Ingeteam ELECTRIFYING A SUSTAINABLE FUTURE

RN8.A.11-5-01

Cláusulas de SI para proveedores

CONTROL DOCUMENTAL	
FECHA:	03/07/2024

CONTENIDO

1 PROPUESTA CLÁUSULA PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN

Ingeteam dispone de una Normativa de Seguridad de los Sistemas de Información que regula las medidas a adoptar en el tratamiento de la información y de los sistemas de información que los soportan. El proveedor asumirá estas Normativas de Seguridad para todos los servicios que son objeto de este contrato.

1.1 DEFINICIONES

a. **Infraestructura de los Sistemas de Información**: Se refiere a los sistemas y servicios de información y comunicaciones electrónicas, así como a la información contenida en los mismos. Esto incluye tanto los sistemas alojados en las instalaciones físicas como aquellos basados en servicios en la nube, propios o de terceros, en todas sus modalidades. La Infraestructura de los Sistemas de Información comprende el hardware y el software utilizados para procesar (crear, acceder, modificar y eliminar), almacenar (en diversos soportes magnéticos, electrónicos u otros) y transmitir (compartir y distribuir) información, así como cualquier combinación de estos elementos. Engloba una amplia gama de dispositivos electrónicos, como ordenadores estándar (de sobremesa/portátiles) con conexión a red, medios de almacenamiento digital, teléfonos móviles, smartphones, asistentes digitales personales (PDA), cámaras digitales y de vídeo (incluyendo sistemas de videovigilancia CCTV), sistemas de navegación móvil, entre otros.

b. **Información Restringida**: Se refiere a toda la información creada, recibida, transmitida o almacenada que, por su naturaleza o valor para Ingeteam, requiere medidas de protección adicionales. Esto incluye, pero no se limita a, información confidencial o reservada, datos personales, datos de tarjetas de crédito, información comercialmente sensible, información relacionada con infraestructuras críticas, datos estratégicos de negocio, credenciales de acceso, datos de cifrado, registros de acceso a sistemas y aplicaciones, así como cualquier otra información sujeta a regulación o que pueda ser considerada sensible.

c. **Fallo de Seguridad de Datos:** Para los fines del Contrato o Pedido, se considerará "Fallo de Seguridad de Datos" a: (A) la pérdida o mal uso de la Información Restringida; (B) el procesamiento, corrupción, modificación, transferencia, venta o cesión no autorizados o ilegales de la Información Restringida; o (C) cualquier acto u omisión que comprometa la seguridad, confidencialidad o integridad de la Información Restringida.

1.2 SUBCONTRATACIÓN

En el caso de que el Proveedor, debidamente autorizado por Ingeteam, decida subcontratar parte de los servicios relacionados con la presente cláusula, se compromete a garantizar que el subcontratista asuma las mismas obligaciones establecidas en este documento. En todo momento, el Proveedor será responsable de cualquier incumplimiento por parte del subcontratista o su personal en lo que respecta a las obligaciones de ciberseguridad y seguridad de la información descritas en el Contrato o Pedido.

1.3 PROPIEDAD DE DATOS E INFORMACIÓN

En los casos en que los datos o la información relacionada con el Contrato o Pedido sean propiedad de Ingeteam, o cuando los elementos de la Infraestructura de los Sistemas de Información sean suministrados al Proveedor por Ingeteam, el Proveedor se compromete a procesar y utilizar dichos datos e información exclusivamente para cumplir con sus obligaciones en virtud del Contrato o Pedido y para ningún otro propósito.

Durante todo el proceso de tratamiento de los datos o información relacionada con el Contrato o Pedido, el Proveedor se compromete a cumplir con todas las leyes y regulaciones aplicables en materia de seguridad y protección de datos. Además, el Proveedor se obliga a no poner a Ingeteam en una situación de incumplimiento, ya sea por acción u omisión.

En los casos en los que se traten datos de carácter personal, se deberá de firmar el contrato de encargado de tratamiento de datos personales.

1.4 PROTECCIÓN DE LA INFORMACIÓN

El Proveedor se compromete a mantener un conocimiento continuo del nivel de protección de la Información Restringida relacionada con el Contrato o Pedido, así como de la normativa y legislación correspondiente aplicable. Adoptará medidas de seguridad técnicas y organizativas apropiadas para garantizar la protección de dicha información.

Estas medidas de seguridad serán proporcionales al tipo de Información Restringida procesada y a los servicios objeto del Contrato o Pedido, asegurando al menos un nivel de seguridad consistente con las mejores prácticas de la industria. Dichas medidas incluirán salvaguardias físicas, electrónicas y procedimentales para proteger la Información Restringida contra posibles fallos de seguridad de datos u otros incidentes de seguridad, así como para cumplir con cualquier requisito de seguridad, obligación, especificación o evento reportable estipulado en el Contrato o Pedido.

