Plan de Seguridad de la Información Nexus*

** Productos Nexus aplicables: Nexus AppXpress (SaaS), Nexus Live Visibility (SaaS), Nexus Factory Management (SaaS), Nexus Inventory Management (SaaS), Nexus Supply Chain Finance (SaaS), Nexus Supply Collaboration (SaaS), Nexus Transportation Management (SaaS), Nexus Supply Chain Visibility (SaaS), Nexus Procure to Pay (SaaS), Nexus Supply Chain Intelligence (SaaS).*

Alcance: Este Plan de Seguridad de la Información (*Information Security Plan* o "ISP") se incorpora a los Contratos ejecutados entre Infor y el Cliente (colectivamente los "Contratos"). En caso de cualquier conflicto o inconsistencia entre los términos de este ISP y cualquier otro término en los Contratos, este ISP prevalecerá, Este ISP establece las medidas vigentes de seguridad de Infor diseñadas para salvaguardar, respecto de todos los Clientes de forma general:

i. las configuraciones de hardware, equipo y sistemas de software en las cuales Infor provee:

   a. Servicios Cloud (a efectos de aclaración, los Servicios Cloud incluyen Soporte); y
   b. Servicios Profesionales.

ii. (todas las configuraciones de hardware, equipo y sistemas de software se definen colectivamente en este ISP como los "Sistemas", y los Servicios Cloud y los Servicios Profesionales se definen colectivamente en este ISP como los "Servicios"); así como

iii. datos del Cliente proporcionados a Infor, ya sea:

   a. como Datos del Cliente, o

   b. según lo proporcionado a Infor con el propósito de realizar los Servicios Profesionales y/o Soporte desde el ambiente de Infor

(todos estos datos se definen colectivamente en este ISP como "Datos").

Definiciones: Los términos en mayúscula utilizados en este ISP y no definidos en el mismo, tienen el significado dado a dichos términos en el Contrato de Software entre Infor y dicho Cliente (el "Contrato").

Exclusiones: Este ISP no se aplica cuando Infor presta servicios en las instalaciones del Cliente y/o se le ha otorgado acceso a los sistemas del Cliente. En tales casos, Infor deberá cumplir con las condiciones administrativas, técnicas y físicas del Cliente según lo acordado mutuamente en una orden de trabajo, y en relación con dicho acceso a los sistemas del Cliente, el Cliente será responsable de proporcionar al personal de Infor autorizaciones de usuario y contraseñas para acceder. sus sistemas y revocar dichas autorizaciones y finalizar dicho acceso, según lo considere apropiado el Cliente.

Actualizaciones: Las amenazas a la seguridad y las medidas diseñadas para protegerse contra esas amenazas evolucionan constantemente, por lo tanto, Infor podrá cambiar este ISP en cualquier momento sin previo aviso al Cliente, siempre que Infor mantenga un nivel de seguridad comparable o mejor para el conjunto de los Sistemas y los Datos.

1. Normas Generales de Seguridad

Infor mantiene medidas de seguridad administrativas, técnicas y físicas diseñadas para proteger contra la destrucción, pérdida, acceso no autorizado o alteración de los Sistemas y los Datos que son: (i) tan rigurosas que las que mantiene Infor para su propia información de naturaleza similar; (ii) igual de rigurosas que los estándares generalmente aceptados de la industria; y (iii) requeridas por las leyes aplicables. Infor no asume responsabilidad alguna por los sistemas operativos de terceros, y los productos y servicios que interoperen con los Sistemas y que el Cliente (a) desarrolle, o haya desarrollado, por sí mismo, o (b) licencie en virtud de los términos de licencia aplicables de dichos terceros.

1.1. Agentes de Seguridad

Infor ha designado uno o más agentes de seguridad que son responsables de coordinar y monitorear las medidas de seguridad en este ISP.

1.2. Controles de Acceso

Infor implementa controles de acceso a los Datos, incluyendo sin limitación las siguientes medidas:

i. Infor asigna un ID único a cada persona con acceso informático a los Datos.

ii. Infor identifica al personal que puede otorgar, modificar o cancelar acceso a los Datos, y restringe el acceso a los Datos sobre la base de privilegios mínimos. El acceso a los Datos solo está permitido al personal que tiene la "necesidad de conocer" para prestar los Servicios, e Infor mantiene y actualiza un registro de dicho personal. Acceso a los Datos es registrado y monitoreado.

iii. Infor instruye a su personal con acceso a los Datos de desactivar las sesiones administrativas cuando las computadoras no estén en uso. Las Aplicaciones utilizan tiempos de espera de sesión para desactivar las sesiones después de un período de tiempo especificado.

