Ciberseguridad - Cláusulas Aplicables

El presente documento establece el clausulado de ciberseguridad aplicable por el grupo Naturgy en la contratación de servicios o productos de terceros, con objeto de asegurar la ciberseguridad de su cadena de suministro.

Dicho Clausulado se estructura en cuatro bloques atendiendo a tipologías de los servicios o productos contratados. En función del tipo de servicio o producto, el proveedor deberá cumplir las cláusulas de uno o varios bloques.

1) **Cláusulas generales**
   De obligado cumplimiento para cualquier servicio o producto contratado, incluidos aquellos que por su naturaleza no impliquen el uso de activos tecnológicos del grupo Naturgy ni manejo de información no pública del grupo Naturgy.

   Con estas medidas se persigue el aseguramiento de un gobierno de la ciberseguridad en la cadena de suministro que garantice la continuidad del servicio prestado al grupo Naturgy, y la comunicación entre ambas partes en caso de potenciales incidentes de ciberseguridad.

2) **Cláusulas aplicables cuando se trate información privada del grupo Naturgy**
   De cumplimiento cuando el servicio trate, acceda o almacene información de Naturgy no accesible de manera pública, incluida aquella de carácter personal, aun en el caso de que no se acceda a redes de información o infraestructura tecnológica del grupo Naturgy. Ejemplos, no excluyentes, de esta categoría pueden ser: consultorías, asesorías o servicios SaaS

   Con estas medidas se persigue salvaguardar la disponibilidad, confidencialidad e integridad de la información privada del grupo Naturgy accesible o gestionada por el proveedor, minimizando el riesgo de fugas de información.

3) **Clausulas aplicables cuando se acceda a redes, sistemas o infraestructura tecnológica del grupo Naturgy**
   De cumplimiento para todos aquellos productos y/o servicios que requieran una dirección de correo electrónico o usuario del grupo Naturgy o acceso sistemas, redes de información o de proceso industrial, CPDs o infraestructuras en cloud del grupo Naturgy. Ejemplos, no excluyentes, de esta categoría pueden ser: servicios de contact center, atención de urgencias, tecnólogos con acceso a redes industriales, gestión de obras, operación y mantenimiento de sistemas de información y comunicaciones, etc.

   Con estas medidas se persigue minimizar el riesgo de que un ciberincidente en la cadena de suministro, se transmita a las infraestructuras y sistemas del grupo Naturgy

   En caso de que el servicio corresponda a este grupo, de manera obligatoria deberá también cumplirse el clausulado del grupo 2).

4) **Clausulas aplicables a la entrega un producto o desarrollo**
   De aplicación general para todos los productos y/o servicios en los que el proveedor genera, desarrolla o suministra productos específicos, enfocándose en términos de entrega, calidad y cumplimiento de especificaciones. Ejemplos, no excluyentes, de esta categoría pueden ser: proveedores que generen desarrollos de software o equipamiento industrial dentro o fuera de las instalaciones de Naturgy,

Con estas medidas se busca la ciberseguridad de base en la entrega de productos al grupo Naturgy.

En caso de que el servicio cumpla las condiciones de este grupo, deberá cumplir las condiciones de los grupos 2 y 3 si también le son de aplicación.

En caso de que el servicio o producto contratado tenga un clausulado específico, que deberá en cualquier caso haberse acordado con Ciberseguridad del grupo Naturgy, prevalecerá lo indicado en el contrato o en el acuerdo contractual.

Para cualquier consulta al respecto del presente documento, el proveedor puede dirigirse a su contacto en el grupo Naturgy, que en caso necesario involucrará a la función de Ciberseguridad del grupo Naturgy aplicable en cada caso.