El Proveedor garantizará un entorno seguro para toda la Información Restringida y para cualquier hardware o software que contenga dicha información y que deba ser proporcionado o utilizado por el Proveedor en el cumplimiento del Contrato o Pedido, siempre que dichos elementos estén en sus instalaciones.

Al tratar información de Ingeteam, el Proveedor debe cumplir con el esquema de clasificación de información de Ingeteam. En el caso de que el Proveedor tenga su propio esquema de clasificación, se deberá elaborar una asociación entre ambos esquemas de clasificación de información.

El Proveedor garantizará la seguridad de las transferencias de información implantando los controles de seguridad necesarios en función del nivel de clasificación de la información a transferir.

El Proveedor no está autorizado a divulgar, proporcionar acceso directo o indirecto, ni permitir el acceso a la Información Restringida de Ingeteam a terceros, ni siquiera para su almacenamiento. Tampoco se le autoriza a proporcionar la capacidad de descifrar claves de cifrado. En caso de que sea necesario involucrar a un tercero, se requerirá una autorización expresa y por escrito de Ingeteam, indicando el propósito, y se exigirán al tercero las mismas obligaciones que al Proveedor.

El personal externo que tenga acceso a información de Ingeteam deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información de Ingeteam a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por Ingeteam.

Se deberá de firmar el acuerdo de confidencialidad entre el Proveedor e Ingeteam antes del inicio de la relación contractual.

1.5 INTERCAMBIO DE INFORMACIÓN

Ninguna persona debe ocultar o manipular su identidad en ninguna circunstancia.

La distribución de información ya sea en formato digital o papel se realizará mediante los recursos determinados en el contrato de provisión de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato. Ingeteam se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre estos recursos de difusión.

En relación con el intercambio de información dentro del marco del contrato de provisión de servicios, se considerarán no autorizadas las siguientes actividades:

a) Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
b) Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
c) Transferencia de ficheros a terceras partes no autorizadas de material de Ingeteam o material confidencial.
d) Transmisión o recepción de ficheros que infrinjan el RGPD o directrices de Ingeteam.
e) Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
f) Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el servicio prestado.

g) Todas las actividades que puedan dañar la buena reputación de Ingeteam están prohibidas en Internet y en cualquier otro lugar.
h) Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso, cumpliendo el procedimiento definido y las leyes vigentes.

1.6 USO DE RECURSOS INFORMÁTICOS DE INGETEAM

En el caso de que Ingeteam ponga a disposición del personal del Proveedor o de su subcontratista dispositivos electrónicos u otros recursos informáticos, o les conceda una cuenta de correo electrónico de Ingeteam o credenciales para acceder a aplicaciones, conexiones u otros elementos de la Infraestructura de los Sistemas de Información de Ingeteam para cumplir con el objeto del Contrato o Pedido, el Proveedor será responsable de garantizar que dicho personal esté plenamente informado y se comprometa expresamente a cumplir con las condiciones de seguridad y con la Normativa de uso aceptable establecidas por Ingeteam. Dichas condiciones serán proporcionadas al Proveedor en un anexo específico. El Proveedor se encargará de custodiar los documentos que acrediten el cumplimiento de estas obligaciones por parte de su personal y los pondrá a disposición de Ingeteam cuando así lo requiera.

1.7 MEDIDAS DE SEGURIDAD A ADOPTAR POR EL PROVEEDOR

a) Conexión entre Redes: La conexión entre la red de Ingeteam y la del Proveedor no está permitida, a menos que se acuerde expresamente en el Contrato o Pedido. En tal caso, se basará en redes privadas virtuales cifradas y autenticadas, con el mínimo número de puntos de interconexión necesarios. Esta conexión se eliminará una vez finalizada su necesidad. No se permitirán conexiones directas de usuarios del Proveedor a la red de Ingeteam, salvo autorización expresa y durante el tiempo acordado. En caso de establecerse una conexión a la red de Ingeteam no se permite realizar simultáneamente conexión a otra red.

b) Control de Acceso Físico: Si el Contrato o Pedido se lleva a cabo en instalaciones del Proveedor, éste establecerá mecanismos de control de acceso físico para evitar el acceso no autorizado a la infraestructura o a la Información Restringida.