iv. Infor desactiva las cuentas de sus empleados de las aplicaciones o almacenes de datos que contienen Datos cuando dichos empleados son despedidos o transferidos, o cuando ya no necesitan acceso a dichos Datos. Infor revisa periódicamente la lista de personas y servicios con acceso a los Datos y elimina las cuentas que ya no requieran dicho acceso. Infor realiza esta revisión por lo menos dos veces al año.

v. Infor no utiliza las contraseñas u otros parámetros de seguridad predeterminados que brinda algún fabricante para ningún Sistema. Infor requiere el uso de "contraseñas seguras" impuestas por el sistema en todos los Sistemas de Infor, de acuerdo con las mejores prácticas generalmente aceptadas de la industria. Infor además requiere que todas las contraseñas y credenciales de acceso se mantengan confidenciales y no sean compartidas entre el personal y desactiva las contraseñas que sabe que han sido corrompidas o reveladas.

vi. Infor mantiene un "bloqueo de cuenta" al deshabilitar las cuentas con acceso a los Datos cuando se supera un número específico de intentos de contraseña incorrecta.

vii. El acceso remoto a los Sistemas que contienen Datos requiere autenticación de dos factores (por ejemplo, requiere al menos dos factores independientes para identificar a los usuarios).

1.3. Detección y Prevención de Intrusiones

Infor utiliza un sistema de detección de intrusiones/sistema de prevención de intrusiones (IDS/IPS) para monitorear sus Sistemas y sus procedimientos en busca de infracciones de seguridad, violaciones y actividades sospechosas. Esto incluye actividad externa sospechosa (que incluye, entre otros, sondeos no autorizados, escaneos o intentos de intrusión) y actividad interna sospechosa (que incluye, entre otros, acceso no autorizado de administrador del sistema, cambios no autorizados en los Sistemas, mal uso o robo de los Sistemas, o mal manejo de los Datos). Infor revisa regularmente los registros de acceso en busca de indicios de comportamiento malicioso o acceso no autorizado.

1.4. Firewall

Infor ha implementado y mantiene tecnologías de firewall de red diseñada para proteger Datos accesibles vía Internet.

1.5. Actualizaciones

Infor mantiene los Sistemas actualizados con mejoras, actualizaciones, correcciones de errores y nuevas versiones.

1.6. Cifrado de Datos

i. En tránsito a través de redes públicas, los Datos se cifran con, como mínimo, TLS 1.2 o su sucesor lógico.

ii. Mientras los Datos están en reposo dentro de los Sistemas, los Datos se cifran, como mínimo, con AES de 256 bits o su sucesor lógico.

1.7. Gestión de Identidad

Infor aprovecha un modelo de seguridad compartida para distribuir la responsabilidad de seguridad en la gestión de identidades. Infor tiene la capacidad de federar las aplicaciones en los Sistemas hacia el proveedor de gestión de identidad del Cliente con fines de autenticación.

1.8. Inicio de Sesión Único (*Single Sign On* or SSO)

Infor Nexus soporta el Inicio de Sesión Único [SSO] utilizando los sistemas de terceros de un Cliente como proveedor de identidad (IDP) e Infor Nexus como el proveedor de servicios. Infor Nexus es compatible con cualquier sistema de proveedor de identidad que utilice los estándares de *Security Assertion Markup Language* (SAML) 2.0. Se asume que el Inicio de Sesión Único del Cliente tiene autenticación de dos factores.

1.9. Pautas de Seguridad

Las recomendaciones de autenticación de Infor Nexus se preparan de acuerdo con las pautas del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. y las mejores prácticas generalmente aceptadas de la industria.

1.10. Sistema de Seguridad de Dos Factores

Infor Nexus siempre recomienda el uso de autenticación de dos factores (*two factor authentication*). El usuario podrá utilizar la aplicación móvil Infor Nexus como segundo factor de autenticación. Sin embargo, se requiere que los usuarios del producto *Procure to Pay* estén obligados a utilizar la autenticación de dos factores.

1.11. Gerenciamiento de Contraseñas

En los casos en los que el Inicio de Sesión Único no esté disponible, los Clientes de Infor Nexus son responsables de configurar una política de contraseñas que cumpla con los estándares de seguridad de su empresa. Todas las cuentas del Cliente se adherirán a esa política de contraseñas.