1) Clausulas generales

ID	Cláusula
Legislación y Regulación	
CU_01	El PROVEEDOR deberá mantener en todo momento el cumplimiento de requisitos legales, regulatorios o contractuales referidos a ciberseguridad, con especial foco en aquellos referidos a infraestructuras críticas o servicios esenciales, y a protección de datos, incluidos aquellos de carácter personal, en todas las ubicaciones e infraestructuras donde se almacene y procese su información.
CU_02	El PROVEEDOR deberá asegurarse de que todas las herramientas utilizadas para prestar el servicio al grupo Naturgy no violan la propiedad intelectual o cualquier regulación, contrato, derecho o interés sobre la propiedad de terceros.
Gobernanza	
GO_01	Al inicio del contrato, el PROVEEDOR deberá designar un responsable de riesgo tecnológico, que será el interlocutor único con el grupo Naturgy en materia de ciberseguridad y se encargará de velar por la integridad, fiabilidad y disponibilidad de los sistemas involucrados en el servicio.
GO_02	El PROVEEDOR deberá identificar los posibles riesgos e impactos que puedan existir en el servicio ayudando a validar las medidas compensatorias que se adopten para eliminar o mitigar el riesgo. Toda excepcionalidad de responsabilidad en ciberseguridad deberá quedar recogida y detallada en el contrato.
Formación	
FO_01	El PROVEEDOR deberá contar con un programa de formación/concienciación en materia de seguridad de la información de forma periódica, que permita a sus empleados y/o subcontratistas conocer la actuación correcta en cualquier sospecha de incumplimiento en materia de seguridad de la información. Asegurándose, además, de que el personal que interviene en la prestación del servicio al cliente conoce y sigue la normativa interna de ciberseguridad aplicable al correcto tratamiento de la información del grupo Naturgy que manejan en el servicio.
FO_02	PROVEEDOR deberá verificar, de forma previa a la contratación, la formación en ciberseguridad de los empleados/externos y facilitar evidencia de ello al grupo Naturgy.
FO_03	A consideración del grupo Naturgy, se podrá solicitar la participación del PROVEEDOR en formaciones o capacitaciones de ciberseguridad, incluyendo, sin carácter excluyente, la participación en ciberejercicios internos que impliquen al servicio contratado.
Custodia de Información	
CI_01	El PROVEEDOR únicamente accederá a la información del grupo Naturgy para la prestación del servicio y se compromete a mantener la seguridad de la información transferida en el contexto de la prestación del servicio.
CI_02	El PROVEEDOR solo almacenará la información permitida y se abstendrá de realizar cualquier almacenamiento de información sin el conocimiento y autorización expresa del grupo Naturgy. Adicionalmente, el proveedor deberá implementar procedimiento para gestionar la salida de activos de información de sus instalaciones dentro del servicio del grupo Naturgy.

ID	Cláusula
	Debiendo implementar mecanismos para impedir la salida de información de los dispositivos que procesan la información del grupo Naturgy. En caso de que la operación requiera la salida de información de los sistemas, esta deberá estar cifrada.
CI_03	El PROVEEDOR deberá tratar los datos e información del grupo Naturgy con absoluta confidencialidad y cumplir en todo momento con las instrucciones recibidas por el grupo Naturgy en relación con su finalidad, contenido, uso y tratamiento.
CI_04	En concreto, El PROVEEDOR garantizará que la información del grupo Naturgy no será transmitida a terceros o activos tecnológicos desconocidos sin la autorización previa y expresa del grupo Naturgy.
Seguridad Física	
SF_01	El PROVEEDOR deberá establecer medidas de seguridad adecuadas para el almacenamiento de información del grupo Naturgy en formato físico, garantizando un nivel de protección equivalente al del formato digital.
SF_02	El PROVEEDOR deberá implementar las medidas físicas de seguridad necesarias para proteger los activos de información, a fin de prevenir daños físicos y accesos no autorizados a la información lógica relacionada con el servicio ofrecido al grupo Naturgy.
SF_03	El PROVEEDOR deberá garantizar el uso de mecanismos adecuados para la destrucción o reciclaje de medios, así como la eliminación segura de la información relacionada con el servicio prestado al grupo Naturgy.
SF_04	PROVEEDOR tiene que eliminar y destruir de formas adecuada y segura todas las instancias de cualquier información o datos del grupo Naturgy y material impreso relacionado para garantizar que las transacciones y otros datos no puedan ser recuperados por personas no autorizadas.
SF_05	En caso de que el PROVEEDOR precise de acceso físico a las instalaciones del grupo Naturgy, este deberá de cumplir con la normativa del grupo Naturgy referente al acceso físico de sus instalaciones.
Medidas Técnicas	
MT_01	El PROVEEDOR deberá identificar sus activos de información implicados en el servicio al Grupo Naturgy, los datos que se gestionarán y los responsables de su gestión.
MT_02	De manera general, el PROVEEDOR se adaptará en primera instancia a las medidas de protección existentes en el grupo Naturgy, en caso de existir algún impedimento que no permita adoptarlas, el PROVEEDOR deberá justificarlo ante el grupo Naturgy y proporcionando la misma protección o superior y facilitar los medios para su seguimiento y monitorización con la mismas garantías y alcances que las medidas internas de ciberseguridad del grupo Naturgy.
MT_03	El PROVEEDOR tendrá la responsabilidad de desarrollar y/o implementar mecanismos de seguridad, basados en últimas versiones de mejores prácticas y estándares internacionales, que aseguren el funcionamiento óptimo de todos los activos de información, incluidos los dispositivos móviles y portátiles, e incluyendo asimismo cualquier nueva adquisición o desarrollo de aplicaciones o sistemas que se usen en el servicio contratado por, o para comunicaciones con el Grupo Naturgy. De manera singular pero no excluyente, el PROVEEDOR deberá contar con un proceso de gestión de vulnerabilidades en sus componentes de hardware o software, de manera que dichos componentes se encuentren actualizados en cuanto a versiones y, en concreto, se trate cualquier debilidad o vulnerabilidad crítica sobre los mismos de manera urgente

