Plan de Seguridad de la Información:

BPCS/LX, XA, System 21

Este Plan de Seguridad de la Información (*Information Security Plan* o "ISP") se incorpora al Formulario de Pedido entre Infor y el Cliente mencionado en el mismo y establece las medidas vigentes de seguridad de Infor diseñadas para salvaguardar la configuración del hardware, equipo y configuración de los sistemas de software (i) en los que Infor soporta el uso del Software de Suscripción (establecido en el Formulario de Pedido) y los Servicios de Suscripción relacionados y (ii) en los cuales se han proporcionado, ingresado o cargado Datos del Cliente para su uso por o con el Software de Suscripción por parte del Cliente o sus Usuarios Autorizados (i y ii colectivamente en adelante los "Sistemas"). Para mayor claridad, 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 como Servicio entre Infor y dicho Cliente (el "Contrato"). Este ISP no se aplica a los contratos de servicios administrados por Infor, en los que Infor aloja el software on-premise del Cliente de conformidad con un contrato de servicios profesionales negociado separadamente.

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 del Cliente.

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 del Cliente que Infor procesa por instrucción del Cliente, 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.

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 del Cliente, incluyendo las siguientes medidas:

i. Infor asigna una identificación única a cada persona con acceso informático a los Datos del Cliente.

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

iii. Infor instruye a su personal que tiene acceso a los Datos del Cliente de desactivar las sesiones administrativas cuando las computadoras no estén en uso.

iv. Infor desactiva las cuentas de sus empleados de las aplicaciones o almacenes de datos que contienen Datos del Cliente cuando dichos empleados son despedidos o transferidos, o cuando ya no necesitan acceso a dichos Datos del Cliente. Infor revisa periódicamente la lista de personas y servicios con acceso a los Datos del Cliente 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 del Cliente cuando se supera un número específico de intentos consecutivos de contraseña incorrecta.

vii. El acceso remoto a los Sistemas que contienen Datos del Cliente 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 del Cliente). Infor revisa regularmente los registros de acceso en busca de indicios de comportamiento malicioso o acceso no autorizado.

1.4. Firewall

Infor mantiene una tecnología de firewall de red diseñada para proteger conectividad y ambientes hospedados accesibles vía Internet.

1.5. Actualizaciones

Infor mantiene los Sistemas suscritos actualizados con mejoras, actualizaciones, correcciones de errores y nuevas versiones. Las actualizaciones/mejoras/correcciones del Sistema Operativo y de los sistemas de aplicaciones se organizan y programan con el Cliente.

1.6. Cifrado de Datos

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

ii. Mientras los Datos del Cliente están en reposo dentro de los Sistemas, los Datos del Cliente 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 seguridad. Infor tiene la capacidad de federar las aplicaciones en los Sistemas con el proveedor de gestión de identidad del Cliente.

1.8. 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 de Suscripción 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 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

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 de Suscripción. Infor ordenará de dicho auditor un informe de acuerdo con la Declaración de Normas para Trabajos de Certificación n.° 18 (*Statement on Standards for Attestation Engagements*, SSAE 18) del Instituto Estadounidense de Contadores Públicos Certificados o una norma equivalente, que puede incluir ISAE 3402 (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.

Además, una vez en cada período de 12 meses durante el Período de Suscripción, Infor contratará, a su costa y cargo, a un auditor independiente debidamente calificado para realizar una revisión de la seguridad de la información en relación con los Servicios de Suscripción para cierto Software de Suscripción de inquilino-múltiple. declarado en www.trust.infor.com bajo ISO27001. Infor ordenará de dicho auditor un informe de acuerdo con el estándar 27001 de la Organización Internacional para la Estandarización (*International Organization for Standardization*, ISO). El informe de auditoría no estará disponible para el Cliente; sin embargo, el Cliente podrá obtener una copia del certificado resultante del sitio de seguridad en la nube de Infor (www.trust.infor.com) en cualquier momento. El certificado identificará el Software de Suscripción que corresponde al informe. Como parte de esta certificación ISO 27001, Infor mantiene un manual del Sistema de Administración de la Seguridad de la Información para el Software de Suscripción incluido en la certificación y los correspondientes Servicios de Suscripción, que ayuda a garantizar la protección, confidencialidad, integridad y disponibilidad de los activos de Infor utilizados para proporcionar dichos Servicios de Suscripción.

3. Administración de Cambios

Infor sigue un proceso de control de cambios que rige la identificación e implementación de cambios dentro de los recursos de entrega de Servicios de Suscripción 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 de Suscripción 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 del Cliente; No Utilización

4.1. Segregación

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

Infor puede recopilar estadísticas agregadas, que son propiedad exclusiva de Infor y no se consideran Datos del Cliente. Las "Estadísticas Agregadas" son 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 del Software de Suscripción y los Servicios de Suscripción.

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 de Suscripción ("Activos"), establecer claramente la propiedad y el control de los Activos, ser capaz de identificar los Activos y gestionar la devolución, destrucción o eliminación de los Datos del Cliente de los Activos aplicables; y

ii. 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, incluidas las pruebas manuales realizadas por humanos, a fin de evaluar los controles de seguridad de los Sistemas de inquilino-múltiple siguiendo metodologías estándar generalmente aceptadas de la industria.

Para el Software de Suscripción 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 Software de Suscripción (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 Sistemas de inquilino-múltiple e inquilino-único 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 del Cliente han sido, o razonablemente se espera que estén, sujetos a un uso o divulgación no autorizados por este ISP (un "Incidente de Seguridad de la Información"), Infor deberá: (i) notificar al Cliente 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 de Suscripción 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

El personal de Infor que presta los Servicios de Suscripción 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

Tras la rescisión o el vencimiento de los Servicios de Suscripción, Infor de inmediato pondrá todos los Datos del Cliente a disposición de éste (dentro de los 3 a 5 días hábiles posteriores a la recepción de la solicitud por escrito del Cliente) todos los Datos del Cliente como exportación de base de datos nativa proporcionada a través del servidor FTP de Infor. En caso de que el Cliente requiera que los Datos del Cliente sean devueltos en un formato alterno 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.

11.2. Destrucción

Infor eliminará de forma permanente todas las instancias (en línea o accesibles por red) de los Datos del Cliente dentro de los 30 días posteriores a la rescisión o vencimiento de los Servicios de Suscripción. Infor utilizará procesos estándar generalmente aceptados de la industria para eliminar el hardware y los componentes físicos que contengan Datos del Cliente. Todo el almacenamiento se borra electrónicamente (se pone a cero) antes de implementarse o retirarse del entorno de producción de Infor.

12. Subcontratistas

Los subcontratistas de Infor que suministren bienes y servicios a Infor con respecto a los Servicios de Suscripción 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 de Suscripción 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 de Suscripción.