SMART-DI Group

Acuerdos de Servicios

Plataforma en la nube

Índice

Propósito del documento

Si estás considerando trasladar tus documentos digitales, información de paneles de impresión o procesos de documentos de flujo de trabajo a la nube, o si ya te encuentras en pleno proceso de migración, este documento será un recurso valioso para comprender las preguntas de cumplimiento en la nube que deberías realizar. Smart-DI ha recopilado respuestas detalladas a muchas preguntas de clientes y las ha presentado en las siguientes secciones de acuerdo con sus respectivos ámbitos.

Cumplimiento en la Nube

Los servicios de Smart-DI (InsightAI360), Smartker, Smart-DI Services) se basan en un marco de cumplimiento que incluye políticas, procesos y actividades de control. El marco de cumplimiento abarca los procesos y tecnologías necesarios para establecer y mantener un entorno que respalde la efectividad operativa de los servicios de Smart-DI. Smart-DI ha desarrollado un programa formal de seguridad de la información diseñado para proteger la confidencialidad, integridad y disponibilidad de los sistemas y datos de los clientes.

Seguridad en la plataforma SaaS Smart-DI Services

La misión de seguridad en la plataforma de Smart-DI services, es proteger la integridad, confidencialidad y disponibilidad de los datos de nuestros clientes, socios y datos internos. Smart-DI se compromete a ser transparente en cuanto a las prácticas de seguridad, lo que ayuda a los clientes y socios a comprender nuestro enfoque.

Application & Interface Security

Utilizas estándares de la industria para construir seguridad en el ciclo de vida de desarrollo de sistemas/software (SDLC)?

- Utilizamos OWASP para evaluaciones de vulnerabilidades y modelado de amenazas, y también usamos documentos de guía de Microsoft SDL en áreas seleccionadas.

¡Utilizas una herramienta de análisis de código fuente automática para detectar defectos de seguridad en el código antes de la producción?

- El análisis de código estático se ejecuta continuamente contra los repositorios de código, y el análisis dinámico se realiza constantemente contra nuestras aplicaciones.

¿Utilizas un análisis de código fuente manual para detectar defectos de seguridad en el código antes de la producción?

- La revisión manual del código se realiza por propietarios autorizados antes de cada compilación y es requerida como parte del proceso de aprobación.

¿Revisas tus aplicaciones por vulnerabilidades de seguridad y abordas cualquier problema antes de desplegar en producción?

- El ciclo de vida de desarrollo del sistema Smart-DI incluye prácticas recomendadas por la industria, que incluyen revisiones formales del diseño por el Equipo de Seguridad Smart-DI, modelado de amenazas y finalización de un análisis de riesgo.

¿Se definen y documentan todas las exigencias y niveles de confianza para el acceso de los clientes?

- Smart-DI proporciona documentación para nuestros clientes sobre nuestros servicios, que también cubre los niveles de confianza.

¿Implementas rutinas de integridad de datos input y output en las interfaces y bases de datos de aplicación para prevenir errores o corrupción manual o sistemática del datos?

- La integridad de datos se mantiene en todo el backend del producto Smart-DI, y Smart-DI realiza comprobaciones de integridad en los datos escritos en sus sistemas de almacenamiento para asegurar la disponibilidad y replicación.

Garantía en Auditoria

¿Produces afirmaciones de auditoría utilizando un formato estructurado y de industria (por ejemplo, CloudAudit/A6 URI Ontología, etc.)?

- Smart-DI ha desarrollado una política de seguridad de información que considera el impacto, amenazas y vulnerabilidades de todos nuestros activos. Nuestro marco robusto ha sido desarrollado para gestionar la protección de datos de clientes tanto en repositorios como en tránsito.

¿Realizas pruebas de penetración de red de tu infraestructura de servicios en la nube con regularidad, según las prácticas y orientaciones de la industria?

- Smart-DI realiza pruebas de penetración anuales contra la infraestructura y aplicaciones de Smart-DI.

¿Realizas pruebas de penetración de aplicación de tu infraestructura de servicios en la nube con regularidad, según las prácticas y orientaciones de la industria?

Smart-DI realiza pruebas de penetración anuales contra la infraestructura y aplicaciones de Smart-DI.

¿Realizas auditorías internas de tu infraestructura de servicios en la nube con regularidad, según las prácticas y orientaciones de la industria?

Smart-DI realiza pruebas de penetración anuales contra la infraestructura y aplicaciones de Smart-DI.

¿Realizas auditorías externas con regularidad, según las prácticas y orientaciones de la industria?

Smart-DI ha desarrollado una política de seguridad de información que considera el impacto, amenazas y vulnerabilidades de todos nuestros activos. Nuestro marco robusto ha sido desarrollado para gestionar la protección de datos de

clientes tanto en repositorios como en tránsito.

¿Tienes un programa interno de auditoría que permite una auditoría interfuncional de evaluaciones?

La gestión interna de auditoría se realiza actualmente basada en nuestra política de seguridad de información.

¿Tienes la capacidad para segmentar lógicamente o cifrar los datos del cliente para producir datos solo para un inquilino específico, sin acceder inadvertidamente a los datos del otro inquilino?

Todos los datos del cliente están aislados lógicamente entre inquilinos. La cifrado en repositorio está habilitado.

¿Tienes la capacidad para recuperar los datos para un cliente específico en el caso de un fallido o pérdida de datos?

Dentro ciertos parámetros, es posible recuperar los datos individuales del cliente. Los escenarios en los que se perderían los datos del cliente específico son pocos, y nuestras estrategias de recuperación por desastre y protección de datos se centran en incidentes más grandes.

¿Tienes la capacidad para restringir el almacenamiento de datos del cliente a países o ubicaciones geográficas específicas?

Smart-DI es una aplicación global y cubre regiones LATAM, EE. UU. y EU.

¿Tienes un programa en lugar que incluya la capacidad para monitorizar cambios en los requisitos regulatorios en jurisdicciones relevantes y ajustar tu programa de seguridad para cambios en los requisitos legales para asegurarte del cumplimiento con los requisitos regulatorios relevantes?

La revisión de los requisitos regulatorios y jurisdicciones relevantes se hace anualmente.

Gestión de Continuidad del Negocio y Resiliencia Operacional en la Planificación de Continuidad del Negocio

¿Proporcionan a los inquilinos opciones de alojamiento geográficamente resilientes?

- Nuestro proveedor de infraestructura proporciona un servicio de alojamiento geográficamente resiliente para nosotros.

¿Proporcionan a los inquilinos capacidad de conmutación por error del servicio de infraestructura a otros proveedores?

- Los clientes de Smart-DI tienen la capacidad de exportar sus datos desde nuestra plataforma en la nube si desean utilizarlo con otro proveedor de plataformas de marketing y ventas. Los clientes de Smart-DI no tienen acceso a la infraestructura del producto de manera que permita un evento de conmutación por error controlado por el cliente. Las operaciones de recuperación ante desastres y resiliencia están gestionadas por equipos de operaciones de Smart-DI.

¿Las planes de continuidad de negocios están sujetos a prueba a intervalos planificados o ante cambios significativos en la organización o el entorno para asegurar su continuación efectiva?

- Smart-DI ha desarrollado un plan para probar su plan de continuidad de negocios de manera regular.

¿Proporcionan a los inquilinos documentación mostrando la ruta de transporte de sus datos entre sus sistemas?

- Smart-DI tiene un mapa de documentación de flujo de datos. Por razones de confidencialidad, Smart-DI no comparte operaciones internas.

¿Están disponibles los documentos del sistema de información para el personal autorizado para configurar la instalación y operación de un sistema de información?

- Smart-DI proporciona guías para administradores de usuarios. Además, el sitio web de Smart-DI contiene documentación sobre la plataforma.

¿Se prevé y diseña la protección física contra daños (por ejemplo, causas naturales, desastres naturales, ataques deliberados) con contramedidas aplicadas?

- Smart-DI utiliza la infraestructura de IONOS y Azure Cloud. Ambos proveedores de servicios han seleccionado estratégicamente sus ubicaciones de centros de datos para mitigar riesgos ambientales. Además, Smart-DI tiene una instancia secundaria de conmutación por error lista para ser utilizada en caso de desastre.

¿Alguno de sus centros de datos está ubicado en lugares que tengan una alta probabilidad de ocurrencia de riesgos ambientales de alto impacto?

- Smart-DI utiliza la infraestructura de IONOS y Azure Cloud. Ambos proveedores de servicios han seleccionado estratégicamente sus ubicaciones de centros de datos para mitigar riesgos ambientales. Además, Smart-DI tiene

una instancia secundaria de conmutación por error en una zona de disponibilidad diferente lista para ser utilizada en caso de desastre.

Si utiliza infraestructura virtual, ¿su solución en la nube incluye capacidades independientes de restauración y recuperación de hardware?

- Smartker y PrinterBI son plataformas SaaS y son independientes del hardware. Nuestra infraestructura está subcontratada a los servicios de Azure Cloud y IONOS.

Si utiliza infraestructura virtual, ¿proporcionan a los inquilinos la capacidad de restaurar una máquina virtual a un estado anterior en el tiempo?

- Los productos de Smart-DI son una oferta de servicio SaaS. Los clientes no tienen la capacidad de introducir o gestionar máquinas en el entorno del producto Smart-DI ni de restaurar esas imágenes de máquinas.

Si utiliza infraestructura virtual, ¿permiten que las imágenes de máquinas virtuales se descarguen y se porten a un nuevo proveedor de nube?

- Los productos de Smart-DI son una oferta de servicio SaaS. Los clientes no tienen la capacidad de introducir o gestionar máquinas en el entorno del producto Smart-DI ni de restaurar esas imágenes de máquinas.

Si utiliza infraestructura virtual, ¿están las imágenes de máquinas disponibles para el cliente de manera que le permita replicar esas imágenes en su propia ubicación de almacenamiento fuera del sitio?

- Los productos de Smart-DI son una oferta de servicio SaaS. Los clientes no tienen la capacidad de introducir o gestionar máquinas virtuales en el entorno del producto Smart-DI ni de restaurar esas imágenes de máquinas.

¿Su solución en la nube incluye capacidades de restauración y recuperación independientes del software/proveedor?

- Proporcionado por los servicios en la nube de Azure y IONOS.

¿Se implementan mecanismos de seguridad y redundancias para proteger el equipo contra interrupciones en los servicios públicos?