c) Control de Acceso Lógico: El Proveedor implementará medidas de identificación, autenticación y control de acceso lógico para evitar el acceso no autorizado a su Infraestructura de los Sistemas de Información y a la Información Restringida de Ingeteam. Se establecerán procedimientos basados en el principio de privilegio mínimo y se mantendrá un inventario actualizado de accesos y permisos. El proveedor prestará especial atención a la custodia de credenciales de acceso a los Sistemas propiedad de Ingeteam. En los casos en que Ingeteam lo exija, el Proveedor deberá implementar el sistema de autenticación de dos factores para el acceso a cualquier sistema de la organización.

d) Continuidad Operativa: El Proveedor establecerá medidas técnicas y organizativas para garantizar la continuidad de las operaciones, incluyendo planes de contingencia, procedimientos de respaldo y recuperación.

e) Equipos Informáticos: En caso de acceso a la Infraestructura de los Sistemas de Información de Ingeteam con equipos informáticos del Proveedor, se garantizarán medidas de seguridad adecuadas, como bloqueo automático, protección contra software malicioso y actualización del sistema operativo. El Proveedor acepta que estos dispositivos sean auditados y monitorizados.

f) Protección de Datos en Papel: Se establecerán procedimientos para proteger y destruir adecuadamente los documentos en papel que contengan información relacionada con el Contrato o Pedido cuando dejen de ser necesarios.

g) Desarrollo de Equipos: Se incluirán medidas de seguridad adecuadas en el desarrollo, mantenimiento y pruebas de los equipos utilizados para el cumplimiento del Contrato o Pedido, incluyendo estándares de desarrollo de código seguro y el uso de datos ficticios en entornos de pruebas.

El Proveedor aplicará estas medidas de seguridad acordes con la sensibilidad de la información involucrada y siguiendo el esquema de clasificación de información de Ingeteam. Además, proporcionará la información solicitada por Ingeteam sobre cualquier tratamiento de la Información Restringida.

1.8 CAMBIOS Y BAJAS DE PERSONAL ASOCIADO AL SERVICIO PRESTADO

El proveedor se compromete a notificar de forma inmediata cualquier cambio o baja de personal que tenga acceso a los sistemas, datos o instalaciones de Ingeteam. Esta notificación debe realizarse a más tardar dentro de las 24 horas siguientes a la finalización del vínculo laboral o contractual del empleado con el proveedor.

En el momento de la notificación del cambio o la baja, el proveedor deberá asegurarse de que todos los accesos del personal saliente a los sistemas, datos y cualquier propiedad de Ingeteam sean revocados de forma inmediata. Esto incluye, pero no se limita a, cuentas de usuario, accesos físicos, credenciales de autenticación, y cualquier otro tipo de acceso que permita la interacción con los recursos de Ingeteam.

1.9 SEGURIDAD EN EL SUMINISTRO DE EQUIPOS Y MATERIALES

En el caso de que el objeto del Contrato o Pedido incluya el suministro de equipos y materiales, el Proveedor deberá garantizar la aplicación de estándares y buenas prácticas de seguridad en el diseño, fabricación, mantenimiento y, en su caso, instalación del material suministrado, así como de sus componentes.

Para los equipos y/o materiales con capacidad de procesamiento de información u opciones de conectividad a redes:

a) El Proveedor deberá proporcionar evidencias o certificados que aseguren el diseño seguro de los equipos, las actualizaciones periódicas de firmware/software y la protección efectiva contra el malware.

b) Se realizará un análisis periódico de vulnerabilidades por parte del Proveedor, quien informará a Ingeteam sobre las actualizaciones necesarias, especialmente aquellas relacionadas con la seguridad.

c) Los dispositivos con capacidad de conectividad deberán estar protegidos por contraseñas con la debida complejidad, permitiendo su modificación por parte de Ingeteam.

d) La configuración de los dispositivos, equipos y materiales deberá ajustarse exclusivamente a las necesidades de Ingeteam, desactivando cualquier funcionalidad no requerida. En caso de que el Proveedor realice la configuración, deberá proporcionar documentación que evidencie dichos ajustes.

1.10 PROCEDIMIENTO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENTES DE SEGURIDAD

El Proveedor implementará un procedimiento de notificación y gestión de incidentes de seguridad, que será difundido entre su personal. Actuará con diligencia especial en casos que involucren elementos críticos de la Infraestructura de los Sistemas de Información de Ingeteam, Información Restringida, o cuando estén en riesgo la reputación, responsabilidad legal, o intereses de las personas cuya información es tratada.

El Proveedor notificará de inmediato a Ingeteam cualquier incidencia de seguridad que pueda afectar a Ingeteam, en un plazo máximo de 24 horas desde su detección o en el plazo legal aplicable, y colaborará con Ingeteam en la comunicación a terceros y en las medidas de remediación requeridas.