ID	Cláusula
	Dichas actualizaciones de seguridad, o cualquier otra necesaria, antes de su instalación en entornos productivos, deben probarse en entornos previos para evaluar su efectividad y los potenciales efectos colaterales sobre el servicio que se presta al grupo Naturgy.
MT_04	El PROVEEDOR deberá contar con una protección de antivirus o EDR (end point detection & response) permanentemente actualizado en sistemas y equipos de usuario implicados en el servicio prestado al grupo Naturgy. El acceso a la administración de esta herramienta deberá estar restringido al personal clave.
MT_05	PROVEEDOR deberá implementar mecanismos de autenticación que garanticen la comunicación inequívoca con el grupo Naturgy.
MT_06	El PROVEEDOR deberá establecer mecanismos que aseguren la identidad del remitente en las comunicaciones con el grupo Naturgy.
MT_07	La información del grupo Naturgy solo debe ser accesible por el personal autorizado para el desarrollo de sus funciones. El PROVEEDOR deberá mantener actualizados y vigilar los permisos de acceso a la información de Naturgy (en formato digital o físico). Este personal, incluso si fuera subcontratado, debe estar identificado nominalmente. Los permisos deben asignarse / otorgarse de acuerdo con el principio de privilegio mínimo (PoLP (Principle of Least Privilege), también conocido como el Principio de Privilegio Mínimo o el Principio de Mínima Autoridad). Los privilegios se deben asignar / otorgar mediante el uso de grupos o roles (es decir, perfiles que identifican grupos y no privilegios asignados a un usuario específico). El PROVEEDOR asegurará, dentro de su proceso interno de gestión de accesos, que cualquier acceso a información de Naturgy es revocado una vez no sea necesario (por ejemplo, en casos de cambio de responsabilidades o bajas en el servicio) Los mecanismos de vigilancia y aseguramiento deben medir y monitorizar el proceso asegurando que se cumple con los requisitos legales, estatuarios, regulatorios o contractuales referidos a ciberseguridad y protección de datos, incluidos aquellos de carácter personal
MT_08	El PROVEEDOR deberá disponer de un procedimiento de revisión periódica sobre los permisos y controles de acceso configurados en los sistemas que dan servicio al grupo Naturgy.
MT_09	El PROVEEDOR deberá garantizar el almacenamiento y transmisión cifrado de las contraseñas del servicio ofrecido al grupo Naturgy de forma segura.
MT_10	PROVEEDOR deberá garantizar el correcto registro de la información mediante la sincronización horaria (NTP) entre todos los componentes del servicio, así como entre los distintos elementos de red y los sistemas asociados a la misma.
MT_11	El PROVEEDOR deberá tener segmentadas las redes de su organización y mantener los niveles de seguridad necesarios en cada uno de los segmentos de red. Debiendo tener los usuarios una conexión mínima necesaria permitida para desarrollar las funciones propias.
MT_12	El PROVEEDOR deberá establecer mecanismos que permitan la disociación, anonimización, ofuscación o tokenización de los datos o información que están sujetos a normas y/o regulaciones pertenecientes al grupo Naturgy.

