UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"ENMASCARAMIENTO EN LA BASE DE DATOS ORACLE PARA RESGUARDAR LA INFORMACIÓN FINANCIERA Y PERSONAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI"

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Ingeniero en Sistemas Computacionales e Informáticos

LÍNEA DE INVESTIGACIÓN: Seguridad de Unidades Informáticas.

AUTOR: Diego Marcelo Coronel Montoya
TUTOR: Ing. Franklin Mayorga, Mg.

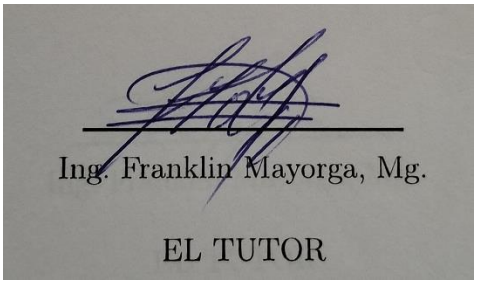
Ambato - Ecuador
2018

CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"ENMASCARAMIENTO EN LA BASE DE DATOS ORACLE PARA RESGUARDAR LA INFORMACIÓN FINANCIERA Y PERSONAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI", de la señor, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad técnica de Ambato

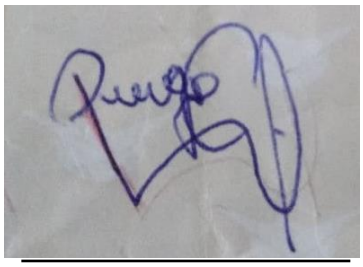
Ambato, Junio de 2018



AUTORÍA DEL TRABAJO

El presente trabajo de investigación titulado: "ENMASCARAMIENTO EN LA BASE DE DATOS ORACLE PARA RESGUARDAR LA INFORMACIÓN FINANCIERA Y PERSONAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Junio de 2018



Diego Marcelo Coronel Montoya

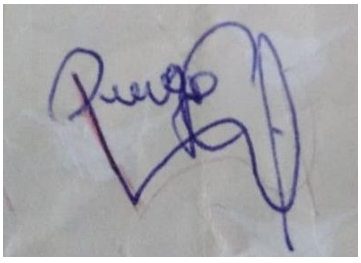
CC: 0503338097

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigacion.

Cedo los derechos de mi trabajo de titulación, con fines de difusión pública además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, Junio de 2018

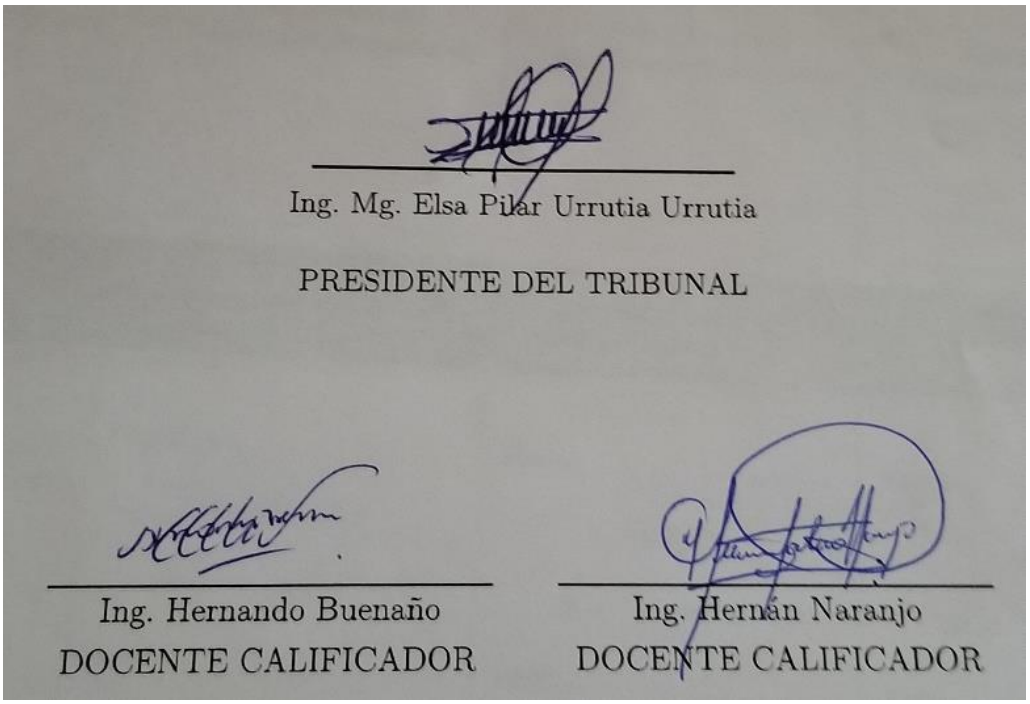


Diego Marcelo Coronel Montoya

CC: 0503338097

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Hernando Buenaño e Ing. Hernán Naranjo, revisó y aprobó el Informe Final del trabajo de graduación titulado "ENMASCARAMIENTO EN LA BASE DE DATOS ORACLE PARA RESGUARDAR LA INFORMACIÓN FINANCIERA Y PERSONAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI", presentado por el Señor Marcelo Coronel de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.



DEDICATORIA

Este proyecto va dedicado a mi madre la persona con mayor fuerza de espíritu que siempre me brindo su apoyo para culminar la carrera universitaria.

Diego Marcelo Coronel Montoya

AGRADECIMIENTO

A la FISEI por abrirme sus puertas y a los docentes que compartieron sus conocimientos, y un muy sincero agradecimiento al Ing. Franklin Mayorga por su guía y apoyo en este proceso.

A la Cooperativa de Ahorro y Crédito CACPECO por permitirme realizar mi trabajo de titulación, al Ing. Fausto Cerda por su buena disposición con su tutoría.

Diego Marcelo Coronel Montoya

ÍNDICE

APROBACIÓN DEL TUTOR ii

AUTORÍA iii

APROBACIÓN COMISIÓN CALIFICADORA v

Dedicatoria vi

Agradecimiento vii

Introducción xviii

CAPÍTULO 1 El problema 1

1.1 Tema de Investigación 1
1.2 Planteamiento del problema 1
1.3 Delimitación 2
1.3.1 Delimitación de Contenido 2
1.3.2 Delimitación Espacial 2
1.3.3 Delimitación Temporal 2
1.4 Justificación 2
1.5 Objetivos 3
1.5.1 General 3
1.5.2 Específicos 3

CAPÍTULO 2 Marco Teórico 4

2.1 Antecendentes Investigativos 4
2.2 Fundamentación teórica 4
2.2.1 Bases de Datos 4
2.2.2 Tipos de bases de Datos 5
2.2.2.1 Bases de datos estáticas 5
2.2.2.2 Bases de datos dinámicas 5
2.2.3 Datos sensibles 5

2.2.4 Entorno de desarrollo 5
2.2.5 Data masking o enmascaramiento de Datos 5
2.2.6 La información 6
2.2.7 Información Personal 6
2.2.8 Información Financiera 6
2.2.9 Seguridad Informática 6
2.3 Propuesta de Solución 6

CAPÍTULO 3 Metodología **8**
3.1 Modalidad Básica de la investigación 8
3.1.1 Modalidad Bibliográfica o Documental 8
3.1.2 Modalidad de Campo 8
3.1.3 Modalidad Aplicada 8
3.2 Población y muestra 8
3.3 Recolección de información 8
3.4 Procesamiento y análisis de datos 8
3.5 Desarrollo del Proyecto 9

CAPÍTULO 4 Desarrollo de la propuesta **10**
4.1 Datos Informativos 10
4.1.1 Titulo 10
4.1.2 Institución ejecutora 10
4.1.3 Beneficiarios 10
4.1.4 Ubicación 10
4.1.5 Tiempo estimado para la ejecución 10
4.1.6 Equipo técnico responsable 10
4.2 Antecedentes 11
4.3 Justificación 11
4.4 Análisis de Factibilidad 11
4.4.1 Política 11
4.4.2 Tecnología 12
4.4.3 Organizacional 12
4.4.4 Equidad de Género 12
4.4.5 Ambiental 12
4.4.6 Económico – Financiera 12
4.4.7 Socio – Cultural 12
4.4.8 Legal 12
4.5 Enmascaramiento de Datos 13

4.5.1 Identificación de los datos sensibles y sus tablas 13
4.5.1.1 Datos Personales 13
4.5.1.2 Datos Financieros 14
4.5.2 Identificar las bases de datos que posee CACPECO y las personas que tienen acceso 18
4.5.2.1 Base de Datos Origen. 18
4.5.2.2 Base de Datos Capacitación. 18
4.5.2.3 Base de Datos Desarrollo. 18
4.5.2.4 Base de Datos Producción. 18
4.5.3 Enumerar los riesgos al tener expuestos los datos de entornos no productivos de la base de datos de la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi 18
4.5.4 Análisis de las opciones disponibles en el mercado para enmascaramiento de datos 19
4.5.4.1 POWERDATA. 19
4.5.4.2 REDPARTNER. 20
4.5.4.3 Proyectos Compartidos Ltda. 20
4.5.4.4 SinergyHard 20
4.5.5 Comparativa de las soluciones de enmascaramiento existentes en el mercado 21
4.5.5.1 Escabilidad 21
4.5.5.2 Reducción de Información 21
4.5.5.3 Experiencia en la Banca 21
4.5.5.4 Reglas Básicas de Enmascaramiento 22
4.5.6 Determinar una solución de enmascaramiento de datos adecuada para la cooperativa 23
4.5.7 Configurar la solucion de enmascaramiento de la base de datos Oracle 23
4.5.7.1 Requisitos de IBM InfoSphere Optim 23
4.5.7.2 Configuración de IBM InfoSphere Optim 24
4.5.7.3 Creación de la definición de acceso 26
4.5.7.4 Creación del Servicio de Extracción 29
4.5.7.5 Mapeo de Columnas 32
4.5.7.6 Reglas de ofuscación 35
4.5.7.7 Configuracion de las reglas de enmascaramiento . 35
4.5.7.8 Configuracion de la regla Mezcla o Shuffle 35

4.5.7.9 Aleatorios con máscara 35
4.5.7.10 Uso de Diccionarios 35
4.5.7.11 Configuracion de la regla Mezcla o Shuffle 36
4.5.7.12 Creación del Servicio de Conversión 37
4.5.7.13 Ejecutar el Servicio de Conversión 38
4.5.7.14 Creación del Servicio de Inserción 39
4.5.7.15 Ejecutar del Servicio de Inserción 40
4.5.8 Comparativa de los datos enmascarados 41
4.5.8.1 Datos Personales y Financieros enmascarados 41

CAPÍTULO 5 Conclusiones y Recomendaciones **44**

Bibliografia **45**

ANEXOS **48**

ÍNDICE DE TABLAS

1 Campos sensibles en FBS_PERSONAS.
Elaborado por el investigador 14
2 Campos sensibles en FBS_CAPTACIONESVISTA.
Elaborado por el investigador 15
3 Campos sensibles en FBS_CAPTACIONESPLAZO.
Elaborado por el investigador 16
4 Campos sensibles en FBS_CARTERA.
Elaborado por el investigador 17
5 Comparativa en ESCALABILIDAD.
Elaborado por el investigador 21
6 Comparativa en REDUCCIÓN DE INFORMACIÓN.
Elaborado por el investigador 21
7 Comparativa en EXPERIENCIA EN LA BANCA.
Elaborado por el investigador 22
8 Comparativa en REGLAS BÁSICAS DE ENMASCARAMIENTO.
Elaborado por el investigador 22

ÍNDICE DE FIGURAS

1 Diagrama Entidad Relación de FBS_PERSONAS.
Elaborado por el investigador. 13
2 Diagrama Entidad Relación de FBS_CAPTACIONESVISTA.
Elaborado por el investigador 15
3 Diagrama Entidad Relación de FBS_CAPTACIONESPLAZO.
Elaborado por el investigador 16
4 Diagrama Entidad Relación de FBS_CARTERA.
Elaborado por el investigador 17
5 Características óptimas del equipo.
Elaborado por el investigador 23
6 Creación del Alias de la Base de Datos.
Elaborado por el investigador 24
7 Configuración de los accesos de conexión.
Elaborado por el investigador 24
8 Configuración host.
Elaborado por el investigador 25
9 Selección del set de caracteres.
Elaborado por el investigador 25
10 Nueva definición de acceso.
Elaborado por el investigador 26
11 Datos de la definición de acceso.
Elaborado por el investigador 26
12 Selección del alias de la base de datos.
Elaborado por el investigador 27
13 Selección de la tabla maestro para la extracción.
Elaborado por el investigador 28
14 Método de extracción de tablas.
Elaborado por el investigador 29
15 Access Definition Editor.
Elaborado por el investigador 29

16 Creación del Servicio de Extracción.
Elaborado por el investigador 30
17 Servicio de extracción.
Elaborado por el investigador 30
18 Selección de acceso.
Elaborado por el investigador 31
19 Editor del servicio de extracción de Datos.
Elaborado por el investigador 31
20 Nuevo mapeo de Columnas.
Elaborado por el investigador 32
21 Datos del mapeo de Columnas.
Elaborado por el investigador 32
22 Seleccionar archivo de extracción.
Elaborado por el investigador 33
23 Selección tabla destino.
Elaborado por el investigador 34
24 Agregar políticas de enmascaramiento.
Elaborado por el investigador 34
25 Asistentente para aplicar la regla shuffle.
Elaborado por el investigador 35
26 Uso de diccionarios para enmascarar.
Elaborado por el investigador 36
27 Asistentente para aplicar la regla shuffle.
Elaborado por el investigador 37
28 Creación Servicio de conversión.
Elaborado por el investigador 37
29 Datos del servicio de conversión.
Elaborado por el investigador 38
30 Servicio de conversión.
Elaborado por el investigador 38
31 Ejecución servicio de conversión.
Elaborado por el investigador 39
32 Datos del servicio de Inserción.
Elaborado por el investigador 39
33 Selección del archivo convertido.
Elaborado por el investigador 40

34 Ejecución del servicio de Inserción.
Elaborado por el investigador 40
35 Datos de le ejecución del servicio.
Elaborado por el investigador 40
36 Monitor del servicio.
Elaborado por el investigador 41
37 Información enmascarada Financial.
Elaborado por el investigador 41
38 Información real Financial.
Elaborado por el investigador 42
39 Información enmascarada.
Elaborado por el investigador 42
40 Información real.
Elaborado por el investigador 43

RESUMEN

Las organizaciones financieras por la naturaleza y giro de negocio, deben mantener la integridad y seguridad de la información. Manejarla de manera adecuada, correcta y segura debe ser una tarea estratégica del negocio, y alinear los recursos a través de la mejora de estos aspectos.