- Proporcionado por los Servicios en la Nube de IONOS y AZURE.

¿Proporcionan a los inquilinos visibilidad continua y reporte de su rendimiento de nivel de servicio operativo (SLA)?

- La información de nivel de servicio aún no se publica en nuestro sitio web, pero esto es parte de nuestra hoja de ruta. Hasta ahora, la información del nivel de servicio se puede recibir enviándonos un correo (support@smart-di.com)

¿Hacen disponibles métricas de seguridad basadas en estándares a sus inquilinos?

- La información de métricas de seguridad aún no se publica en nuestro sitio web, pero esto es parte de nuestra hoja de ruta. Hasta ahora, la información del nivel de servicio se puede recibir enviándonos un correo (support@smart-di.com)

¿Se establecen y ponen a disposición políticas y procedimientos para todo el personal para respaldar adecuadamente los roles de las operaciones de servicios?

- Smart-DI ha estructurado sus controles de TI para asegurar suficiente rigor en la gestión de acceso, gestión de cambios y funciones relacionadas. Dentro de TI, las actividades de desarrollo e ingeniería, los roles y responsabilidades están explícitamente asignados, publicados y bien entendidos por todos los empleados.

¿Tienen capacidades de control técnico para hacer cumplir las políticas de retención de datos de los inquilinos?

- Sí, todos los datos de los servicios de Smart-DI se realizan copias de seguridad y se almacenan en ubicaciones globales de Azure.

¿Tienen un procedimiento documentado para responder a solicitudes de datos de inquilinos por parte de gobiernos o terceros?

- Smart-DI no divulgará datos del cliente a ningún gobierno, excepto en la medida necesaria para cumplir con la ley o una orden válida y vinculante de una agencia de cumplimiento de la ley (como una citación o orden judicial). Si una agencia de cumplimiento de la ley envía una solicitud de datos del cliente a Smart-DI, Smart-DI intentará redirigir a la agencia de cumplimiento de la ley para que solicite esos datos directamente del cliente. Como parte de este esfuerzo, Smart-DI puede proporcionar información de contacto básica del cliente a la agencia de cumplimiento de la ley. Si se ve obligado a divulgar datos de clientes a una agencia de cumplimiento de la ley, entonces Smart-DI le notificará razonablemente al cliente sobre la solicitud para que pueda buscar una orden de protección u otro remedio adecuado, a menos que Smart-DI esté legalmente prohibido de hacerlo.

¿Han implementado mecanismos de respaldo o redundancia para asegurar el cumplimiento con los requisitos regulatorios, estatutarios, contractuales o comerciales?

- Se realizan pruebas de redundancia y recuperación regularmente como parte de las operaciones normales de Smart-DI.

Control de Cambios y Gestión de Configuraciones

¿Está disponible documentación que describa la instalación, configuración y uso de productos/servicios?

- Smart-DI Services es una plataforma SaaS y tiene documentos internos que describen las instalaciones y configuraciones de la plataforma de productos de Smart-DI. Por razones de confidencialidad, Smart-DI no comparte documentación interna.

¿Tienen controles en lugar para asegurar que se cumplen los estándares de calidad para todo el desarrollo de software?

- Se establecen directrices para las mejores prácticas de desarrollo, y las funciones de intercambio de conocimientos y mejora de procesos son parte estándar de las actividades de ingeniería. Existen métricas específicas y cruzadas para todos los grupos de desarrollo.

¿Tienen controles para detectar defectos de seguridad del código fuente en cualquier actividad de desarrollo de software subcontratada?

- Todas las actualizaciones al repositorio de código fuente son revisadas antes de aprobar el cambio. Las revisiones incluyen análisis de código estático y revisiones de código por miembros senior del equipo.

¿Proporcionan a sus inquilinos documentación que describa su proceso de aseguramiento de calidad?

- El proceso de aseguramiento de calidad está descrito en el documento de procedimientos de desarrollo de software de Smart-DI. Debido a la confidencialidad de la información, Smart-DI no comparte informes internos.

¿Existen políticas y procedimientos para clasificar y remeditar errores y vulnerabilidades de seguridad reportadas para productos y servicios?

- Los estándares para la medición de riesgos y la prioridad de errores están documentados, y las métricas de prioridad son utilizadas para establecer los tiempos de resolución esperados.

¿Están en funcionamiento mecanismos para asegurar que todos los elementos de depuración y código de prueba sean eliminados de las versiones de software liberadas?

- Las prácticas estándar de desarrollo incluyen requisitos para una correcta documentación y limpieza del código. El proceso de implementación asegura que las configuraciones de depuración estén disponibles durante las etapas apropiadas.

¿Tienen controles en su lugar para restringir y monitorear la instalación de software no autorizado en sus sistemas?

- El acceso a la infraestructura del producto está estrictamente controlado y se previenen desviaciones de los compilados esperados.

¿Proporcionan a los inquilinos documentación que describa sus procedimientos de gestión del cambio en producción y sus roles/derechos/responsabilidades dentro de esta?

- Smart-DI mantiene un proceso de gestión de cambios que es parte de la documentación interna. Por razones de confidencialidad, Smart-DI no comparte operaciones internas.

Seguridad de Datos y Gestión del Ciclo de Vida de la Información

¿Tienen la capacidad de usar la ubicación geográfica del sistema como factor de autenticación?

- La autenticación a nuestros servicios para clientes está restringida a la autenticación ID de Azure.

¿Pueden proporcionar la ubicación física/geográfica del almacenamiento de los datos de un inquilino a pedido?

- No, la información confidencial del inquilino no será compartida con terceros.

¿Pueden proporcionar la ubicación física/geográfica del almacenamiento de los datos de un inquilino por adelantado?

- No, la información confidencial del inquilino no será compartida con terceros.

¿Pueden asegurar que los datos no se muevan más allá de una residencia geográfica definida?

- La infraestructura de Smart-DI Services existe en ubicaciones particulares bien definidas. Las ubicaciones de almacenamiento de datos están diseñadas en la infraestructura y solo se pueden cambiar como parte de cambios de diseño e implementación intencionados.

¿Proporcionan metodologías de encriptación abiertas (3.4ES, AES, etc.) a los inquilinos para que protejan sus datos si es necesario moverlos a través de redes públicas (por ejemplo, Internet)?

- Todas las interacciones sensibles con los productos de Smart-DI (por ejemplo, llamadas API, inicio de sesión, sesiones autenticadas en el portal del cliente, etc.) están encriptadas con TLS 1.2, o 1.3 y claves de 2,048 bits.

¿Utilizan metodologías de encriptación abierta en cualquier momento en que sus componentes de infraestructura necesiten comunicarse entre ellos a través de redes públicas?

- Todas las comunicaciones entre nuestros componentes de infraestructura a través de Internet están encriptadas.

¿Tienen procedimientos para asegurar que los datos de producción no se repliquen ni se utilicen en entornos no productivos?

- Smart-DI separa entornos de producción de entornos de prueba y desarrollo. Los datos de producción nunca se utilizan con fines de prueba.

¿Soportan la eliminación segura (por ejemplo, degaussing/borrado criptográfico) de datos archivados y respaldados según lo determinado por el inquilino?

Smart-DI apoya la eliminación segura de los datos del cliente.

Gestión de Activos de Seguridad de Centros de Datos

¿Mantienen un inventario completo de todos sus activos críticos que incluya la propiedad del activo?

- Sí, todos los activos importantes se rastrean y se registran detalles completos de la propiedad de los activos.

¿Mantienen un inventario completo de todas sus relaciones críticas con proveedores?

- Smart-DI tiene una lista completa de todas sus relaciones con proveedores de infraestructura.

¿Proporcionan a los inquilinos documentación que describa escenarios en los que los datos pueden moverse de una ubicación física a otra? (por ejemplo, respaldos fuera del sitio, conmutaciones por error de continuidad de negocios, replicación)

- Smart-DI no contempla escenarios donde los datos puedan moverse de una ubicación a otra porque no almacenamos directamente los datos. En caso de necesitar mover físicamente los datos, los servicios de Azure Cloud Services aseguran la protección y la integridad de los datos.

¿Pueden proporcionar evidencia de que su personal y terceros involucrados han sido capacitados sobre sus políticas, estándares y procedimientos documentados?

- Smart-DI subcontrata el alojamiento de su infraestructura de producto a los principales servicios de alojamiento en la nube, actualmente IONOS y Azure Cloud Services, que proporcionan altos niveles de seguridad física y de red y mantienen varios niveles de seguridad auditada, incluyendo el cumplimiento de SOC 2 Tipo II e ISO 27001. No alojamos la infraestructura del producto dentro de ninguna oficina corporativa.

¿Permiten a los inquilinos especificar en qué ubicaciones geográficas se permite mover sus datos dentro o fuera para abordar consideraciones jurisdiccionales legales basadas en dónde se almacenan frente a dónde se acceden los datos?

- Smart-DI subcontrata el alojamiento de su infraestructura de producto a los principales servicios de alojamiento en la nube, actualmente IONOS y Azure Cloud Services, que proporcionan altos niveles de seguridad física y de red y mantienen varios niveles de seguridad auditada, incluyendo el cumplimiento de SOC 2 Tipo II e ISO 27001. No alojamos la infraestructura del producto dentro de ninguna oficina corporativa.

Encriptación y Gestión de Claves

¿Tienen políticas de gestión de claves que vinculan las claves a propietarios identificables?

- Smart-DI mantiene documentación de su proceso de gestión de claves y proporciona controles para gestionar las claves de encriptación durante su ciclo de vida y proteger contra el uso no autorizado.

¿Tienen la capacidad de gestionar claves de encriptación en nombre de los invitados?

- Smart-DI Services gestiona las claves de encriptación utilizadas, con políticas de retención y rotación de claves configurables por el cliente.

¿Mantienen procedimientos de gestión de claves?

- Smart-DI mantiene documentación sobre su proceso de gestión de claves.

¿Tienen documentada la propiedad de cada etapa del ciclo de vida de las claves de encriptación?

- Smart-DI mantiene documentación sobre su proceso de gestión de claves y proporciona controles para gestionar las claves de encriptación durante su ciclo de vida y proteger contra el uso no autorizado.

¿Utilizan algún marco de terceros/código abierto/propietario para gestionar las claves de encriptación?

- Smart-DI utiliza un sistema propietario basado en las mejores prácticas de la industria para gestionar las claves de encriptación.

