ANEXO VII -

MEDIDAS DE SEGURIDAD APLICABLES A LA PRESTACIÓN DE SERVICIOS POR PARTE DEL PROVEEDOR

1. Definiciones

Desarrollo seguro: proceso de diseño y desarrollo de aplicaciones de forma segura que garantice desde el inicio del diseño la seguridad y protección de la aplicación.

Dato Personal o Datos Personales: tendrán el significado que le asigna el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE -Reglamento general de protección de datos- ("**RGPD**").

Empleados del PROVEEDOR: hace referencia a todo el personal que forme parte del PROVEEDOR o de sus sociedades filiales que para el desarrollo de sus funciones precise acceder a la Información de TRASA GLOBAL en el marco del Encargo y todas aquellas personas que, sin pertenecer a la organización del PROVEEDOR, por razón de su oficio, formación o experiencia y en virtud de una relación que las vincule con el PROVEEDOR vayan a tener acceso a la Información de TRACASA GLOBAL por ser necesario en el marco del Encargo.

Encargo: hace referencia a los servicios, el trabajo o el proyecto cuyo detalle se incluye en la RFP, y que será ejecutado por el Proveedor que resulte adjudicatario.

Información de TRACASA GLOBAL: tendrá tal consideración toda la información ya sea oral, escrita, electrónica, digital o recogida en cualquier otro soporte físico o lógico, de carácter técnico, científico, tecnológico, comercial, financiero o de cualquier otra naturaleza revelada por TRACASA GLOBAL, o por sus sociedades filiales o participadas, personal o cualquier otra física o jurídica que hubiese colaborado con TRACASA GLOBAL o trabajado para ésta, al PROVEEDOR o ya sea con anterioridad o posterioridad a la firma de este Anexo, o conocida por este último como consecuencia de su participación en el Encargo, con independencia de que contenga o no Datos Personales, ya sea relativa a TRACASA GLOBAL o a sus sociedades filiales o participadas, así como la correspondiente a cualesquiera terceros que estuvieren trabajando o colaborando con éstas en el desarrollo de trabajos o proyectos o que hubieran cedido a TRACASA GLOBAL alguna información de carácter confidencial a cualesquiera efectos, y cualesquiera análisis, estudios, recopilaciones, informes o documentación o información similar preparados por el PROVEEDOR que contengan Información de TRACASA GLOBAL o hayan sido preparados a partir de Información de TRACASA GLOBAL.

Pruebas de hacking ético o test de intrusión: proceso de revisión que verifica que la solución desplegada o proporcionada por EL PROVEEDOR no cuenta con ninguna configuración insegura o vulnerabilidad que pueda concluir en el acceso, borrado o manipulación de la información propiedad de TRACASA GLOBAL de manera no autorizada o ilegítima. Estas pruebas, en ningún caso incluirán actividades que pueda culminar una denegación del servicio.

Pruebas de seguridad de código, procesos de revisión y aceptación de código: proceso de revisión que verifica que el código generado en el Encargo por parte de EL PROVEEDOR cumple con la calidad y especificaciones de seguridad establecidas, sin vulnerabilidades, y que logra su cometido antes de su puesta en marcha (aceptación).

Sistema de Información: conjunto de programas, soportes, equipos, dispositivos, recursos, infraestructuras, plataformas y elementos técnicos y/o físicos análogos a través de los cuales se realizan operaciones de tratamiento de la Información de TRACASA GLOBAL, ya sean del PROVEEDOR, de TRACASA GLOBAL o de un tercero.

Tercero: hace referencia a cualquier persona física o jurídica distinta a los Empleados del PROVEEDOR.

Vulnerabilidades en Sistemas y Aplicaciones: agujeros de seguridad identificados en Sistemas de Información que pueden ser aprovechados por ataques maliciosos para generar brechas de seguridad, tales sean fugas o robos de información. Estos agujeros pueden ser solventados a través de distintos mecanismos de seguridad.