Las actividades clave incluyen el manejo de un sistema especializado de administración y enmascaramiento de datos, con lo que se asegura el cumplimiento frente a las entidades reguladoras del Gobierno, y sobre todo la confidencialidad de los datos sensibles de manera interna y externa, protegiendo la información del negocio contra cualquier tipo de filtración de información intencionada o no del activo más importante del negocio: LOS DATOS.

En el mercado actual existen varias herramientas que ayudan a ofuscar los datos por eso importante analizarlas y conocer las reglas de enmascaramiento que ayudaran a mantener segura toda la información de los entornos no productivos.

Por eso el presente trabajo tiene como finalidad ayudar a mejorar la seguridad en los entornos no productivos dando a conocer soluciones de enmascaramiento que existen en el mercado, los métodos que existen para enmascarar y como una base ofuscada evita que se pierda información relevante de la empresa.

Descriptores: Integridad, Seguridad de la Información, Enmascaramiento de Datos, Entidades Reguladoras, Confidencialidad, Filtración, Dato, Entornos no Productivos.

ABSTRACT

Financial organizations by nature and business, must maintain the integrity and security of information, handle it adequate, correctly and safely must be a strategic business task, and align resources through the improvement of these aspects.

The key activities include the management of a specialized system of administration and masking of data, which ensures compliance of laws the government regulatory entities, and above all the confidentiality of sensitive data internally and externally, protecting the information of the business against any type of leak of intentional information or not of the most important asset of the business: THE DATA.

In the current market there are several tools that help obfuscate the data, which is why it is important to analyze them and know the masking rules that will help to keep all the information in non-productive environments safe.

The present work has the purpose of of helping to improve security in non-productive environments presenting masking solutions that exist in the market, the methods that exist to mask and as an obfuscated base, it avoids losing relevant information about the company.

Descriptors: Integrity, Information Security, Data Masking, Regulatory Entities, Confidentiality, Filtration, Data, Non-Productive Environments.

INTRODUCCIÓN

El presente Trabajo de Investigación tiene como tema: "Enmascaramiento en la Base de Datos Oracle para Resguardar la Información Financiera y Personal en La Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi".

A continuación se detalla la estructura del trabajo por sus capítulos:

El CAPÍTULO I, denominado El Problema, contiene el planteamiento del problema, la delimitación del objeto de investigación, la justificación, el objetivo general y los objetivos específicos que se buscarán cumplir en la investigación.

El CAPÍTULO II llamado Marco Teórico, está conformado por los antecedentes investigativos, fundamentación teórica y la propuesta de solución.

El CAPÍTULO III, Metodología, contiene la modalidad básica de la investigación, la población y muestra, las técnicas e instrumentos de recolección de la información, el plan de procesamiento y análisis de datos y el proceso a seguir en el desarrollo del proyecto.

El CAPÍTULO IV corresponde al desarrollo de la propuesta, que se divide en datos informativos, antecedentes,justificacion, análisis de factibilidad y el enmascaramiento de datos

En el CAPÍTULO V se incluyen las Conclusiones y Recomendaciones de la investigación.

Finalmente se documenta la Bibliografía y se adjuntan los Anexos.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

"Enmascaramiento en la base de datos Oracle para resguardar la información financiera y personal en la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi"

1.2. Planteamiento del problema

Anteriormente la seguridad de la información se realizaba a través de medios físicos, como una caja fuerte, en la cual se resguardaban objetos o información valiosa. Con la introducción de las computadoras, y el uso de internet, las empresas y usuarios, en general, almacenan la información en medios electrónicos. Los datos corren el riesgo de perder su confidencialidad y es necesario protegerla, en entornos productivos como no productivos en este punto es donde se hace presente el uso de la encriptación, la misma que dificulta el robo de información mientras es transmitida por algún medio, pero no impide el abuso de la misma o que sea susceptible de filtraciones.
Es por ello que es necesario buscar maneras eficientes de proteger los datos y evitar filtraciones de información confidencial. A nivel mundial en el paso de la historia se han creado varias leyes que ayudan a este cometido comenzando con el artículo 12 de la declaración universal de derechos humanos en que señala que todas las personas tienen derecho a la protección de sus datos personales[1], Alemania la ley federal de protección de Datos,¿ impide la transmisión de cualquier datos personal sin la autorización de la persona interesada [2], en Estados Unidos se creó la Ley de Privacidad de 1974 en la cual prohíbe la publicación no autorizada de registros personales [3].

En Ecuador la Superintendencia de Economía Popular y Solidaria a evidenciado la necesidad de salvaguardar la información razón por la cual fue agregado el literal 4.3.8.16 en la RESOLUCIÓN JB-2012-2148, del 26 de abril del 2012 en la cual se dispuso que las instituciones del sistema financiero implementen suficientes medidas de seguridad para aplacar el riesgo de fraude mediante el uso

de información y comunicaciones, solicitando que enmascaren las bases de datos en entornos de desarrollo y pruebas[Anexo 1]. La Cooperativa de Ahorro y Credito de la Pequeña Empresa de Cotopaxi analizando la importancia de mantener seguros los datos de los clientes y dar cumplimiento a la resolución JB-2012-2148, comenzará con un proyecto de enmascaramiento de datos en la agencia de la ciudad de Latacunga, con el que se busca ofuscar los datos sensibles de sus socios con el debido enmascaramiento en las bases de datos de pruebas y desarrollo, la finalidad es evitar la vulnerabilidad de los entornos no productivos dando mayor seguridad a la cooperativa y sus usuarios, evitando fugas de información.

1.3. Delimitación

1.3.1. Delimitación de Contenido

Área Académica: Administrativas Informáticas.

Líneas de Investigación: Normas y estándares.

Sublínea de Investigación: Seguridad de Unidades Informáticas.

1.3.2. Delimitación Espacial

La presente investigación se realizará en la empresa "La Cooperativa de Ahorro Y Crédito de la Pequeña Empresa de Cotopaxi ".

1.3.3. Delimitación Temporal

El desarrollo del proyecto se realiza en el semestre académico Octubre 2017-Febrero 2018

1.4. Justificación

La información financiera de la institución es uno de los principales activos, por ese motivo la investigación de este tema tiene un gran interés para la cooperativa de ahorro y crédito ya que permite cumplir con una parte de la RESOLUCIÓN JB-2012-2148, la cual solicita que los entornos de desarrollo mantengan enmascarados sus datos[Anexo1].

Al tener la base de datos enmascarada ayudará a gestionar de una manera eficiente la información sensible como números de cuentas, saldos y datos personales, protegerla de posibles robos o filtraciones sin perder la consistencia de los datos

para poder usarlos en un entorno no productivo.

Esta implementación es factible ya que se cuenta con el apoyo del área de seguridades de la Cooperativa de Ahorro y Creditos de la Pequeña Empresa de Cotopaxi. Adicionalmente se cuenta con los conocimientos de la estructura de la base de datos para poder identificar la informacion sensible. Los principales beneficiarios de la investigación son los socios de la cooperativa ya que existirá mayor seguridad en la información financiera y personal lo cual genera confianza en la ciudadanía permitiendo captar más socios.

1.5. Objetivos

1.5.1. General

- Implementar un sistema de Enmascaramiento en la base de datos Oracle para resguardar la información financiera y personal en la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi

1.5.2. Específicos

- Analizar los datos sensibles expuestos a los entornos no productivos de la base de datos de la Cooperativa de Ahorro y Credito de la Pequeña Empresa de Cotopaxi.
- Determinar la mejor propuesta de solución para el enmascaramiento de datos para la cooperativa.
- Configurar las reglas de ofuscación necesarias para la implementación de la solución del enmascaramiento de la base de datos Oracle.
- Implementar el Enmascaramiento en la base de datos Oracle

CAPÍTULO 2

Marco Teórico

2.1. Antecendentes Investigativos

A Net 2000 Ltd. White Paper menciona su definición " El enmascaramiento de datos consiste en el reemplazo de información existente en bases de datos de prueba o desarrollo con información que parezca real y que no sea útil a nadie que podria usarla mal. En general, los usuarios de las bases de datos de prueba, desarrollo o capacitación no necesitan ver la información real, siempre y cuando lo que vean parezca real y sea consistente." [4].

Rajesh Ravichandran en su investigación afirma " El enmascaramiento de datos es el proceso de reemplazar la información sensible en las bases de datos de prueba o de desarrollo con información realista pero no real. Las técnicas de enmascaramiento de datos no afectarán a los datos específicos de una base de datos, sino que se mantendrá la seguridad de los datos. El enmascaramiento de datos ha excluido las aplicaciones y los ambientes para mantener la integridad del negocio"[5].

Waleed Ahmed, JaganAthreya menciona porque usar enmascaramiento de datos: Muchas empresas para seguir siendo competitivas requieren nuevas aplicaciones y mejorar las existentes en produccion y para lograrlo es entregan a los desarrolladores ambientes identicos a produccion, incluidos copias de las bases de datos, como resultado la informacion sensible de las organizaciones es expuesta a posbles robos[6].

2.2. Fundamentación teórica

2.2.1. Bases de Datos

Son un conjunto de datos dispuestos que tiene como objetivo almacenar y proporcionar información a los usuarios[7], entre las principales ventajas esta la disminución de redundancia porque no es necesario repetir los datos, integridad al existir mayor dificultad de perder información y que exista incoherencia en los datos[8].

2.2.2. Tipos de bases de Datos

2.2.2.1. Bases de datos estáticas

Son bases de datos solo de lectura usadas principalmente para almacenar datos históricos que posteriormente se pueden utilizar para estudiar el comportamiento un conjunto de datos a traves del tiempo[9].

2.2.2.2. Bases de datos dinámicas

La información almacenada en estas base de datos es para ser modificada constantemente permitiendo operaciones como la actualización , borrado e insercion de datos[9].

2.2.3. Datos sensibles

Es el nombre que recibe la información personal privada de un individuo, el origen racial, las opiniones politicas, filosoficas, religiosas, la afiliacion sindical, la vida sexual,estado de salud y situacion patrimonial y financiera [10].

2.2.4. Entorno de desarrollo

Es un entorno diseñado para cumplir varias tareas como codificación, pruebas y mantenimiento de software.[11]

2.2.5. Data masking o enmascaramiento de Datos

El enmascaramiento de datos es el método de despersonalización, depuracion o camuflaje de los datos para que la informacion personal sea cambiada o eliminada, proporcionando una base de datos realista y utilizable sin la necesidad de una violacion a la privacidad de las empresas.

.

Los datos mantienen las mismas caracteristicas que son importantes para mantener un realismo en la información y garantiza la usabilidad en los entornos de pruebas y capacitación, el proceso a diferencia de la encripacion es irreversible.

La usabilidad de los datos es el factor clave y la principal diferencia entre encriptación y enmascaramiento de datos, los datos cifrados están protegidos contra una violación de la privacidad siempre que esté en reposo, pero para poder manipularlo deben estar sin encriptar, exponiendo así los datos a una violación a la privacidad. Comparado, los datos enmascarados mantienen su

comportamiento y usabilidad completos, pero no exponer información personal específica a empleados y contratistas que no deberías tener acceso a los datos reales[12].

2.2.6. La información

Es el resultado de procesar datos sin elaborar para dejar ver su significado[13].O un conjunto de datos estructurados que tienen como objetivo dar una idea.[7]

2.2.7. Información Personal

Es cualquier dato que puede ser usado para identificar a un individuo especifico[14]

2.2.8. Información Financiera

Es derivada del uso y manejo de los recursos financieros de una institución o una persona, esta información produce una contabilidad. Es procesada y concentrada para el uso de la misma.

La importancia de la información financiera que será presentada a los usuarios sirve para que formulen sus conclusiones sob re el desempeño financiero de la entidad. Por medio de esta información y otros elementos de juicio el usuario general podrá evaluar el futuro de la empresa y tomar decisiones de carácter económico sobre la misma[15].

2.2.9. Seguridad Informática

La seguridad informática es la diciplina que con base en políticas y normas internas y externas de una empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que esta expuesta. [16]

2.3. Propuesta de Solución

Mediante el análisis sistemático de los datos de los socios de la institución financiera se estudiará las zonas sensibles de la base de datos para iniciar con el tratamiento de estos, mediante el enmascaramiento y luego de exhaustivas pruebas se procederá a implementar la solución en una de base paralela a la

original probando los puntos fuertes y débiles de la misma y que sus datos no sean vulnerables. Se realizara el documento donde se encuentren detallados los pasos a seguir para enmascarar los datos y se implementará la solución completamente en la base realizando las respectivas pruebas.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la investigación

3.1.1. Modalidad Bibliográfica o Documental

Esta modalidad fue considerada ya que se apoyo en diferentes fuentes que de información como libros, artículos que nos ayudaron para tener un mejor enfoque.