¿Encriptan los datos de los inquilinos en reposo (en disco/almacenamiento) dentro de su entorno?

- Encriptamos los datos en reposo en la plataforma de Smart-DI Services.

¿Usan encriptación para proteger datos e imágenes de máquinas virtuales durante el transporte a través de y entre redes e instancias de hipervisor?

- Smart-DI habilita la encriptación HTTPS para asegurar la transmisión de datos. La plataforma Smart-DI utiliza la encriptación HTTPS para la transmisión de datos. La plataforma Smartker y PrinterBI utiliza el protocolo SSL/TLS estándar de la industria.

¿Tienen documentación que establezca y defina sus políticas, procedimientos y directrices de gestión de encriptación?

- Smart-DI mantiene documentación sobre su proceso de gestión de claves.

¿Tienen encriptación adecuada para la plataforma y los datos que utiliza formatos abiertos/validados y algoritmos estándar?

- PrinterBI y Smartker apoyan la criptografía fuerte utilizando formatos estándar validados, incluyendo AES-256.

¿Almacenan claves de encriptación en la nube?

- Sí, están almacenadas en nuestra plataforma en la nube.

¿Tienen funciones de gestión de claves y uso de claves separadas?

- Smart-DI ha establecido e implementado procedimientos para hacer cumplir la segregación de la gestión de claves y las funciones de uso de claves.

Gobernanza y Gestión de Riesgos

¿Tienen la capacidad de monitorear y reportar continuamente el cumplimiento de su infraestructura con sus líneas base de seguridad de la información?

- Sí, tenemos reglas estandarizadas contra las cuales se realiza una verificación de cumplimiento periódicamente basada en nuestro entorno de infraestructura basado en el cual se deriva el informe de cumplimiento de infraestructura.

¿Proporcionan datos de salud del control de seguridad para permitir a los inquilinos implementar la Monitoreo Continuo estándar de la industria (que permite la validación continua del inquilino del estado de su control físico y lógico)?

- Smart-DI realiza una evaluación de riesgos que cubre riesgos de seguridad, continuidad y operacionales. Como parte de este proceso, se identifican amenazas a la seguridad y se evalúan formalmente los riesgos de estas amenazas.

¿Son los gerentes técnicos, comerciales y ejecutivos responsables de mantener la conciencia y el cumplimiento de las políticas, procedimientos y estándares de seguridad tanto para ellos como para sus empleados en lo que respecta al área de responsabilidad del gerente y empleados?

- La gerencia de Smart-DI es responsable de asegurar que los empleados en sus funciones tengan la conciencia adecuada sobre la seguridad de la información, hayan completado la capacitación necesaria sobre seguridad de la información y conozcan y sigan los controles de seguridad de la información relevantes para su rol. La gerencia también es responsable de asegurar un proceso de autorización adecuado para los empleados dentro de sus funciones. La gerencia es responsable de asegurar que se cumplan los requisitos de seguridad durante todo el ciclo de vida del empleo para todos los empleados e individuos externos contratados.

¿Proporcionan a los inquilinos documentación que describa su Programa de Gestión de Seguridad de la Información (ISMP)?

- El White Paper de Seguridad de Smart-DI está disponible para los socios bajo solicitud.

¿Tienen acuerdos para asegurar que sus proveedores adhieren a sus políticas de seguridad de la información y privacidad?

- Smart-DI revisa a los proveedores y asegura que puedan cumplir con los requisitos de seguridad de la información de Smart-DI.

¿Divulgan los controles, estándares, certificaciones y/o regulaciones con los que cumplen?

- Smart-DI aprovecha las mejores prácticas y orientación de seguridad de una amplia variedad de fuentes.

¿Notifican a los inquilinos cuando realizan cambios materiales en sus políticas de seguridad de la información y/o privacidad?

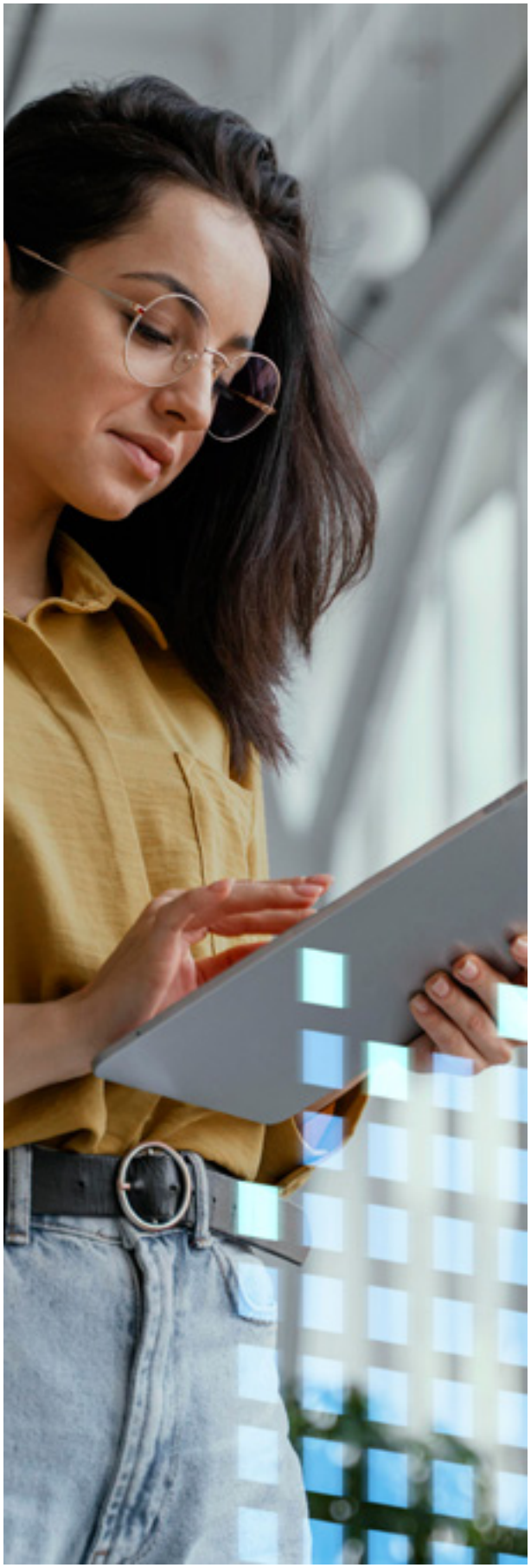
- El White Paper de Seguridad de Smart-DI y la documentación relevante de seguridad para los inquilinos se actualiza regularmente para reflejar los cambios.

¿Realizan revisiones, como mínimo, anuales de sus políticas de privacidad y seguridad?

- Las políticas de privacidad y seguridad se revisan al menos anualmente.

¿Se alinean las evaluaciones de riesgo formales con el marco general de la empresa y se realizan al menos anualmente, o en intervalos planificados, determinando la probabilidad e impacto de todos los riesgos identificados, utilizando métodos cualitativos y cuantitativos?

- Smart-DI está adaptándose al marco IS027001 y planea obtener la certificación para finales de 2023. La evaluación de riesgos se realiza anualmente y se revisan y realizan cambios para mitigar riesgos.



Recursos Humanos

¿Están en funcionamiento sistemas para monitorear violaciones de privacidad y notificar oportunamente a los inquilinos si un evento de privacidad pudo haber afectado sus datos?

- Las violaciones reales, sospechadas o potenciales serán reportadas inmediatamente a la Gerencia de Smart-DI. En caso de una violación, la Gerencia de Smart-DI deberá notificar al cliente final implicado dentro de las 72 horas.
- Dependiendo del tamaño y la gravedad de la violación de datos, la Gerencia puede llevar a cabo una investigación sobre las circunstancias que rodean la violación. Las investigaciones pueden incluir un examen en sitio de los sistemas y procedimientos y podrían llevar a una recomendación para informar a los sujetos de los datos sobre un incidente de violación de seguridad si el cliente final aún no lo ha hecho.

¿Su Política de Privacidad está alineada con los estándares de la industria?

- Smart-DI está adaptándose al marco IS027001 y planea obtener la certificación para finales de 2023.
- Conforme a las leyes locales, regulaciones, ética y restricciones contractuales, ¿están todos los candidatos a empleo, contratistas y terceros involucrados sujetos a verificación de antecedentes?
- Smart-DI realiza la verificación de información de todos los empleados.

¿Están todos los empleados obligados a firmar NDA o acuerdos de confidencialidad como condición de empleo para proteger la información del cliente/inquilino?

- Un acuerdo de confidencialidad es parte del contrato de trabajo de Smart-DI.

¿Se considera la finalización exitosa y oportuna del programa de capacitación un requisito previo para adquirir y mantener el acceso a sistemas sensibles?

- Los acuerdos de empleados deben completarse antes de que se conceda el acceso.

¿Están los procedimientos y directrices mencionados arriba destinados a contemplar la revocación oportuna del acceso y el retorno de activos?

- Las políticas y procedimientos de terminación cubren todos los aspectos de la separación, incluyendo el retorno de activos, insignias, equipos de cómputo y datos, y se mencionan en el contrato del empleado/partner.

¿Se identifican, documentan y revisan a intervalos planificados los requisitos para acuerdos de no divulgación o confidencialidad que reflejen las necesidades de la organización para la protección de datos y detalles operativos?

- Los contratos de clientes de Smart-DI incluyen términos específicos de confidencialidad, y nuestras relaciones con proveedores externos incluyen requisitos de confidencialidad que se revisan cuando sea necesario.

¿Recogen o crean metadatos sobre el uso de datos de inquilinos a través de tecnologías de inspección (motores de búsqueda, etc.)?

- Los metadatos contienen información sobre trabajos de impresión o imágenes escaneadas, que son información específica del trabajo. Estos datos están encriptados.

¿Permiten a los inquilinos optar por no permitir que sus datos/metadatos sean accedidos a través de tecnologías de inspección?

- Smart-DI no recoge datos de inquilinos para tecnologías de inspección.

¿Se informa a los usuarios sobre sus responsabilidades para mantener la conciencia y el cumplimiento de las políticas de seguridad, procedimientos, estándares y requisitos regulatorios aplicables publicados?

- Parte de la capacitación anual de concientización así como de la comunicación continua.

¿Son informados los usuarios sobre sus responsabilidades para mantener un entorno de trabajo seguro y protegido?

- Parte de la capacitación anual de concientización así como del Manual del Empleado.

