Ciberseguridad - Cláusulas Aplicables

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

En caso de que el servicio o producto contratado tenga un clausulado de ciberseguridad específico, que deberá en cualquier caso haberse acordado con la función de 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

El 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 y la comunicación entre las partes en caso de incidentes.

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.

En caso de que el servicio corresponda a este grupo, de manera obligatoria deberá también cumplirse el clausulado del grupo 1)

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 de correo electrónico o usuario del grupo Naturgy, o acceso a 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 u operación y mantenimiento de sistemas de información y comunicaciones.

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 de los grupos 1) y 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 corresponda a este grupo, de manera obligatoria deberá también cumplirse el clausulado del grupo 1) y las condiciones de los grupos 2) y 3) si también le son de aplicación.

1) Clausulas generales

ID	Cláusula
Gobierno y Regulación	
GR_01	El PROVEEDOR se compromete a garantizar el cumplimiento continuo de todos los requisitos legales, regulatorios y contractuales aplicables en materia de ciberseguridad, con especial énfasis en aquellos relacionados con infraestructuras críticas, servicios esenciales y protección de datos. Este compromiso será válido para todas las ubicaciones e infraestructuras donde se almacene, procese o transmita información del grupo Naturgy. A modo de ejemplo y sin que ello limite lo anterior, el PROVEEDOR deberá cumplir, cuando le sea de aplicación, con las disposiciones establecidas en la Directiva NIS 2 (y su transposición a nivel local), el Cyber Resilience Act, así como cualquier otra legislación o normativa aplicable en el ámbito de la ciberseguridad.
GR_02	El PROVEEDOR deberá garantizar de que todas las herramientas utilizadas para prestar el servicio al grupo Naturgy no infringen derechos de propiedad intelectual o contractual de terceros.
GR_03	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.
GR_04	El PROVEEDOR deberá identificar los posibles riesgos e impactos que puedan existir en el servicio e implementar las medidas compensatorias que se adopten para eliminar o mitigar el riesgo. Las excepciones de responsabilidad en ciberseguridad deberán quedar documentadas en el contrato.
GR_05	En caso de poseer un certificado de un estándar de ciberseguridad, se deberá renovar según los plazos estipulados según certificación y, en caso de perdida, se deberá comunicar al grupo Naturgy en el menor tiempo posible.
Formación	
FO_01	El PROVEEDOR deberá disponer de un programa continuo y actualizado de formación y concienciación en ciberseguridad, que ayude a mitigar los riesgos que pudieran afectar al servicio que proporciona al grupo Naturgy.
FO_02	PROVEEDOR deberá verificar, de forma previa a la contratación, las competencias en ciberseguridad de los empleados/externos para el desempeño

ID	Cláusula
	de sus funciones y facilitar evidencia de ello al grupo Naturgy, en caso de ser requeridas.
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.
Segregación de funciones	
SD_01	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, deberá estar identificado nominalmente. Los permisos deben asignarse y otorgarse bajo el principio de privilegio mínimo (PoLP), utilizando grupos o roles que definan perfiles colectivos, evitando asignar privilegios directamente a usuarios específicos.
SD_02	El PROVEEDOR deberá disponer de un procedimiento de revisión periódica sobre los permisos y controles de acceso a la información del grupo Naturgy, y asegurándose que se actualicen según corresponda, con especial atención a la revocación una vez no sean necesarios (por ejemplo, en casos de cambio de responsabilidades o bajas en el servicio).
SD_03	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.
Integridad y confidencialidad	
IC_01	El PROVEEDOR únicamente accederá a la información del grupo Naturgy cuando sea estrictamente necesario para la prestación del servicio y se compromete a mantener la seguridad y absoluta confidencialidad de la información compartida en el contexto de la prestación del servicio. Dicho acceso deberá mantenerse dentro de los límites de su finalidad autorizada.
IC_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.