3.1.2. Modalidad de Campo

Se empleo la investigación de campo, pues se acudio a la fuente para evaluar los procesos adicionalmente se realizo un estudio técnico y se verifico las herramientas que son necesarias para cumplir los objetivos propuestos.

3.1.3. Modalidad Aplicada

Se utilizo la investigación aplicada pues se procedio a seguir los pasos necesarios para poder aplicar correctamente la metodología que se escogerá para este proyecto.

3.2. Población y muestra

La presente investigación por su característica, no amerita definir una muestra.

3.3. Recolección de información

Para la recolección de la información se aplico entrevistas al personal a cargo del Departamento de Informática y seguridades de CACPECO. Ademas, se revisó el diagrama entidad relación de la base de datos para obtener la ubicación de la información.

3.4. Procesamiento y análisis de datos

Para el enmascaramiento de datos se realizo las siguientes actividades:

- Identificar las herramientas existentes para data masking en el mercado actual.
- Detallar que datos son sensibles y vulnerables de la base de datos Oracle de CACPECO.
- Analizar los accesos que se tiene a los entornos no productivos.
- Establecer las reglas que pueden usarse al enmascarar datos.

3.5. Desarrollo del Proyecto

Para el desarrollo de proyecto se realizará las siguientes actividades:

1. Identificación de los datos sensibles y sus tablas.
2. Identificar las bases de datos que posee CACPECO y las personas que tienen acceso.
3. Enumerar los riesgos al tener expuestos los datos de entornos no productivos de la base de datos de la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi.
4. Análisis de las opciones disponibles en el mercado para enmascaramiento de datos.
5. Comparativa de las soluciones de enmascaramiento existentes en el mercado
6. Determinar una solución de enmascaramiento de datos adecuada para la cooperativa.
7. Configurar la solucion de enmascaramiento de la base de datos Oracle.
8. Comparativa de los datos enmascarados.

CAPÍTULO 4

Desarrollo de la propuesta

4.1. Datos Informativos

4.1.1. Titulo

"ENMASCARAMIENTO EN LA BASE DE DATOS ORACLE PARA RESGUARDAR LA INFORMACIÓN FINANCIERA Y PERSONAL EN LA COOPERATIVA DE AHORRO Y CRÉDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI"

4.1.2. Institución ejecutora

Facultad de Ingeniería En Sistemas, Electrónica e Industrial
Diego Marcelo Coronel (Investigador)

4.1.3. Beneficiarios

Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi

4.1.4. Ubicación

Ecuador

Latacunga: Calle Fernando Sánchez de Orellana.

4.1.5. Tiempo estimado para la ejecución

El tiempo estimado para la ejecución es de seis meses, desde el análisis de situación actual, hasta la búsqueda de salvaguardas adecuadas que nos permitan el cumplimiento de nuestro objetivo.

4.1.6. Equipo técnico responsable

Ing. Franklin Mayorga, Mg. (Tutor)
Diego Marcelo Coronel (Investigador)
Ing. Fausto Cerda. (Jefe de Sistemas y Comunicaciones en CACPECO)

4.2. Antecedentes

Actualmente la cooperativa posee tres bases de datos usadas en el ambiente de producción, desarrollo y capacitación, los ambientes no productivos poseen una copia identica de la base de datos de produccion, y cuando se contrata a proveedores externos son enviados datos reales de los socios.

4.3. Justificación

La información financiera de la institución es uno de los principales activos, por ese motivo la investigación de este tema tiene un gran interés para la cooperativa de ahorro y crédito ya que permite cumplir con una parte de la RESOLUCIÓN JB-2012-2148, la cual solicita que los entornos de desarrollo mantengan enmascarados sus datos Anexo1.

Al tener la base de datos de entornos no productivos ofuscados ayudará a gestionar de una manera eficiente la información sensible como números de cuentas, saldos y datos personales, protegerla de posibles robos o filtraciones sin perder la consistencia de los datos para poder usarlos en un entorno no productivo.

Esta implementación es factible ya que se cuenta con el apoyo del área de seguridades de la Cooperativa de Ahorro y Créditos de la pequeña Empresa de Cotopaxi, adicionalmente se cuenta con los conocimientos de la estructura de la base de datos para poder identificar los datos sensibles. Los principales beneficiarios de la investigación son los socios de la cooperativa ya que existirá mayor seguridad en la información financiera y personal lo cual genera confianza en la ciudadanía permitiendo captar más socios.

4.4. Análisis de Factibilidad

4.4.1. Política

A nivel de Política existe la RESOLUCIÓN JB-2012-2148 en el punto 4.3.8.16 que solicita que la información contenida en ambientes de desarrollo y pruebas, debe ser enmascarada o codificada, por ese motivo la Cooperativa de Ahorro y Crédito CACPECO Ltda. para evitar el uso indebido de la información y cumplir todas las normativas que solicita el Gobierno se autoriza la elaboración de este trabajo.

4.4.2. Tecnología

La tecnología, es la base principal para elaborar este proyecto, ya que su uso y análisis permite elaborar las rutinas de enmascaramientos que son necesarias para elaborar el proyecto.

4.4.3. Organizacional

La Cooperativa de Ahorro y Crédito contara con la seguridad y procedimientos adecuados para que los entornos no productivos sean usados por los desarrolladores sin riesgo de fuga de información o uso indebido de los datos.

4.4.4. Equidad de Género

Se involucra a todos los géneros, ya que su utilidad no distingue ni hace diferencia entre hombres y mujeres, encontrándose al alcance de todos.

4.4.5. Ambiental

El desarrollo de este proyecto no afectará al medio ambiente, sino más bien minimizará su impacto en la organización, sin alterarlo.

4.4.6. Económico – Financiera

La Cooperativa de Ahorro y Crédito CACPECO Ltda. cuenta con un presupuesto económico para adquirir el software de enmascaramiento y personal con conocimientos de la estructura de la Base de Datos para usar la herramienta de enmascaramiento.

4.4.7. Socio – Cultural

El trabajo tiene un impacto positivo en los socios y clientes de la cooperativa ya brinda seguridad y tranquilidad al saber que su información personal y financiera se encuentra protegida.

4.4.8. Legal

Para el desarrollo de este trabajo, se toman en cuenta la normativa RESOLUCIÓN JB-2012-2148 de la Superintendencia de Bancos del Ecuador. Para mas información ver **Anexo A.**

Después de tomar en cuenta cada aspecto analizado y valido que no se tendrá efectos negativos que quizás no sean relacionados al tema, sino más bien contribuyan a su desarrollo, se puede determinar la factibilidad del mismo.

4.5. Enmascaramiento de Datos

4.5.1. Identificación de los datos sensibles y sus tablas

Los datos sensibles serán divididos en personales y financieros.

4.5.1.1. Datos Personales

Es toda información que puede identificar a una persona, y para evitar un filtrado de estos datos se enmascarara los siguientes campos de la base de datos Oracle.

- Identificación.
- Nombre.
- Teléfonos.
- Dirección.
- Email.

Ubicación de los campos

La base de datos se encuentra divida en varios esquemas encontrándose la ubicación Personal en el esquema FBS_PERSONAS.

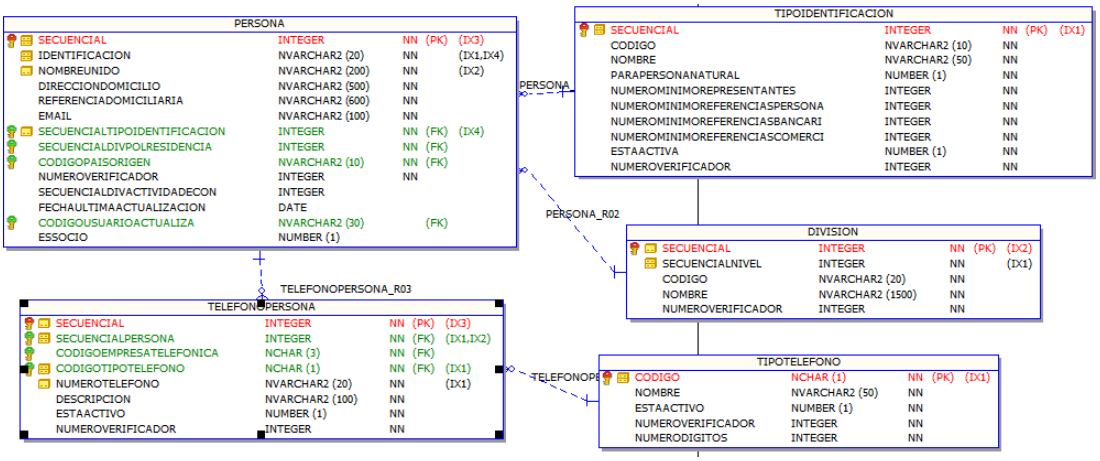


Figura 1: Diagrama Entidad Relación de FBS_PERSONAS.
Elaborado por el investigador.

Dato:	Identificación
Esquema:	FBS_PERSONAS
Tabla:	PERSONA
Campo:	IDENTIFICACION
Dato:	Nombre
Esquema:	FBS_PERSONAS
Tabla:	PERSONA
Campo:	NOMBREUNIDO
Dato:	Teléfonos
Esquema:	FBS_PERSONAS
Tabla:	TELEFONOPERSONA
Campo:	NUMEROTELEFONO
Dato:	Dirección
Esquema:	FBS_PERSONAS
Tabla:	PERSONA
Campo:	DIRECCIONDOMICILIO
Dato:	Dirección
Esquema:	FBS_PERSONAS
Tabla:	PERSONA
Campo:	EMAIL

Tabla 1: Campos sensibles en FBS_PERSONAS.
Elaborado por el investigador

4.5.1.2. Datos Financieros

Es la información económica de la persona se divide en Captaciones Vista, Captaciones Plazo y Préstamos.

Captaciones Vista.

Son los recursos que la cooperativa recibe de sus socios y se almacena en cuentas de ahorro los Datos sus Datos más relevantes son:

- Número de Cuenta.
- Saldo.
- Numero Tarjeta de débito

Ubicación de los campos

La información financiera se encuentra en el esquema FBS_CAPTACIONESVISTA.

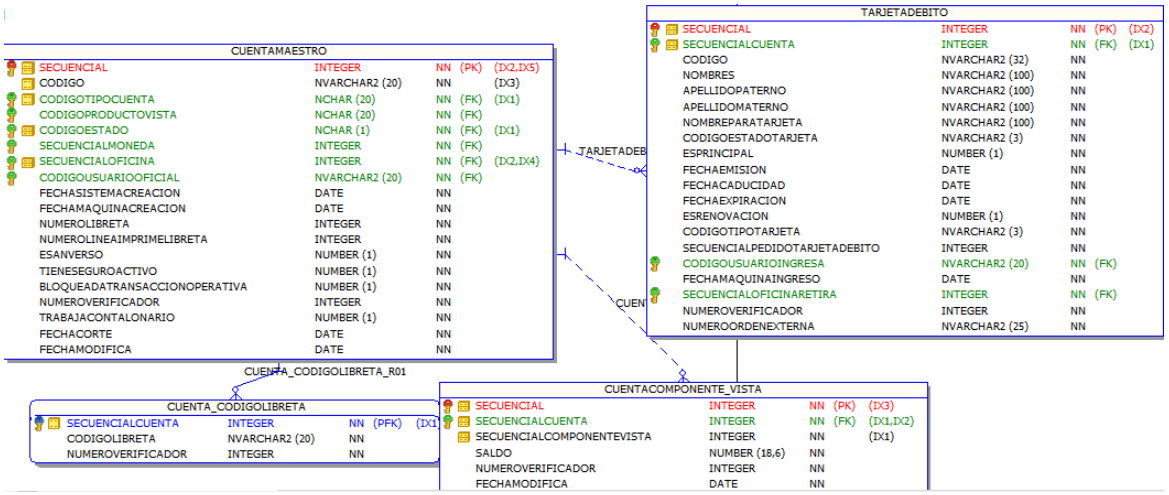


Figura 2: Diagrama Entidad Relación de FBS_CAPTACIONESVISTA.
Elaborado por el investigador

Dato:	Número de Cuenta
Esquema:	FBS_CAPTACIONESVISTA
Tabla:	CUENTAMAESTRO
Campo:	CODIGO
Dato:	Saldo Cuenta
Esquema:	FBS_CAPTACIONESVISTA
Tabla:	CUENTACOMPONENTE_VISTA
Campo:	SALDO
Dato:	Numero Tarjeta de debito
Esquema:	FBS_CAPTACIONESVISTA
Tabla:	TARJETADEBITO
Campo:	CODIGO

Tabla 2: Campos sensibles en FBS_CAPTACIONESVISTA.
Elaborado por el investigador

Captaciones Plazo.

Captaciones Plazo

Son los montos depositados por la cooperativa a un tiempo determinado, y al finalizar ese plazo el socio puede retirar el dinero más el interés, la información que debe ser protegida es:

- Numero Plazo Fijo.
- Monto.

Ubicación de los campos

La información financiera se encuentra en el esquema FBS_CAPTACIONESPLAZO.