¿Son informados los usuarios sobre sus responsabilidades para dejar el equipo desatendido de manera segura?

- Parte de la capacitación anual de concientización así como de la comunicación continua.

Gestión de Identidad y Acceso

¿Restringen, registran y monitorean el acceso a sus sistemas de gestión de seguridad de la información? (por ejemplo, hipervisores, firewalls, escáneres de vulnerabilidades, capturadores de red, API, etc.)

- A los empleados de Smart-DI se les concede acceso a los sistemas internos en función de su rol en la empresa, comúnmente referido como controles de acceso basados en roles (RBAC) o, si está preaprobado, según sea necesario.

¿Monitorean y registran el acceso privilegiado (nivel de administrador) a los sistemas de gestión de seguridad de la información?

Sí, como parte de la gestión de control de acceso.

¿Tienen controles para garantizar la eliminación oportuna del acceso a sistemas que ya no es necesario para fines comerciales?

- Los derechos de acceso se revisan al menos anualmente o cuando cambian los roles de los usuarios.

¿Proporcionan métricas para rastrear la velocidad con la que pueden eliminar el acceso a sistemas que ya no es necesario para fines comerciales?

- El acceso a sistemas se elimina el mismo día hábil en que se produce un cambio en el rol del usuario y ya no es necesario el acceso.

¿Utilizan redes seguras dedicadas para

proporcionar acceso de gestión a su infraestructura de servicios en la nube?

- Se necesita autenticación de 2FA antes de acceder a la infraestructura de servicios en la nube. Los grupos de seguridad están en la lista blanca con IPs específicas que pueden acceder al entorno de la nube.

¿Gestionan y almacenan la identidad de todo el personal que tiene acceso a la infraestructura de TI, incluyendo su nivel de acceso?

- Smart-DI subcontrata el alojamiento de su infraestructura de producto a los principales servicios de alojamiento en la nube, actualmente IONOS y Azure Cloud Services, que proporcionan altos niveles de seguridad física y de red y mantienen varios niveles de seguridad auditada, incluyendo SOC 2 Tipo II y cumplimiento ISO 27001. No alojamos la infraestructura del producto dentro de ninguna oficina corporativa.

¿Gestionan y almacenan la identidad de usuario de todo el personal que tiene acceso a la red, incluyendo su nivel de acceso?

- Smart-DI mantiene un sistema de gestión de identidad y autorización.

¿Proporcionan a los inquilinos documentación sobre cómo mantienen la segregación de funciones dentro de su oferta de servicios en la nube?

- El acceso basado en roles es seguido por Smart-DI. Se proporciona el acceso con los privilegios mínimos necesarios a los empleados para que realicen sus respectivas tareas.

¿Existen controles para prevenir el acceso no autorizado a su aplicación, programa o código fuente de objeto, y asegurar que esté restringido solo al personal autorizado?

- El código fuente del Smartker y PrinterBI está almacenado en el sistema de control de versiones y el acceso está limitado a miembros autorizados del desarrollo de software.

¿Existen controles para prevenir el acceso no autorizado a la aplicación, programa o código fuente de objeto del inquilino, y asegurar que esté restringido solo al personal autorizado?

- El código fuente del Smartker y PrinterBI está almacenado en el sistema de control de versiones y el acceso está limitado a miembros autorizados del desarrollo de software.

¿Proporcionan capacidad de recuperación ante desastres múltiples fallas?

- La ubicación de los servicios de nube de IONOS y Azure proporciona esta capacidad.

¿Monitorean la continuidad del servicio con proveedores upstream en caso de falla del proveedor?

- Smart-DI monitorea el cumplimiento del SLA de Azure y IONOS y, en caso de falla del proveedor, la información sobre el incidente se publica en el sitio web de Azure y IONOS.

¿Tienen más de un proveedor para cada servicio en el que dependen?

- Smart-DI depende de la infraestructura en la nube de Azure y IONOS como proveedor de servicios.

¿Proporcionan acceso a resúmenes de redundancia operativa y continuidad, incluyendo los servicios en que dependen?

- Los datos son replicados en múltiples Zonas de Disponibilidad, lo que reduce el tiempo de recuperación.

¿Proporcionan al inquilino la capacidad de declarar un desastre?

- Sí, un inquilino puede contactar al soporte 24/7 para plantear problemas y, con base en el SLA, se tomarán las medidas necesarias.

¿Proporcionan una opción de conmutación por error activada por el inquilino?

- Smartker y PrinterBI son plataformas SaaS y se encargan de la recuperación ante desastres.

¿Comparten sus planes de continuidad de negocios y redundancia con sus inquilinos?

- Smart-DI depende principalmente de la redundancia de infraestructura, replicación en tiempo real y copias de seguridad. Las pruebas de recuperación ante desastres son parte del procesamiento normal de Smart-DI. Los datos son replicados y respaldados en múltiples ubicaciones de almacenamiento duradero.
- Smart-DI también depende de los planes de recuperación y continuidad de los muchos proveedores de servicios en la nube que utiliza para la infraestructura del producto y de uso interno. Nuestros proveedores de infraestructura subcontratada tienen numerosas salvaguardas contra peligros ambientales en su lugar, y sus planes de continuidad y recuperación han sido validados de manera independiente.

¿Documentan cómo otorgan y aprueban acceso a los datos de los inquilinos?

- Los procesos y políticas internas de datos de Smart-DI están diseñados para prevenir que personas y/o sistemas no autorizados accedan a los sistemas utilizados para procesar datos personales. Smart-DI busca diseñar sus sistemas para permitir sólo a personas autorizadas accesar a los datos que están autorizados a acceder, y asegurar que los datos personales no puedan ser leídos, copiados, alterados o eliminados sin autorización durante el procesamiento, uso y después de ser registrados. Los sistemas están diseñados para detectar cualquier acceso inapropiado. Smart-DI emplea un sistema de gestión de acceso centralizado para controlar el acceso del personal al servidor de producción y sólo proporciona acceso a un número limitado de personal autorizado.

¿Tienen un método para alinear las metodologías de clasificación de datos del proveedor y del inquilino para propósitos de control de acceso?

- Los datos del inquilino son clasificados con el nivel más alto de confidencialidad y el control de acceso a los sistemas que procesan datos de los

inquilinos está restringido solo a administradores nombrados. El acceso es monitoreado y se recopila un registro de auditoría.

¿Proporcionan a los inquilinos a solicitud acceso de usuarios (por ejemplo, empleados, contratistas, clientes (inquilinos), socios comerciales y/o proveedores) a datos y cualquier aplicación, sistema de infraestructura y componentes de red que posean o gestionen (físicos y virtuales)?

- Damos uno o más representantes de los clientes acceso de nivel administrador a sus propios datos, y los clientes pueden crear, modificar y eliminar a sus usuarios normales y niveles de acceso de usuarios mediante esta cuenta administradora.
- Si se descubre que los usuarios tienen derechos inapropiados, ¿se registran todas las acciones de remediación y certificación?
- Smart-DI registra todos los cambios en los permisos de usuario. Smart-DI revoca el acceso cuando ya no es necesario.

¿Compartirán los informes de remediación y certificación de derechos de usuario con sus inquilinos si se permitió el acceso inapropiado a los datos del inquilino?

- Cuando sea necesario, los problemas de seguridad se comunican a los clientes de acuerdo con métodos de confidencialidad adecuados.

¿Cualquier cambio en el estado de acceso del usuario está destinado a incluir la terminación del empleo, contrato o acuerdo, cambio de empleo o transferencia dentro de la organización?

- El acceso a todos los activos/sistemas se revoca cuando se produce una terminación del empleo. Los cambios en roles o responsabilidades desencadenan la revisión de los derechos de acceso donde el acceso se cambia al mínimo necesario dentro del nuevo rol.

¿Soportan el uso de, o integración con, soluciones existentes de autenticación única (SSO) basadas en clientes para su servicio?

- Smart-DI ha implementado Azure ID como método de autenticación.

¿Utilizan estándares abiertos para delegar capacidades de autenticación a sus inquilinos?

- Smart-DI ha implementado Azure ID como método de autenticación.

¿Soportan estándares de federación de identidad (SAML, SPML, WS-Federation, etc.) como un medio de autenticar/ autorizara a los usuarios?

- Smart-DI ha implementado Azure ID como método de autenticación.

¿Proporcionan a los inquilinos opciones de autenticación fuerte (multifactor) (certificados digitales, tokens, biometría, etc.) para el acceso de usuario?

- Smart-DI ha implementado Azure ID como método de autenticación.

¿Permiten a los inquilinos utilizar servicios de aseguramiento de identidad de terceros?

- Smart-DI ha implementado Azure ID como método de autenticación.

¿Soportan la política de contraseñas (longitud mínima, edad, historial, complejidad) y el cumplimiento de la política de bloqueo de cuentas (umbral de bloqueo, duración del bloqueo)?

- La creación y asignación de contraseñas se gestionan a través de los procesos estándar de gestión de cuentas, en el sistema de autenticación del cliente, como Azure AD.

¿Permiten a los inquilinos/clientes definir políticas de contraseñas y bloqueo de cuentas para sus cuentas?

- Los clientes son responsables de configurar los ajustes de inicio de sesión fallido para el acceso a través de su propia autenticación o la autenticación de Azure AD mediante a) imponer un límite de 3 intentos consecutivos de acceso fallido por un usuario durante un intervalo de 5 minutos; y b) bloquear automáticamente la cuenta durante 30 minutos, bloquear la cuenta hasta que sea liberada por un administrador, o retrasar el siguiente intento de acceso por el intervalo definido por la organización cuando se excede el número máximo de intentos fallidos.

¿Soportan la capacidad de forzar cambios de contraseña en el primer inicio de sesión?

- El cliente puede definir sus propias políticas de contraseñas y flujos de trabajo de restablecimiento de contraseñas en Azure AD.

¿Tienen mecanismos para desbloquear cuentas bloqueadas (por ejemplo, autoservicio a través de correo electrónico, preguntas de desafío definidas, desbloqueo manual)?

- Los administradores del portal de clientes pueden autoservirse de todas las necesidades de gestión de usuarios.

¿Se evitan los ataques que apuntan a la infraestructura virtual mediante controles técnicos?

- La infraestructura de la plataforma en la nube está adecuadamente endurecida para minimizar la superficie de ataque.

