Stambia Privacy Protect

La confiabilidad de los sistemas de TI es un requisito clave de casi cualquier organización. Las fallas inesperadas de los sistemas empresariales pueden resultar costosas y perjudiciales para una organización. Por lo tanto, es vital que los procesos y procedimientos de prueba sean rigurosos y completos.

Lo destacado del Producto

Una parte esencial del proceso de prueba son los datos utilizados durante la ejecución de la prueba. Si bien se crean artificialmente, los datos de prueba pueden ser un punto de partida valioso porque pueden replicar las características únicas e inesperadas de los datos de producción.

Por lo tanto, para evitar fallas inesperadas cuando las aplicaciones se activan, la mayoría de las organizaciones utilizan datos derivados de la producción como parte del proceso de prueba.

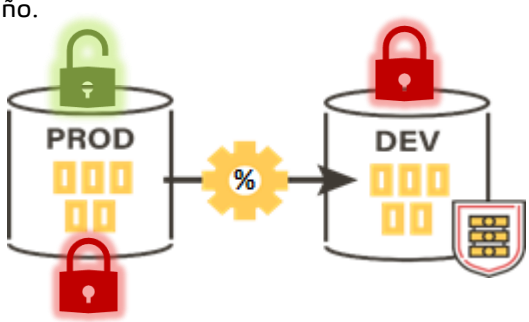
Sin embargo, el uso de datos reales puede plantear desafíos tanto en términos de tamaño de datos como de privacidad.

Tanto para uso interno (en producción) como para subcontratación, los datos deben enmascararse, des identificarse u ofuscarse para proteger la privacidad de los clientes y garantizar que las organizaciones cubran con los requisitos de cumplimiento.

Los datos de producción también pueden ser muy grandes. El uso de terabytes de datos como parte del proceso de prueba puede agregar retrasos y costos significativos tanto en términos de preparación de datos de prueba como de ejecutar el proceso de prueba en sí.

Stambia con "Privacy Protect" es una solución altamente productiva, automatizada y repetible para la creación consistente de datos de prueba seguros y manejables.

Con "Privacy Protect" de Stambia, las organizaciones pueden enmascarar rápidamente los datos de producción de toda la empresa, o solo los sensibles entregando datos no identificables para el proceso de prueba que cumplen con los requisitos de privacidad y están optimizados en tamaño.



Beneficios Clave

Cumplimiento normativo y regulatorio con privacidad de datos de prueba.

La legislación de privacidad de datos y las regulaciones de la industria como LFPDPP, GDPR, PCI, HIPAA, Basel II, Sarbanes Oxley y otras requieren que la información de identidad personal esté protegida.

Si bien los sistemas de producción suelen tener capas de seguridad bien desarrolladas, tanto lógicas como físicas para proteger los datos del uso indebido, un entorno de desarrollo tiene pocas (si las hay) de estas salvaguardas.

"Privacy Protect" proporciona un mecanismo automatizado centralizado para enmascarar las fuentes y destinos de datos empresariales sensibles a la exfiltración.

Crea constantemente datos seguros, no identificables pero realistas, que se pueden usar durante el proceso de desarrollo y prueba, lo que brinda cumplimiento y reduce el riesgo de una violación de datos.

"Privacy Protect" proporciona un entorno de formación esencial y seguro para los usuarios finales, cuando se utilizan datos de producción en vivo para pruebas, entrenamientos, análisis por terceros, etc.

- "Privacy Protect" está alineado con los artículos regulatorios de protección de datos personales y GDPR, fortaleciendo y unificando la protección de datos para los individuos y entidades.
- Visualice y seleccione los datos considerados sensibles y seleccione usando sus metadatos.
- Proporciona opciones múltiples para el enmascaramiento o desidentificación de datos.

Mejora de la productividad de las pruebas y tiempo de comercialización

Proporcionar el entorno de datos de prueba adecuado puede mejorar significativamente el proceso de entrega de aplicaciones y, en consecuencia, la calidad de las aplicaciones comerciales y la agilidad general de las iniciativas de modernización.

Los procesos de prueba engorrosos, manuales o mal integrados agregan tiempo, costo y riesgo significativos a la tarea.