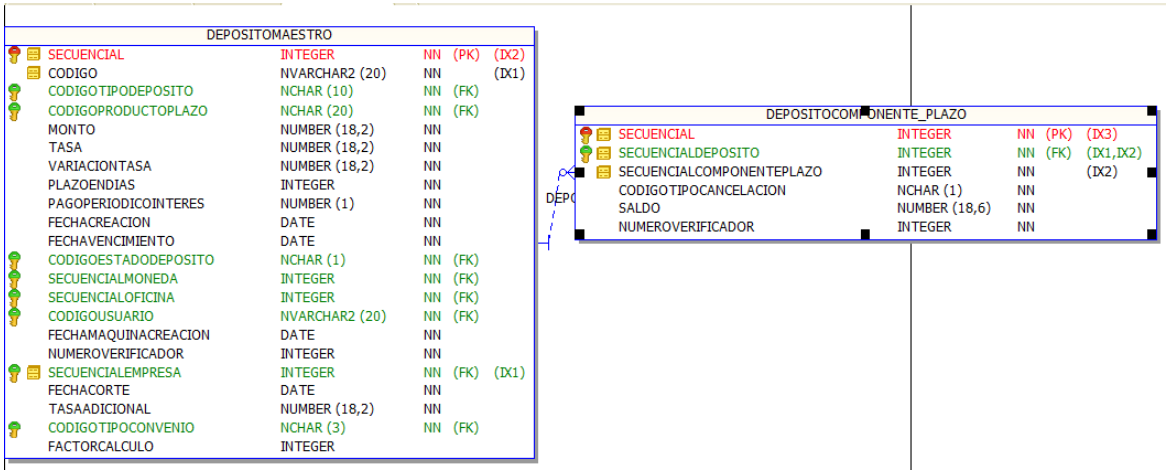


Figura 3: Diagrama Entidad Relación de FBS_CAPTACIONESPLAZO.
Elaborado por el investigador

Dato:	Numero Plazo Fijo
Esquema:	FBS_CAPTACIONESPLAZO
Tabla:	DEPOSITOMAESTRO
Campo:	CODIGO
Dato:	Monto plazo fijo
Esquema:	FBS_CAPTACIONESPLAZO
Tabla:	DEPOSITOMAESTRO
Campo:	MONTO

Tabla 3: Campos sensibles en FBS_CAPTACIONESPLAZO.
Elaborado por el investigador

Préstamos.

Son operaciones en las que la cooperativa pone a disposición de los socios una cierta cantidad de dinero mediante un pagare, en el que se estipula el plazo e intereses. Los datos más importantes son:

- Numero de Préstamo.
- Monto.
- Garantes.

Ubicación de los campos

La información financiera se encuentra en el esquema FBS_CARTERA.

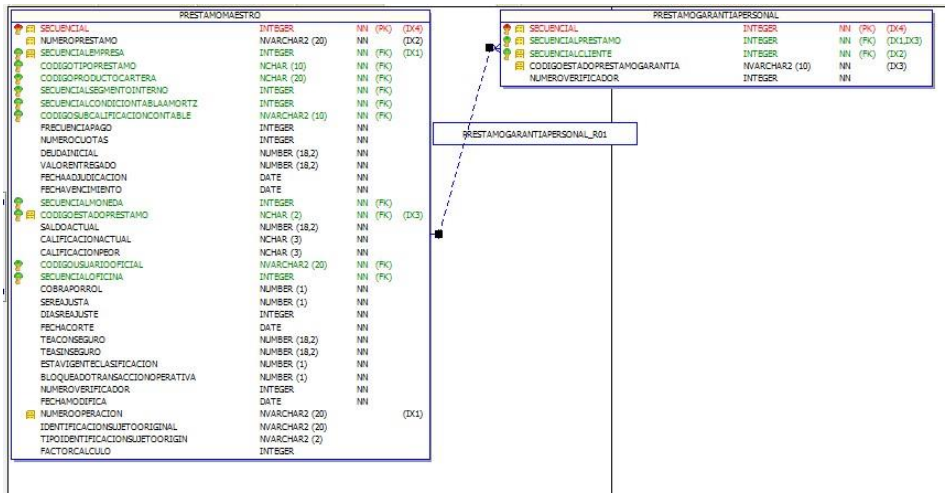


Figura 4: Diagrama Entidad Relación de FBS_CARTERA.
Elaborado por el investigador

Dato:	Numero de Préstamo
Esquema:	FBS_CARTERA
Tabla:	PRESTAMOMAESTRO
Campo:	NUMEROPRESTAMO
Dato:	Monto préstamo
Esquema:	FBS_CARTERA
Tabla:	PRESTAMOMAESTRO
Campo:	DEUDAINICIAL
Dato:	Garantes
Esquema:	FBS_CARTERA
Tabla:	PRESTAMOGARANTIAPERSONAL
Campo:	SECUENCIALCLIENTE

Tabla 4: Campos sensibles en FBS_CARTERA.
Elaborado por el investigador

Es importante tener esta información enmascarada porque en cuando las base de datos son llevadas con proveedores externos, no debe existir la posibilidad de poder contactar a los socios de CACPECO, ni conocer su estado económico.

4.5.2. Identificar las bases de datos que posee CACPECO y las personas que tienen acceso

En la cooperativa de Ahorro de Ahorro y Crédito CACPECO Ltda. existen 4 bases de datos con diferentes funciones y acceso cada una, para comenzar el enmascaramiento se realiza un detalle del uso de cada base.

4.5.2.1. Base de Datos Origen.

Es un respaldo de la Base del fin de mes anterior que es usada para obtener reportes y estructuras que son reportadas a las entidades de control. Sera la base donde se extrae los datos Originales para el enmascaramiento, el acceso esta limitado al administrador de la base de datos.

4.5.2.2. Base de Datos Capacitación.

Base usada para realizar inducciones al personal nuevo su uso se limita al personal encargado de las capacitaciones y auditoria, el principal acceso es por el core Financiero, esta base no será enmascarada.

4.5.2.3. Base de Datos Desarrollo.

Usada por los programadores internos y externos para realizar cambios en el sistema. Es la base más vulnerable a robo de información porque en muchas ocasiones es sacada de la institución para trabajos externos y es la base que se ofuscara antes de ser pasada a los programadores.

4.5.2.4. Base de Datos Producción.

Es la base usada por la cooperativa para almacenar todas las transacciones que se realizan diariamente, su acceso es limitado a 3 desarrolladores, que solo tienen permiso de lectura para revisiones de posibles errores, el administrador de la base de datos y el jefe de Sistemas que tienen acceso total.

4.5.3. Enumerar los riesgos al tener expuestos los datos de entornos no productivos de la base de datos de la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Cotopaxi

Los principales riesgos de tener una base no enmascarada en un entorno no productivo son los siguientes:

- Multas de organismos de control al no cumplir la normativa JB-2012-2148.

- Fugas de información.
- Mal uso de los datos por parte de los proveedores que se les da la base de datos

4.5.4. Análisis de las opciones disponibles en el mercado para enmascaramiento de datos

Para seleccionar la mejor solución de enmascaramiento de datos se analizo varias propuestas de enmascaramiento del mercado.

4.5.4.1. POWERDATA.

Empresa Española especializada en la gestión de datos Corporativos y propone la solución de enmascaramiento de Informatica Persistent Data Masking.

Informatica Persistent Data Masking.- Es un software de enmascaramiento de datos escalable, que permite a las organizaciones crear copias seguras y protegidas de datos al ofuscar información que podría amenazar la privacidad, seguridad o cumplimiento de leyes. Estas copias de datos se pueden usar para pruebas, investigaciones, análisis en otros entornos que no sean de producción. El software protege los datos confidenciales, como la información de la tarjeta de crédito, los números de la Seguridad Social, los nombres, direcciones y números de teléfono, mediante el cambio de los datos originales para evitar la visualización no autorizada de datos críticos. Proporciona una escalabilidad, robustez, conectividad de bases de datos tradicionales y una política de enmascaramiento de datos coherente en toda la empresa con un único seguimiento de auditoría que permite realizar un seguimiento de los procedimientos para proteger datos confidenciales a través de registros e informes de auditoría completos.

Proporciona simulación de reglas de enmascaramiento antes de la ejecución real para validar las políticas de privacidad, y define y reutiliza las reglas de enmascaramiento de datos para adherirse a las políticas de privacidad y producir resultados rápidos con soporte para el enmascaramiento en el lugar y en el flujo. El enmascaramiento minimiza el riesgo de acceso no autorizado a datos, al enmascarar los conjuntos de datos de prueba, analíticos o de desarrollo creados a partir de datos de producción; independientemente de la base de datos, la plataforma o la ubicación. El software proporciona reglas de enmascaramiento sofisticadas pero flexibles que le permiten aplicar diferentes tipos de técnicas de enmascaramiento a diversos datos utilizados en pruebas, capacitación y otros

entornos de no producción[17].

4.5.4.2. REDPARTNER.

Empresa Ecuatoriana desarrolladora y distribuidora de software empresarial la alta calidad y un servicio muy especializado así como personalizado y adaptado a las necesidades del cliente, propone una solución en Base a rutinas PL/SQL pegadas en ORACLE.

Rutinas PL/SQL.- Es un desarrollo a medida que consiste en diseñar unas rutinas PL/SQL que apliquen el enmascaramiento al conjunto de columnas sensibles identificado por CACPECO. Estas rutinas se aplicarán en la base de datos de pruebas, antes de poner disponible los datos a los desarrolladores, y cada vez que se efectúen copias de producción a desarrollo[18] .

4.5.4.3. Proyectos Compartidos Ltda.

Empresa Colombiana dedicada a crear software a medida y su Propuesta con ELLENTON.

Ellenton.- Es una solución de software que construye datos de prueba de forma rápida y sencilla a partir de cambios de los datos reales de su sistema de información. Al enmascarar toda la información confidencial, los datos mantienen sus características esenciales, pero pierden su valor para usos indebidos[19].

4.5.4.4. SinergyHard

Empresa Ecuatoriana especializada en soluciones de de seguridad informática y consultorías en hardware y software, Parter de IBM, su propuesta es IBM InfoSphere Optim.

IBM InfoSphere Optim.- La gestión de datos de prueba IBM® InfoSphere Optim™ ayuda a las organizaciones a optimizar y automatizar los procesos que crean y gestionan datos del entorno que no son de producción. Y ayuda a crear bases de datos de pruebas ficticias de tamaño adecuado para usos en entornos de pruebas, los datos confidenciales, como números de tarjetas de crédito, direcciones de correo electrónico e información corporativa confidencial pueden enmascararse para protegerlos contra el uso indebido y el fraude al tiempo que conservan el significado contextual[20].

4.5.5. Comparativa de las soluciones de enmascaramiento existentes en el mercado

4.5.5.1. Escabilidad

A excepción de las rutinas de enmascaramiento, que es código quemado en un Package, Las soluciones de enmascaramiento tienen módulos que permiten agregar nuevas tablas o mapear nuevos campos lo que da la posibilidad de adaptarse a los cambios que se realizan en los entornos de desarrollo.

Empresa	Escalabilidad
Informatica Persistent Data Masking	X
Rutinas PL/SQL en Oracle	
ELLENTON	X
IBM InfoSphere Optim	X

Tabla 5: Comparativa en ESCALABILIDAD.
Elaborado por el investigador

4.5.5.2. Reducción de Información

Las soluciones de IBM y PowerData tienen un módulo especifico que permiten realizar crear una copia de la base enmascarada pero solo con menos cantidad de datos, eso ayuda a minimizar la fuga de información y agilizar proceso en los desarrollos.

Empresa	Reducción de Información
Informatica Persistent Data Masking	X
Rutinas PL/SQL en Oracle	
ELLENTON	
IBM InfoSphere Optim	X

Tabla 6: Comparativa en REDUCCIÓN DE INFORMACIÓN.
Elaborado por el investigador

4.5.5.3. Experiencia en la Banca

Todas las soluciones tienen experiencia en Bancos o Cooperativas, pero la única comprobada fue la de IBM InfoSphere Optim que se encuentra en el Banco Central de Ecuador.

Empresa	Experiencia en la Banca
Informatica Persistent Data Masking	X
Rutinas PL/SQL en Oracle	X
ELLENTON	X
IBM InfoSphere Optim	X

Tabla 7: Comparativa en EXPERIENCIA EN LA BANCA.
Elaborado por el investigador

4.5.5.4. Reglas Básicas de Enmascaramiento

Las soluciones de enmascaramiento tienen reglas básicas de enmascaramiento previamente programadas que pueden ser usadas de manera automática en los campos designados para el enmascaramiento, las reglas son las siguientes:

Random masking: Permite realizar una mezcla entre todos los datos de una misma columna.

Expression masking: Es una regla que permite reemplazar o crear datos en base a mascaras.

Sustitución: Reemplaza la información de una columna por otro dato con el que se encuentra en otra columna

Uso de Diccionarios Es la capacidad para reemplazar datos por información guardada en Diccionarios, se utiliza para reemplazar direcciones o nombres.

Copiar Objetos: Crea Script de los Objetos como tablas, triguers, secuencias de las base de datos, para poder utilizarlos en otro momento.

Reglas Propias: La soluciones expuestas por las empresas Informática y IBM tienen reglas previamente diseñadas que enmascaran identificaciones, números de teléfono, tarjetas de crédito.

	Random masking	Expression masking	Sustitución	Uso de Diccionarios	Copiar Objetos
Informatica Persistent Data Masking	X	X	X		X
Subrutinas en Oracle	X	X	X		
ELLENTON	X		X		
IBM InfoSphere Optim	X	X	X	X	X

Tabla 8: Comparativa en REGLAS BÁSICAS DE ENMASCARAMIENTO.
Elaborado por el investigador

4.5.6. Determinar una solución de enmascaramiento de datos adecuada para la cooperativa

Las dos soluciones más completas son Informatica Persistent Data Masking y IBM InfoSphere Optim, pero la experiencia dentro del mercado ecuatoriano y en el banco central son que más peso tienen por eso se decide ir por la herramienta propuesta por SynergyHard, **IBM InfoSphere Optim**.

4.5.7. Configurar la solucion de enmascaramiento de la base de datos Oracle

4.5.7.1. Requisitos de IBM InfoSphere Optim

Los requisitos mínimos previos para la instalación de la solución de enmascaramiento son:

- Procesador CORE I7.
- 4 GB RAM.
- Windows Server o Windows 7.

Para un mejor desempeño se instala un Windows 7 de 64 bits 12 GB en RAM.