2. Seguridad de la Información y los Sistemas de TRACASA GLOBAL. Requerimientos generales

Requerimientos de seguridad a cumplir por parte del PROVEEDOR referentes a obligaciones legales y normativas según los marcos de seguridad aplicables, así como obligaciones ante contrataciones de cuartas partes, trazabilidad de eventos en relación al Encargo y respuesta ante incidentes, que garanticen la protección de la información y los sistemas de TRACASA GLOBAL.

2.1. General

a. El PROVEEDOR deberá cumplir con las obligaciones y adoptar los requisitos establecidos en el presente Anexo y en cualquier otra documentación o acuerdo que se alcance entre TRACASA GLOBAL y el PROVEEDOR en relación al Encargo, habida cuenta del estado de la tecnología, la naturaleza de la Información de TRACASA GLOBAL y los riesgos a que está expuesta, ya provengan de la acción humana o del medio físico o natural, alineándose en todo momento con los estándares internacionales de referencia y buenas prácticas de mercado.

b. El PROVEEDOR se obliga a cumplir el marco normativo, nacional, comunitario o internacional, que pudiera resultar aplicable al tratamiento de la Información de TRACASA GLOBAL y/o a los Sistemas de Información utilizados y/o a los procesos y mecanismos técnicos desplegados.

   En particular, el PROVEEDOR declara conocer el Esquema Nacional de Seguridad (ENS) y el estándar internacional UNE – ISO / IEC 27002 y se compromete a desplegar en el contexto del Encargo, los mecanismos organizativos y técnicos basados en el ENS o equivalentes bajo los estándares internacionales de referencia y buenas prácticas de mercado.

c. El PROVEEDOR deberá cumplir aquéllos otros requisitos introducidos por nuevas regulaciones, o por la modificación de cualesquiera regulaciones vigentes, nacionales, comunitarias o internacionales, que resulten de aplicación en el ámbito de las materias reguladas en este Anexo o en relación al Encargo.

d. El PROVEEDOR deberá notificar a TRACASA GLOBAL la falta o incapacidad conocida y deliberada de mantener el cumplimiento del marco normativo y leyes aplicables.

e. El PROVEEDOR deberá disponer de políticas para la seguridad de la información, suficientes para garantizar la protección de la Información de TRACASA GLOBAL, que deberán ser informadas a TRACASA GLOBAL y comunicadas a los Empleados del PROVEEDOR y terceros que participen en el Encargo.

Las políticas de seguridad de la información deberán revisarse periódicamente y, en cualquier caso, siempre que se produzcan cambios normativos, incidentes de seguridad o eventos significativos de cualquier clase, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

f. El cumplimiento de las obligaciones y requisitos de seguridad y protección de la Información de TRACASA GLOBAL recogidos en el presente Anexo, no podrá suponer un coste adicional para TRACASA GLOBAL, ni directo ni repercutido por parte del PROVEEDOR.

2.2. Formación

a. El PROVEEDOR dará a los Empleados del PROVEEDOR la necesaria formación y capacitación en materia de seguridad de la información (incluyendo, a título ilustrativo, sesiones de formación específicas, entrega de guías o materiales fácilmente accesibles sobre seguridad de la información, etc.).

2.3. Auditorías y trazabilidad

a. El PROVEEDOR deberá facilitar a TRACASA GLOBAL toda aquella información que resulte necesaria para demostrar el cumplimiento de sus obligaciones en virtud del presente Anexo, y, en su caso, informar a TRACASA GLOBAL de su adhesión a un código de conducta aprobado o su adscripción a cualquier mecanismo de certificación que pueda garantizar el cumplimiento de sus obligaciones en relación con el tratamiento de la Información de TRACASA GLOBAL. En caso de que el PROVEEDOR esté adscrito a un código de conducta o mecanismo de certificación, TRACASA GLOBAL podrá requerir al PROVEEDOR en cualquier momento su justificación documental.