La notificación de los incidentes de seguridad se realizará mediante correo electrónico a la dirección: csirt.global@ingeteam.com.

En caso de incidentes que involucren datos de carácter personal, el Proveedor deberá informar, además, al responsable de tratamiento de datos personales de Ingeteam.

Las incidencias a ser notificadas incluyen, pero no se limitan a:

a. Accesos no autorizados o intentos a sistemas, equipos, aplicaciones, archivos, dispositivos, etc.

b. Revelación o compromiso de credenciales, datos de autenticación o cifrado. Suplantación de cuentas de correo electrónico.

c. Pérdida total o parcial de datos o información por cualquier causa.

d. Distribución no autorizada de información.

e. Pérdida o robo de equipos o soportes informáticos.

f. Ataques de virus o software malicioso.

g. Otras irregularidades relacionadas con los criterios de seguridad establecidos.

Se acordarán acciones, tiempos de resolución y mecanismos de seguimiento entre el Proveedor e Ingeteam según la gravedad del incidente.

En el caso de incidentes relevantes en el Proveedor, aun no habiendo podido definir grado de afección a Ingeteam, se notificará igualmente en un plazo menor de 24 horas de ser conocedor, Se define incidente relevante como aquel que:

- Ha causado o puede causar serias interrupciones operativas en los servicios o pérdidas financieras para la entidad afectada.
- Ha afectado o puede afectar a otras personas o entidades legales al causar daños materiales o inmateriales considerables.

1.11 Devolución y Destrucción de Información y Equipos

Una vez finalizada la prestación contractual o en caso de resolución del Contrato o Pedido, el Proveedor deberá devolver a Ingeteam o destruir de manera segura, a elección de esta última, toda la información perteneciente a Ingeteam que esté en su posesión, así como cualquier soporte o documento que contenga Información Restringida. En el caso de optar por la destrucción de la información, el Proveedor proporcionará un certificado correspondiente, siguiendo estándares reconocidos para ello.

Además, se devolverán todos los equipos, dispositivos y soportes propiedad de Ingeteam, y se cancelarán todas las posibles conexiones con la Infraestructura de los Sistemas de Información de Ingeteam. Este proceso se llevará a cabo cuando los elementos de infraestructura o la información ya no sean necesarios para cumplir con las obligaciones del Contrato o Pedido.

Si el Proveedor está obligado por la normativa aplicable a conservar Información Restringida de Ingeteam, deberá mantenerla debidamente protegida y solo durante el tiempo requerido por la ley. Una vez transcurrido este período, la información será destruida o devuelta a Ingeteam, según la elección de esta última, al igual que cualquier soporte o documento que contenga dicha información, sin conservar copias adicionales.

1.12 Evaluaciones y Auditorías de Seguridad

El Proveedor deberá proporcionar, a solicitud de Ingeteam, pruebas de evaluaciones o auditorías de seguridad, e incluso permitir, a petición de Ingeteam, que se realicen auditorías e inspecciones independientes en sus instalaciones de tratamiento de datos o en servicios en la nube, con respecto a las medidas de seguridad establecidas en las cláusulas presentes.

Estas auditorías o inspecciones podrán ser llevadas a cabo por Ingeteam o por una entidad auditora encargada por Ingeteam. El Proveedor se compromete a cumplir con cualquier plan de acción resultante de dichas auditorías.

1.13 Apoyo en Respuesta a Comunicaciones Relacionadas con Datos

El Proveedor se compromete a ofrecer a Ingeteam un apoyo eficiente y oportuno en la respuesta a cualquier solicitud, queja u otras comunicaciones recibidas por parte de entidades gubernamentales, autoridades reguladoras o similares en el uso, divulgación o mal uso de cualquier dato o información

1.14 Formación y Concienciación

El Proveedor se asegurará de que su personal disponga de la formación necesaria para la tarea que desempeña, sobre todo en los procedimientos de específicos de seguridad de la información (por ejemplo, la resolución de incidentes de seguridad).

El Proveedor también debe de asegurar de que el personal tiene un nivel de concienciación adecuado acerca de la seguridad de la información y está al día de las técnicas más comunes de ingeniería social y otro tipo de ataques de ciberseguridad.

1.15 CONTACTOS RELEVANTES

El Proveedor debe poner a disposición de Ingeteam al inicio de relación laboral, un listado con las personas de contacto relevantes en términos de seguridad de la información, así como con los canales de comunicación que se deben de emplear.

1.16 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. POLÍTICA DE DESARROLLO SEGURO.

Los siguientes requisitos son de aplicación a todo servicio de mantenimiento o desarrollo de software para Ingeteam.

