**Plan de Seguridad de la Información**
**Anexo Regulatorio de la UE**

Este Anexo describe los compromisos de Infor con respecto a requisitos específicos bajo las directivas, regulaciones y leyes nacionales de implementación aplicables de ciberseguridad y gobernanza de datos de la UE **("Ley de Ciberseguridad y Gobernanza de Datos Aplicable")**, y se incorpora, donde sea aplicable al Cliente (con aplicabilidad como se define a continuación), en los contratos del Cliente ejecutados con Infor (colectivamente, los **"Contratos"**). En caso de cualquier conflicto o inconsistencia entre los términos de este Anexo y cualquier otro término de los Contratos, este Anexo prevalecerá.

## I. GENERAL

### 1. DEFINICIONES

1.1 Los términos en mayúsculas utilizados pero no definidos en este Anexo tendrán los significados proporcionados en el Plan de Seguridad de la Información, ubicado en www.infor.com/security-plan (el **"PSI"**). Los términos "Proceso TIC", "Producto TIC", "Servicio TIC", "Incidentes", "Sistemas de Red e Información", "Riesgo" y "Amenaza Cibernética Significativa" tendrán el significado que se les da en la Ley de Ciberseguridad y Gobernanza de Datos Aplicable.

### 2. CUMPLIMIENTO Y COOPERACIÓN

2.1 Infor cumplirá con las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables a su negocio y, a solicitud razonable, cooperará con cualquier autoridad gubernamental competente relevante y/o Cliente respecto al cumplimiento por parte de Infor de sus obligaciones bajo los Contratos a la luz de las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables. Tanto Infor como el Cliente se informarán y alertarán mutuamente sobre cualquier cambio significativo o evento, dificultad, riesgo o información que pueda tener un efecto adverso en los Servicios TIC o en el cumplimiento de los Contratos (a menos que la distribución de dicha información esté prohibida bajo la Ley Aplicable).

### 3. FECHA DE ENTRADA EN VIGOR

3.1 Los términos de este Anexo entran en vigor en la fecha en que la Ley de Ciberseguridad y Gobernanza de Datos Aplicable se haga efectiva y exigible.

### 4. ACTUALIZACIONES

4.1 El Cliente reconoce que las medidas de seguridad técnicas y organizativas descritas en este Anexo están sujetas a requisitos actualizados bajo las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables y al progreso y desarrollo técnico, y que Infor puede actualizar o modificar las medidas de vez en cuando, siempre que tales actualizaciones y modificaciones no resulten en la degradación de la seguridad general de los Servicios proporcionados al Cliente.

### 5. LEY APLICABLE

5.1 Este Anexo se rige y se hace cumplir de acuerdo con la ley aplicable establecida en los Contratos, a menos que una ley aplicable separada sea requerida por la Ley de Ciberseguridad y Gobernanza de Datos Aplicable, en cuyo caso, para los propósitos de este Anexo, la ley aplicable así requerida controlará sobre la ley aplicable de los Contratos.

### 6. RESPONSABILIDAD

6.1 Infor y el Cliente acuerdan que la responsabilidad total de cada parte y sus Afiliadas (según se define en los Contratos) que surja de o esté relacionada con este Anexo, ya sea basada en incumplimiento de contrato, agravio u otro, está, entre las partes (incluidas las Afiliadas), sujeta a las disposiciones aplicables sobre limitación de responsabilidad en los Contratos. Además, Infor no será responsable por ninguna violación por parte del Cliente de las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables o por un incumplimiento del Cliente con los requisitos de la autoridad competente.

## II. DIRECTIVA NIS 2

### 1. ALCANCE Y DEFINICIONES

1.1 Los términos y condiciones establecidos en la Sección II de este Anexo se aplican únicamente a los Clientes de la UE que cumplan con los criterios y umbrales de entidades "importantes" o "esenciales" reguladas bajo la Directiva NIS 2. Para evitar dudas, se considera que la Sección I se incorpora a esta Sección II.

1.2 **"Directiva NIS 2"** significa la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre medidas para un alto nivel común de Ciberseguridad en toda la UE, que enmienda el Reglamento (UE) No 910/2014 y la Directiva (UE) 2018/1972, y que deroga la Directiva (UE) 2016/1148, y cualquier regulación de implementación correspondiente.

