológico intermediário.
CA_08	As funções críticas do FORNECEDOR devem ser identificadas e separadas das funções não críticas.
CA_09	O FORNECEDOR deve estabelecer medidas suficientes e necessárias para garantir que o acesso às ferramentas de administração do sistema do serviço oferecido à Naturgy seja estritamente reservado ao pessoal-chave. Dependendo da criticidade da atividade, a Naturgy concordará com o FORNECEDOR sobre a necessidade de usar autenticação robusta, tanto no nível de gerenciamento de senhas quanto no nível de dois fatores, no acesso do pessoal para desempenhar suas funções. Além disso, o FORNECEDOR deve implementar os mecanismos necessários para garantir que o acesso dos administradores aos sistemas de informação que prestam serviços ao Grupo Naturgy seja realizado por meio de canais criptografados e autenticação forte
CA_10	O FORNECEDOR deve implementar os mecanismos necessários para garantir que o acesso remoto ao ambiente tecnológico do serviço oferecido ao grupo Naturgy seja controlado e monitorado.
CA_11	O FORNECEDOR deve monitorar e registrar toda a atividade de acesso às informações de propriedade do grupo Naturgy, e armazenar os dados dessa atividade de forma adequada por um período mínimo de quinze (15) meses. Essas medidas são especialmente relevantes no caso de acesso a informações de identificação e sensíveis dos clientes do grupo Naturgy.
CA_12	O FORNECEDOR deve acordar com o grupo Naturgy um procedimento para a rescisão do serviço que inclua aspectos relacionados à segurança da informação. Deve incluir pelo menos: a devolução de qualquer ativo de informação que pertença ao grupo Naturgy em condições que permitam ao grupo Naturgy incorporar informações em seus sistemas e infraestruturas, garantindo sua integridade, disponibilidade e confidencialidade durante o processo, custódia de logs, exclusão segura de todas as informações do grupo Naturgy hospedadas em ativos do FORNECEDOR no final do processo.
Segurança física (SF)	
SF_01	O FORNECEDOR deve alojar todos os servidores de bases de dados, servidores de arquivos e repositórios de sua propriedade que contenham informação do grupo Naturgy em locais com segurança física reforçada. O FORNECEDOR deve garantir o equivalente se sua cadeia de suprimentos também armazenar informações da Naturgy.

ID	Cláusula
Integridade e confidencialidade (IC)	
IC_01	O envio de informações sensíveis nunca deve ser feito por e-mail, mas por meio de gateways de comunicação destinados a esse fim entre os sistemas do grupo Naturgy e o FORNECEDOR.
IC_02	O FORNECEDOR deve implementar os controles necessários para garantir a integridade das informações privadas do grupo Naturgy. Ou seja, controles destinados a impedir modificações não autorizadas nas informações. Além disso, o FORNECEDOR deve realizar processos de verificação dos referidos controles
IC_03	No caso específico de informações classificadas como confidenciais, o FORNECEDOR deverá assinar um acordo de confidencialidade com o grupo Naturgy e garantir sua conformidade. 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 pertencentes ou operados pelo grupo Naturgy com base na classificação atual do grupo Naturgy.
IC_04	Nas comunicações com os clientes, o FORNECEDOR deve utilizar as ferramentas necessárias para controlar que estas ocorram de forma a garantir a integridade das informações enviadas pela Naturgy.
Criptografia e ofuscação de informações (CF)	
CF_01	O FORNECEDOR não utilizará dados ou informações reais do grupo Naturgy em ambientes que não sejam de produção ou testes autorizados. Caso sejam necessários dados reais, o FORNECEDOR deverá ter o consentimento explícito do titular e responsável pelos dados
CF_02	O FORNECEDOR deve ter a capacidade de criptografar as informações do grupo Naturgy usando algoritmos de criptografia robustos e reconhecidos. Essa criptografia deve ser aplicada ao armazenamento temporário e permanente dessas informações em seus sistemas. Além disso, o FORNECEDOR deve garantir que os mecanismos de criptografia implementados estejam em conformidade com os regulamentos e padrões de segurança vigentes.
CF_03	O FORNECEDOR deve estabelecer a encriptação dos dados e comunicações realizadas através de redes públicas e/ou privadas e através das quais trafegam as informações relacionadas com o serviço do grupo Naturgy, especialmente quando se trata de dados confidenciais ou dados sujeitos a qualquer regulamentação. Protegendo informações contra divulgação não autorizada