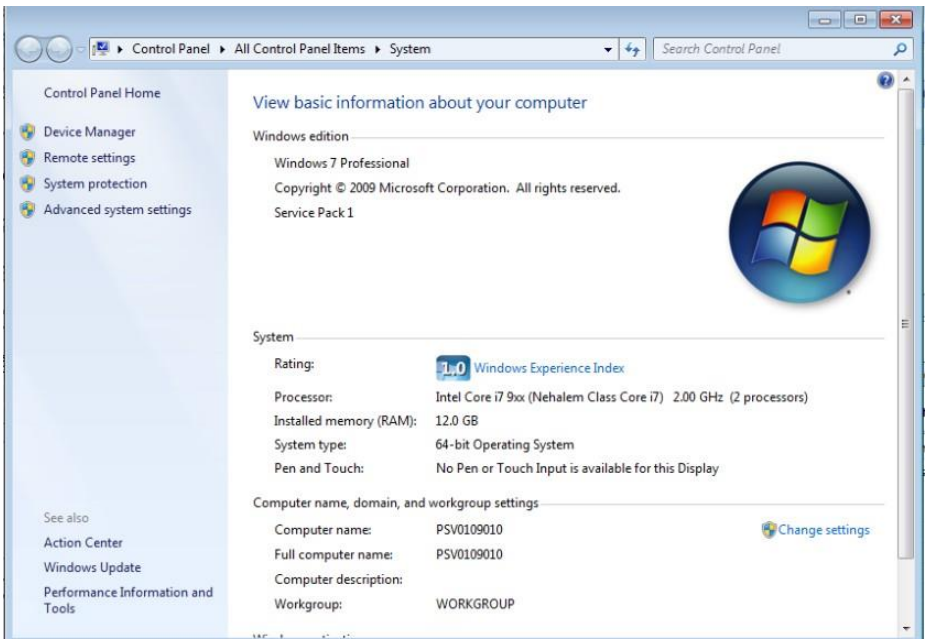


Figura 5: Características óptimas del equipo.
Elaborado por el investigador

4.5.7.2. Configuración de IBM InfoSphere Optim

Creación del alias de la Base de Datos: Es la parametrización de las bases a usar en el enmascaramiento, su configuración está en "Data Store Alias".

Figura 6: Creación del Alias de la Base de Datos.
Elaborado por el investigador

Se crea las conexión a la base de datos, la primera en usarse es origen.

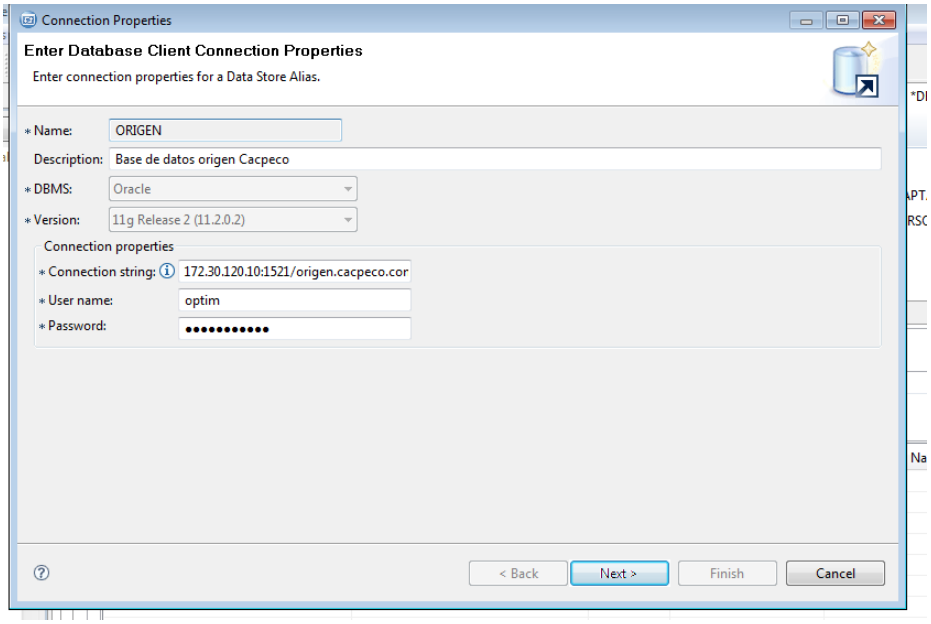


Figura 7: Configuración de los accesos de conexión.
Elaborado por el investigador

Se configura la IP del host y el puerto que se utilizará para la conexión.

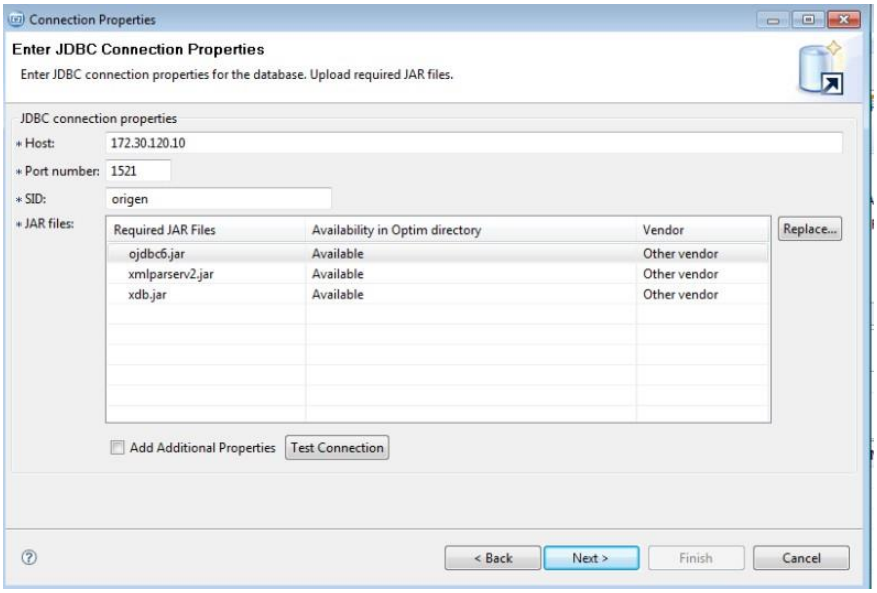


Figura 8: Configuración host.
Elaborado por el investigador

Seleccionar el carácter set que usa la base de datos.

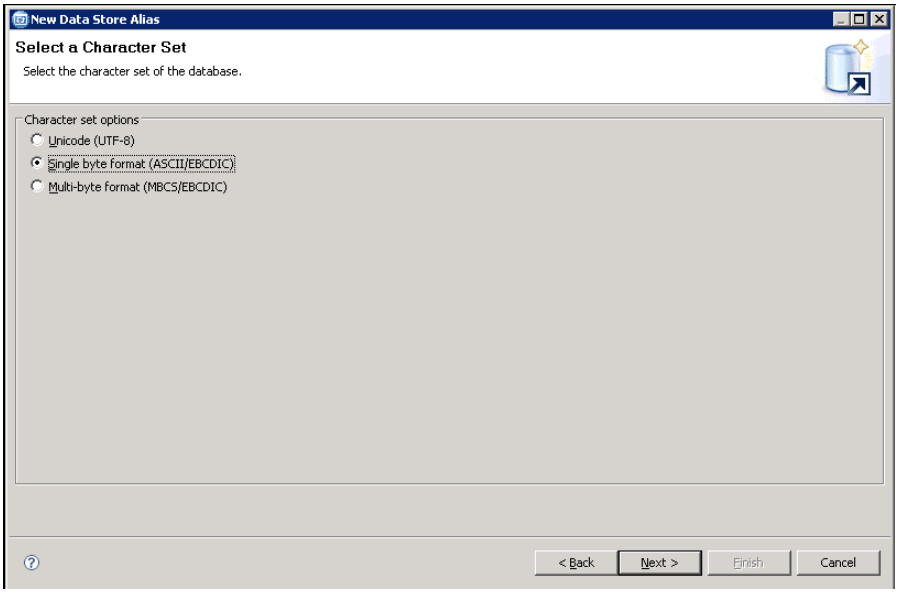


Figura 9: Selección del set de caracteres.
Elaborado por el investigador

Una vez creada el acceso los accesos a la Base de Datos se crea las siguientes configuraciones para enmascarar los datos:

- Definición de acceso.
- Servicio de extracción.

- Mapeo de columnas.
- Servicio de conversión.
- Servicio de inserción.

4.5.7.3. Creación de la definición de acceso

Se crea en a Access Definition seleccionando "New Access Definition"

Figura 10: Nueva definición de acceso.
Elaborado por el investigador

Se coloca el nombre de la definición de acceso y una pequeña descripción.

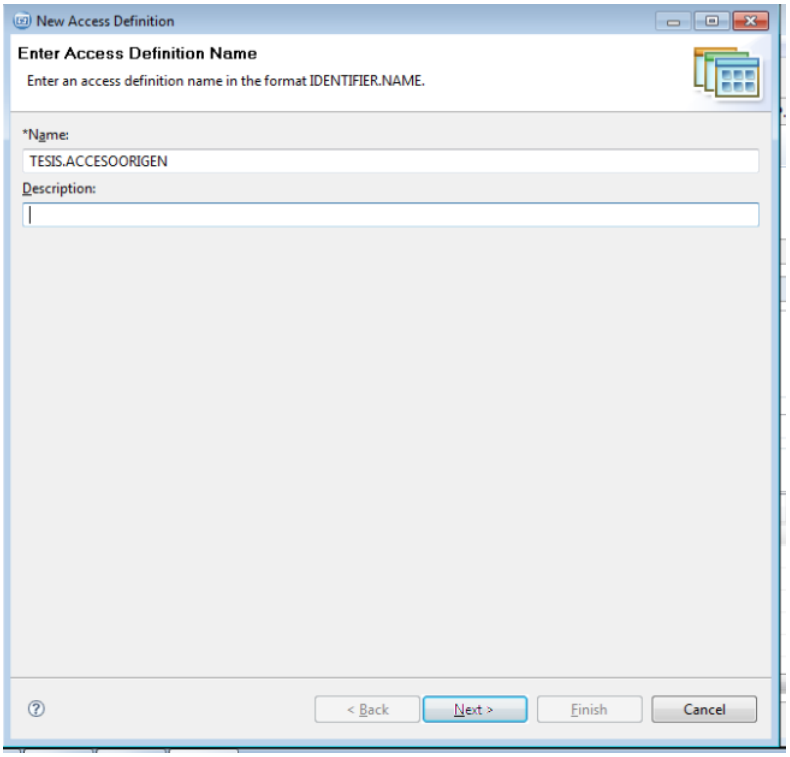


Figura 11: Datos de la definición de acceso.
Elaborado por el investigador

Se selecciona el alias de base de datos de donde se obtendrá la información

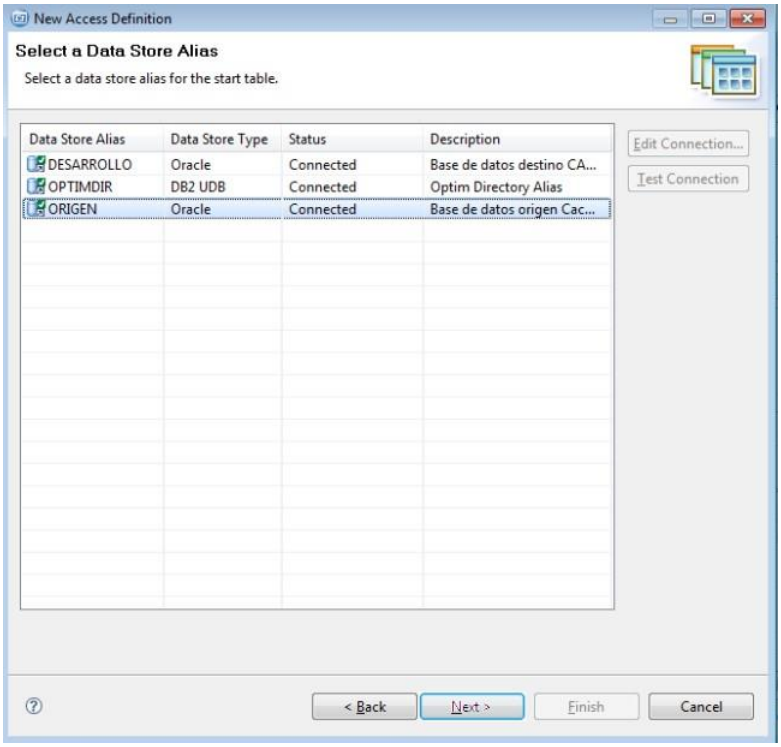


Figura 12: Selección del alias de la base de datos.
Elaborado por el investigador

Se parametriza la tabla maestro para el enmascaramiento de datos.