b. El PROVEEDOR deberá colaborar con TRACASA GLOBAL para dar cumplimiento a las obligaciones internas y externas de auditoría.

c. TRACASA GLOBAL podrá realizar revisiones de seguridad (incluyendo pruebas de hacking ético o de seguridad de código) / continuidad de negocio y/o auditar los sistemas de información del PROVEEDOR que traten, almacenen o gestionen información de su propiedad (incluidos los procesos que soporten dichos tratamientos, almacenamiento y/o gestión), previo aviso a EL PROVEEDOR.

d. El PROVEEDOR pondrá a disposición de TRACASA GLOBAL, en caso de que así se solicite, la definición, el diseño y los esquemas de los elementos, mecanismos y arquitecturas, tanto de seguridad de la información, como de continuidad de negocio, desplegados sobre la infraestructura tecnológica, junto con los procedimientos y procesos que soporten o relacionados con el Encargo.

e. Asimismo, en el caso de que TRACASA GLOBAL así lo solicite, el PROVEEDOR permitirá la realización de auditorías e inspecciones en relación con el tratamiento de la Información de TRACASA GLOBAL con el fin de comprobar si el PROVEEDOR cumple con las obligaciones asumidas por éste en virtud del presente Anexo.

Las auditorías podrán ser realizadas bien por parte de TRACASA GLOBAL o de otro auditor autorizado por ésta en cualquier local donde existan informaciones, archivos o datos de TRACASA GLOBAL, o de forma remota. TRACASA GLOBAL notificará por escrito al PROVEEDOR con un plazo de antelación de al menos siete (7) días naturales la realización de dichas auditorías o inspecciones, salvo que la misma se lleve a cabo por un organismo regulador que impida tal preaviso, en cuyo caso TRACASA GLOBAL lo comunicará con la mayor antelación que le sea posible.

2.4. Gestión de incidentes y continuidad de negocio

a. El PROVEEDOR deberá comunicar a TRACASA GLOBAL cualquier incidente de seguridad que tenga o pueda tener un impacto negativo en la integridad, la disponibilidad, la confidencialidad o la autenticidad de los servicios ofrecidos a TRACASA GLOBAL en el Encargo, incluyendo, las infraestructuras, servicio, sus usuarios o su reputación.

b. El PROVEEDOR deberá notificar, de forma inmediata, a TRACASA GLOBAL cualquier brecha de seguridad que afecte a la Información de TRACASA GLOBAL y, en cualquier caso, dentro de los tiempos que establecen las normativas aplicables en su caso (NIS, GDPR, PCI, LPIC).

c. El PROVEEDOR deberá recopilar y proporcionar toda información que le sea requerida por TRACASA GLOBAL y, en los plazos indicados por TRACASA GLOBAL, identificando una persona única de contacto que asuma la responsabilidad de las acciones de comunicación formales en la gestión y comunicación de incidentes de seguridad, según viene indicado en las normativas de TRACASA GLOBAL.

d. El PROVEEDOR deberá disponer de un procedimiento de gestión y comunicación de incidentes de seguridad que afecten al Encargo y/o a la Información de TRACASA GLOBAL. El procedimiento implicará, al menos, la elaboración y mantenimiento de un registro de incidencias en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

e. El PROVEEDOR no podrá realizar comunicación alguna con el incidente en la que se haga referencia a TRACASA GLOBAL, sin la comunicación y consentimiento previo de TRACASA GLOBAL.

f. TRACASA GLOBAL se reserva el derecho de exigir a El PROVEEDOR la entrega de un certificado de resolución de incidente por parte de un tercero independiente.

g. El PROVEEDOR debe garantizar la salvaguarda de la Información de TRACASA GLOBAL a través de mecanismos de respaldo y recuperación, así como la continuidad del Encargo.

h. El PROVEEDOR deberá disponer de un procedimiento de continuidad del servicio y recuperación de la información, así como de las medidas necesarias que garanticen tanto la continuidad del servicio que se presta, como la recuperación de la información de acuerdo a los requisitos de continuidad de TRACASA GLOBAL, siendo revisadas tanto el procedimiento como las medidas de manera periódica.

i. El PROVEEDOR informará, inmediatamente, a TRACASA GLOBAL cualquier cambio en el entorno del PROVEEDOR que afecte al negocio o al Encargo.