ID	Cláusula
	Adicionalmente, el proveedor deberá implementar procedimiento para gestionar la salida de activos de información de sus instalaciones dentro del servicio del grupo Naturgy. 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.
IC_03	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.
IC_04	El PROVEEDOR deberá garantizar el almacenamiento y transmisión cifrado de las contraseñas del servicio ofrecido al grupo Naturgy de forma segura.
IC_05	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.
IC_06	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.
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, con especial atención a servidores de bases de datos y archivos, a fin de prevenir daños físicos y accesos no autorizados a la información lógica relacionada con el servicio ofrecido al grupo Naturgy.
SF_03	Al término del servicio, o cuando corresponda en otras circunstancias, 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, tanto en formato físico como lógico, para garantizar que las transacciones y otros datos no puedan ser recuperados por personas no autorizadas.
SF_04	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.

ID	Cláusula
Gestión de activos y Operaciones	
GO_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, garantizando su adecuada protección y registro.
GO_02	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. 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.
GO_03	El PROVEEDOR deberá contar con una protección de antivirus o EDR 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.
GO_04	PROVEEDOR deberá implementar mecanismos de autenticación que garanticen la comunicación inequívoca con el grupo Naturgy.
GO_05	El PROVEEDOR deberá establecer mecanismos robustos que aseguren la identidad del remitente en las comunicaciones con el grupo Naturgy.
GO_06	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.
GO_07	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.
Respuesta A Incidentes de Ciberseguridad	

ID	Cláusula
RI_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. En la notificación de incidentes de seguridad el PROVEEDOR deberá aportar cuanta información y evidencias sean requeridas por el grupo Naturgy en relación con el incidente
RI_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.
RI_03	Para todo lo anterior, 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.
Subcontratación o Cuartas partes	
SC_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. 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.

ID	Cláusula
SC_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.
Evaluaciones de Ciberseguridad	
EC_01	El PROVEEDOR podrá ser susceptible de ser objeto de revisión en la 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.
EC_02	El PROVEEDOR deberá facilitar el cumplimiento de las obligaciones de inspección, supervisión y revisión del grupo Naturgy, a cargo de: (a) cualquier regulador competente en la materia, (b) la unidad de revisión 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. Esto incluye todos los aspectos de los servicios prestados al grupo Naturgy y cualquier tipo de información relacionada. Los encargados de la inspección o revisión 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.
EC_03	Las revisiones 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 quince (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

ID	Cláusula
	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.
EC_04	En caso de que el servicio o producto contratado sea un SaaS que tenga una certificación SOC1 o SOC2 de tipo 2 o ENS de nivel Alto, de común acuerdo entre las partes las revisiones de ciberseguridad podrán ser sustituidas por la entrega anual de los informes de renovación de certificación
Inteligencia Artificial	
IA_01	En caso de que el PROVEEDOR desee hacer uso de herramientas que contengan soluciones, modelos, sistemas o componentes de inteligencia artificial (en adelante, “Sistemas IA"), informará al Grupo Naturgy antes de iniciar del uso de dichos Sistemas IA, estando dicho uso supeditado a la autorización previa por escrito del Grupo Naturgy.
IA_02	Cuando el PROVEEDOR utilice, desarrolle o despliegue Sistemas IA en el marco de la prestación del Servicio, garantizará la aplicación por defecto del principio de minimización de los datos personales de modo que, únicamente sean objeto de tratamiento, aquellos datos estrictamente necesarios e imprescindibles, debiendo aplicar las técnicas de seudonimización y anominización que resulten necesarias para asegurar el cumplimiento efectivo de dicho principio.
IA_03	El PROVEEDOR en ningún caso utilizará los datos personales titularidad del Grupo Naturgy con el objeto de entrenar, configurar, mejorar, escalar, desarrollar u optimizar dichos Sistemas IA.