La configuración predeterminada de contraseñas es la siguiente:

- Todas las contraseñas se verifican contra las contraseñas reales previamente expuestas en filtraciones de datos. Las contraseñas que se encuentren en esta lista no serán permitidas;
- Todas las contraseñas deben tener al menos 8 caracteres de longitud;
- Se permiten espacios en las contraseñas y se fomenta el uso de una frase fácil de recordar;
- No se permite ninguno de los siguientes, a menos que haya al menos 8 caracteres adicionales en la contraseña (o el mínimo configurado que sea mayor de 8):
    - Nombre o apellido del usuario;
    - Nombre de inicio de sesión del usuario;
    - Cualquier palabra en el nombre de la organización del usuario que tenga más de tres caracteres;
    - Número de teléfono y número de fax del usuario u organización;
    - Dirección de correo electrónico del usuario.

1.12. Medidas Integradas

Para evitar el robo de contraseñas por fuerza bruta, un algoritmo de limitación de velocidad impedirá los intentos de adivinación de contraseñas. Los clientes podrán configurar su política de contraseñas:

- Longitud mínima de la contraseña (superior a 8);
- Uso obligatorio de letras mayúsculas y minúsculas en la contraseña;
- Uso obligatorio de números en la contraseña;
- Uso obligatorio de símbolos en la contraseña;
- Uso obligatorio de números o símbolos en la contraseña;
- Expiración de la contraseña después de un cierto número de días;
- Cuentas de usuario bloqueadas después de un cierto número de intentos fallidos de contraseña.

La longitud mínima de la contraseña es de 8 caracteres de forma predeterminada y no puede establecerse por debajo de ese valor. El resto de estas configuraciones, de acuerdo con las mejores prácticas modernas, no están activadas de forma predeterminada, pero pueden ser configuradas para las organizaciones del Cliente por Infor Nexus como parte de la implementación.

1.13. Software Malicioso

Infor mantiene software antimalware/antivirus estándar generalmente aceptado en la industria y, en la medida de lo posible, utiliza características de protección casi en tiempo real en un esfuerzo por proporcionar Servicios Cloud, que no contengan "bombas de tiempo", "gusanos", "virus", "caballos de Troya", "códigos de protección", "claves de destrucción de datos" u otros dispositivos de programación destinados a modificar, eliminar, dañar, desactivar o deshabilitar los Datos del Cliente o para evitar o limitar el acceso del Cliente a los Datos del Cliente.

1.14. Seguridad Física

Las instalaciones que contienen los Sistemas:

i. estarán estructuralmente diseñadas para resistir el clima adverso y otras condiciones naturales razonablemente predecibles;

ii. tendrán medidas de protección ambiental físicas apropiadas para ayudar a proteger los Sistemas de daños relacionados con el humo, el calor, el agua, el fuego, la humedad o fluctuaciones en la energía eléctrica;

iii. estarán respaldadas por sistemas de generación de energía en sitio; y

iv. tendrán controles apropiados diseñados para garantizar que solo el personal autorizado tenga acceso físico a la instalación.

2. Auditoría

2.1. Derechos de Auditoría

Como parte de su programa de supervisión de proveedores, el Cliente y (de corresponder) su agencia reguladora gubernamental podrán solicitar, una vez al año en forma de auditoría postal (por ejemplo, un cuestionario basado en ISO 27001), documentación procesal de Infor con respecto a su Plan de Seguridad de la Información, procesos y controles. Infor acepta que, en la medida en que dicha documentación procesal esté prontamente disponible, Infor proporcionará la documentación que el Cliente pueda razonablemente solicitar, siempre que dicha documentación no (a) amenace la confidencialidad, integridad o disponibilidad de los datos o servicios de otros Clientes de Infor o (b) viole la confidencialidad, integridad y disponibilidad de los datos o servicios de terceros que brindan Servicios al Cliente en nombre de Infor. La documentación de procedimiento proporcionada por Infor no incluirá evidencia (por ejemplo, sin limitación a, evidencia de capacitación, evidencia de prueba, resultados de evaluaciones de riesgo). Infor responderá al cuestionario en un plazo de 30 días; si no se puede cumplir con este plazo, Infor trabajará con el Cliente para acordar mutuamente en un plazo razonable la finalización. Toda la documentación referida será Información Confidencial de Infor. Infor no tendrá en cuenta los hallazgos del Cliente que resulten de esta auditoría postal.