Los proveedores deben aplicar procesos de ingeniería de sistemas seguros para los desarrollos que afecten a Ingeteam. Estos procesos buscan proporcionar garantías objetivas respecto a la seguridad del software producido. Para ello se deben aplicar mecanismos y producir evidencias durante el proceso (medibles, verificables, y repetibles) que garanticen que el software exhibe de manera consistente las propiedades de seguridad que se le requieran.

Ingeteam supervisará y controlará el software desarrollado por terceros, en concreto:

- Licencias y propiedad del código fuente,
- Tipos de pruebas a realizar al software subcontratado.
- Cumplimiento de los requisitos de seguridad y funcionalidad del software.

El desarrollo de sistemas sólo debe ser realizado por desarrolladores de sistemas cualificados con los conocimientos necesarios demostrados de programación segura.

El proveedor deberá seguir y utilizar metodologías de desarrollo seguro y herramientas de apoyo para el correcto desarrollo de las aplicaciones.

Al abordar el desarrollo de la aplicación, será necesario cumplir con todos los requerimientos en materia de protección de datos de carácter personal contemplados en el Reglamento General de Protección de Datos, especialmente en lo que se refiere a la seguridad por diseño y por defecto.

No se permite el uso de componentes, librerías, etc. sin licencia válida o limitada a uso privado y no profesional en los desarrollos provistos por el Proveedor.

El proveedor deberá establecer una línea de base de requisitos de seguridad, durante todo el ciclo de vida del desarrollo software, con el objetivo de prevenir y solventar posibles amenazas/errores en fases tempranas el desarrollo. En caso de duda se debe validar con el equipo de ciberseguridad.

Se debe revisar la arquitectura del sistema para determinar si cumple con los requisitos de una infraestructura segura.

Todo el desarrollo de los sistemas debe ser controlado mediante procedimientos de control de cambios.

Las fechas de validez de los permisos de acceso deben definirse para todos los miembros del proyecto, restringiendo el acceso durante el tiempo estrictamente necesario.

Previamente al paso a producción de la aplicación, deberá someterse a pruebas de seguridad, definidas por Ingeteam, con el objeto de detectar vulnerabilidades.

El entorno de desarrollo deberá estar continuamente mantenido, siendo separado de los entornos de producción y pruebas.

Los entornos de desarrollo, pre-producción y producción deberán estar aislados a nivel lógico entre sí.

1.17 PROPIEDAD INTELECTUAL

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por Ingeteam para el desarrollo de sus funciones.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los Sistemas de Información de Ingeteam.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

Ingeteam únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

1.18 ENTORNOS CLOUD

Los siguientes requisitos son de aplicación a todo servicio contratado ubicado en la nube:

Con el fin de proteger la información que se encuentra y transmite en la nube, el proveedor deberá establecer medidas de seguridad relativas al desarrollo de una infraestructura de seguridad que contemple:

- Medidas de cifrado para el almacenamiento y la transmisión de la información utilizando algoritmos seguros.
- Asegurar la disponibilidad de la información almacenada en la nube y la posibilidad de acceso por parte de Ingeteam.
- Un sistema de comunicaciones entre los aplicativos o sistemas de Ingeteam y los del proveedor que se efectúen de forma cifrada, sean autenticadas en cada extremo y estén ocultas hacia el exterior.
- En el caso de que la información de Ingeteam comparta nube con la información de otros clientes se deberá establecer una separación lógica que impida accesos no autorizados.
- El acceso a los datos de Ingeteam por parte de los técnicos de los proveedores deberá estar siempre aprobado y registrado
- En caso de que Ingeteam lo requiera, el proveedor deberá:
- Enviar la actividad realizada por los usuarios de los sistemas y aplicaciones, de forma online y continua para que Ingeteam pueda monitorizar el servicio mediante sus herramientas corporativas.
- Proveer un aislamiento a nivel físico y lógico para el servicio de Ingeteam, asignando los dispositivos (servidores, bases de datos, unidades de almacenamiento, etc.) de forma exclusiva para el servicio de Ingeteam, no pudiendo ser utilizados para dar servicio a otros clientes del proveedor salvo acuerdo expreso con Ingeteam.
- Aislar completamente la red interna, a partir de las comunicaciones, del proveedor en la que se encuentren los sistemas y aplicaciones destinados al servicio de Ingeteam, del resto de su red, y de las otras redes que utilice el proveedor para otros clientes.

1.19 ACTUALIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, Ingeteam se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados en estas políticas serán divulgados a todas las empresas proveedoras de servicios a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento de las políticas de seguridad más recientes de Ingeteam por parte de su personal.