ID	Cláusula
MT_13	El PROVEEDOR deberá realizar tareas de mantenimiento sobre la infraestructura tecnológica utilizada en el servicio ofrecido al grupo Naturgy, con el propósito de evitar posibles daños o averías.
MT_14	El PROVEEDOR deberá implementar y mantener medidas de seguridad adecuadas para asegurar la integridad y la inmutabilidad de los logs y las copias de seguridad.
Respuesta a Ciberincidentes	
GI_01	El PROVEEDOR deberá notificar al grupo Naturgy los incidentes de ciberseguridad que afecten a sus datos y/o servicios, tan pronto como estos sean detectados. La notificación se realizará de manera que permita al grupo Naturgy cumplir con los tiempos establecidos en la legislación vigente en cada momento. En concreto, y con carácter no excluyente, El PROVEEDOR deberá notificar inmediatamente al grupo Naturgy en el caso de que se detecte o se tenga una sospecha fundada de que los sistemas, soportes o datos hayan sido comprometidos o utilizados sin autorización dentro de la prestación del servicio, así como cualquier exposición o fuga de información del grupo Naturgy Dicha notificación se realizará mediante e-mail al SOC del grupo Naturgy (soc@naturgy.com). En caso de que el email del PROVEEDOR no estuviera disponible, deberá contactar por otros medios con su punto de contacto del grupo Naturgy. En el caso de fuga de datos, deberá comunicarse en paralelo a su interlocutor en el grupo Naturgy. El PROVEEDOR deberá aportar cuanta información y evidencias sean requeridas por el grupo Naturgy en relación con el incidente. Para ello, típicamente el PROVEEDOR dispondrá de un procedimiento de gestión y reporte de incidentes de seguridad, que debe ser revisado y ensayado por el proveedor periódicamente.
GI_02	Igualmente, en caso de un incidente de seguridad en el grupo Naturgy relacionado con el servicio prestado por PROVEEDOR, este deberá dar soporte y ayuda en todo lo requerido.
Gestión de Terceros y Subcontratación	
GT_01	En el caso de que el PROVEEDOR contrate a una empresa subcontratista para la prestación de servicios relacionados con el presente acuerdo, el PROVEEDOR se compromete a garantizar que dicho subcontratista cumpla, como mínimo, con los mismos requisitos de ciberseguridad establecidos en este documento. El PROVEEDOR deberá asegurarse de que todos los subcontratistas entiendan y se adhieran a las políticas, procedimientos y controles de ciberseguridad especificados por el grupo Naturgy. En caso de cualquier incumplimiento por parte de un subcontratista, el PROVEEDOR asumirá la plena responsabilidad y tomará las medidas correctivas necesarias para resolver cualquier incidencia de ciberseguridad.
GT_02	El grupo Naturgy se reserva el derecho de revisar y aprobar previamente a cualquier subcontratista propuesto por el PROVEEDOR. El grupo Naturgy puede, a su entera discreción, rechazar la utilización de cualquier subcontratista si determina que dicho subcontratista no cumple con los requisitos de ciberseguridad especificados en este documento, o si su participación representa un riesgo inaceptable para la seguridad de la información del grupo Naturgy.
Revisiones y auditorías de ciberseguridad	