2.2. Auditoría de Terceros

3. Una vez en cada período de 12 meses durante el Período de Suscripción, Infor deberá, a su costo y gasto, contratar a un auditor independiente debidamente calificado para realizar una revisión del diseño y la efectividad operativa de los objetivos y las actividades de control definidos por Infor en relación con los Servicios Cloud (excluyendo Soporte). Infor ordenará de dicho auditor un informe SOC II Tipo 2 y, según aplicable, un informe SOC I Type 2 para Servicios Cloud (colectivamente el "Informe de Auditoría"). El informe de Auditoría es información confidencial de Infor, pero estará disponible para el Cliente en el portal de soporte de Infor. El Cliente podrá compartir una copia de dicho Informe de Auditoría con sus auditores y reguladores, siempre y cuando se informe a los auditores y reguladores que dicho Informe de Auditoría es Información Confidencial de Infor y deberá protegerse adecuadamente.**Administración de Cambios para Servicios Cloud**

Infor sigue un proceso de control de cambios que rige la identificación e implementación de cambios dentro de los recursos de entrega de Servicios Cloud de Infor para ayudar a prevenir cambios no deseados en el código fuente de la aplicación, interfaces, sistemas operativos o cambios de back-end en los datos dentro de los campos y tablas existentes. Todo cambio solicitado a los recursos de entrega de los Servicios Cloud de Infor deben seguir un proceso de control de cambios de implementación. Infor documenta y conserva un registro detallado de su cumplimiento con este proceso, como un sistema de emisión de tickets y registros de los procedimientos de prueba para cualquier cambio, lo que incluye, entre otros, la fecha y la hora de dicho cambio y una descripción de la naturaleza del mismo.

4. Segregación de Datos; No Utilización

4.1. Segregación

Los Datos se mantienen lógicamente separados de los datos de Infor y los datos de cualquier otro cliente de Infor mediante medios técnicos apropiados.

4.2. No Utilización; Estadísticas Agregadas

Los Datos constituyen Información Confidencial del Cliente y este posee todos los derechos de propiedad sobre los mismos. Infor no explotará comercialmente los Datos y no accederá a los Datos excepto cuando sea necesario para prestar los Servicios y cumplir con sus obligaciones en conformidad con el Contrato.

Infor colecta datos estadísticos e información de rendimiento, generados a través de instrumentación y sistemas de registro, en relación con el uso y la operación del Cliente de los Servicios (“Estadísticas Agregadas”). Las Estadísticas Agregadas son propiedad exclusiva de Infor y no se consideran Datos.

5. Gestión de Activos

Infor tiene un proceso formal de gestión de activos que incluye:

i. Mantener un inventario de los activos utilizados para proporcionar Servicios ("Activos"), diseñados para identificar y establecer claramente la propiedad y el control de los Activos;

ii. Procesos diseñados para gestionar la devolución, destrucción o eliminación de los Datos de los Activos aplicables; y

iii. procedimientos diseñados para proteger los Activos de amenazas y vulnerabilidades, ya sean internas o externas, deliberadas o accidentales.

6. Escaneo de Vulnerabilidades y Pruebas de Penetración

Infor mantiene un proceso de gestión de vulnerabilidades para buscar riesgos resultantes de la explotación de fallas o debilidades publicadas o identificadas que podrían ejercerse (accidental o intencionalmente) y resultar en daño o acceso no autorizado a los Sistemas ("Vulnerabilidades"). Infor abordará las Vulnerabilidades dentro de los marcos de tiempo estándares generalmente aceptados de la industria. Infor remediará o mitigará las Vulnerabilidades de manera acorde con el riesgo que dichas Vulnerabilidades representen, de acuerdo con el marco definido por Infor, que es consistente con los estándares generalmente aceptados de la industria.

Anualmente, Infor contrata, a su propio costo, a un tercero independiente para realizar pruebas de penetración para Servicios Cloud de inquilino-múltiple, incluidas las pruebas manuales realizadas por humanos, a fin de evaluar los controles de seguridad de los Sistemas siguiendo metodologías estándar generalmente aceptadas de la industria.

Para Servicios Cloud de inquilino-múltiple, las evaluaciones de pruebas de seguridad, incluidos los escaneos del código fuente y los escaneos de Vulnerabilidades, se llevan a cabo antes del lanzamiento del código y durante todo el ciclo de vida del producto del Servicio Cloud (por ejemplo, en ambientes de desarrollo y producción) para ayudar a identificar posibles Vulnerabilidades que deban repararse o mitigarse. Anualmente, se realizan pruebas de penetración en Servicios Cloud de inquilino-múltiple para identificar Vulnerabilidades que requieren reparación o mitigación.