Seguridad de Infraestructura y Virtualización

¿Se implementan herramientas de detección de integridad de archivos (host) e intrusión en la red (IDS) para ayudar a facilitar la detección oportuna, la investigación mediante análisis de causa raíz y la respuesta a incidentes?

- Smart-DI ha implementado tecnología de detección de intrusiones que detecta y responde a posibles violaciones de seguridad.

¿El acceso físico y lógico de los usuarios a los registros de auditoría está restringido a personal autorizado?

- Smart-DI restringe el acceso físico y lógico a los registros de auditoría sólo a usuarios autorizados.

¿Pueden proporcionar evidencia de que se ha realizado un mapa de diligencia debida de las regulaciones y estándares a sus controles/arquitectura/procesos?

- Este informe es confidencial y no puede compartirse.

¿Se revisan regularmente los registros de auditoría para eventos de seguridad (por ejemplo, con herramientas automatizadas)?

- Se configuran alertas para eventos clave de seguridad. Además, los registros se revisan regularmente.

¿Utilizan un protocolo de servicio de tiempo sincronizado (por ejemplo, NTP) para asegurar que todos los sistemas tengan una referencia de tiempo común?

- Todos los servicios de Smart-DI (PrinterBI y Smartker) utilizan un protocolo de servicio de tiempo sincronizado para asegurar que todos los sistemas tengan una referencia de tiempo común.

¿Proporcionan documentación sobre los niveles de sobresuscripción del sistema (red, almacenamiento, memoria, I/O, etc.) que mantienen y en qué circunstancias/ escenarios?

- Smart-DI supervisa la capacidad y el rendimiento de la red, almacenamiento, memoria y I/O de los servicios de infraestructura.

¿Las necesidades de capacidad del sistema toman en cuenta las necesidades

actuales, proyectadas y anticipadas de capacidad para todos los sistemas utilizados para proporcionar servicios a los inquilinos?

- La escalabilidad del servicio se realiza de manera mayoritariamente automatizada. Las necesidades de capacidad a futuro consideran el crecimiento de los clientes, el modelado de requerimientos y las ganancias de eficiencia.

¿Se supervisa y ajusta el rendimiento del sistema para cumplir continuamente con los requisitos regulatorios, contractuales y comerciales para todos los sistemas utilizados para proporcionar servicios a los inquilinos?

- Smart-DI supervisa el rendimiento y los requisitos de capacidad usando herramientas de monitoreo automatizadas.

¿Las herramientas o servicios de evaluación de vulnerabilidades de seguridad acomodan las tecnologías de virtualización que se están utilizando (por ejemplo, conscientes de la virtualización)?

- Smart-DI realiza pruebas de seguridad como análisis de accesibilidad de la red, análisis de comportamiento en tiempo de ejecución, análisis de vulnerabilidades comunes y de exposición y evaluación comparativa de operación y seguridad CIS para todas sus máquinas virtuales.

¿Actualizan regularmente los diagramas de arquitectura de red que incluyen el flujo de datos entre dominios/zona de seguridad?

- Smart-DI mantiene información detallada sobre su arquitectura de red. Debido a la complejidad y las consideraciones de confidencialidad de los diagramas de red, Smart-DI no los publica a clientes actuales o potenciales.

¿Revisan regularmente la adecuación del acceso/conectividad permitidos (por ejemplo, reglas de firewall) entre dominios/ zona de seguridad dentro de la red?

- Las listas de control de acceso y las reglas de firewall son monitoreadas programáticamente contra una línea de base de configuración estandarizada. Los cambios que se desvían de la línea de base esperada disparan una revisión humana automáticamente. Además, las listas de control de acceso se revisan periódicamente para asegurar que las restricciones y permisos logren los objetivos previstos.

¿Están documentadas todas las listas de control de acceso de firewall con justificación comercial?

- Las listas de control de acceso de firewall con justificación comercial están documentadas en las guías de configuración interna de Smart-DI para los administradores del sistema y de gestión solamente.

¿Las listas de control de acceso y las reglas de firewall son monitoreadas programáticamente contra una línea de base de configuración estandarizada?

- Las listas de control de acceso y las reglas de firewall son monitoreadas programáticamente contra una línea

de base de configuración estandarizada. Los cambios que se desvían de la línea de base esperada disparan una revisión humana automáticamente. Además, las listas de control de acceso se revisan periódicamente para asegurar que las restricciones y permisos logren los objetivos previstos.

¿Están los sistemas y entornos de red protegidos por un firewall o firewall virtual para asegurar el cumplimiento con los requisitos legislativos, regulatorios y contractuales?

- Smart-DI utiliza la infraestructura en la nube de IONOS y Azure para alojar sus servicios, que están protegidos con firewalls externos e internos.

¿Están los sistemas y entornos de red protegidos por un firewall o firewall virtual para asegurar la separación de entornos de producción y no producción?

- Smart-DI utiliza la infraestructura en la nube de IONOS y Azure para alojar sus servicios, que están protegidos con firewalls externos e internos.

¿Están los sistemas y entornos de red protegidos por un firewall o firewall virtual para asegurar la protección y aislamiento de datos sensibles?

- Se implementa segregación lógica para restringir el acceso no autorizado de clientes a archivos/directorios de otros clientes. Además, Smart-DI utiliza la infraestructura en la nube de IONOS y Azure para alojar sus servicios, que están protegidos con firewalls externos e internos.

¿Se utilizan canales de comunicación seguros y encriptados al migrar servidores físicos, aplicaciones o datos a servidores virtuales?

- La comunicación entre componentes, por ejemplo, entre el servidor y la base de datos o servidor a servidor, está protegida por TLS y una infraestructura PKI.

¿Utilizan una red segregada de redes de nivel de producción al migrar servidores físicos, aplicaciones o datos a servidores virtuales?

- La red de producción de los servicios de Smart-DI está segregada de redes no productivas.

¿Restringen el acceso del personal a todas las funciones de gestión de hipervisores o consolas administrativas para sistemas que alojan sistemas virtualizados basados en el principio de privilegio mínimo y soportado a través de controles técnicos?

- Todo acceso a sistemas de producción está basado en el privilegio mínimo basado en roles, requiere autenticación de dos factores.

¿Sus diagramas de arquitectura de red identifican claramente entornos de alto riesgo y flujos de datos que pueden tener impactos de cumplimiento legal?

- Los componentes del servicio Smart-DI con impactos regulatorios o de cumplimiento están bien designados.

¿Implementan medidas técnicas y aplican técnicas de defensa en profundidad (por ejemplo, análisis profundo de paquetes,

limitación de tráfico y blackholing) para la detección y respuesta oportuna a ataques basados en la red asociados con patrones de tráfico de entrada o salida anómalos (por ejemplo, suplantación de MAC y ataques de envenenamiento ARP) y ataques de denegación de servicio distribuido (DDoS)?

- Smart-DI tiene un servicio de detección de amenazas que monitorea continuamente la actividad maliciosa y el comportamiento no autorizado para proteger el entorno de smartDI Services. Previene y detecta actividades como minería de criptomonedas, comportamiento de compromiso de credenciales, comunicación con servidores conocidos de comando y control o llamadas API desde IP conocidas como maliciosas.

Interoperabilidad y Portabilidad

¿Publican una lista de todas las API disponibles en el servicio e indican cuáles son estándar y cuáles son personalizadas?

- Los detalles de las API disponibles de Smart-DI se pueden encontrar en nuestra documentación interna y no se comparten con el público.

¿Proporcionan políticas y procedimientos que rigen el uso de API para la interoperabilidad entre su servicio y aplicaciones de terceros?

- En este momento, Smart-DI no publica ninguna API pública, por lo que no proporcionamos ninguna política o procedimiento.

¿Puede realizarse la importación de datos, exportación de datos y la gestión de servicios sobre protocolos de red seguros (por ejemplo, texto no claro y autenticado), estandarizados y aceptados por la industria?

- Todas las interacciones sensibles con Smart-DI (por ejemplo, llamadas API, inicio de sesión, sesiones autenticadas en el portal del cliente, etc.) están encriptadas en tránsito.

¿Proporcionan a los consumidores (inquilinos) documentación que detalla los estándares de protocolo de red relevantes para la interoperabilidad y portabilidad que están involucrados?

- Smart-DI proporciona un documento de solución durante la etapa de POC que incluirá todos los detalles de red necesarios para la comunicación adecuada entre los componentes de los servicios SmartDI.

Gestión de Incidentes de Seguridad

¿Tienen un plan documentado de respuesta a incidentes de seguridad?

- Las violaciones reales, sospechadas o posibles se informarán de inmediato a la Gerencia de Smart-DI. En caso de una violación, la Gerencia de Smart-DI deberá notificar al cliente final implicado dentro de las 72 horas.

¿Integran los requisitos personalizados de los inquilinos en sus planes de respuesta a incidentes de seguridad?

- El plan de respuesta a incidentes está a cargo de la Gerencia de Smart-DI y ya está personalizado para los requisitos de los inquilinos.

¿Han probado sus planes de respuesta a incidentes de seguridad en el último año?

- Los planes de respuesta de seguridad e incidentes se actualizan y prueban continuamente al menos una vez al año.

¿Su marco de registro y monitoreo permite la aislación de un incidente a inquilinos específicos?

- Todos los objetos de datos están etiquetados con identificadores específicos del cliente. Cuando sea necesario, las solicitudes pueden rastrearse a inquilinos específicos, usuarios de clientes específicos y conjuntos de datos específicos.

¿Su plan de respuesta a incidentes cumple con los estándares de la industria para procesos y controles de gestión de la cadena de custodia legalmente admisibles?

- El programa de respuesta a incidentes de seguridad de Smart-DI es practicado, repetible y cumple con los más altos estándares de la industria. Cuando sea necesario, nuestros esfuerzos de investigación asegurarían que se tomen los pasos apropiados.

¿Su capacidad de respuesta a incidentes incluye el uso de técnicas de recolección y análisis de datos forenses legalmente admisibles?

- Si es necesario, Smart-DI puede apoyar solicitudes válidas de datos específicos de inquilinos por parte de la ley.

¿Son capaces de soportar retenciones ligadas a litigios (congelación de datos desde un punto específico en el tiempo) para un inquilino específico sin congelar datos de otros inquilinos?

- Desde la copia de seguridad se puede crear un entorno forense donde el enfoque puede ser únicamente un inquilino.

¿Hacen cumplir y atestiguan la separación de datos de inquilinos cuando producen datos en respuesta a citaciones legales?