### 2. GOBERNANZA

2.1 Infor tiene cuerpos de gestión dentro de su oficina de seguridad que aprueban, supervisan y son responsables de la implementación de las medidas de gestión de riesgos de ciberseguridad de Infor, incluido el PSI.

### 3. PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN

3.1 Infor ha implementado y mantendrá el PSI de manera que: (A) esté diseñado para: (1) asegurar la seguridad y confidencialidad de los Sistemas de Red e Información de Infor; (2) proteger contra cualquier amenaza o peligro anticipado a la seguridad o integridad de los Sistemas de Red e Información de Infor; y (3) proteger contra el acceso no autorizado o el uso de los Sistemas de Red e Información; y (B) establezca la política de Infor para responder a cualquier Incidente.

3.2 El PSI está disponible en: www.infor.com/security-plan.

### 4. MEDIDAS DE GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

4.1 Infor ha implementado y mantendrá medidas de gestión de riesgos de ciberseguridad que:

(A) sean proporcionales a los riesgos planteados a los Sistemas de Red e Información de Infor teniendo en cuenta el estado de la técnica y, cuando sea aplicable, los estándares europeos e internacionales relevantes, así como el costo de implementación;

(B) se basen en un enfoque de "todos los peligros", que tiene como objetivo proteger los Sistemas de Red e Información de Infor y el entorno físico de esos sistemas de Incidentes; y

(C) incluyan al menos lo siguiente: (a) políticas sobre análisis de riesgos y seguridad de sistemas de información; (b) medidas para identificar cualquier riesgo de Incidentes, incluidos procedimientos de manejo de incidentes; (c) continuidad del negocio, como gestión de copias de seguridad y recuperación ante desastres, y gestión de crisis; (d) seguridad de la cadena de suministro, incluidos aspectos relacionados con la seguridad en las relaciones entre Infor y sus proveedores o prestadores de servicios directos; (e) seguridad en la adquisición, desarrollo y mantenimiento de Sistemas de Red e Información, incluidos la gestión y divulgación de vulnerabilidades; (f) políticas y procedimientos para evaluar la efectividad de las medidas de gestión de riesgos de ciberseguridad de Infor; (g) prácticas básicas de higiene cibernética, como principios de confianza cero, actualizaciones de software, configuración de dispositivos, segmentación de red, gestión de identidades y accesos o concienciación de los usuarios, formación en ciberseguridad para el personal de forma regular y concienciación sobre amenazas cibernéticas, phishing o técnicas de ingeniería social; (h) políticas y procedimientos respecto al uso de criptografía y encriptación; (i) seguridad de recursos humanos, políticas de control de acceso y gestión de activos; y (j) el uso de autenticación multifactorial o soluciones de autenticación continua, comunicaciones seguras de voz, video y texto y sistemas de comunicación de emergencia seguros dentro de Infor.

### 5. CADENA DE SUMINISTRO

5.1 Infor declara y garantiza que las medidas de seguridad de la cadena de suministro implementadas por Infor toman en cuenta los siguientes criterios: (a) las vulnerabilidades específicas de cada proveedor directo y prestador de servicios de Infor; (b) la calidad general de los productos y prácticas de ciberseguridad de los proveedores y prestadores de servicios de Infor, incluidos sus procedimientos de desarrollo seguro; y, cuando sea aplicable, (c)

los resultados de cualquier evaluación coordinada de riesgos de seguridad de cadenas de suministro específicas críticas de Servicios TIC, Productos TIC o Procesos TIC llevadas a cabo por los Estados Miembros de la UE y cualquier autoridad competente.

5.2 Infor realiza la debida diligencia en sus proveedores de servicios externos para evaluar sus medidas de gestión de riesgos de ciberseguridad y ejecuta contratos con dichos proveedores de servicios externos con requisitos de ciberseguridad y gobernanza de datos sustancialmente similares a este Anexo.

5.3 Infor proporcionará evidencia razonable de tales medidas de seguridad de la cadena de suministro dentro de un plazo razonable después de la solicitud del Cliente.

**6. RESPUESTA ANTE INCIDENTES**

6.1 Infor monitoreará sus Sistemas de Red e Información para detectar accesos no autorizados e implementará una política de respuesta ante Incidentes que especifique las acciones a tomar cuando Infor detecte o se entere de cualquier Incidente.