Las pruebas pueden convertirse en un pasivo y no en un activo de TI, y a menudo pueden limitar la flexibilidad general de TI y la alineación comercial. "Privacy Protect" permite a las organizaciones mejorar el proceso de prueba proporcionando datos de prueba de forma rápida y consistente cuando sea necesario y en el formato que se necesite.

Esto ayuda a los desarrolladores, equipos de control de calidad y administradores de bases de datos a trabajar de manera eficiente con datos seguros, completos y compatibles.

Costos reducidos y calidad mejorada

El proceso de prueba es un elemento importante del ciclo de vida del desarrollo.

La disponibilidad de datos apropiados y precisos para las pruebas del sistema, las pruebas unitarias y las pruebas de aceptación es fundamental.

Los procesos manuales para proteger y administrar los datos de las pruebas pueden requerir tiempo y recursos y, al mismo tiempo, generar resultados inconsistentes.

Al proporcionar una solución repetible y automatizada, "Privacy Protect" reduce los recursos necesarios para crear datos de prueba, lo que ahorra tiempo y costos en el ciclo de prueba y brinda una calidad mejorada.

Al proporcionar un enfoque centralizado que comprende las relaciones de datos, "Privacy Protect" puede reducir sustancialmente el tamaño de los datos de prueba, con los volúmenes de datos de prueba típicos , eliminando el riesgo de "falsos positivos" y mejorando la eficiencia.

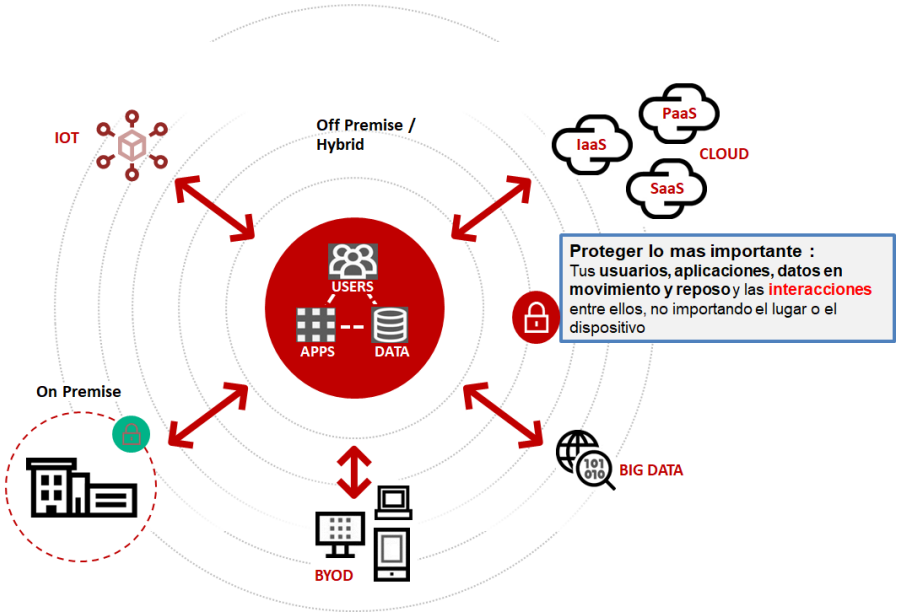


Figura 1. Interacciones de Pruebas Protegidas no importa en donde sucedan

Funciones Clave

La integración de datos permite al componente de "Privacy Protect" aplicar la mejor alternativa para des identificar los datos, para los ambientes de pruebas o cualquier otro que se requiera.

Se puede usar o configurar diccionarios específicos y en idiomas específicos para realizar la sustitución de datos al des identificar los mismos.

Esto se puede lograr desde un solo punto de administración del proceso de integración y transformación de datos hacia las áreas de prueba produciendo una administración única de datos de misión crítica, una versión única desde la cual subconjuntos consistentemente.