En caso de que ocurra cualquier incidente, tal como se comenta en este apartado del Anexo habrá que comunicarlo a Tracasa Global de acuerdo a los siguientes contactos:

- Correo electrónico dirigido a: ayesa CSOC <csoc@ayesa.com>; Rodrigo Abad Ruiz <rabad@itracasa.es>; Emilio Rubio Cia <erubio@itracasa.es>; Helpdesk Sistemas Helpdesk.Sistemas@itracasa.es
- Teléfonos:
  - 948289000 extensión 107
  - 683 628 219 (Iñigo Carrera – SOC)

Las obligaciones anteriores a cargo del PROVEEDOR son, sin perjuicio, de aquellas que le sean de aplicación y aquellas otras que se acuerden entre las partes en los casos en los que la Información de TRACASA GLOBAL implique información confidencial, altamente confidencial o el tratamiento de Datos Personales, así como en los casos que impliquen a sistemas o usos de tecnologías.

3. Seguridad de la Información de TRACASA GLOBAL. Requerimientos específicos

El PROVEEDOR se compromete a aplicar las obligaciones de seguridad requeridas en el ámbito de la seguridad de la información incluidas en el presente Anexo y en cualquier otra documentación o acuerdo que se alcance entre TRACASA GLOBAL y el PROVEEDOR en relación al Encargo. Las obligaciones de seguridad a continuación descritas son, sin perjuicio, de aquellas que le sean de aplicación en relación al Encargo.

3.1. Cumplimiento

Requisitos referentes al cumplimiento normativo de Tracasa Global, donde se especifica la aceptación y adaptación por parte del proveedor de las prácticas de seguridad de la información definidas por Tracasa Global.

Aplicable al proveedor en caso de que tenga acceso o trate información de Tracasa Global, independientemente de su nivel de sensibilidad.

a. El PROVEEDOR conoce y se obliga a aplicar y cumplir, sin restricciones, la normativa y prácticas internas en materia de seguridad de la información del grupo TRACASA GLOBAL. En el caso de que el PROVEEDOR identifique la imposibilidad de cumplir alguna norma o práctica interna de TRACASA GLOBAL, lo notificará de manera inmediata a ésta facilitando una alternativa que garantice, en cualquier caso la seguridad y protección de la Información de TRACASA GLOBAL y que deberá ser objeto de aceptación por TRACASA GLOBAL. En otro caso, se considerará que el PROVEEDOR ha incurrido en un incumplimiento de sus obligaciones.

b. El PROVEEDOR se compromete a hacer uso de las metodologías de seguridad definidas por TRACASA GLOBAL, así como implementar todos los requerimientos de seguridad que se comuniquen, en su caso, durante el periodo de ejecución del Encargo.

3.2. Protección de la información

Requisitos referentes a la garantía de preservación de la confidencialidad e integridad de la información, así como la disponibilidad de esta misma y de los servicios prestados.

Aplicable al proveedor en caso de que tenga acceso o trate información de Tracasa Global confidencial, altamente confidencial o afectados por regulaciones. Queda incluido en la obligatoriedad de cumplimiento de este requisito, el proveedor que soporte un servicio sobre sus sistemas y/o infraestructuras.

a. El PROVEEDOR deberá garantizar la integridad y confidencialidad de la Información de TRACASA GLOBAL a través de los oportunos mecanismos que garanticen que la Información de TRACASA GLOBAL no sea inteligible ni manipulada por terceros, así como mecanismos que garanticen la confidencialidad de la Información de TRACASA GLOBAL, como el de cifrado, con independencia del estado de reposo o tránsito en el que se encuentre, y con independencia del o de los Sistemas de Información, y/o dispositivos en que se maneje y redes por las que transite, utilizando algoritmos estándar seguros para el apropiado cifrado de la Información así como protocolos de transferencia seguros y securización de los canales de comunicación, especialmente ante el intercambio de Información confidencial de TRACASA GLOBAL.