ID	Cláusula
AU_01	El PROVEEDOR podrá ser susceptible de ser objeto de auditorías en las que se verifique el correcto cumplimiento de las cláusulas incluidas en el presente contrato y tendrá que aportar las evidencias e información necesarias para garantizar dicho cumplimiento de estas. En caso del no incumplimiento de alguna de las cláusulas incluidas en el presente contrato, el PROVEEDOR deberá aplicar las medidas correctoras necesarias para eliminar o mitigar el riesgo detectado.
AU_02	El PROVEEDOR deberá facilitar el cumplimiento de las obligaciones de inspección, supervisión y auditoría del grupo Naturgy, a cargo de: (a) cualquier regulador competente en la materia, (b) la unidad de auditoría interna del grupo Naturgy o cualquiera de sus unidades locales, ya sea directamente o a través de un tercero designado para ello, y (c) sus auditores en el ejercicio de sus responsabilidades. Esta obligación abarca todos los aspectos de los servicios proporcionados al grupo Naturgy, incluyendo cualquier tipo de activo de información. Esto incluye todos los aspectos de los servicios prestados al grupo Naturgy y cualquier tipo de información relacionada. Los encargados de la inspección o auditoría tendrán acceso libre a las instalaciones, equipos, sistemas y documentos del PROVEEDOR, siempre que estén relacionados con los servicios para el grupo Naturgy. La información obtenida será confidencial y tratada como tal por ambas partes.
AU_03	Las auditorías e inspecciones del PROVEEDOR o sus subcontratistas, donde se maneje información del grupo Naturgy, podrán realizarse durante el horario habitual de trabajo y con un preaviso mínimo de siete (15) días, especificando el objeto y justificación, para minimizar interrupciones en los procesos de negocio. El PROVEEDOR proporcionará los recursos necesarios para el análisis y corrección de incidencias, permitiendo al grupo Naturgy investigar los logs de sistemas y otros elementos de seguridad, asegurando su integridad durante al menos siete (7) días desde la notificación de la incidencia, y custodiará cualquier evidencia útil para una posible copia forense. Si el grupo Naturgy designa a un tercero para la revisión de ciberseguridad, el PROVEEDOR podrá oponerse en caso de conflicto de intereses, y el grupo Naturgy designará a otro tercero con experiencia acreditada. Antes de la verificación, el PROVEEDOR podrá requerir un acuerdo de confidencialidad en términos habituales.
AU_04	En caso de que El PROVEEDOR sea auditado, desde el grupo Naturgy se le remitirá el informe final. El PROVEEDOR deberá subsanar las debilidades de control identificadas en dicho informe, siguiendo los planes de acción acordados entre ambas partes.
AU_05	En caso de que el servicio o producto contratado sea un SaaS que tenga una certificación SOC1 o SOC2 de tipo 2, de común acuerdo entre las partes, las auditorías podrán ser sustituidas por la entrega anual de los informes de renovación de certificación

2) Cláusulas aplicables cuando se trate información privada del grupo Naturgy

ID	Cláusula
Segmentación lógica y acceso a la información de Naturgy	
CA_01	El PROVEEDOR deberá conocer y cumplir el cuerpo normativo de ciberseguridad establecido en el grupo Naturgy para la prestación del servicio, en especial, y de manera no exclusiva, en lo relativo a gestión de acceso lógico. Es responsabilidad del PROVEEDOR mantenerse actualizado respecto a cualquier cambio o actualización en dichas normativas internas de ciberseguridad. De manera muy singular, pero no excluyente, se requerirá la instalación, en cualquier activo que trate o almacene información de Naturgy, elementos con la capacidad de realizar análisis de comportamiento, para la detección y respuesta ante amenazas no conocidas (EDR)
CA_02	En caso de que se contrate un servicio o producto SaaS al PROVEEDOR, este deberá estar correctamente securizado y cifrado, contando con una certificación SOC 2 Tipo 2 sobre el servicio contratado. Siempre que dicha web sea accedida por clientes del grupo Naturgy deberá contar con un certificado Extended Validation.
CA_03	En caso de que se contrate un servicio o producto SaaS que sea relevante para el control interno sobre la información financiera del grupo Naturgy, de manera adicional dicho servicio o producto deberá tener una certificación SOC 1 tipo 2 sobre el servicio contratado.
CA_04	El PROVEEDOR deberá implementar y comunicar las medidas de seguridad lógica perimetral adecuadas para proteger la información de los servicios contratados por el grupo Naturgy.
CA_05	El PROVEEDOR deberá establecer un procedimiento de gestión de contraseñas para los sistemas involucrados en el servicio a Naturgy. Este procedimiento deberá requerir, entre otros aspectos, el cambio de la contraseña inicial, una longitud mínima, nivel de complejidad de las claves y que defina la caducidad de las contraseñas o el número de registros para evitar la reutilización. Adicionalmente, el PROVEEDOR deberá incluir en su política de gestión de contraseñas un procedimiento de distribución de las mismas, que garantice que éstas únicamente son conocidas por el usuario, para la prestación del servicio ofrecido a Naturgy.
CA_06	La infraestructura tecnológica del PROVEEDOR que almacene o trate información del grupo Naturgy, deberá disponer de medidas que permitan la separación lógica de información en caso de infraestructuras compartidas con otros clientes o servicios con múltiples clientes. Garantizando, además, de esta manera el aislamiento de cada servicio/cliente para evitar la propagación de ataques entre clientes.
CA_07	En caso de que el servicio o producto contratado requiera una base de datos alojada en infraestructura del PROVEEDOR se deberá tener en cuenta que esta base de datos deberá ubicarse en un sistema distinto al de ejecución de la aplicación. Adicionalmente, no deberá haber una comunicación directa desde internet a esta(s) base(s) de datos debiendo hacer uso de algún componente tecnológico intermedio.
CA_08	Las funciones críticas del PROVEEDOR deberán estar identificadas y separadas de las funciones no críticas.