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

ID	Cláusula
Gobierno y Regulación	
GR_06	El PROVEEDOR deberá conocer y cumplir el cuerpo normativo del grupo Naturgy, y en especial, las políticas relativas a la gestión de acceso lógico a información del grupo, siendo responsabilidad del PROVEEDOR mantenerse actualizado respecto a cualquier cambio o actualización en dichas políticas. 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. 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.
GR_07	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 o ENS de nivel Alto sobre el servicio contratado. La certificación no será de obligatoriedad en el caso de que el servicio o producto SaaS contratado soporte proceso/s de negocio de Naturgy con BIA (Business Impact Analysis) calificado como 'Bajo', si bien será recomendable ENS de nivel medio. En cualquier caso, siempre que dicha web sea accedida por clientes del grupo Naturgy deberá contar con un certificado Extended Validation.
GR_08	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.
Control de Accesos	
CA_01	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.

ID	Cláusula
CA_02	El PROVEEDOR deberá establecer y mantener un procedimiento integral de gestión de contraseñas para los sistemas involucrados en el servicio a Naturgy. Este procedimiento deberá incluir, entre otros aspectos: 1. El cambio obligatorio de la contraseña inicial, 2. Requisitos mínimos de una longitud mínima y nivel de complejidad de las contraseñas 3. la caducidad de las contraseñas 4. restricciones sobre la reutilización de contraseñas anteriores. 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_03	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_04	En caso de que el servicio o producto contratado por el grupo Naturgy incluya bases de datos alojadas en la infraestructura del PROVEEDOR, estas deberán ubicarse en sistemas diferenciados de los de ejecución de las aplicaciones asociadas. Adicionalmente, no deberá haber una comunicación directa desde internet a esta(s) base(s) de datos debiendo hacer uso de algún componente tecnológico intermedio que gestione dicho acceso.
CA_05	Las funciones críticas, por ejemplo administración, del PROVEEDOR deberán estar identificadas y separadas de las funciones no críticas, por ejemplo operación habitual.
CA_06	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

ID	Cláusula
CA_7	El PROVEEDOR deberá implementar los mecanismos que garanticen el control y monitoreo continuo de los accesos remotos al entorno tecnológico del servicio ofrecido al grupo Naturgy, a fin de prevenir accesos no autorizados y garantizar la seguridad de la información.
CA_8	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_09	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. Este procedimiento deberá incluir al menos: 1. La devolución de todos los activos e información propiedad del grupo Naturgy en condiciones que permitan su reincorporación a los sistemas de Naturgy. 2. La custodia segura de los registros y logs relevantes relacionados con el servicio. 3. El borrado seguro de toda información del grupo Naturgy almacenada en los sistemas del PROVEEDOR, asegurando que esta no pueda ser recuperada o utilizada posteriormente.
CA_10	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).
CA_11	El PROVEEDOR deberá garantizar que todos los recursos utilizados para la prestación del servicio cuenten con autenticación multifactor (MFA).
Integridad y Confidencialidad	
IC_07	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_08	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.

ID	Cláusula
IC_09	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 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_10	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 protección de datos	
CP_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.
CP_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.
CP_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 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 incluyendo aquellos que almacenen o traten información del grupo Naturgy, con el objetivo de prevenirlas, solventarlas y, alertar al grupo Naturgy según corresponda. Estas medidas deberán ser revisadas y actualizadas periódicamente para garantizar su efectividad.

ID	Cláusula
BP_02	En concreto, El PROVEEDOR deberá instalar, en cualquier activo de información del PROVEEDOR que trate, almacene, o acceda a información de Naturgy, elementos con la capacidad de realizar análisis de comportamiento, para la detección y respuesta ante amenazas no conocidas (EDR)
Continuidad Tecnológica y de negocio	
PC_01	El PROVEEDOR se compromete a implementar y mantener un plan de continuidad de negocio que garantice la continuidad de la prestación del servicio a Naturgy en caso de interrupciones significativas. Este plan deberá revisarse de manera periódica para identificar y mitigar posibles nuevos riesgos que puedan afectar la continuidad del negocio y probarse de manera periódica para garantizar su efectividad y realizar ajustes según sea necesario. El PROVEEDOR deberá proporcionar al grupo Naturgy informes periódicos sobre el estado y la efectividad del programa de continuidad de negocio, así como cualquier actualización o cambio significativo en el mismo.
PC_02	El PROVEEDOR deberá realizar periódicamente copias de respaldo de los sistemas y/o información 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
PC_03	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.
PC_04	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 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

ID	Cláusula
	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.
PC_06	El PROVEEDOR deberá implementar copias de seguridad inmutables y fuera de línea para proteger los datos.