3.3. Gestión de accesos

Requisitos de seguridad para asegurar el control de accesos a la información y los sistemas que soporten el servicio.

Aplicable al proveedor en caso de que establezca conexiones directas a la infraestructura de Tracasa Global, así como en el caso de que soporte un servicio sobre sus sistemas y/o infraestructuras. De la misma manera queda incluido en la obligatoriedad de cumplimiento de estos requisitos el proveedor con acceso y/o tratamiento a la información de Tracasa Global confidencial, altamente confidencial y/o afectada por regulaciones, independientemente del entorno donde se realice el tratamiento.

a. El PROVEEDOR deberá identificar los diferentes colectivos que accedan a la Información de TRACASA GLOBAL o a sus Sistemas de Información, incluyendo los Empleados del PROVEEDOR, y los empleados de TRACASA GLOBAL, distinguiendo aquellos con mayores permisos sobre la Información y/o los Sistemas de Información, en adelante usuarios privilegiados, como cuentas administradoras de sistemas.

b. El PROVEEDOR deberá establecer y desplegar mecanismos de control que garanticen el acceso restringido y adecuado a la Información de TRACASA GLOBAL , adoptando las medidas que garanticen la correcta identificación y autenticación personal y unívoca de todos los Empleados del PROVEEDOR que accedan a la Información de TRACASA GLOBAL o a sus Sistemas de Información como usuarios (los "**Usuarios**"), así como que los Usuarios son usuarios autorizados.

   Los Usuarios accederán por medio de unas credenciales formadas por un identificador y una contraseña o por otro mecanismo que provea igual o mayor seguridad.

   Los Usuarios no identificados nominalmente, usuarios genéricos, estarán prohibidos para el acceso a los Sistemas de Información involucrados en el Encargo, únicamente pudiendo ser utilizados previa autorización de TRACASA GLOBAL.

c. Las funciones y obligaciones de cada uno de los Usuarios o perfiles de Usuarios con acceso a la Información de TRACASA GLOBAL estarán claramente definidas. Los Usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones y solo aquellos que, por razón de sus funciones lo precisen, podrá tener acceso a la Información de TRACASA GLOBAL y a los lugares donde se hallen instalados los equipos físicos que den soporte a los Sistemas de Información.

d. El PROVEEDOR deberá definir la metodología y controles específicos a aplicar para la gestión segura de acceso de usuarios privilegiados a los Sistemas de Información con el fin de reducir violaciones de seguridad, comprometiéndose a hacer uso de estas durante la ejecución del Encargo, como por ejemplo el aumento de complejidad en la creación de contraseñas, permitiendo controlar, proteger y securizar cuentas de usuarios y sus privilegios asignados.

e. El PROVEEDOR deberá disponer de una relación actualizada de Usuarios y perfiles de Usuarios, y los accesos autorizados para cada uno de ellos, que será disponible por TRACASA GLOBAL en cualquier momento previa petición razonada.

f. El PROVEEDOR deberá disponer e implementar un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al Sistema de Información. La periodicidad con la que tienen que ser cambiadas las contraseñas en ningún caso será superior a un año y, mientras estén vigentes, se almacenarán de forma ininteligible.

   De cada intento de acceso se guardarán, como mínimo, la identificación del Usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. El período mínimo de conservación de los datos registrados será de dos años. Esta información será accesible a TRACASA GLOBAL previo a su solicitud debidamente razonada.

g. Los mecanismos que permiten el registro de accesos no deben permitir la desactivación ni la manipulación de los mismos.

3.4. Gestión de acceso a la infraestructura de TRACASA GLOBAL

Requisitos de seguridad para asegurar el control de accesos a la información y los sistemas de información de Tracasa Global.