ID	Cláusula
CA_09	El PROVEEDOR deberá establecer las medidas suficientes y necesarias para asegurar que el acceso a las herramientas de administración de sistemas del servicio ofrecido a Naturgy está estrictamente reservado para personal clave. En función de la criticidad de la actividad, Naturgy acordará con PROVEEDOR la necesidad de emplear una autenticación robusta, tanto a nivel de gestión de contraseñas como a nivel de doble factor, en el acceso del personal para el desempeño de sus funciones. Adicionalmente, el PROVEEDOR deberá implementar los mecanismos necesarios para asegurar que el acceso de administradores a los sistemas de información que prestan servicio al Grupo Naturgy se realicen empleando canales cifrados y autenticación fuerte
CA_10	El PROVEEDOR deberá implementar los mecanismos necesarios para asegurar que los accesos remotos al entorno tecnológico del servicio ofrecido al grupo Naturgy sean controlados y monitorizados.
CA_11	El PROVEEDOR deberá monitorizar y registrar toda la actividad de acceso a información de propiedad del grupo Naturgy, y almacenar los datos de dicha actividad de forma adecuada a un periodo mínimo de quince (15) meses. Estas medidas son especialmente relevantes, en caso de acceder a información identificativa y sensible de clientes del grupo Naturgy,
CA_12	El PROVEEDOR deberá acordar con el grupo Naturgy un procedimiento para la finalización del servicio que incluya aspectos referentes a la seguridad de la información. Debiendo incluir al menos: la devolución de cualquier activo de información que sea del grupo Naturgy en condiciones que permitan al grupo Naturgy la incorporación de información a sus sistemas e infraestructuras, asegurando su integridad, disponibilidad y confidencialidad durante el proceso, custodia de logs, borrado seguro toda la información del grupo Naturgy alojada en activos del PROVEEDOR al final del proceso.
Seguridad física	
SF_01	El PROVEEDOR deberá alojar todos los servidores de bases de datos, servidores de archivos y repositorios de su propiedad que contengan información del grupo Naturgy en ubicaciones con seguridad física reforzada. El PROVEEDOR deberá asegurar lo equivalente si su cadena de suministro también almacena información de Naturgy.
Integridad y Confidencialidad	
IC_01	El envío de información sensible nunca deberá realizarse a través de correo electrónico, sino a través de pasarelas de comunicación destinadas a tal fin entre los sistemas del grupo Naturgy y del PROVEEDOR.
IC_02	El PROVEEDOR deberá implementar los controles necesarios para asegurar la integridad de la información privada del grupo Naturgy. Es decir, los controles orientados a evitar modificaciones no autorizadas sobre la información. Además, el PROVEEDOR deberá realizar procesos de verificación de dichos controles
IC_03	En el caso específico de información clasificada como confidencial, el PROVEEDOR deberá firmar un acuerdo de confidencialidad con el grupo Naturgy y garantizar su cumplimiento. El PROVEEDOR deberá disponer de procedimientos y mecanismos de clasificación de la información, considerando los requisitos legales aplicables, así como la criticidad y sensibilidad