- La separación de datos de inquilinos se hace cumplir en caso de respuesta a citaciones legales.

Gestión de la Cadena de Suministro

¿Diseñan e implementan controles para mitigar y contener riesgos de seguridad de datos mediante la separación adecuada de funciones, acceso basado en roles y acceso con el mínimo privilegio para todo el personal dentro de su cadena de suministro?

- Los controles de acceso se aplican estrictamente y se proporcionan como una función del rol del usuario o mediante solicitudes de acceso rigurosas just-in-time.

¿Proporcionan información sobre incidentes de seguridad a todos los clientes y proveedores afectados periódicamente a través de métodos electrónicos (por ejemplo, portales)?

- Los clientes individuales son notificados si un incidente afecta sus datos.

¿Recogen datos de capacidad y uso para todos los componentes relevantes de su oferta de servicios en la nube?

- Smart-DI gestiona los datos de capacidad y utilización para su uso interno únicamente.

¿Proporcionan a los inquilinos informes de planificación de capacidad y uso?

- Smart-DI es una plataforma SaaS y los informes de planificación de capacidad y uso son para uso interno de Smart-DI únicamente.

¿Seleccionan y monitorean proveedores subcontratados en cumplimiento con las leyes del país donde se procesan, almacenan y transmiten los datos?

- Azure Cloud Storage y IONOS son los únicos proveedores de servicios para la plataforma Smart-DI y los seleccionamos porque cumplen con las leyes establecidas para el procesamiento y alojamiento de datos.

¿Seleccionan y monitorean proveedores subcontratados en cumplimiento con las leyes del país de origen de los datos?

- Azure Cloud Storage y IONOS son los únicos proveedores de servicios para la plataforma Smart-DI y los seleccionamos porque cumplen con las leyes establecidas para el procesamiento y alojamiento de datos.

¿Incluyen los acuerdos con terceros disposiciones para la seguridad y protección de la información y los activos?

- Azure Storage e IONOS son los únicos proveedores de servicios para la plataforma Smart-DI y tienen certificados para ISO27001, SOC2, y varios certificados de cumplimiento de seguridad.

¿Están establecidas políticas y procedimientos, y se implementan procesos comerciales y medidas técnicas de apoyo, para mantener acuerdos completos, precisos y relevantes (por ejemplo, SLA) entre proveedores y clientes (inquilinos)?

- El objetivo de Smart-DI es identificar y abordar rápidamente y de manera transparente el problema. Para obtener más información sobre un SLA para su uso de los productos de Smart-DI, hable con su Representante de Ventas o Gerente de Cuenta.

¿Revisan todos los acuerdos, políticas y procesos al menos una vez al año?

- Los acuerdos y contratos correspondientes se revisan al menos con la frecuencia que requieren sus términos. En general, los contratos de Smart-DI se acuerdan y revisan anualmente.

¿Aseguran una seguridad de la información razonable a lo largo de toda su cadena de suministro mediante una revisión anual?

- Smart-DI asegura una seguridad razonable de la información en toda nuestra cadena de suministro.

¿Su revisión anual incluye a todos los socios/proveedores terceros de los cuales depende su cadena de suministro de información?

- Los acuerdos y contratos correspondientes se revisan al menos con la frecuencia que requieren sus términos.

Gestión de Amenazas y Vulnerabilidades Antivirus

¿Tienen programas anti-malware que soporten o se conecten a sus ofertas de servicios en la nube instalados en todos sus sistemas?

Sí, tenemos agentes de detección de intrusiones instalados para proteger nuestro entorno en la nube junto con agentes instalados en máquinas virtuales que pueden identificar problemas de seguridad de aplicaciones, minería de criptomonedas, comportamiento de compromiso de credenciales, comunicación con servidores conocidos de comando y control o llamadas API desde IP conocidas como maliciosas.

¿Aseguran que los sistemas de detección de amenazas de seguridad que uti-

lizan firmas, listas o patrones de comportamiento se actualizan en todos los componentes de la infraestructura dentro de los plazos aceptados por la industria?

Sí, tenemos agentes actualizados de detección de intrusiones instalados para proteger nuestro entorno en la nube junto con agentes instalados en máquinas virtuales que pueden identificar problemas de seguridad de aplicaciones, minería de criptomonedas, comportamiento de compromiso de credenciales, comunicación con servidores conocidos de comando y control o llamadas API desde IP conocidas como maliciosas.

¿Realizan escaneos de vulnerabilidades a nivel de red regularmente según lo prescrito por las mejores prácticas de la industria?

Los escaneos de vulnerabilidades a nivel de red se realizan mensualmente y se analizan y rastrean los hallazgos necesarios.

¿Realizan escaneos de vulnerabilidades a nivel de aplicación regularmente según lo prescrito por las mejores prácticas de la industria?

Los escaneos de vulnerabilidades a nivel de aplicación se realizan mensualmente y se analizan y rastrean los hallazgos necesarios.

¿Realizan escaneos de vulnerabilidades a nivel de sistemas operativos locales regularmente según lo prescrito por las mejores prácticas de la industria?

Los escaneos de vulnerabilidades a nivel de sistemas operativos se realizan mensualmente y se analizan y rastrean los hallazgos necesarios.

¿Tienen la capacidad de parchear rápidamente vulnerabilidades en todos sus dispositivos de cómputo, aplicaciones y sistemas?

Sí, Smart-DI es una plataforma SaaS y si alguna vulnerabilidad se considera dañina, el plazo de parcheo es máximo de 1 semana según el nivel de criticidad de la vulnerabilidad.

¿Proporcionarían a sus inquilinos sus plazos de parcheo de sistemas basados en riesgos a solicitud?

Sí, Smart-DI es una plataforma SaaS y si alguna vulnerabilidad se considera dañina, el plazo de parcheo es máximo de 1 semana según el nivel de criticidad de la vulnerabilidad.

Historial de Versiones

Mayo de 2023 - Versión 1.5

Nota: Este documento no crea ninguna garantía, representación, compromiso contractual, condiciones de Smart-DI, sus afiliados, proveedores o licenciatarios. Las responsabilidades y obligaciones de Smart-DI hacia sus clientes están controladas por acuerdos contractuales, y este documento no forma parte ni modifica ningún acuerdo entre Smart-DI y sus socios o clientes.

Julio de 2022 - Versión 1.4

Nota: Este documento no crea ninguna garantía, representación, compromiso contractual, condiciones de Smart-DI, sus afiliados, proveedores o licenciatarios. Las responsabilidades y obligaciones de Smart-DI hacia sus clientes están controladas por acuerdos contractuales, y este documento no forma parte ni modifica ningún acuerdo entre Smart-DI y sus socios o clientes.

Enero de 2022 - Versión 1.3

Nota: Este documento no crea ninguna garantía, representación, compromiso contractual, condiciones de Smart-DI, sus afiliados, proveedores o licenciatarios. Las responsabilidades y obligaciones de Smart-DI hacia sus clientes están controladas por acuerdos contractuales, y este documento no forma parte ni modifica ningún acuerdo entre Smart-DI y sus socios o clientes.

Agosto de 2021 - Versión 1.2

Nota: Este documento no crea ninguna garantía, representación, compromiso contractual, condiciones de Smart-DI, sus afiliados, proveedores o licenciatarios. Las responsabilidades y obligaciones de Smart-DI hacia sus clientes están controladas por acuerdos contractuales, y este documento no forma parte ni modifica ningún acuerdo entre Smart-DI y sus socios o clientes.

Junio de 2021 - Versión 1.1

Nota: Este documento no crea ninguna garantía, representación, compromiso contractual, condiciones de Smart-DI, sus afiliados, proveedores o licenciatarios. Las responsabilidades y obligaciones de Smart-DI hacia sus clients están controladas por acuerdos contractuales y este documento no forma parte ni modifica ningún acuerdo entre Smart-DI y sus socios o clientes.

White Paper
Smart-DI
Cloud Services

Los servicios mencionados en este documento contienen información que es propiedad de Smart-DI Group Inc.. Es importante tener en cuenta que estos servicios están en constante desarrollo y evolución, por lo que la información aquí proporcionada está sujeta a cambios sin previo aviso. Los derechos de propiedad intelectual e información contenidos en este documento son confidenciales y exclusivos de Smart-DI Group, y solo pueden ser accedidos por esta organización y el cliente. Si encuentra algún error en la documentación, le pedimos que nos lo comunique por escrito al siguiente correo electrónico admin@smart-di.com.

Smart-DI no puede garantizar que este documento esté libre de errores.

Renuncia de responsabilidad

Este documento ha sido redactado con cuidado y la información incluida proviene de fuentes confiables. Sin embargo, no asumimos ninguna responsabilidad por la precisión, integridad o pertinencia de la información proporcionada. Por lo tanto, no se aceptarán reclamaciones derivadas del uso de la información contenida en este documento. Smart-DI Group se reserva el derecho de modificar esta información en cualquier momento sin previo aviso.

Además, recomendamos encarecidamente a los usuarios que verifiquen la información actualizada y consulten a profesionales cualificados antes de tomar decisiones basadas en la misma.

Esta renuncia de responsabilidad se aplica tanto a Smart-DI Group como a sus empleados, directores, afiliados y socios comerciales.

Finalidad de este documento

PrinterBI es una solución cuya finalidad es la de realizar el análisis de información de impresión generada por soluciones DAS – Document Accounting Solutions (MyQ, Equitrac, PaperCut, Docupro, OneQ, etc.), Soluciones MPS – Managed Print Services y Otras; Smartker es un servicio de Gestión documental y automatización de flujos de trabajo; y CaptureBI es una solución de captura y digitalización de información. Estas tres soluciones/servicios conforman actualmente la plataforma de servicios de Smart-DI, llamada Smart-DI Services.

El presente documento describe las características técnicas de la plataforma Smart-DI Services, centrándose en las medidas técnicas y de proceso que Smart-DI Group ha implementado en las áreas de seguridad (seguridad TI y protección de datos) y capacidad de ampliación de la plataforma.

Este documento está dirigido, en concreto, a empleados técnicos de posibles clientes, empresas interesadas y socios de ventas, así como a consultores o medios especializados.