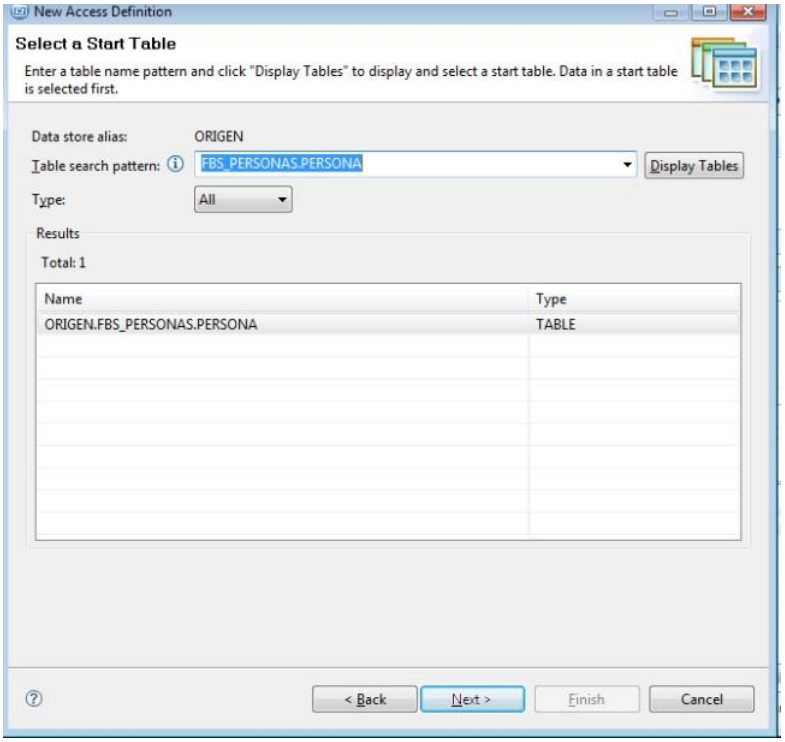


Figura 13: Selección de la tabla maestro para la extracción.
Elaborado por el investigador

Finalmente se selecciona el método para la selección de tablas que servirán para extraer la información.

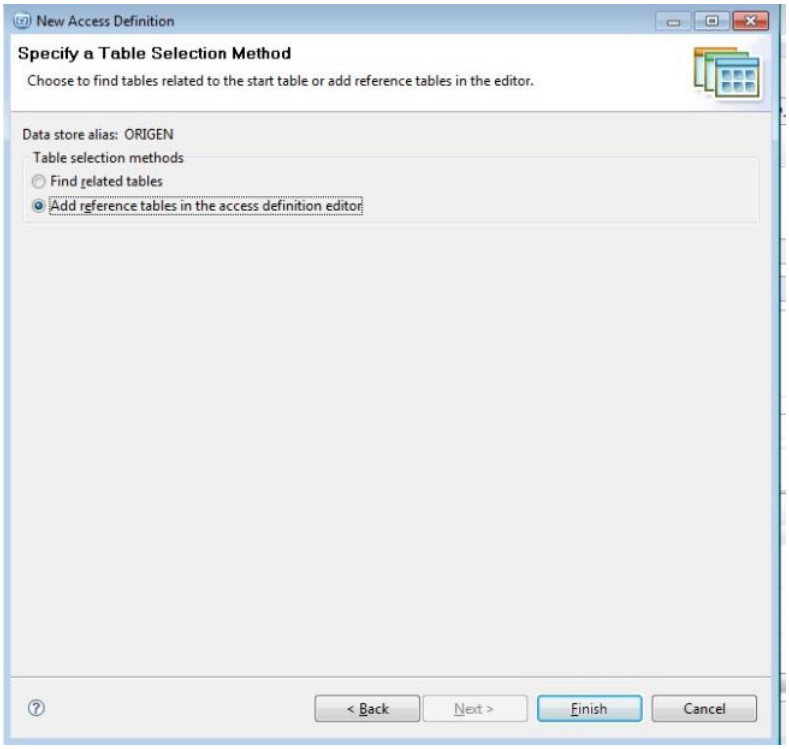


Figura 14: Método de extracción de tablas.
Elaborado por el investigador

Una vez creado la definición de acceso, se podrán observar las tablas relacionadas en el "Access Definition Editor".

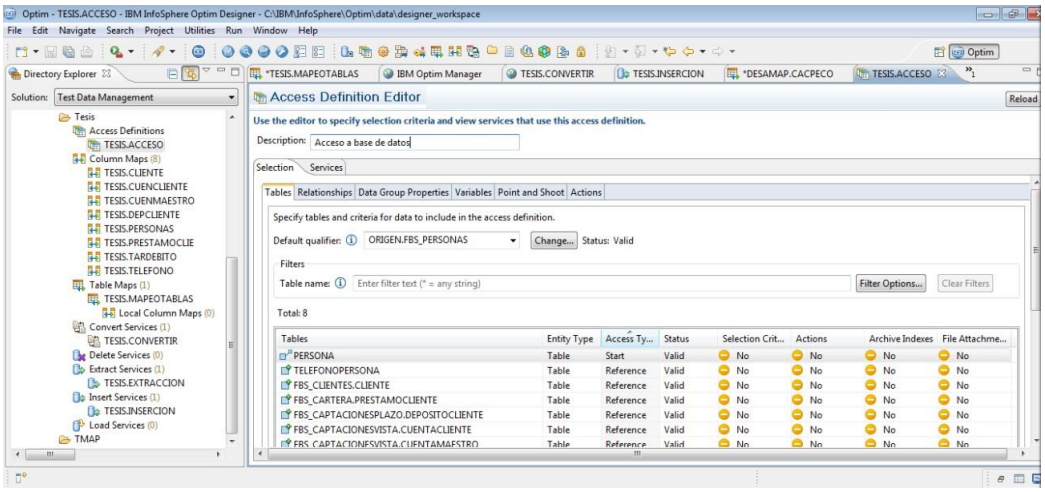


Figura 15: Access Definition Editor.
Elaborado por el investigador

4.5.7.4. Creación del Servicio de Extracción

Para extraer la información es necesario un crear un servicio de extracción.

Figura 16: Creación del Servicio de Extracción.
Elaborado por el investigador

Se coloca un nombre para el nuevo servicio de extracción y una descripción. Se verifica que este seleccionada la opción de "Extract" en la categoría "Service Type".

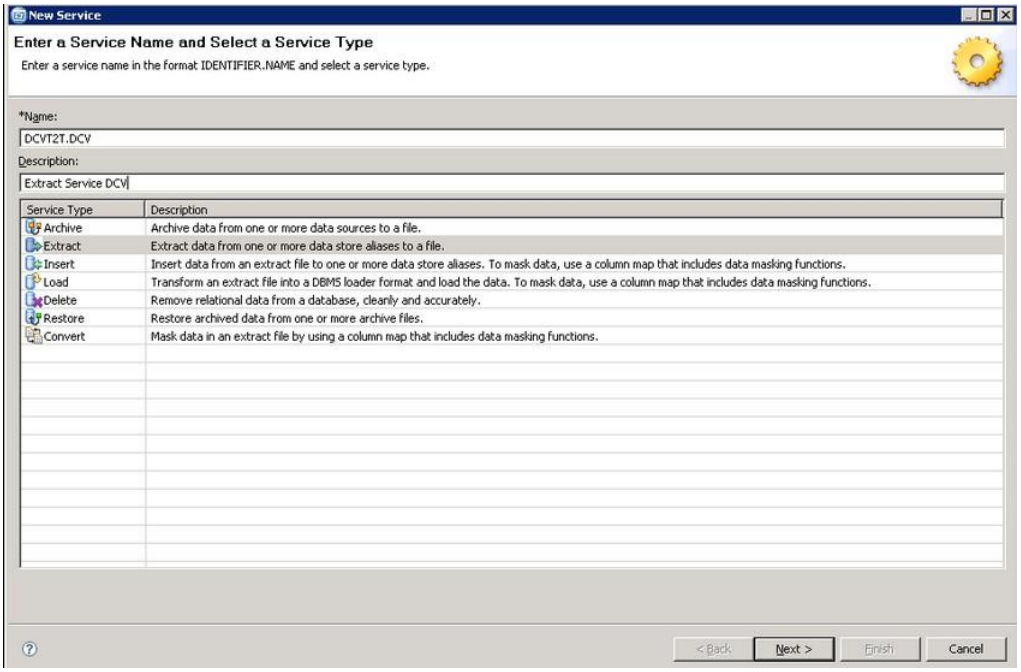


Figura 17: Servicio de extracción.
Elaborado por el investigador

Se selecciona la definición de acceso que será utilizado para realizar la extracción de los datos.

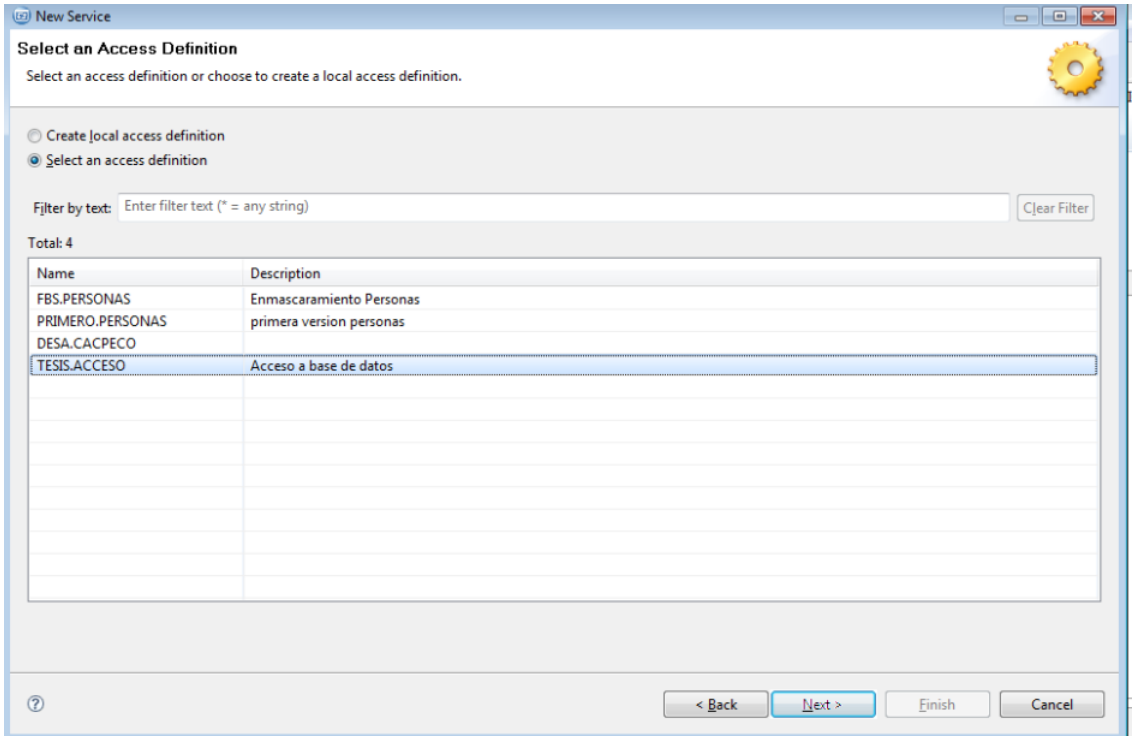


Figura 18: Selección de acceso.
Elaborado por el investigador

Una vez creado el servicio de extracción, podemos ver su configuración en el "Extract Service Editor"

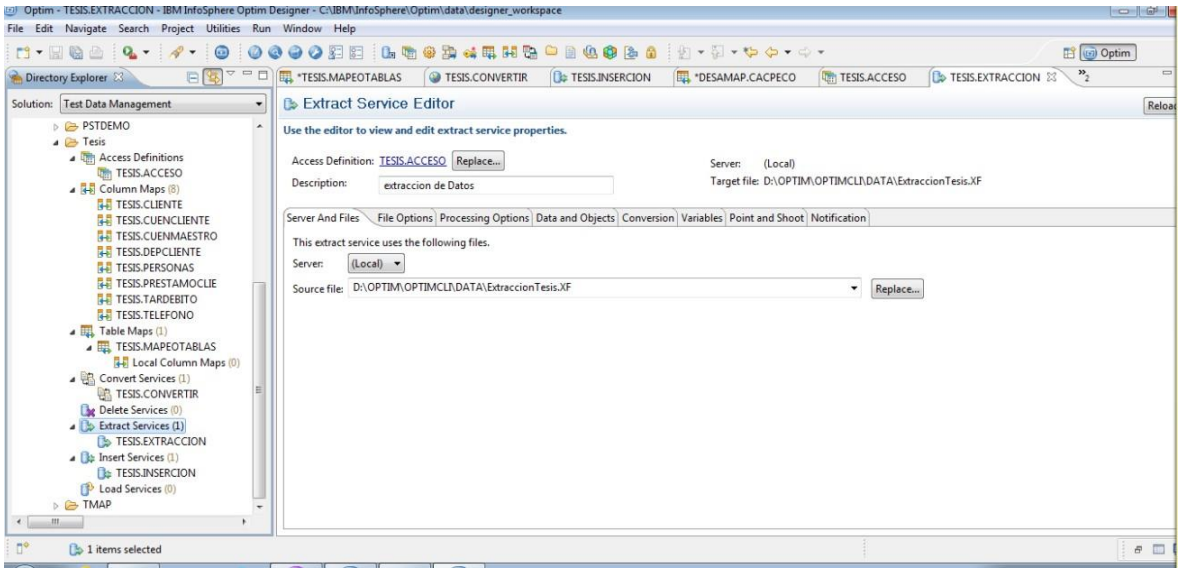


Figura 19: Editor del servicio de extracción de Datos.
Elaborado por el investigador

4.5.7.5. Mapeo de Columnas

En el mapeo de Columnas se define que tablas y columnas van a ser enmascaradas y las reglas a ser usadas.
Se selecciona la opción Column Map y "New Column Map

Figura 20: Nuevo mapeo de Columnas.
Elaborado por el investigador

Se coloca un nombre para el nuevo mapeo de columnas y una pequeña descripción.