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

ID	Cláusula
	Seguridad en Redes y Conectividad
RC_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.
RC_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.
RC_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 riesgos se realizarán mediante técnicas de “acceso condicional” y “posture”. Lo anterior incluye, entre otras opciones, la posibilidad de exigir el uso de MFA para el acceso a sus activos, en función del contexto de ciberseguridad y gestión de riesgos que considere adecuado para el control de acceso, por lo cual El PROVEEDOR deberá garantizar que todos los recursos que intervienen en la prestación del servicio puedan autenticarse utilizando multifactor.
RC_04	El PROVEEDOR deberá notificar al grupo Naturgy, de manera inmediata, aquellos usuarios, que estén bajo su responsabilidad, 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.
RC_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

ID	Cláusula
	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.
RC_06	En caso de que el PROVEEDOR acceda a los sistemas del grupo Naturgy, aquel 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
Producto o Desarrollo seguro	
	En el caso de que el alcance de los trabajos del PROVEEDOR incluya un desarrollo de software, éste se llevará a cabo conforme a las mejores prácticas de seguridad establecidas en frameworks internacionalmente reconocidos y acordados entre ambas partes, garantizando la implementación de medidas de seguridad desde las fases iniciales del ciclo de vida del desarrollo de software, incluyendo la validación y sanitización de datos, la autenticación y autorización seguras, y la protección de datos sensibles mediante cifrado
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,

ID	Cláusula
	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 mejores prácticas de desarrollo seguro establecidas en frameworks internacionalmente reconocidos, garantizando la implementación de medidas de seguridad desde las fases iniciales del ciclo de vida del desarrollo de software, incluyendo la validación y sanitización de datos, la autenticación y autorización seguras, y la protección de datos sensibles mediante cifrado.
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?
PD_06	Todo software desarrollado o entregado por el PROVEEDOR deberá someterse a análisis de vulnerabilidades con herramientas reconocidas como SAST y DAST antes de su entrega a Naturgy para implementación en entornos productivos.
PD_07	El PROVEEDOR validará la seguridad de integraciones con infraestructuras del grupo Naturgy, asegurando que no comprometen la operación ni la ciberseguridad de los sistemas existentes.

Glosario de términos y abreviaturas

- **AES-256:** Advanced Encryption Standard.
- **DAST:** Dynamic application Security testing.
- **DRP:** (Disaster Recovery Plan) Plan de recuperación ante desastres.
- **ENS:** Esquema Nacional de Seguridad.
- **EDR:** Endpoint detection and response.
- **GDPR:** Reglamento general de protección de datos.
- **IEC-62443:** Estándar global para la seguridad cibernética en sistemas industriales.
- **MFA:** Autenticación multifactorial.
- **NTP:** Network time protocol.
- **PoLP:** Principio de privilegio mínimo (Principle of least privilige).
- **Posture:** Estado de cumplimiento de un dispositivo en relación con los controles de ciberseguridad definidos, evaluado para determinar si cumple con los requisitos mínimos para acceder a una red o sistema
- **SaaS:** Software as a Service.
- **SAST:** Static application security testing.
- **SOC:** Centro de operaciones.
- **SOC 1:** Informe que evalúa los controles internos de una organización relacionados con la generación de informes financieros.
- **SOC 2 Tipo 2:** Informe que evalúa los controles internos de una organización sobre la seguridad, disponibilidad, integridad, confidencialidad y privacidad.
- **TLS 1.2:** Trasport Layer Security 1.2.
- **Zero trust:** Modelo de seguridad que elimina la confianza implícita y exige verificar continuamente la identidad y los permisos de todos los usuarios y dispositivos.