Los métodos de desidentificación para proteger los datos pueden ser varios:

- Sustitución por diccionarios:
  - ◊ Suministrado por Stambia y/o
  - ◊ Hechos partiendo de sus datos
- Deducción de los diccionarios proporcionados.
- Generación aleatoria.
- Transformación por expresiones SQL.
- Ofuscación.
- Encriptación.
- Tabla de sustitución por correspondencia temporal.
- Generación de numeración (secuencias)
- Borrado

Una vez construido el método de desidentificación por cada campo no es necesario repetir este proceso incluso puede optar por cambiarlo fácilmente dependiendo de la necesidad de la prueba o negocio.

Si cambian los criterios de enmascaramiento o subconjuntos. La solución permite un mantenimiento sencillo , no necesita mantener o administrar una base de conocimientos o llaves a medida que evolucionan los almacenes de datos.

Interface sencilla y flexible para el enmascaramiento para los datos

El módulo de "Privacy Protect" admite la desidentificación por cada campo definido como sensible. Las reglas y criterios son integrados con los metadatos asociados.

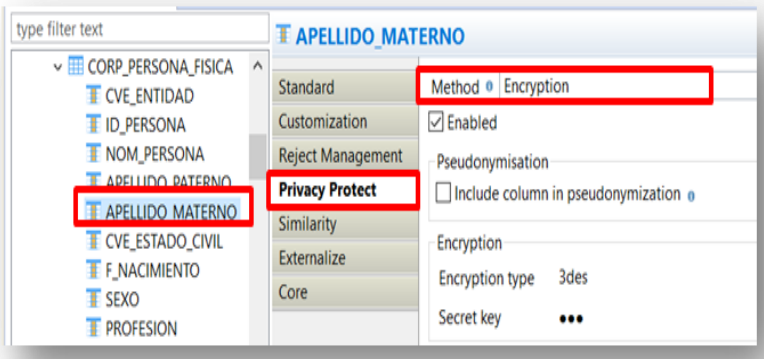


Figura 2. Tipo de Protección por campo especifico

La ejecución va de la mano con el mapeo del proceso que se quiera lograr y da como resultado los datos privados usando el método deseado , solo arrastrando, soltando y configurando.

Stambia "Privacy Protect" facilita la rápida generación de entornos de prueba consistentes y entornos de producción protegidos

Esto elimina aquellos elementos de datos que puedan ser utilizados para obtener conocimientos adicionales sobre temas sensibles de información y hace que sea imposible rastrear información personal.

Para la desidentificación de datos, la solución permite :

- Localizar fácil y rápidamente el inventario datos y sus metadatos que contiene información sensible.
- Cumplimiento de la catalogación de datos personales y sensibles, incluidos en su análisis de Gestión de Datos.
- El enmascaramiento de la identificación personal datos (datos personales, códigos, etc.) hacer que los datos confidenciales sean anónimos en entornos de prueba.
- La creación de datos de prueba no identificados que respeta el enmascaramiento con integridad referencial consistentemente en todos los almacenes de datos para pruebas precisas y significativas
- Cumplimiento con regulaciones Locales y Globales como LFPDPP, ISO 27000, ISO 31000, PCIDSS, GDPR, BASILEA II, MIFID, Sarbanes-Oxley y HIPAA, entre otras..

Las propiedades del proceso de enmascaramiento de datos son:

- Creación y uso de rutinas proporcionadas al personal administrador de datos para adaptar la desidentificación a un requerimiento de negocio y permitirle incorporar procesos de enmascaramiento existentes si es requerido.
- Rutinas de enmascaramiento predefinidas que pueden convertir nombre; apellido; fechas; números telefónicos; formatos regionales como números de RFC en México o SSN de EE. UU.; Italiano, español y Códigos tributarios extranjeros; correos electrónicos; crédito números de tarjetas; números de cuentas bancarias; nombres de empresas, números de IP; y otra códigos de identificación únicos a valores significativos.
- La aplicación del mismo enmascaramiento esquema a diferentes campos con respecto a relaciones clave.
- Rutinas de enmascaramiento portátiles comunes **en múltiples plataformas.**

Estándares de desidentificación avalados por NIST:

- AES128, AES256, AES192,
- AESWrap
- ARCFOUR
- Blowfish
- CCM
- DES, 3DES_2KEY, 3DES
- DESedeWrap
- ECIES
- GCM
- MD5
- SHA1, SHA224, SHA256, SHA384, SHA512
- PBEWith<digest> & <encryption> PBEWith<prf> & <encryption>
- RC2, RC4, RC5
- RSA

Ventajas de "Privacy Protect" en la Protección de Datos.