ID	Cláusula
	de cada tipo de información. Y ayudará en la clasificación de sus activos en propiedad o explotación por el grupo Naturgy en base a la clasificación vigente del grupo Naturgy.
IC_04	En las comunicaciones con clientes el PROVEEDOR deberá utilizar las herramientas necesarias para controlar que éstas se produzcan de manera que se asegure la integridad sobre la información enviada de Naturgy.
Cifrado y ofuscación de Información	
CF_01	El PROVEEDOR no utilizará datos o información reales del grupo Naturgy en entornos que no sean de producción o de prueba autorizados. En caso de requerirse datos reales el PROVEEDOR deberá disponer del consentimiento explícito del propietario y responsable de los datos
CF_02	El PROVEEDOR deberá contar con la capacidad de cifrar la información del grupo Naturgy utilizando algoritmos de cifrado robustos y reconocidos. Este cifrado debe aplicarse tanto al almacenamiento temporal como permanente de dicha información en sus sistemas. Además, el PROVEEDOR deberá asegurar que los mecanismos de cifrado implementados cumplen con las normativas y estándares de seguridad vigentes.
CF_03	El PROVEEDOR deberá establecer el cifrado de los datos y las comunicaciones que se realicen a través de redes públicas y/o privadas y a través de las cuales viaje información relativa al servicio del grupo Naturgy, especialmente cuando se trate de datos confidenciales o sujetos a alguna regulación. Protegiendo la información contra la divulgación no autorizada
Bastionado y protección frente a amenazas	
BP_01	El PROVEEDOR deberá implementar los controles, mecanismos y herramientas de seguridad necesarias para la detección y la gestión de la amenaza sobre todos los activos de información del PROVEEDOR, con el objetivo de prevenirlas, solventarlas y, en el caso de que se trate de amenazas avanzadas y complejas, alertar al grupo Naturgy al ser detectadas. Debiendo revisar periódicamente las configuraciones de sus sistemas de información que almacenen o traten información del grupo Naturgy.
Continuidad Tecnológica	
CT_01	El PROVEEDOR deberá realizar periódicamente copias de respaldo de los sistemas implicados en la prestación del servicio al grupo Naturgy de forma que le permita su recuperación en caso de desastre. PROVEEDOR deberá contar con los procedimientos necesarios para la generación de copias de respaldo de los datos del servicio que presta al grupo Naturgy. Estas copias deberán alojarse en ubicaciones alternativas a las que soportan la operativa habitual.
CT_02	El PROVEEDOR deberá implementar las medidas necesarias, tanto físicas como lógicas, para asegurar la correcta manipulación de las copias de seguridad sobre la información relativa a la prestación del servicio del grupo Naturgy. Estas copias deben ser tratadas y almacenadas correctamente para poder ser recuperadas sin que la seguridad e integridad de la información pueda haberse visto comprometida durante la cadena de custodia de las mismas.
CT_03	El PROVEEDOR deberá contar con un Plan de Recuperación ante Desastres (DRP) detallado y actualizado para todos los sistemas involucrados en la prestación del servicio al grupo Naturgy. Este plan debe incluir procedimientos específicos para la restauración rápida

ID	Cláusula
	y efectiva de los sistemas críticos en caso de desastres, asegurando la continuidad del servicio. Además, el DRP deberá contemplar pruebas periódicas y revisiones regulares para garantizar su efectividad y estar en conformidad con las mejores prácticas y normativas vigentes, personal involucrado en los procesos de recuperación, actividades y responsabilidades a detalle por cada participante, procedimientos de notificación al grupo Naturgy y árbol de escalado para la toma de decisiones. Asimismo, el PROVEEDOR deberá capacitar a su personal en la ejecución de este plan para minimizar el impacto de cualquier interrupción en el servicio.

3) Clausulas aplicables cuando se acceda a redes, sistemas o infraestructura tecnológica del grupo Naturgy

ID	Cláusula
AN_01	Los accesos a las infraestructuras y sistemas del grupo Naturgy se deberán realizar siguiendo las políticas del grupo vigentes en cada momento, incluyendo, para los casos que se requiera acceso a redes de proceso industrial, las políticas referentes a seguridad industrial del grupo Naturgy, basadas en el estándar IEC-62443. En concreto, la solución general de acceso a sistemas del grupo Naturgy no publicados en Internet será la solución de Zerotrust que el grupo Naturgy pondrá a disposición del tercero y que el tercero debe utilizar.
AN_02	El PROVEEDOR, en su ámbito de responsabilidad, deberá implementar los mecanismos necesarios para garantizar que las comunicaciones entre su infraestructura y la del grupo Naturgy conserven la confidencialidad, integridad y disponibilidad de la información, limitándose a las necesidades del servicio.
AN_03	Según la modalidad de acceso, las políticas de acceso a redes y sistemas del grupo Naturgy podrán requerir que el PROVEEDOR tenga controles de ciberseguridad adicionales para los terminales de acceso que estén involucrados en la prestación del servicio. Incluyendo, de manera no excluyente, el tener instalado en sus puestos unos determinados componentes de seguridad actualizados y con una serie de características mínimas. En concreto, el grupo Naturgy se reserva el derecho de aplicar técnicas de análisis de riesgo del dispositivo y el usuario que quieran conectarse a activos del grupo Naturgy, no permitiendo el acceso si el riesgo de conexión se considera no admisible por los algoritmos de análisis de riesgo automatizados. Estos análisis de riesgo se realizara mediante técnicas de “acceso condicional” y “posture”
AN_04	El PROVEEDOR deberá notificar al grupo Naturgy aquellos usuarios que dejen de prestar servicio y cuenten con acceso lógico a los sistemas del grupo Naturgy, con objeto de que el grupo Naturgy realice el proceso de baja en su área de responsabilidad.
AN_05	Como parte de los planes de respuesta a amenazas y planes de respuesta a incidentes del grupo Naturgy, los accesos a del PROVEEDOR a activos y redes del grupo Naturgy podrán ser suspendidos o restringidos en caso de que se detecte que la situación del PROVEEDOR representa una amenaza para la seguridad de los activos del grupo Naturgy.
AN_06	En caso de que el PROVEEDOR acceda a los sistemas del grupo Naturgy, este deberá contemplar como mínimo su colaboración en las pruebas periódicas del DRP (Plan de Recuperación ante Desastres) del grupo Naturgy.