ID	Cláusula
Bastioning e proteção contra ameaças (BP)	
BP_01	O FORNECEDOR deve implementar os controles, mecanismos e ferramentas de segurança necessários para a detecção e gestão da ameaça a todos os ativos de informação do FORNECEDOR, com o objetivo de preveni-los e resolvê-los e, no caso de ameaças avançadas e complexas, alertar o grupo Naturgy quando forem detectados. Eles devem revisar periodicamente as configurações de seus sistemas de informação que armazenam ou processam informações do grupo Naturgy.
Continuidade Tecnológica (CT)	
CT_01	O FORNECEDOR deve fazer periodicamente cópias de segurança dos sistemas envolvidos na prestação do serviço ao grupo Naturgy, a fim de permitir a sua recuperação em caso de desastre. O FORNECEDOR deve ter os procedimentos necessários para gerar cópias de segurança dos dados do serviço que presta ao grupo Naturgy. Essas cópias devem ser armazenadas em locais alternativos àqueles que suportam as operações usuais.
CT_02	O FORNECEDOR deve implementar as medidas necessárias, tanto físicas como lógicas, para garantir o correto tratamento das cópias de segurança das informações relativas à prestação do serviço do grupo Naturgy. Essas cópias devem ser tratadas e armazenadas corretamente para serem recuperadas sem que a segurança e integridade das informações sejam comprometidas durante a cadeia de custódia das mesmas.
CT_03	O FORNECEDOR deve ter um Plano de Recuperação de Desastres (DRP) detalhado e atualizado para todos os sistemas envolvidos na prestação do serviço ao grupo Naturgy. Este plano deve incluir procedimentos específicos para o restabelecimento rápido e eficaz dos sistemas críticos em caso de catástrofes, garantindo a continuidade do serviço. Além disso, o DRP deve incluir testes periódicos e revisões regulares para garantir sua eficácia e estar de acordo com as melhores práticas e regulamentos atuais, pessoal envolvido nos processos de recuperação, atividades e responsabilidades detalhadas para cada participante, procedimentos de notificação ao grupo Naturgy e árvore de dimensionamento para tomada de decisão. Da mesma forma, o FORNECEDOR deve treinar seu pessoal na execução deste plano para minimizar o impacto de qualquer interrupção no serviço.

3) Cláusulas aplicáveis ao acesso a redes, sistemas ou infraestrutura tecnológica do grupo Naturgy:

ID	Cláusula
AN_01	O acesso às infraestruturas e sistemas do grupo Naturgy deve ser realizado de acordo com as políticas do grupo em vigor em todos os momentos, incluindo, nos casos em que o acesso às redes de processos industriais é necessário, as políticas de segurança industrial do grupo Naturgy, com base na norma IEC-62443. Especificamente, a solução geral para acesso aos sistemas do grupo Naturgy não publicados na Internet será a solução Zerotrust que o grupo Naturgy disponibilizará ao terceiro e que o terceiro deverá utilizar.
AN_02	O FORNECEDOR, dentro de sua área de responsabilidade, deve implementar os mecanismos necessários para garantir que as comunicações entre sua infraestrutura e a do grupo Naturgy preservem a confidencialidade, integridade e disponibilidade das informações, limitadas às necessidades do serviço.
AN_03	Dependendo da modalidade de acesso, as políticas de acesso à rede e ao sistema do grupo Naturgy podem exigir que o FORNECEDOR tenha controles adicionais de segurança cibernética para os terminais de acesso envolvidos na prestação do serviço. Incluindo, mas não se limitando a, ter certos componentes de segurança atualizados instalados em suas estações de trabalho com uma série de características mínimas. Especificamente, o grupo Naturgy reserva-se o direito de aplicar técnicas de análise de risco ao dispositivo e ao usuário que deseja se conectar a ativos do grupo Naturgy, não permitindo o acesso se o risco de conexão for considerado inadmissível pelos algoritmos automatizados de análise de risco. Essas análises de risco serão realizadas usando técnicas de "acesso condicional" e "postura"
AN_04	O FORNECEDOR deve notificar o grupo Naturgy sobre os usuários que deixam de prestar o serviço e têm acesso lógico aos sistemas do grupo Naturgy, para que o grupo Naturgy possa realizar o processo de cancelamento de registro em sua área de responsabilidade.
AN_05	Como parte dos planos de resposta a ameaças e planos de resposta a incidentes do grupo Naturgy, o acesso do FORNECEDOR aos ativos e redes do grupo Naturgy pode ser suspenso ou restrito caso seja detectado que a situação do FORNECEDOR representa uma ameaça à segurança dos ativos do grupo Naturgy.
AN_06	Caso o FORNECEDOR acesse os sistemas do grupo Naturgy, deve pelo menos considerar sua colaboração nos testes periódicos do DRP (Plano de Recuperação de Desastres) do grupo Naturgy.