Aplicable al proveedor en caso de que establezca conexiones directas a la infraestructura y/o sistemas de Tracasa Global, especialmente de establecer un acceso a la infraestructura a través de equipos no gestionados por Tracasa Global.

a. El PROVEEDOR y los Empleados del PROVEEDOR quedarán obligados al cumplimiento de la normativa interna del grupo TRACASA GLOBAL que le sea de aplicación como Usuarios temporales de los Sistemas de TRACASA GLOBAL y sus infraestructuras, todo ello, con el fin de garantizar la confidencialidad de la Información de TRACASA GLOBAL.

b. El PROVEEDOR y los Empleados del PROVEEDOR respetarán y aplicarán, al menos, aquellas medidas de seguridad que TRACASA GLOBAL tuviera implantadas en sus instalaciones, servidores o Sistemas de Información.

c. En el caso de requerir acceso lógico a la infraestructura de TRACASA GLOBAL, entendiendo por infraestructura sistemas de Información, aplicaciones y plataformas, para la administración y gestión del Encargo, el PROVEEDOR deberá hacer uso de las herramientas de seguridad remota a los sistemas proporcionadas por TRACASA GLOBAL, en caso de que estas sean proporcionadas.

d. TRACASA GLOBAL se reserva el derecho a monitorear, suspender, restringir o revocar el acceso a través de los códigos de Usuario facilitados, en cualquier momento y sin previo aviso. El PROVEEDOR queda obligado a informar a los Empleados del PROVEEDOR de esta facultad de monitorizar el acceso a los Sistemas de Información de TRACASA GLOBAL y la actividad que se realice por los Usuarios con la cuenta de usuario facilitada.

e. TRACASA GLOBAL no será responsable por cualquier pérdida o daño resultante de la adopción de cualquiera de las medidas citadas en el párrafo anterior. Si la suspensión, restricción o cancelación del acceso a los Empleados del PROVEEDOR se realiza a instancias de TRACASA GLOBAL y sin dolo o culpa del PROVEEDOR, e interfiriere en la ejecución del Encargo de forma que la hiciera imposible, en ningún caso será considerado como un incumplimiento de las obligaciones del PROVEEDOR de ejecutar el Encargo.

3.5. Desarrollo seguro de aplicativos y protección de aplicaciones

Requisitos de desarrollo de sistemas y software para el aseguramiento de la calidad de este, así como de aplicaciones utilizadas para la prestación de servicios.

Aplicable al proveedor en caso de que desarrolle un software u aplicativo específico para Tracasa Global o que preste una solución/herramienta corporativa, especialmente si esta solución es accesible desde la red externa o maneja datos confidenciales o afectados por regulaciones.

3.5.1. Desarrollo seguro de aplicativos

a. El PROVEEDOR del servicio deberá garantizar la calidad y seguridad del código generado, siguiendo de manera razonable el modelo de desarrollo seguro instaurado en TRACASA GLOBAL por el que se definen las guías en materia de seguridad en el desarrollo de software y que será compartido con el PROVEEDOR al inicio del Encargo.
b. TRACASA GLOBAL podrá realizar una evaluación a El PROVEEDOR en conocimientos de desarrollo seguro para garantizar que tiene una visión holística de la seguridad, conoce aspectos teóricos de seguridad y conoce los errores de codificación más comunes con impacto desde el punto de vista de la seguridad.

c. El PROVEEDOR deberá desarrollar y configurar el aplicativo siguiendo los estándares de seguridad para una estrategia de defensa en profundidad y mínima superficie expuesta, incluyendo, en caso que sea de aplicación, los siguientes requerimientos:

    i. La aplicación deberá estar diseñada para evitar problemas de fuga de información, como datos confidenciales enviados a través de URL, manejo de errores, credenciales codificadas, almacenamiento de credenciales de texto plano y enmascaramiento de datos entre entornos.