6.2 Si Infor se entera de un Incidente Significativo que afecta al Cliente, Infor deberá:

(A) Notificar al Cliente de la siguiente manera:

(1) Rápidamente y sin demora indebida (y en cualquier caso dentro de las 24 horas de haberse enterado de dicho Incidente Significativo): (a) notificar al Cliente sobre la ocurrencia de dicho Incidente Significativo; y (b) proporcionar al Cliente información detallada sobre el Incidente Significativo, incluyendo lo siguiente: (i) si se sospecha que el Incidente Significativo fue causado por actos ilícitos o malicioso o podría tener un impacto transfronterizo; (ii) cualquier información para determinar cualquier impacto transfronterizo del Incidente Significativo; y (iii) una evaluación inicial del Incidente Significativo, incluyendo su gravedad e impacto, así como, cuando esté disponible, los indicadores de compromiso;

(2) Rápidamente y sin demora indebida, proporcionar al Cliente la siguiente información complementaria sobre el Incidente Significativo: (a) una descripción detallada del Incidente Significativo, incluyendo su gravedad e impacto; (b) el tipo de amenaza o causa raíz que probablemente haya desencadenado el Incidente Significativo; (c) medidas de mitigación aplicadas y en curso; y (d) donde sea aplicable, el impacto transfronterizo del Incidente Significativo.

(B) Investigar y llevar a cabo un análisis razonable de la(s) causa(s) de dicho Incidente Significativo;

(C) Proporcionar actualizaciones periódicas de cualquier investigación en curso al Cliente;

(D) Desarrollar e implementar un plan adecuado para mitigar y remediar la causa de dicho Incidente Significativo en la medida en que dicha causa esté bajo el control de Infor; y

(E) Cooperar con la investigación razonable del Cliente y los esfuerzos del Cliente para cumplir con cualquier notificación aplicable a dicho Incidente Significativo, incluyendo asistir en la redacción de cualquier informe sobre el Incidente Significativo a las autoridades competentes.

6.3 Si Infor se entera de una Amenaza Cibernética Significativa que afecta al Cliente (incluidas las vulnerabilidades de las aplicaciones de Infor publicadas que cumplen con la definición de Amenaza Cibernética Significativa), Infor deberá:

(A) Notificar al Cliente rápidamente y sin demora indebida sobre dicha Amenaza Cibernética Significativa;

(B) Proporcionar al Cliente información detallada sobre el impacto de la Amenaza Cibernética Significativa en el Cliente, según lo conocido por Infor;

(C) Investigar y llevar a cabo un análisis razonable de la(s) causa(s) de dicha Amenaza Cibernética Significativa;

(D) Desarrollar e implementar un plan adecuado para remediar la causa de dicha Amenaza Cibernética Significativa en la medida en que dicha Amenaza Cibernética Significativa se materialice y la causa esté bajo el control de Infor; y

(E) Cumplir con las solicitudes razonables del Cliente para proporcionar información sobre la Amenaza Cibernética Significativa que el Cliente pueda usar en sus notificaciones a terceros requeridas relacionadas con la Amenaza Cibernética Significativa, si es que alguna es requerida bajo las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables.

## 7. AUDITORÍA

7.1 Infor mantendrá al menos una de las siguientes certificaciones y declaraciones relacionadas con sus Servicios Cloud (según corresponda), e Infor, a solicitud por escrito del Cliente, proporcionará al Cliente prueba de tales certificaciones y/o declaraciones:

(1) SSAE SOC 2 Tipo 2 (también conocido como AICPA TSC 2014 Tipo 2)
(2) ISO 27001:2022
(3) FedRAMP

Infor se asegurará que sus proveedores de servicios externos mantengan al menos una de las certificaciones y declaraciones anteriores relacionadas con los servicios que dicho proveedor de servicios externo proporciona a Infor y/o a los clientes de Infor, o proporcione evidencia alternativa satisfactoria de sus medidas de gestión de riesgos de ciberseguridad en relación con el alcance de los servicios proporcionados.