4) Clausulas aplicables cuando se entrega un producto o desarrollo

ID	Cláusula
PD_01	El PROVEEDOR deberá proporcionar información técnica sobre los recursos que va a servir al grupo Naturgy, con el objetivo de que se puedan realizar tests de compatibilidad de aplicaciones antes de la implementación. En el caso de modificaciones sustanciales (actualizaciones, mejoras, parches...) en las certificaciones o medidas de seguridad que apliquen sobre el servicio proporcionado al grupo Naturgy, el PROVEEDOR deberá proporcionar la información necesaria al grupo Naturgy para poder solventar las posibles incidencias derivadas de estas modificaciones. En especial el PROVEEDOR deberá disponer de medios que garanticen la compatibilidad de actualizaciones, parches y configuraciones con el resto del sistema, mediante validaciones de fabricantes o aportando evidencias de compatibilidad en entornos no productivos.
PD_02	El PROVEEDOR deberá comunicar cualquier cambio o pérdida en las certificaciones o aprobaciones de ciberseguridad y protección de datos de las marcas de forma inmediata, y se hará cargo de los perjuicios que pudiera ocasionar al grupo Naturgy. Adicionalmente, el proveedor deberá presentar el alineamiento de su producto y servicio con cualquier certificación internacional y/o nacional que sea recomendable o necesaria para la implementación o despliegue del producto en un entorno industrial o IT propiedad del grupo Naturgy.
PD_03	El PROVEEDOR deberá establecer los controles de seguridad en relación con la adquisición o desarrollo de nuevas aplicaciones o sistemas para la prestación del servicio ofrecido al grupo Naturgy. Debiendo contar con una segmentación entre los entornos de desarrollo, pruebas y producción para los aplicativos del servicio del grupo Naturgy. Debiendo realizar cualquier tipo de revisión de seguridad, desarrollo, actualización o compra sobre cualquier componente del sistema incorporado en el servicio prestado al grupo Naturgy en entornos diferentes al de producción.
PD_04	En caso de que el PROVEEDOR realice desarrollos de software, deberá aplicar técnicas y estándares alineadas con las buenas prácticas de desarrollo seguro, para las aplicaciones ofrecidas al grupo Naturgy.
PD_05	En el caso, de que el PROVEEDOR proporcione productos o proyectos de carácter industrial al grupo Naturgy, deberán estar alineados con las arquitecturas de ciberseguridad industrial del grupo Naturgy y con estándares industriales de ciberseguridad industrial y en concreto con el Estándar IEC 62443, específicamente, y de manera no excluyente, en: 1. Segmentación entre redes. 2. Accesos remotos para operación y mantenimiento. 3. Gestión de antivirus, robustez y/o parcheado. 4. Ciclo de vida. Estas medidas deben ser revisadas y actualizadas prioritaria y periódicamente para asegurar su eficacia. El PROVEEDOR deberá indicar los riesgos y contramedidas relacionadas con el producto y su integración con infraestructuras de Naturgy. Desde la perspectiva de ciberseguridad, deberá contestar explícitamente a las siguientes preguntas: 1. ¿Qué riesgos tiene el producto y/o solución? 2. ¿Qué riesgos pueden aparecer al integrar el producto con infraestructuras Naturgy? 3. ¿Qué medidas se aplican para proteger tanto el producto como la infraestructura de los riesgos identificados anteriormente?