ii. Todos los flujos de la lógica de negocio deberán estar protegidos contra alteraciones o modificaciones, especialmente cualquier funcionalidad transaccional. Cualquier excepción al flujo de trabajo deberá ser registrado y los usuarios deberán ser redirigidos a páginas de error personalizadas.
iii. Toda entrada de la aplicación deberá ser sanitizada y se deberá aplicar la codificación de salida utilizando un enfoque de lista blanca. Toda validación de datos deberá realizarse en el lado cliente y servidor y se deberá prestar especial atención a las funcionalidades de carga de archivos para aplicar restricciones en función del tipo de contenido, el tamaño y las restricciones de extensión de los archivos admitidos así como para analizar todos los archivos con un software antimalware con el fin de identificar archivos maliciosos.
iv. El diseño de la aplicación deberá contener controles contra las condiciones de Denegación de Servicio Distribuido, evitar solicitudes de procesamiento pesadas y limitar la respuesta o automatizar el envío de solicitudes, evitando una indisponibilidad en la aplicación. La aplicación se implementará utilizando las soluciones de Denegación de Servicio Distribuido disponibles, cuando corresponda.

d. El PROVEEDOR se compromete a resolver aquellas vulnerabilidades críticas o explotables y altas existentes, que puedan poner en riesgo la disponibilidad, confidencialidad e integridad de los servicios en entornos productivos. Esta resolución deberá llevarse a cabo antes de la puesta en producción del código desarrollad y de acuerdo con los tiempos de resolución definidos en el Apéndice A.

e. Si fuentes externas o internas a TRACASA GLOBAL revelan, publican o comunican la existencia de vulnerabilidades críticas o explotables y altas correspondientes a entornos/aplicaciones que han sido desarrolladas por EL PROVEEDOR en el ejercicio del Encargo, estas deberán ser resueltas igualmente en los plazos definidos en el Apéndice A.

f. El PROVEEDOR se compromete a no utilizar datos de producción en entornos de no-producción, salvo aprobación explícita y documentada de TRACASA GLOBAL.

g. El PROVEEDOR se compromete a que, en caso de acceder a datos personales, no podrán usarse tales datos sin anonimizar en entornos no productivos. De ser necesario, estos entornos tendrán que estar protegidos con el mismo nivel de seguridad que el aplicado a un entorno productivo.

3.5.2. Protección de aplicaciones

a. El PROVEEDOR deberá describir los elementos de seguridad que implementará, operará y administrará para la protección de aplicaciones utilizadas en el Encargo, compartiendo estos esquemas con TRACASA GLOBAL.
b. Las aplicaciones deberán ser sometidas al proceso de revisión de seguridad definido por TRACASA GLOBAL, determinando en cada caso cuándo es aplicable dependiendo de la criticidad, tipo de exposición y/o los datos que se manejen. Esta revisión puede incluir, entre otras, la revisión de código fuente de la aplicación, análisis de vulnerabilidades en dependencias así como actividades de pruebas de hacking ético o test de intrusión que TRACASA GLOBAL considere oportunas, con autorización previa del PROVEEDOR.

3.6. Respuesta de incidentes y gestión de continuidad de negocio

Requisitos que garanticen la correcta notificación de incidentes, así como planes de respuestas, asegurando la continuidad del servicio prestado.

Aplicable al proveedor en caso de que soporte un servicio sobre sus sistemas y/o infraestructuras, especialmente si en esta infraestructura se almacena y/o trata información de Tracasa Global confidencial, altamente confidencial o datos regulados (GDPR, PCI, SCIF…).

a. El PROVEEDOR deberá comunicar planes de tratamiento de datos que el PROVEEDOR contempla ante posibles violaciones de seguridad y los tiempos que tendrán efecto esas acciones.