7.2 Además de los informes de auditoría descritos en la Sección 7.1 anterior, si es solicitado por el Cliente y sujeto a las obligaciones de confidencialidad de los Contratos, no más de una vez al año, a menos que el Cliente actúe conforme a una solicitud de autoridad gubernamental competente (en cuyo caso los límites anuales no se aplicarán), Infor responderá prontamente por escrito a cualquier consulta razonable o cuestionario del Cliente (y/o sus agentes) respecto al contenido del programa de seguridad de Infor y proporcionará evidencia razonable de su cumplimiento con los requisitos de este Anexo, incluyendo copias generalmente disponibles de datos, documentos e información relacionados con los Servicios necesarios para asistir al Cliente con su cumplimiento de cualquier solicitud u orden vinculante recibida de cualquier autoridad gubernamental competente. Infor proporcionará la información relevante sin demora indebida (y en cualquier caso dentro del plazo proporcionado en la solicitud u orden vinculante que el Cliente haya recibido de la autoridad gubernamental competente).

7.3 El Cliente puede, una vez al año, auditar el cumplimiento de Infor con sus obligaciones bajo este Anexo, incluyendo auditar las prácticas de seguridad de TI de Infor y los entornos de control aplicables, de acuerdo con el proceso descrito en esta Sección 7, solo si:

(A) Infor no ha proporcionado evidencia suficiente de su cumplimiento con las medidas de gestión de riesgos de ciberseguridad descritas en este Anexo a través de los informes y documentación referenciados en la Sección 7.2 anterior, o, si aplica, cualquier otro informe de auditoría u otra información que Infor ponga generalmente a disposición de sus clientes;

(B) Ha ocurrido un Incidente Significativo;

(C) Infor ha notificado al Cliente que está sujeta a una solicitud de acceso gubernamental relacionada con los Datos del Cliente;

(D) Una auditoría es solicitada formalmente por una autoridad gubernamental competente con jurisdicción sobre el Cliente; o

(E) La Ley de Ciberseguridad y Gobernanza de Datos Obligatoria Aplicable confiere al Cliente un derecho de auditoría directo.

7.4 Antes del inicio de una auditoría, el Cliente e Infor acordarán mutuamente el alcance, tiempo, duración, control y requisitos de evidencia. El Cliente puede usar una firma auditora externa independiente acreditada para realizar la auditoría en su nombre, siempre que el auditor externo sea mutuamente acordado por el Cliente e Infor (lo cual no incluirá auditores externos que sean competidores de Infor o que no estén adecuadamente calificados o sean independientes). El Cliente acepta que la auditoría se realizará sin interferir de manera irrazonable con las actividades comerciales de Infor (o de sus subcontratistas), durante el horario comercial regular con una notificación razonable por adelantado, y sujeto a las políticas de seguridad aplicables y procedimientos de

confidencialidad de Infor (o de sus subcontratistas). Cuando no se permitan auditorías in situ de centros de datos físicos, sistemas o instalaciones, Infor trabajará con el Cliente (y sus subcontratistas, si corresponde) para alcanzar una resolución mutuamente aceptable suficiente para proporcionar la información necesaria para que el Cliente cumpla con los requisitos de auditoría bajo las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables. Ni el Cliente, ni el auditor, tendrán acceso a ningún dato de otros clientes de Infor o a sistemas o instalaciones de Infor no involucradas en los Servicios proporcionados al Cliente. El Cliente proporcionará los resultados de cualquier auditoría a Infor. Las partes acordarán mutuamente cualquier informe o remediación correspondiente. Infor utilizará esfuerzos comerciales razonables para abordar las remediaciones acordadas.

7.5 El Cliente es responsable de todos los costos y tarifas relacionados con la auditoría, incluidos todos los costos y tarifas razonables que Infor incurra para la auditoría y cualquier costo y tarifa que Infor incurra de cualquier subcontratista cuando la auditoría involucre a un subcontratista, a menos que dicha auditoría revele un incumplimiento material por parte de Infor de este Anexo, en cuyo caso Infor asumirá sus propios gastos de esa parte de la auditoría relacionada con el incumplimiento.

## III. DORA

### 1. ÁMBITO Y DEFINICIONES

1.1 Los términos y condiciones establecidos en la Sección III de este Anexo se aplican exclusivamente a los Clientes de la UE que cumplan con los criterios y umbrales para entidades financieras reguladas por DORA. Para evitar dudas, se considera que la Sección I se incorpora a esta Sección III; párrafos específicos en la Sección II también se aplican si se hace referencia específica en esta Sección III.