Finalidad de este documento:

El propósito de este documento es describir las características técnicas de la plataforma Smart-DI Services, que incluye servicios como PrinterBI, Smartker y CaptureBI. Estas soluciones fueron diseñadas entre otras cosas para para realizar el análisis de información de impresión generada por soluciones DAS (Document Accounting Solutions) como MyQ, Equitrac, PaperCut, Docupro, OneQ, etc., Soluciones MPS (Management Printer Services) com NDD MPS, Nubeprint, KFS (Kyocera Fleet Services) y Soluciones IMS (Incident Management Solutions); ofrecer servicios gestión documental y automatización de flujos de trabajo a través de Smartker; y proporcionar una solución de captura y digitalización de información mediante CaptureBI. Estos son algunos de los servicios que conforman la plataforma integral de Smart-DI Services.

El enfoque principal de este documento se centra en las medidas técnicas y procesos implementados por Smart-DI Group en las áreas de seguridad (seguridad TI y protección de datos) y capacidad de expansión de la plataforma.

Este documento está dirigido específicamente a empleados técnicos de posibles clientes, empresas interesadas y socios de ventas, así como a consultores y medios especializados que deseen obtener información detallada sobre la plataforma Smart-DI Services.

Introducción

Smart-DI Services ofrece un conjunto de soluciones o servicios basados en el modelo “Software as a Service” (SaaS), los cuales se prestan en un entorno compartido para múltiples clientes y usuarios. Para ofrecer estos servicios, Smart-DI Services utiliza servicios especializados de terceros, como AWS, Microsoft Azure y IONOS. Todos los documentos y archivos del cliente que requieran ser almacenados se guardarán exclusivamente utilizando el servicio de Azure Storage. No se almacenará ningún documento o archivo en unidades locales.

Según el tamaño y los requisitos del cliente, la información de todos los servicios se almacena en una base de datos relacional PostgreSQL. Por defecto, esta base de datos se aloja en nuestra infraestructura de servidores de IONOS. Sin embargo, según los requisitos del cliente, también se puede alojar en Azure Database for PostgreSQL o utilizar la infraestructura en la nube del propio cliente. Ambos servicios cuentan con procedimientos de copia de seguridad diaria a nivel de cada base de datos, de cada instancia y además se siguen las mejores prácticas de seguridad de la información las cuales permiten poder recuperar la información en el menor tiempo posible en caso de presentarse alguna incidencia de “desastre” del servicio.

Este documento se limita a describir los servicios ofrecidos y desarrollados directamente por Smart-DI. Nuestros asociados comerciales (AWS, Microsoft Azure y IONOS) proporcionan información detallada sobre el funcionamiento de los servicios que incorporamos de ellos, como Microsoft Azure Storage, Microsoft Azure Database for PostgreSQL, Lambdas AWS, Airflow AWS, Microsoft PowerBI, Microsoft Azure Defender, Microsoft Authentication Services, etc. Asimismo, estos asociados describen las medidas relacionadas con la seguridad TI y la protección de datos en las que se basa Smart-DI.

Seguridad

Los datos del cliente utilizados en las plataformas de Smart-DI Services están protegidos de acuerdo con las normas de tecnología generalmente aceptadas (GDPR, ISO 27001, etc.). Esto se logra mediante el uso de la infraestructura de TI de IONOS Hosting Services y las tecnologías de Microsoft Azure AD Authentication Services, Microsoft Azure Storage Services y Microsoft Azure Database for PostgreSQL, asegurándose de que se cumplan las directivas actuales de protección de datos.

Los datos del cliente utilizados y almacenados en la plataforma de Smart-DI Services están protegidos de acuerdo con las mejores prácticas de seguridad reconocidas en la industria. Para lograr esto, nos apoyamos en la infraestructura de TI de IONOS Hosting Services y en las tecnologías proporcionadas por Microsoft Azure, como Microsoft Azure AD Authentication Services, Microsoft Azure Storage Services, Microsoft Azure Database for PostgreSQL, etc. Estas tecnologías nos permiten cumplir con las directivas actuales de protección de datos, incluyendo normas como el Reglamento General de Protección de Datos (GDPR) y las pautas de la norma ISO 27001, entre otras.

Seguridad de TI:

Smart-DI se esfuerza por garantizar la seguridad de los datos mediante la implementación de medidas de protección. Estas incluyen la encriptación de documentos, bases de datos y comunicaciones, así como un sofisticado concepto de derechos y/o restricciones de acceso a la información y auditorías de seguridad. Smart-DI Group, está comprometida a seguir las mejores prácticas de seguridad y a actualizar constantemente nuestros sistemas para proteger los datos de nuestros clientes y minimizar cualquier riesgo.

En cuanto a la comunicación, en el centro de datos de IONOS utilizado por Smart-DI, todos los datos de comunicación del cliente están protegidos mediante una VPN (Red Privada Virtual). Además, la infraestructura de red está virtualizada y la red virtual está protegida contra amenazas externas.

Para la codificación del tráfico de datos entre los usuarios y el centro de datos, se utiliza el protocolo TLS (Secure Transport Layer), sucesor del SSL. TLS se emplea para todo el tráfico basado en HTTP (HTTPS) y TCP, y los usuarios pueden verificar en su navegador si su conexión está segura y validada.

Además, se implementan capas y funciones adicionales de seguridad, como HSTS (HTTP Strict Transport Security), que protege contra ataques de degradación de protocolo y secuestro de cookies.

En cuanto a los servicios de recolección de información de PrinterBI, se utiliza un servicio de conexión directa a nuestra plataforma, donde la información se envía cifrada al centro de datos. También se cuenta con un servicio de SFTP (Protocolo de Transferencia de Archivos SSH) ubicado en IONOS como método de respaldo de comunicación, en caso de que no se pueda acceder directamente

a través del puerto 8787. En este caso, la información del cliente se almacena en un archivo ZIP encriptado con WinZip AES Encryption de 256 bits y se elimina después de que los datos se han procesado e ingresado en la base de datos PostgreSQL correspondiente al cliente.

Codificación de documentos:

Todos los documentos archivados en la plataforma Smart-DI Services se encriptan automáticamente utilizando el método AES (Advanced Encryption Standard) de 256 bits, que es un método criptográfico simétrico de alta seguridad. Esta codificación AES genera un par de claves asimétricas para cada archivo, donde la clave privada se utiliza para codificar las claves simétricas generadas durante la codificación de los documentos. A su vez, la clave de codificación del archivo se vuelve a codificar con una clave maestra.

Para lograr la máxima protección, Smart-DI Services utiliza una longitud de codificación de 256 bits con AES, lo que impide la detección de patrones y hace que las claves de codificación sean imposibles de calcular incluso mediante criptoanálisis.

Concepto de derechos de acceso y restricción a los documentos:

Las soluciones de Smart-DI Services utilizan un sofisticado sistema de derechos de acceso, que puede diferenciar entre derechos funcionales y derechos de acceso en los servicios proporcionados a través de la plataforma Smart-DI Services (PrinterBI, Smartker DMS y CaptureBI).

Los derechos funcionales se asignan por organización de Smart-DI y se refieren a las acciones que un usuario puede realizar dentro de cada solución. Estas acciones pueden incluir la administración de usuarios, la configuración de archivos y bandejas, el diseño de flujos de trabajo, el uso de sellos, la administración de departamentos, indicadores, paneles de control, entre otros.

Los derechos de acceso se refieren al acceso a información/carpetas/especificas y a los documentos almacenados en ellas. Estos derechos pueden incluir la gestión de autorizaciones administrativas, como derechos de diálogo o descarga de documentos, la búsqueda, edición o eliminación de autorizaciones generales para documentos en un archivo, y autorizaciones de superposición, como la aplicación de sellos, anotaciones y elementos gráficos a los documentos, o la eliminación de anotaciones. También se pueden asignar autorizaciones para campos de índice, como cambiar los contenidos de los campos o utilizar entradas de campos que no están en una lista de selección.

Derechos para usuarios y administradores:

En todas las configuraciones de Smart-DI Services, como bandejas, archivos o formularios, se asignan permisos tanto a los usuarios directamente como a través de roles. Existen dos tipos diferentes de permisos: los derechos de usuario permiten el uso del objeto en cuestión,

mientras que los derechos de administrador permiten realizar cambios en el objeto o su configuración.

Restricción de acceso mediante separación de datos:

Las soluciones de Smart-DI Services separan de manera estricta los datos del cliente de los datos del sistema. Esto significa que la plataforma utiliza una organización (base de datos, usuarios, accesos, roles, etc.) de los servicios de Smart-DI para cada cliente. Esto permite que los servicios de Smart-DI utilicen nuestros propios recursos de infraestructura o los recursos del cliente, según sea necesario. Por ejemplo, los servicios pueden utilizar la base de datos y las cuentas de Azure Storage del cliente.

Auditoría de seguridad:

Se realizan pruebas regulares de penetración externa e interna para mantener la seguridad de los sistemas. Los auditores externos examinan cuidadosamente los resultados de estas pruebas, que se llevan a cabo mensualmente o antes de incorporar una nueva funcionalidad a la plataforma.

Además, Azure Security Services proporciona informes detallados sobre los riesgos identificados para que cualquier problema que surja con los servicios en Microsoft Azure pueda ser resuelto rápidamente.

Los clientes tienen la capacidad de registrar y exportar los registros de documentos, archivos y organizaciones dentro de su propia organización en formato CSV universal para facilitar su lectura. Estos registros permiten, por ejemplo, rastrear quién modificó una determinada configuración o guardó/eliminó documentos. Los registros también demuestran el cumplimiento de las directrices legales.

Análisis de datos telemétricos

En los análisis de seguridad en tiempo real de los datos telemétricos, se comprueba si se producen eventos inusuales dentro de los sistemas de Smart-DI en comparación con el servicio normal. En caso de detección de tales eventos, se tomarán las medidas adecuadas. Las investigaciones incluyen:

Acceso a la base de datos (acceso y semántica de comandos)

- Índice de errores
- Modificaciones en el rendimiento
- Intentos de conexión
- Actualizaciones críticas del sistema
- Trafico de red

Seguridad y protección de datos

Smart-DI Services garantiza la seguridad, protección y recuperación de los datos del cliente de forma fiable cuando se configura y maneja adecuadamente. Por lo tanto, brinda apoyo al cliente en su cumplimiento con la ley de protección de datos regional.

Seguridad de los datos en el servicio Smartker DMS

Todos los documentos utilizados por los clientes (datos productivos) se almacenan en un centro de datos de Microsoft Azure (ubicación principal US-EAST). Esto se aplica tanto a los documentos en archivos como a los de las bandejas. Además, a fin de salvaguardar todo el inventario de datos productivos para grandes datos, como terremotos o accidentes aéreos, se realizan tres copias de cada documento en un segundo centro de datos ubicado otra región, US-CENTRAL.