Proceso de manejo automático de la llave o método de Protección de Datos

⇒ Llave generada automáticamente en el proceso de integración

⇒ Consumir cualquier diccionario de datos

Facilidad de Protección de Datos durante el proceso de Transformación

⇒ Parametrización muy sencilla

⇒ Aplicar reglas de calidad y Protección a la vez.

⇒ No se requiere sincronización con otras herramientas.

Protección de datos sencilla e Invisible para el negocio y clientes

⇒ Nada cambia del lado del cliente o su proceso.

⇒ No existen conflictos con estrategias adicionales.

⇒ Mantenimiento a las reglas de protección en un ambiente gráfico.

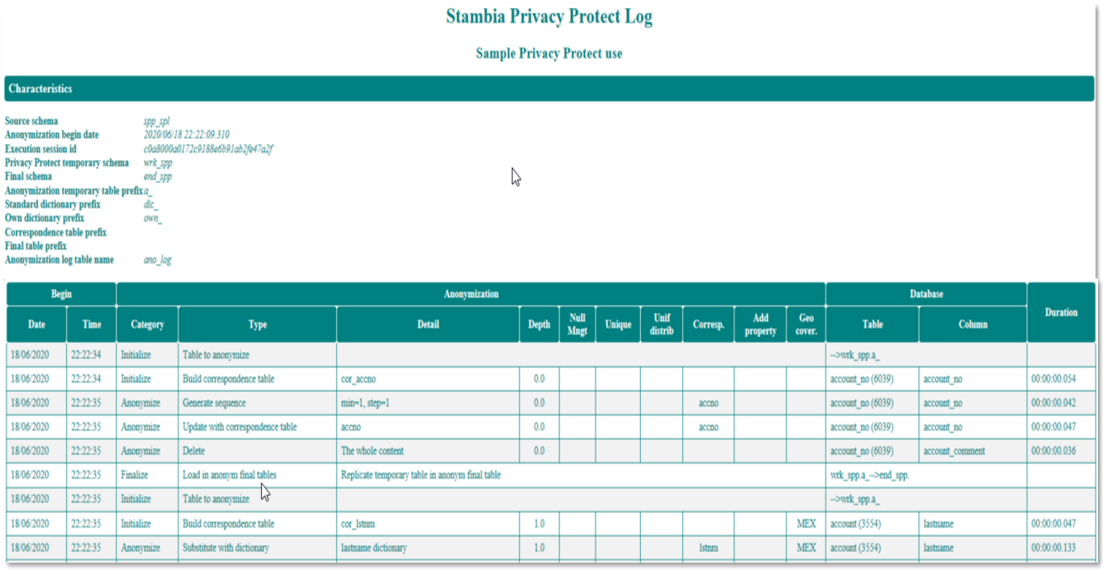
Componentes Integrados al diseño o proceso de Integración de datos.

⇒ Propiedades en una pestaña dedicada.

⇒ Implementación de privacidad por diseño.

⇒ En una categoría totalmente dedicada.

⇒ Listos para arrastrar, soltar y configurar.



Stambia Privacy Protect Log

Sample Privacy Protect use

Characteristics

Source schema	spp_spl
Anonymization begin date	2020/06/18 22:22:09.310
Execution session id	c0a8000a0172c9188e6b91ab2f647a2f
Privacy Protect temporary schema	wrk_spp
Final schema	end_spp
Anonymization temporary table prefix	a_
Standard dictionary prefix	dic_
Own dictionary prefix	own_
Correspondence table prefix	
Final table prefix	
Anonymization log table name	ano_log