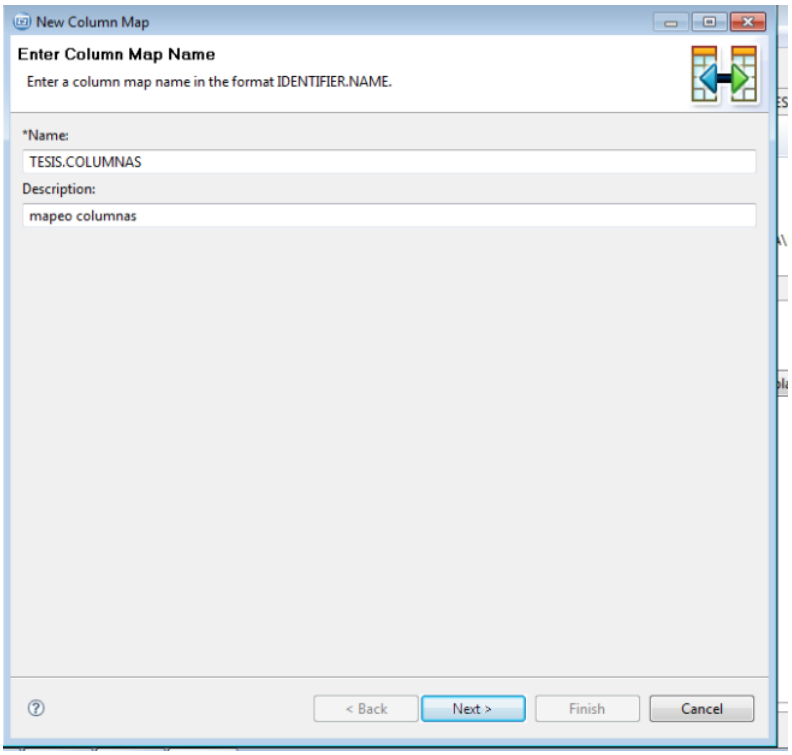


Figura 21: Datos del mapeo de Columnas.
Elaborado por el investigador

En la opción “Browse to an Optim File” seleccionamos el archivo de extracción.

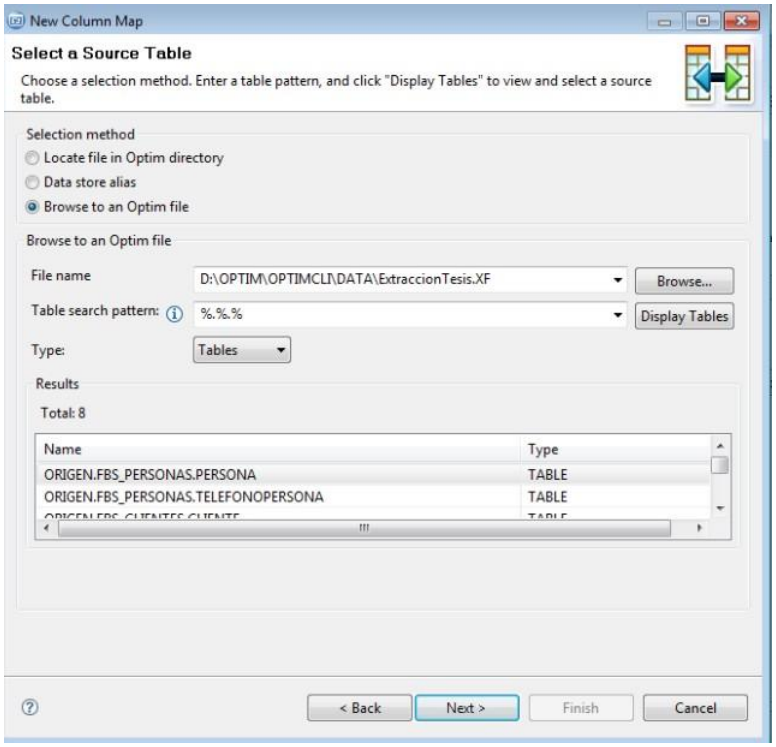


Figura 22: Seleccionar archivo de extracción.
Elaborado por el investigador

Se selecciona el alias de la base de datos destino y se elige la tabla con el mismo formato que la tabla origen que fue seleccionada en la **Figura 22** para colocar los datos enmascarados dentro de la base destino.

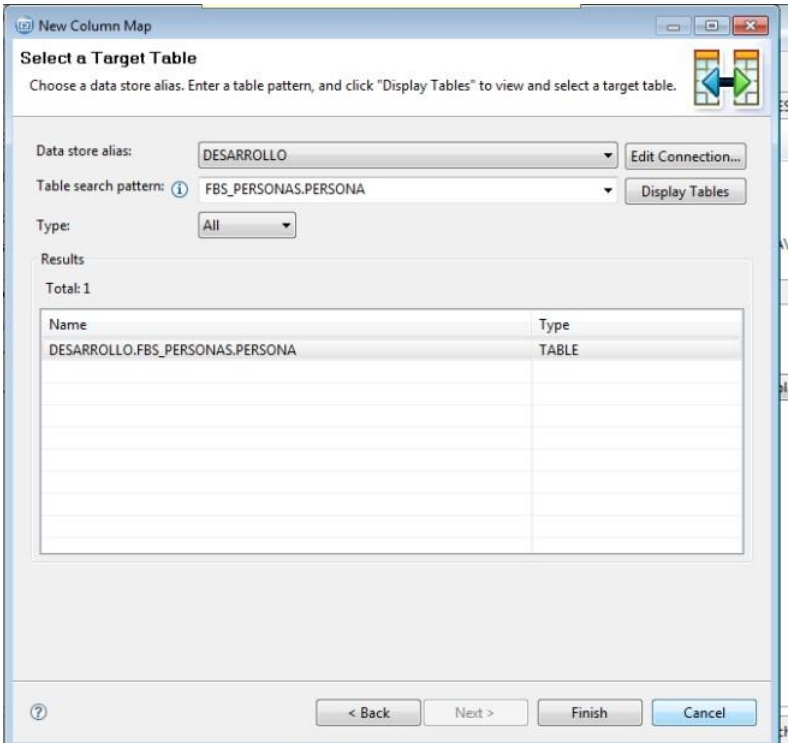


Figura 23: Selección tabla destino.
Elaborado por el investigador

Una vez mapeadas las columnas de la tabla origen y destino, se puede editar las reglas de enmascaramiento. Para agregar una política se lo realiza en la opción "Add Policy"

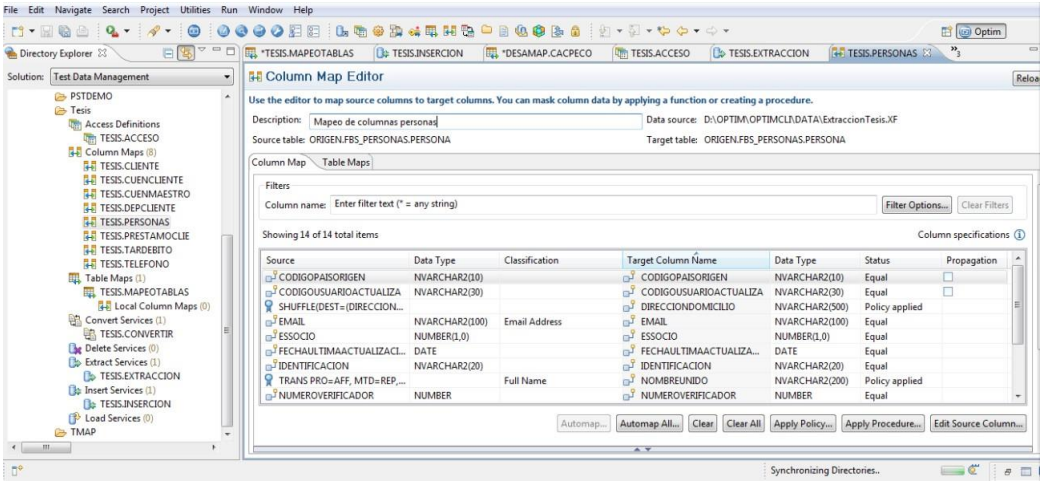


Figura 24: Agregar políticas de enmascaramiento.
Elaborado por el investigador

4.5.7.6. Reglas de ofuscación

Las reglas son tareas o algoritmos propios de las soluciones de enmascaramientos que nos permiten realizar un cambio especifico en un dato dentro de una columna..

4.5.7.7. Configuracion de las reglas de enmascaramiento

4.5.7.8. Configuracion de la regla Mezcla o Shuffle

Este método mezcla todos los valores de la misma columna su configuracion puede programar con el codigo SHUFFLE(DEST=(SECUENCIALCLIENTE), RETRY=10, IGNORE=(SECUENCIALCLIENTE(NULL,SPACES,ZERO_LEN))) donde SecuencialCLiente es la columna a mezclar o se lo puede realizar de manera vizual con el asistente

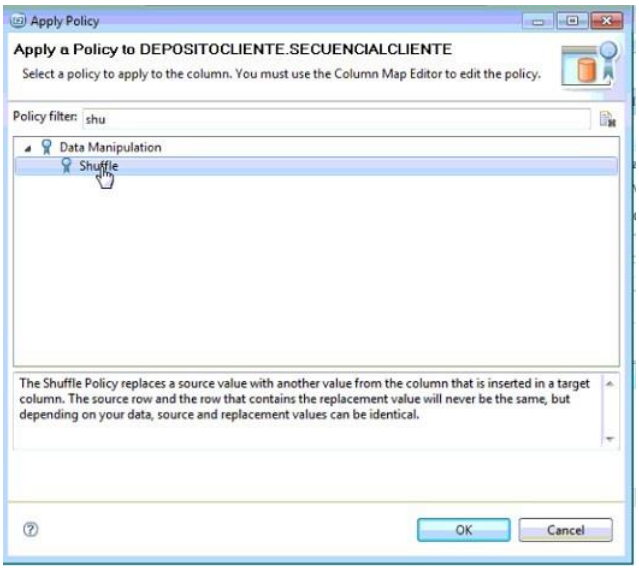


Figura 25: Asistentente para aplicar la regla shuffle.
Elaborado por el investigador

4.5.7.9. Aleatorios con máscara

Sirve para generar números o caracteres aleatorios para que cumplan con un formato específico o máscara se enmacro el mal usando este metodo su el codigo es TRANS PRO=AFF, MTD=REP, FLDDEF1=(NAME=NOMBREUNIDO, DT=WVARCHAR_SZ) los parametros son nombre del campo y tipo de dato.

4.5.7.10. Uso de Diccionarios

Este enmascaramiento usa datos propios de la solucion para enmascarar los datos se utiliza para enmascarar el mail

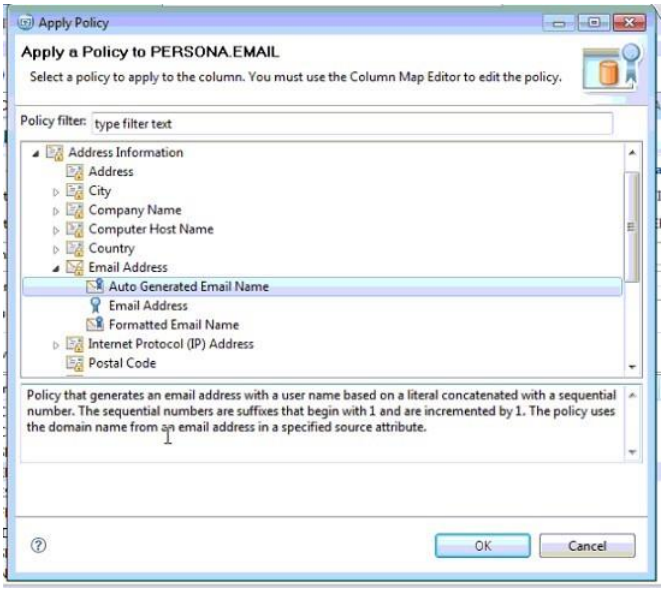


Figura 26: Uso de diccionarios para enmascarar.
Elaborado por el investigador

Todas estas reglas cumplen con las normas básicas de enmascaramiento que son mantener la integridad referencial y que no sean reversibles para de esta manera tener datos consistentes y que no se pueda regresar la información original.

4.5.7.11. Configuracion de la regla Mezcla o Shuffle

La configuracion del shuffle se puede programar con el codigo SHUFFLE(DEST=(SECUENCIALCLIENTE), RETRY=10, IGNORE=(SECUENCIALCLIENTE(donde SecuencialCLiente es la columna a mezclar o se lo puede realizar de manera vizual con el asistente

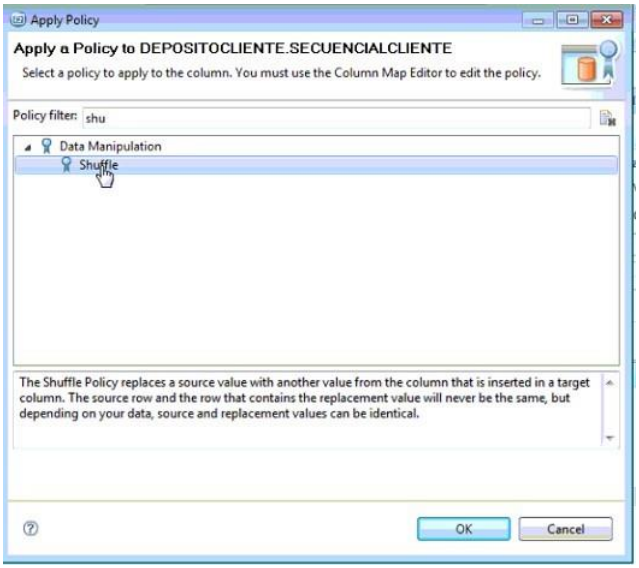


Figura 27: Asistentente para aplicar la regla shuffle.
Elaborado por el investigador

4.5.7.12. Creación del Servicio de Conversión

Se crea el servicio de conversión en "Convert Service" opción "New Service"