Protección de datos

El funcionamiento de los sistemas este sujeto a la ley regional de protección de datos. Los datos de nuestros clientes de la región de América del Norte y América del Sur se alojan en centros de datos ubicados en Estados Unidos. La ubicación principal actual se encuentra en el estado de New York y la alterna en Texas. Los datos de clientes americanos están sujetos a la política de protección de datos de EE. UU.

Copia de seguridad Smartker DMS y CaptureBI

Si el cliente eliminó documentos accidentalmente, es posible restaurarlos en caso necesario. Incluso si los documentos se han modificado incorrectamente, se puede restaurar cualquier borrador anterior. En ambos casos, se aplican las siguientes restricciones.

Para permitir un restablecimiento, tanto las bases de datos como los documentos están respaldados por Smart-DI como copias de seguridad en su propio Cold Storage. Dicho Cold Storage se encuentra en un centro de datos de Microsoft en el estado de Texas (EE. UU.).

Para ello, se realiza y se almacena una copia de seguridad de cada documento. Dicha copia se realiza poco después de que el documento se haya guardado o modificado en Smartker DMS. En el caso de una copia de seguridad tras la modificación del documento, se crea una

nueva copia del documento. Dicha copia se guarda, además de las copias de seguridad existentes del documento. Esto siempre se aplica, tanto con la versión de documentos activada como no activada en Smartker DMS.

Al importar manualmente los datos de la copia de seguridad en el sistema productivo, una organización de Smart-DI Services se puede restaurar completamente en cooperación con nuestro grupo de soporte. Si el cliente requiere datos de la copia de seguridad debido a un manejo inadecuado (por ejemplo, eliminación o modificación accidental de documentos), el cliente se hará cargo de los gastos de soporte en la recuperación.

Además de los documentos, las copias de seguridad completas de las bases de datos de PostgreSQL se llevan a cabo en Cold Storage, principalmente los fines de semana y en horario nocturno en la región.

Copia de seguridad InsightAI360

Para permitir un restablecimiento de las bases de datos y del servicio completo de PrinterBI, cada base de datos de los clientes es respaldada es respaldada de forma diaria y es almacenada en un Datacenter de Microsoft en el Este de US (New York). Adicionalmente se hace una copia de seguridad de la imagen de los servidores de Bases de datos de forma diaria y se almacena en un Datacenter alterno que se encuentra en un centro de datos de Microsoft en el estado de Texas (EE. UU.).

Capacidad y rendimiento

Smart-DI Services Capacidad de ampliación

Tanto Smart-DI como, Azure ID Services, Amazon Web Services, Azure Storage and IONOS Hosting Services ofrecen métodos y tecnologías de capacidad de ampliación extensiva de la infraestructura en caso de ser requeridos y que son utilizados por los servicios de SmartDiServices.

Capacidad de ampliación por cliente

Los servicios ofrecidos son compatibles con todo tipo y tamaño de empresas. Se pueden adaptar de manera flexible en términos de volumen de almacenamiento, capacidad de procesamiento y número de licencias de usuario al tamaño de la empresa en cuestión y al volumen de datos y/o documentos procesados.

Capacidad de ampliación del sistema Smart-DI Services

La plataforma de Smart-DI Services tiene la capacidad de ampliarse automáticamente según la cantidad de usuarios, la cantidad de datos y el tamaño de la carga de procesamiento. Dado que Smart-DI Services es una Public Cloud, la ampliación se realiza por sistema y no por organización del cliente. Actualmente, la configuración mínima de los servidores que se usan para la administración de los diferentes servicios es de mínimo 8 Cores, 64 GB de RAM y Discos Duros SSD/NVMe, sin embargo, se debe de tener en cuenta que la configuración es “elástica” y puede cambiar automáticamente de acuerdo a lo mencionado anteriormente.

Rendimiento y distribución de carga

La distribución de la carga en todos los servicios disponibles garantiza un alto rendimiento constante de todos los servicios disponibles en la plataforma de Smart-DI Services, respondiendo rápida y dinámicamente a condiciones de carga fluctuantes a través de una escala mayor o menor de los servicios existentes o la agregación de servicios completos.

Capacidad de integración

Para maximizar el uso de la administración del control de impresión, la gestión de documentos y la automatización del flujo de trabajo, la plataforma de Smart-DI Services se podría conectar a prácticamente cualquier aplicación empresarial. Esto funciona solamente si dicha aplicación funciona como un sistema basado en la nube y requiere de ser coordinada a través de nuestro grupo de ingenieros de servicios profesionales.

Control y mantenimiento

El centro de datos de IONOS y los servicios de monitore de Microsoft Azure, controlan constantemente todas las operaciones efectuadas dentro de la plataforma de SmartDI. Los incidentes destacados se notifican automáticamente a nuestro grupo de soportepara su valoración y revision. El control incluye:

Controles constantes del rendimiento

Pruebas completas de las funciones básicas de los servicios de Smart-DI

Revisión de patrones de uso de clientes, como el tiempo que acceden a los servicios, el número de usuarios durante el día, la cantidad de acciones que realizan los clientes en una ventana de tiempo determinada (por ejemplo, la búsqueda y archivado de documentos, inicio de sesión) para permitir mejoras de rendimiento.

En el caso de irregularidades, el soporte del sistema de Smart-DI Services interviene inmediatamente con servicio ininterrumpido.

Revisiones y actualización

Al menos 2 veces al año, está planeado el lanzamiento de una nueva versión de los servicios de Smart-DI y esta nueva versión debe de publicarse para ser usada por todos los clientes/organizaciones. Para ello, la organización se desconecta por un tiempo máximo de 8 horas, se realiza la actualización y, a continuación, la organización vuelve a conectarse con la nueva versión de los servicios de Smart-DI.

Smart-DI Group, informa a los clientes sobre la actualización planificada con cuatro semanas de antelación. En caso de error, la organización se volverá a poner en línea con la versión anterior, para evitar periodos de inactividad prolongados.

Los componentes instalados localmente (Desktop Apps como PrinterBI Client, Smartker Connector, Smart-DI Plugins, etc.) siempre deben mantener a los clientes actualizados. Los propios usuarios pueden realizar dichas actualizaciones de forma sencilla, siempre y cuando estén autorizados para instalar software localmente. De lo contrario, el administrador de TI puede realizar la actualización con la ayuda de nuestro grupo de soporte de aplicaciones.

Mantenimiento

Ciertas actividades de mantenimiento requieren derechos de administración completos o avanzados a los sistemas Smart-DI Services. Para garantizar la seguridad de los datos que cumple con las normas de tecnología generalmente aceptadas, el acceso de los administradores de mantenimiento este sujeto a registro y puede ser visualizada y monitoreada por el cliente.

Además, se aplican los siguientes mecanismos de seguridad:

Todos los accesos a los sistemas de Smart-DI Services se realizan a través de una sesión RDP con puertos y usuarios controlados.

Para poder iniciar una sesión RDP, un administrador debe seleccionarla a través de direcciones IP definidas por el Firewall Externo y especialmente protegidas en una VPN que está protegida por certificados y solo esté disponible para los administradores.

Cada administrador de Smart-DI Services cuenta con su propia identificación. Por lo tanto, siempre se puede saber quién ha iniciado sesión en que sistema.

Todos los administradores están capacitados y han recibido formación específica sobre la manipulación y protección de datos, como certificados y contraseñas.

Finalización del contrato

Transferencia de datos al final del contrato

Los datos del cliente son siempre propiedad del cliente. En caso de que un cliente decida rescindir el contrato, Smart-DI le brindara asistencia para descargar toda la información almacenada en las bases de datos o de los documentos de Smartker. Existen dos opciones para esto:

En Smartker, las pequeñas cantidades de documentos pueden exportarse de una manera fácil y rápida usando la funcionalidad de Folder Export, la cual le permitirá almacenar todos los documentos conservando la estructura del gestor de documentos. Esta opción está limitada a un máximo de 30.000 documentos o 10 GB de almacenamiento. En caso de tener cantidades mayores de documentos, se debe de coordinar con nuestro grupo de soporte para realizar el proceso de exportación de manera desatendida.

Los especialistas de Smart-DI Professional Services prestan ayuda en caso de grandes volúmenes de datos y muchos documentos integrados en los procesos actuales. Sus servicios de pago ofrecen las siguientes ventajas:

Tras consultar con el cliente, el acceso a los documentos se realiza directamente en el centro de datos y, por lo tanto, se transfieren grandes cantidades de datos en el menor tiempo posible.

Los documentos dinámicos e integrados en los procesos actuales se migran a los procesos de un nuevo sistema de manera oportuna, minimizando así las interrupciones de los flujos de trabajo.

Se desarrollan soluciones a medida del flujo de trabajo y los tipos de documentos utilizados por los clientes.

PrinterBI. La descarga de las bases de datos de la información almacenada en PrinterBI, se refiere a todos los datos “CRUDOS” (información proveniente de los sistemas externos) extraídos de las herramientas de control de impresión, de MPS, etc. NO SE REFIERE al modelo de bussines intelligence generado con esos datos que es propiedad intelectual de Smart-DI

Tras la recisión del contrato, todos los datos del cliente dentro de los sistemas de Smart-DI Services y todos los datos de las copias de seguridad se eliminarán de manera segura e irrevocable: después de 30 días en la ubicación principal y durante el siguiente trimestre, en Cold Storage. A partir de este momento la re-

cuperación de datos ya no será posible.

Cumplimiento y legalidad

Microsoft y Amazon Web Services, se han destacado en el sector por el establecimiento de requisitos claros de seguridad y privacidad, y por cumplir estos requisitos de forma constante. Ambos cumplen un amplio abanico de normas internacionales y especificas del sector, como el Reglamento General de Protección de Datos (RGPD), ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2.

Auditorias de terceros rigurosas, como las del Instituto Británico de Normalización, confirman que Azure se adhiere a los estrictos controles de seguridad que estos estándares exigen. Mas información sobre las certificaciones de Microsoft Azure.

Contácto de soporte

Juan Sebastián Hernández

+573165123072

juan.hernandez@smart-di.com

+1 226-240-0462 Office Canada

59 Shoreacres Dr. Kitchener, ON N2R 0k7 - Canada

www.smart-di.com