b. El PROVEEDOR deberá conservar una copia de respaldo de la Información de TRACASA GLOBAL y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los Sistemas de Información en los que se encuentra, que deberá cumplir en todo caso las medidas de seguridad exigidas en este Anexo y en cualquier otra documentación o acuerdo que se alcance entre TRACASA GLOBAL y el PROVEEDOR en relación al Encargo, o se utilicen mecanismos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

c. El PROVEEDOR deberá garantizar que la disponibilidad, calidad, capacidad y los recursos adecuados sean planificados, preparados y medidos para proporcionar el rendimiento requerido del sistema de acuerdo con las obligaciones legales y de cumplimiento normativo. Además, se realizarán previsiones de necesidades futuras de capacidad para mitigar el riesgo de sobrecarga del Sistema de Información.

4. Reglas de jerarquía

En caso de conflicto o contradicción entre el presente Anexo y el Contrato o, en su ausencia del mismo, la RFP, respecto de las materias aquí reguladas, prevalecerá, en todo caso, lo dispuesto en el presente Anexo.

En caso de conflicto o contradicción referente a la remediación en cuestiones de seguridad citadas a lo largo del presente Anexo y el apartado de Acuerdo de Nivel de Servicio del Contrato o, en ausencia del mismo, la RFP, prevalecerá los plazos estipulados en el presente Anexo.

En caso de conflicto o contradicción entre diferentes apartados del presente Anexo, prevalecerá el contenido que establezca un mayor nivel de protección.

En todo lo no regulado expresamente en el presente Anexo, aplicará lo dispuesto en el Contrato o, en su ausencia del mismo, la RFP.

TRABAJOS CATASTRALES	EL PROVEEDOR

Firma

Cargo

Fecha:

Firma

Cargo

Apéndice A: Tiempos de resolución de vulnerabilidades detectadas en códigos software

(Cláusula 3.5.1. d)

En caso de que el Encargo incluya desarrollo software de aplicativos por parte de el PROVEEDOR, el PROVEEDOR deberá resolver las vulnerabilidades identificadas según los tiempos definidos en base a la clasificación de éstas, siguiendo las buenas prácticas de seguridad:

Clasificación de las vulnerabilidades	Tiempo de Resolución
Críticas o Explotables	Inmediato
Altas	1 mes
Medias	3 meses
Bajas	1 año

Definiéndose las criticidades en base a las vulnerabilidades/anomalías encontradas y al riesgo que suponen:

- Crítica o Explotable: impacto severo a los activos de TRACASA GLOBAL. Vulnerabilidades cuya puntuación se encuentra entre 9.0-10.0 del sistema de puntajes Common Vulnerability Score System, en adelante CVSS,y que implica el compromiso de los servidores y/o infraestructura que afecta al Encargo. Su explotación es directa ya que no es necesario que un usuario malintencionado requiera altos niveles de conocimiento para irrumpir en los sistemas de forma sencilla o conocimientos sobre la víctima.
- Alto: impacto significativo a los activos de TRACASA GLOBAL. Vulnerabilidades cuya puntuación se encuentra entre 7.0-8.9 del sistema de puntajes CVSS y suele conllevar un grado de dificultad elevado. Su explotación puede dar lugar a una elevación de privilegios e incluso puede llevar a la filtración de datos, viéndose afectadas las operaciones diarias de los distintos negocios de TRACASA GLOBAL.
- Medio: impacto moderado sobre los activos de TRACASA GLOBAL. Vulnerabilidades cuya puntuación se encuentra entre 4.0-6.9 del sistema de puntajes CVSS. Son vulnerabilidades que requieren del uso de técnicas de ingeniería social, que el usuario malintencionado se encuentre en la misma red que la víctima o de un usuario con privilegios.
- Bajo: impacto bajo o limitado sobre los activos de TRACASA GLOBAL. Vulnerabilidades cuya puntuación se encuentra entre 0.1-3.9 del sistema de puntajes CVSS. Normalmente este tipo de vulnerabilidades suelen requerir para su explotación de acceso físico o local por parte de un usuario malintencionado a los sistemas de TRACASA GLOBAL.