Figura 28: Creación Servicio de conversión.
Elaborado por el investigador

Se coloca un nombre para el nuevo servicio de conversión y una descripción

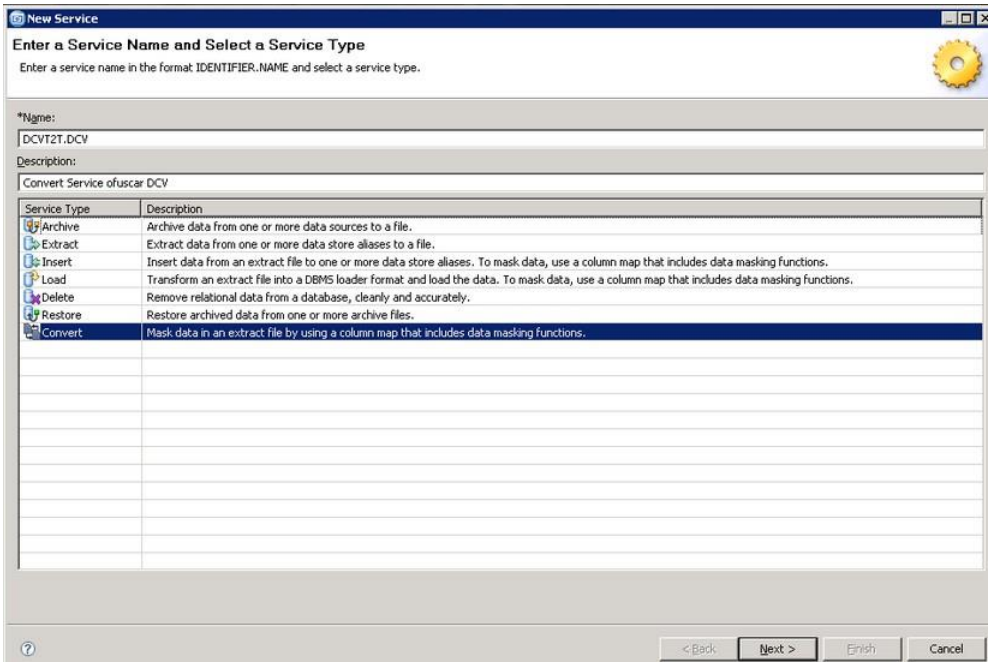


Figura 29: Datos del servicio de conversión.
Elaborado por el investigador

4.5.7.13. Ejecutar el Servicio de Conversión

Se da clic derecho en el nombre del servicio de conversión creado en la **Figura 25** y se ejecuta el servicio. Esta opción enmascara todos los datos extraídos

Figura 30: Servicio de conversión.
Elaborado por el investigador

Figura 31: Ejecución servicio de conversión.
Elaborado por el investigador

4.5.7.14. Creación del Servicio de Inserción

Una vez que se extraen y convierten los datos, es necesario un servicio de inserción para enmascarar la base de desarrollo o cualquier otra de entorno no productivo

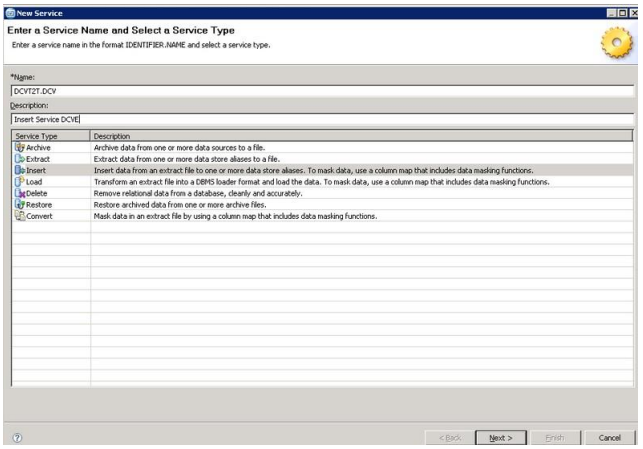


Figura 32: Datos del servicio de Inserción.
Elaborado por el investigador

Se configura el archivo convertido que sera insertado en la nueva Base

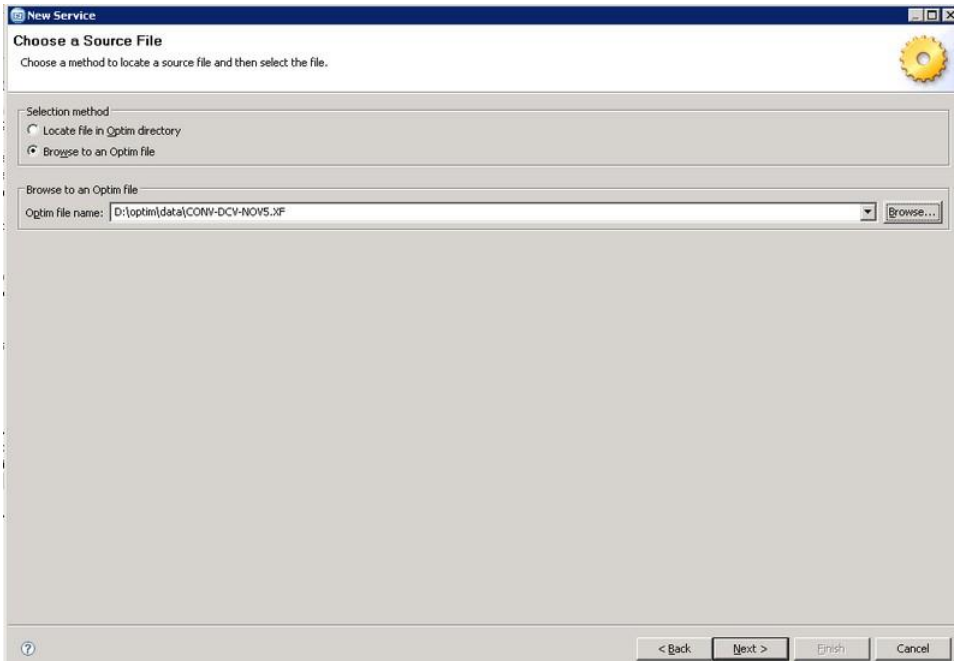


Figura 33: Selección del archivo convertido.
Elaborado por el investigador

4.5.7.15. Ejecutar del Servicio de Inserción

Se da clic derecho en el nombre del Servicio de Inserción creado en la figura 4.29 y se "Ejecutar servicio"

Figura 34: Ejecución del servicio de Inserción.
Elaborado por el investigador

Figura 35: Datos de le ejecución del servicio.
Elaborado por el investigador

Dentro de pestaña "Optim Manager" que se abre automáticamente, se puede ver estado del servicio.

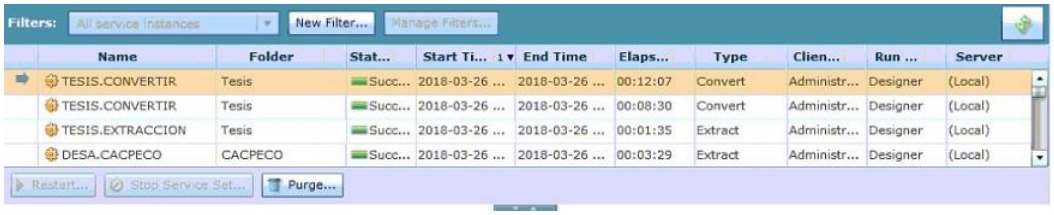


Figura 36: Monitor del servicio.
Elaborado por el investigador

Para actualizar el servicio tuvo una demora de 3 horas

4.5.8. Comparativa de los datos enmascarados.

Para que los datos tenga una mejor consistencia se uso la regla de la solución random masking, en el cual se realizo una mezcla de todos los datos y evitar de esta manera encontrar los originales

4.5.8.1. Datos Personales y Financieros enmascarados

Para el análisis de datos enmascarados se realiza una visualización desde el sistema Financial y la base de datos, que son los únicos accesos que existen a la información de los socios.

Figura 37: Información enmascarada Financial.
Elaborado por el investigador

Figura 38: Información real Financial.
Elaborado por el investigador

En la **Figura 34** y **Figura 35** se puede verificar que una identificación muestra nombres cuentas y saldos distintos, con eso si la información llega a filtrase se tendrían datos incorrectos, que no afectarían de ninguna manera al socio de la cooperativa.
De la base se obtiene una muestra de personas y sus cuentas de base de origen y enmascarada para realizar una comparación.

IDENTIFICACION	NOMBRE	DIRECCION	TELEFONO	CUENTA	SALDO
0009420	ALMACHI PINCAY DOLORES	BARRIO	032725071	0601001127786	10.27
0201381654	PALLO GUAMAN MARIA MERCEDES	PALOUCTOPAMBA	022624786	0602001126712	0.2812
				0600001126712	17.982671
0202195814	GUEVARA ROMERO FABIAN GONZALO	BARRIO ISINCHE LA GLORIA CALLE PRINCIPAL CAJETIN	0988462863	0602001127616	1.4
				0600001127616	122.949802
				0601001127616	15.52
0400359592	CHILUISA YUPANGUI ROSA CRISTINA	S34K OE12-186 PB	032803018	0600002043881	25.95
				0602001043881	0.1903
				0601001043881	229.09
0500003595	AIMACAÑA TELLO VICTOR ALFONSO	COTOPAXI>LA MANA>LA MANA	2804693	0600001013458	17.982671
				0606001013458	55.902
				0606001013458	55.902

Figura 39: Información enmascarada.
Elaborado por el investigador

IDENTIFICACION	NOMBRE	DIRECCION	TELEFONO	CUENTA	SALDO
0009420	ANCHATIPAN HERRERA STALYN RAUL	BARRIO ROSITA PAREDES	023022136	0611001127784	5.9356
0201381654	CAMACHO YANEZ XIMENA ISABEL	JOSE MALDONADO S18 75 Y RIO CONURIS	0995361066	0601001126706	194.3137
0202195814	REA QUINALOA HECTOR ROGELIO	AV SEGUNDO CHIMBORAZO	0988462863	0600001127614	19.022671
					27.7107
0400359592	RODRIGUEZ RODRIGUEZ JOSE	CONJ HAB LAS ACACIAS C 6 ENTRE E Y	0984614330	0600002043880	15
				0601002043880	25.0563
0500003595	RES AMORES CARLOS NE	CDLA LAS FUENTES	2804693	060100013457	8.16
0500369657	TOAPANTA VARGAS JOSE RAFAEL	YANAHURCO GRANDE	0995204419	0600001126127	16.29
				0601001126127	82.9116

Figura 40: Información real.
Elaborado por el investigador

Igual que la consulta realizada por el sistema la base muestra datos enmascarados que puede ser usada en entornos de desarrollo sin riesgo a que exista fuga de información.

CAPÍTULO 5

Conclusiones y Recomendaciones

Conclusiones

En el desarrollo y implementación de este proyecto se pudo llegar a las siguientes conclusiones:

- El enmascaramiento debe ser periodicamente ya que al ser una intitucion financiera la información cambia constatemente
- Los datos enmascarados pueden ser usados en entornos de programación sin afectar los nuevos desarrollos.
- La seguridad en entornos no productivos se incremento porque ahora es mucho mas difícil que la información de los socios sea cambiada.
- Los desarrollos externos que implican la entrega de la base de datos ya no significan un riesgo de perdida de Datos para la Cooperativa de Ahorro y Crédito CACPECO Ltda.

Recomendaciones

- Se recomienda que mensualmente sean actualizadas las bases de datos de los entornos no productivos para que mantengan una estructura idéntica a producción.
- Se recomienta enmascarar las base de datos el primer dia de cada mes , que es cuando se actualizan los entornos no productivos.
- Se debe crear un nuevo mapeo de campos cada vez que se creen nuevas tablas para que no se pierda la integridad referencial.
- Se recomiendan limitar el acceso a la Base de producción para evitar que la información sea filtrada.

Bibliografia

[1] O. d. l. n. Unidas, "Declaración universal de los derechos humanos," *TEMOA*, 2008.

[2] P. G. y R. Schomerus, "Bundesdatenschutzgesetz," *Alemania: Beck (Munich)*, 2017.

[3] N. Organization, "The privacy act of 1974," *National Archives USA*, 2017.

[4] N. . Ltd., "Data masking: What you need to know," *Net 2000 Ltd.*, 2000.

[5] R. Ravichandran, "Data masking techniques for insurance," *niit-tech.*, 2016.

[6] J. A. W. Ahmed, "Data masking best practice," *U.S.A: Oracle Corporation*, 2013.

[7] A. Arias, "Bases de datos con mysql," *IT Campus Academy*, 2014.

[8] A. Arias, "Introduccion a las bases de datos relacionales," *Vision Libros*, 2016.

[9] J. L. Herrera, "Programacion en tiempo real y bases de datos: Un enfoque practico," *Universidad Politecnica de Catalunya*, 2015.

[10] I. S. Gabina, "Atencion medica frente a la economia y la diversidad," *DYKINSON E-book*, 2015.

[11] C. C. Iglesias, "Entornos de desarrollo. cfgs," *RA-MA EDITORIAL*, 2012.

[12] I. J. Turnbull, "Privacy in the workplace," *CCH a wolters klumers business*, 2012.

[13] S. Morris, "Bases de datos diseno implentacion y administracion," *Cengage Learning*, 2012.

[14] M. Rouse, "Retos de la privacidad de los datos y el cumplimiento normativo," *searchdatacenter.techtarget.com*, 2016.

[15] C. E. P. Coello, "La informacion financiera y administrativa: enlace estrategico para la toma de decisiones," *Instituto mexicano de contadores publicos*, 2016.

[16] G. B. Urbina, "Introduccion a la seguridad informatica," *grupo editorial patria*, 2016.

[17] I. LLC, *Informatica Persistent Data Masking*. Informatica, 2017.

[18] A. M. Chaparro, *Oracle 11g PL/SQL : curso practico de formacion*. RC libros, 2012.

[19] proyectos compartidos, "Ellenton," *Vector ITC group*, 2014.

[20] IBM, "Ibm infosphere optim," *IBM*, 2018.

Anexos y Apéndices

Anexo A

Anexo A