Begin		Anonymization									Database		Duration
Date	Time	Category	Type	Detail	Depth	Null Mngt	Unique	Unif distrib	Corresp.	Add property	Geo cover.	Table	Column	
18/06/2020	22:22:34	Initialize	Table to anonymize									-->wrk_spp.a_		
18/06/2020	22:22:34	Initialize	Build correspondence table	cor_accno	0.0							account_no (6039)	account_no	00:00:00.054
18/06/2020	22:22:35	Anonymize	Generate sequence	min=1, step=1	0.0				accno			account_no (6039)	account_no	00:00:00.042
18/06/2020	22:22:35	Anonymize	Update with correspondence table	accno	0.0				accno			account_no (6039)	account_no	00:00:00.047
18/06/2020	22:22:35	Anonymize	Delete	The whole content	0.0							account_no (6039)	account_comment	00:00:00.036
18/06/2020	22:22:35	Finalize	Load in anonym final tables	Replicate temporary table in anonym final table								wrk_spp.a_->end_spp.		
18/06/2020	22:22:35	Initialize	Table to anonymize									-->wrk_spp.a_		
18/06/2020	22:22:35	Initialize	Build correspondence table	cor_lstnm	1.0						MEX	account (3554)	lastname	00:00:00.047
18/06/2020	22:22:35	Anonymize	Substitute with dictionary	lastname dictionary	1.0				lstnm		MEX	account (3554)	lastname	00:00:00.133

Figura 3. Monitoreo y seguimiento por campo protegido

- Capacidades de monitorear los campos protegidos

Una vez construida el método de desidentificación por cada campo no es necesario repetir este proceso incluso puede optar por cambiarlo fácilmente dependiendo de la necesidad de la prueba o negocio.

Si cambian los criterios de enmascaramiento o subconjuntos. el soporte permite un mantenimiento sencillo , no necesita mantener o administrar una base de conocimientos o llaves a medida que crecen los campos des identificados.

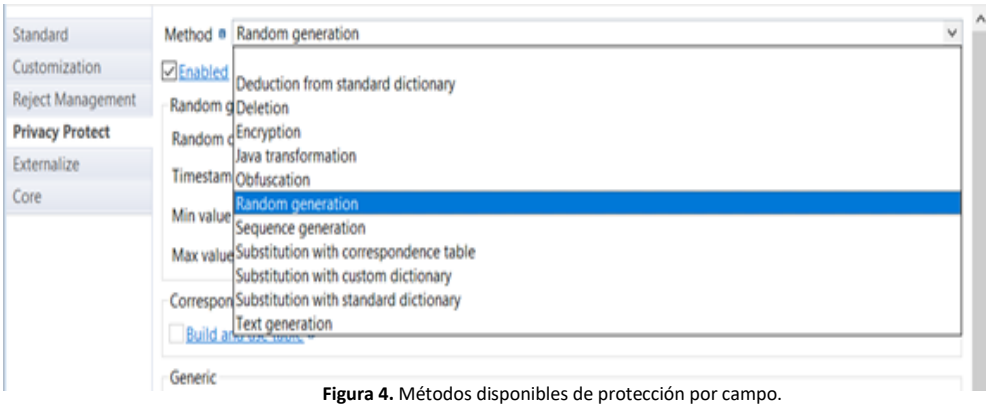


Figura 4. Métodos disponibles de protección por campo.

Buscamos cerrar el superficie de exfiltración de datos.

Podemos asegurar el dato sensible, no importando en donde se encuentre.

De manera local, en la nube o una combinación en un esquema híbrido.

La arquitectura para el escenario de protección descansa en tres componentes básicos:

1. El Diseñador
2. El Runtime
3. El Analytics

Ya que Stambia ejecuta la integración, transformación y anonimización del dato directamente de las fuentes de información desde el origen al destino, sin añadir un motor propietario o servidor dedicado.

Utiliza estructuras de modelos de procesos preensamblados llamados "**templates**" que generan el código de la integración en automático. Es por ello que logra integrarse a tecnologías, anteriores y actuales sin ningún problema.

Todo esto es realizado mediante una interfaz gráfica simple, liviana usando componentes como: Metadatos, Mapas y Procesos.

La inteligencia de la solución se encuentra en el componente del "Diseñador" quien el que crea la lógica y crea los procesos de integración y/o transformación de datos anonimizando su contenido por lo que la solución no requiere instalar "agentes" para funcionar su capacidad de conexión y extracción de metadatos la hace única.