1.2 "**DORA**" significa el Reglamento de Resiliencia Operativa Digital (Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022).

### 2. SERVICIOS

2.1 El Servicio TIC proporcionado por Infor al Cliente se describe en los Contratos.

### 3. UBICACIÓN

3.1 Para evitar dudas, los datos de producción del Cliente se almacenan en la ubicación de despliegue seleccionada e Infor no moverá ningún dato de producción del Cliente fuera de esta ubicación sin la aprobación y dirección previas por escrito del Cliente. A la dirección del Cliente, cantidades limitadas de datos personales pueden ser accedidos remotamente desde fuera de la ubicación de despliegue seleccionada para los fines de proporcionar soporte y servicios al Cliente. Infor notificará al Cliente con antelación si prevé cambiar las ubicaciones (es decir, las regiones o países) donde se proporcionarán los Servicios y donde se almacenarán y procesarán los Datos del Cliente, según se establece en los Contratos.

### 4. PROGRAMA DE SEGURIDAD Y SLA

4.1 Se aplican las medidas de gestión de riesgos de ciberseguridad descritas anteriormente en la Sección II.3 y Sección II.4. Los compromisos de respuesta ante incidentes de Infor en la Sección II.6 también se aplican. Para evitar dudas, se considera que la insolvencia de Infor se agrega como una obligación para la devolución de los Datos del Cliente bajo el PSI.

4.2 Los compromisos de disponibilidad del nivel de servicio de Infor se describen en el Acuerdo de Nivel de Servicio en https://www.infor.com/service-level-description (**"SLA"**). Los compromisos de soporte específicos del producto se describen en el Formulario de Pedido, si corresponde.

### 5. PROGRAMA DE ENTRENAMIENTO Y CONCIENCIACIÓN EN SEGURIDAD TIC

5.1 En caso de que Infor acceda a los sistemas de información de red locales del Cliente como parte de los Servicios, el Cliente puede solicitar a Infor participar, con un aviso razonable, en cualquier programa de concienciación en seguridad TIC y/o entrenamiento en resiliencia operativa digital que el Cliente proporcione u opere en conexión con su negocio ("Entrenamiento"). En este sentido, las partes acuerdan que:

(A) La frecuencia, el tiempo y la duración de dicho Entrenamiento se acordarán por adelantado entre las partes;

(B) Infor se reserva el derecho de recuperar del Cliente sus gastos razonables y debidamente incurridos; y

(C) La participación de Infor en dicho Entrenamiento no requerirá que haga algo que pueda interferir, prevenir o impedir que Infor proporcione los Servicios TIC o de otra manera cumpla con sus obligaciones bajo los Contratos.

## 6. TERMINACIÓN

6.1 Además de los derechos de terminación establecidos en los Contratos y en otros lugares en estos términos y condiciones, según lo autorizado por el Artículo 28 Sección 7 de DORA y sujeto al proceso de terminación en los Contratos, el Cliente puede terminar el Contrato total o parcialmente solo en los siguientes casos: (i) si Infor no ha subsanado un incumplimiento significativo de las Leyes de Ciberseguridad y Gobernanza de Datos Aplicables o este Anexo, (ii) si el Cliente identifica circunstancias que se consideren capaces de alterar el desempeño de Infor de los Servicios TIC, incluidos cambios materiales que afecten a los Contratos o a la situación de Infor, (iii) si se encuentran debilidades evidenciadas en relación con la gestión general de riesgos de TIC de Infor y en particular en la forma en que Infor asegura la disponibilidad, autenticidad, integridad y confidencialidad de los datos, ya sean datos personales u otros datos sensibles, o datos no personales, o (iv) si la autoridad gubernamental competente ya no puede supervisar efectivamente al Cliente como resultado de las condiciones de, o circunstancias relacionadas con, Infor o los Contratos.

## 7. TRATOS CON AUTORIDADES GUBERNAMENTALES COMPETENTES

7.1 Infor cooperará plenamente con las autoridades gubernamentales competentes y las autoridades de resolución del Cliente, incluidas las personas designadas por ellas.