4) Cláusulas aplicáveis quando um produto ou desenvolvimento é entregue (PD):

ID	Cláusula
PD_01	O FORNECEDOR deve fornecer informações técnicas sobre os recursos que atenderá ao grupo Naturgy, para que os testes de compatibilidade de aplicativos possam ser realizados antes da implementação. Em caso de modificações substanciais (atualizações, melhorias, patches, etc.) nas certificações ou medidas de segurança aplicáveis ao serviço prestado ao grupo Naturgy, o FORNECEDOR deverá prestar as informações necessárias ao grupo Naturgy para poder resolver quaisquer possíveis incidentes decorrentes dessas modificações. Em particular, o FORNECEDOR deve ter meios que garantam a compatibilidade de atualizações, patches e configurações com o resto do sistema, através de validações do fabricante ou fornecendo evidências de compatibilidade em ambientes não produtivos.
PD_02	O FORNECEDOR deve comunicar imediatamente qualquer alteração ou perda nas certificações ou aprovações de segurança cibernética e proteção de dados das marcas, e será responsável por quaisquer danos que possam ser causados 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 recomendada ou necessária para a implementação ou implantação do produto em um ambiente industrial ou de TI de propriedade do grupo Naturgy.
PD_03	O FORNECEDOR deve estabelecer controles de segurança em relação à aquisição ou desenvolvimento de novos aplicativos ou sistemas para a prestação do serviço oferecido ao grupo Naturgy. Deve ter uma segmentação entre os ambientes de desenvolvimento, teste e produção para as aplicações do serviço do grupo Naturgy. Eles devem realizar qualquer tipo de revisão de segurança, desenvolvimento, atualização ou compra de qualquer componente do sistema incorporado ao serviço prestado ao grupo Naturgy em ambientes diferentes da produção.
PD_04	Caso o FORNECEDOR realize desenvolvimentos de software, deverá aplicar técnicas e padrões alinhados com as boas práticas de desenvolvimento seguro, para as aplicações oferecidas ao grupo Naturgy.
PD_05	Caso o FORNECEDOR forneça produtos ou projetos de natureza industrial ao grupo Naturgy, estes devem estar alinhados com as arquiteturas de cibersegurança industrial do grupo Naturgy e com as normas de cibersegurança industrial e especificamente com a Norma IEC 62443, especificamente, e não exclusivamente, em: 1. Segmentação entre redes. 2. Acesso remoto para operação e manutenção. 3. Gerenciamento, robustez e/ou aplicação de patches de antivírus. 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 relacionados ao produto e sua integração com as infraestruturas da Naturgy.

ID	Cláusula
	Do ponto de vista da segurança cibernética, você precisará responder explicitamente às seguintes perguntas: 1. Quais são os riscos do produto e/ou solução? 2. Que riscos podem surgir ao integrar o produto com as infraestruturas da Naturgy? 3. Que medidas estão em vigor para proteger o produto e a infraestrutura dos riscos acima identificados?