7. Respuesta a Incidentes de Seguridad de la Información

Si Infor toma conocimiento de que los Datos han sido, o razonablemente se considera que han estado, sujetos a un uso o divulgación no autorizados bajo el Contrato (un "Incidente de Seguridad de la Información"), Infor deberá: (i) notificar al Cliente afectado sobre la ocurrencia de dicho Incidente de Seguridad de la Información prontamente y sin demora indebida (y en cualquier caso, dentro de un plazo de 48 horas a la toma de conocimiento de dicho Incidente de Seguridad de la Información); (ii) investigar y realizar un análisis razonable de la(s) causa(s) de dicho Incidente de Seguridad de la Información; (iii) proporcionar actualizaciones periódicas sobre cualquier investigación en curso al Cliente; (iv) elaborar e implementar un plan apropiado para subsanar la causa de dicho Incidente de Seguridad de la Información en la medida en que dicha causa esté bajo el control de Infor; y (v) cooperar con la investigación razonable del Cliente o los esfuerzos del Cliente para cumplir con cualquier notificación u otros requisitos normativos aplicables a dicho Incidente de Seguridad de la Información. Previa solicitud del Cliente y por su cuenta, en caso de un Incidente de Seguridad de la Información, Infor entregará al Cliente (en la medida en que lo permita la ley y sujeto a las correspondientes protecciones de confidencialidad) copias de los registros de la actividad de los Sistemas aplicables (únicamente con respecto al Incidente de Seguridad de la Información en relación con el Cliente) para su uso en cualquier procedimiento legal o normativo del Cliente o en cualquier investigación gubernamental.

8. Registro y Monitoreo

Infor monitorea sus recursos utilizados para proporcionar Servicios utilizando un conjunto de herramientas, configuradas específicamente para administrar registros y alertas. Los registros se mantienen protegidos física y virtualmente para evitar alteraciones. La información sensible y las contraseñas no se registran bajo ninguna circunstancia. Además de capturar información relacionada con el Servicio, las herramientas de monitoreo permiten a los administradores realizar un seguimiento de la actividad del usuario al ingresar y salir del Sistema.

9. Seguridad de Recursos Humanos y Capacitación

El personal de Infor que presta los Servicios está sujeto a obligaciones de confidencialidad, conoce las amenazas y preocupaciones sobre la seguridad de la información, recibe capacitación general en seguridad al menos una vez al año, y están equipados para respaldar las políticas de seguridad de la información de la organización en general, así como dentro de sus funciones laborales específicas.

10. Controles de Dispositivos Endpoint (Laptop, estaciones de trabajo y dispositivos móviles de Infor)

Infor implementa medidas de seguridad acordes con las prácticas generalmente aceptadas de la industria para la protección de endpoints, incluyendo automatización de la gestión de parches de aplicaciones y sistemas operativos y protección antivirus.

11. Devolución y Destrucción de Datos

11.1. Devolución

El Cliente tiene acceso a sus datos durante la vigencia de su suscripción, sujeto a tiempos de inactividad programados, mantenimiento de emergencia y otras directrices de disponibilidad de niveles de servicio. En caso de que el Cliente requiera que los Datos del Cliente sean devueltos en un formato no estándar o solicite cualesquiera otros servicios de asistencia tras la rescisión, Infor y el Cliente convendrán de mutuo acuerdo el alcance de los servicios de asistencia a la rescisión y las cuotas y gastos por pagar por tales servicios. No obstante lo anterior, los Datos Compartidos deben permanecer en la Plataforma Infor Nexus, ya que no son propiedad del Cliente, sino que son compartidos. Los Datos Compartidos son cualquier dato que sea visible tanto para el Cliente/Miembro como para uno o más miembros autorizados adicionales en la Plataforma Infor Nexus, tales como proveedores y prestadores de servicios. Los datos se almacenan a nivel de transacción y no a nivel de cliente.

Los datos proporcionados a Infor con el propósito de brindar Soporte (es decir, a través de un ticket de Soporte registrado en el portal de Soporte) se eliminan cinco años después de la fecha de cierre del ticket del incidente. El nombre individual del cliente y la información de contacto (por ejemplo, dirección de correo electrónico del usuario, nombre y número de teléfono) utilizados para administrar el ciclo de vida del ticket de Soporte se desactivan y anonimizan al finalizar el Soporte.

12. Subcontratistas

Los subcontratistas de Infor que suministren bienes y servicios a Infor con respecto a los Servicios de Infor deberán suministrar dichos bienes y servicios en términos sustancialmente similares a los establecidos en este ISP. Antes de contratar a dicho tercero subcontratista para prestar cualquiera de los Servicios conforme a este plan, Infor examinará a dicho tercero con diligencia razonable para ayudar a asegurar que dicho tercero pueda cumplir con estas obligaciones de confidencialidad y seguridad. Infor es responsable de todas las acciones de sus subcontratistas en respaldo de los Servicios.