El componente de Runtime parte de una estrategia descentralizada y se puede instalar para cualquier ambiente o sistema operativo.

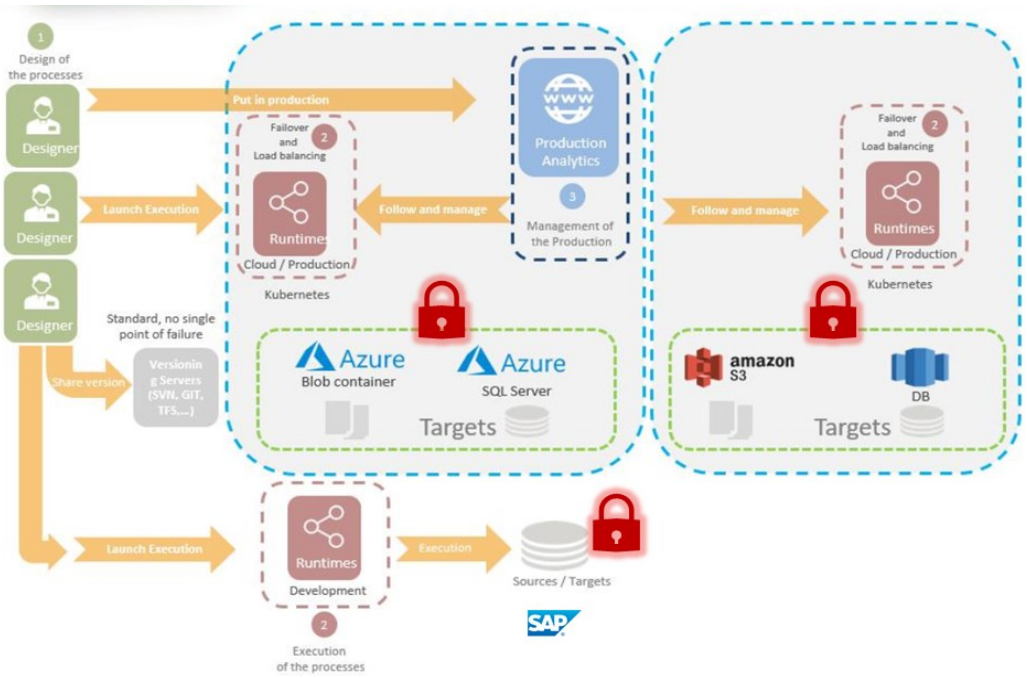


Figura 5. Arquitectura en un ambiente híbrido

El módulo de Analytics es la "torre de control" para que operaciones pueda monitorear las integraciones, transformaciones y anonimización de datos.

En términos prácticos solo requerimos conocer el a,b,c :

a. La fuente de información
b. El método de anonimización o des identificación de datos deseado— aquí usaremos el "template" y
c. El destino en donde depositaremos los datos.

La solución Stambia es una solución desarrollada en tecnología Java/ Eclipse, beneficiándose así de la robustez y potencia que Eclipse ha demostrado desde hace más de quince años en el mercado tecnológico.

Puede operar en cualquier plataforma que soporte Java : Windows, Linux, MAC..

La propuesta de valor de Stambia reposa, sobre un modelo arquitectural distribuido en el cual los Metadatos no son almacenados en un repositorio centralizado sino en archivos XML.

Cada componente de la solución es totalmente autónomo evitando así tener un punto central de falla.

Stambia es el nombre de la solución de nueva generación de Integración de Datos tipo ELT desarrollada por Stambia SAS, empresa de software francesa basada en la ciudad de Villeurbanne (Lyon) Francia. Stambia con fuerte crecimiento a nivel internacional.

Su tecnología es utilizada por mas de 200 clientes.

Cuenta actualmente con cinco oficinas regionales y con inversiones fuertes para los equipos de soporte y de investigación y desarrollo .

El soporte técnico está organizado a nivel internacional en tres sedes: Europa, Asia y América Latina con base en México.

Conoce mas en:

https://www.stambia.com/es/

Figura 6. Ejemplo de como luce gráficamente el "template".