0/N.2021
A30
IV
(4.2)
42949

TERCER INFORME PARCIAL

SISTEMA DE COPARTICIPACIÓN INVERSA ENTRE LOS MUNICIPIOS Y LA PROVINCIA DE CÓRDOBA

CONSEJO FEDERAL DE INVERSIONES

CONSEJO FEDERAL DE INVERSIONES
BIBLIOTECA
Dr. Manuel Belgrano

Lic. Marina ASSANDRI

Diciembre 2000

INDICE

INDICE 2

1. DESARROLLO DEL SISTEMA DE INFORMACIÓN Y CONTROL DEL MODELO DE COPARTICIPACIÓN INVERSA EN LA PROVINCIA DE CÓRDOBA. 4

1.1. INTRODUCCION AL TERCER INFORME PARCIAL 4

1.2. Objetivos de Sistema 6

1.3. Esquema General de funcionamiento del Sistema 7

1.4. Actores que participan del Sistema 8
1.4.1. Municipalidad 8
1.4.2. Contribuyentes 8
1.4.3. Provincia 8
1.4.4. Entes de recaudación y gestión 8
1.4.5. Banco de la Provincia de Córdoba 9

1.5. Arquitectura del Sistema 10
1.5.1. Introducción 10
1.5.2. Usos de la comunicación de datos 10
1.5.3. El Modelo Internet 11
1.5.3.1. El Modelo Cliente / Servidor 11
1.5.4. Arquitectura Física del Sistema 14
1.5.5. Arquitectura de Almacenamiento 16

1.6. Estructura lógica del Sistema 18
1.6.1. Relaciones externas del Sistema 18
1.6.2. Componentes internos del sistema 21
1.6.2.1. Subsistemas 21
1.6.2.2. Subsistema de mantenimiento de datos: 22
1.6.2.3. Subsistema de liquidación: 22
1.6.2.4. Subsistema de deuda: 23
1.6.2.5. Subsistema de notificación: 23
1.6.2.6. Subsistema de recaudación: 23
1.6.2.7. Subsistema de información al contribuyente: 24
1.6.2.8. Subsistemas de gestión y de control 24
1.6.2.9. Subsistema de seguridad y comunicación 24
1.6.2.10. Subsistema de Gestión de Base de Datos Distribuida 24
1.6.2.11. Cuadro de usuarios de los distintos subsistemas 26
1.6.3. Manual de Procedimientos 27
1.6.3.1. Solicitar Estado de Deuda 28
1.6.3.2. Solicitud de Financiación 31
1.6.3.3. Solicitar libre deuda 33
1.6.3.4. Recaudación 37
1.6.3.5. Solicitar Baja Bien 44
1.6.3.6. Solicitar Alta Bien 49
1.6.3.7. Liquidar Contribuciones 57
1.6.3.8. Emitir recibos de Pago 63
1.6.3.9. Generar y emitir Notificaciones o intimaciones de deuda 67
1.6.3.10. Bloqueo Masivo de Registros Cobro Vía Judicial 72

1.6.4. Equipo de Especialistas a cargo del Sistema 75

1.7. Seguridad y control 77
1.7.1. Seguridad en la Red 79
1.7.1.1. Cifrado 83
1.7.1.2. Controles de Hardware 86
1.7.1.3. Controles de seguridad en terminales: 89
1.7.1.4. Controles de los Circuitos 90
1.7.1.5. Controles de las Computadoras Personales 91
1.7.1.6. Controles de las bases de datos. 92
1.7.1.7. Controles de Protocolos 93
1.7.1.8. Controles de Administración: 96
1.7.1.9. Controles para recuperación / respaldo / desastres 97
1.7.1.10. Matriz de Controles 99

1. DESARROLLO DEL SISTEMA DE INFORMACIÓN Y CONTROL DEL MODELO DE COPARTICIPACIÓN INVERSA EN LA PROVINCIA DE CÓRDOBA.

1.1. INTRODUCCION AL TERCER INFORME PARCIAL

El presente trabajo que corresponde al tercer informe del estudio titulado "Sistema de Coparticipación Inversa entre los municipios y la Provincia de Córdoba" pretende, de acuerdo al cronograma de trabajo y al alcance acordado, presentar el desarrollo preliminar del sistema de información que administrará los procesos de ingreso de los impuestos y tasas municipales que se incluyan en el modelo de Coparticipación Inversa propuesto.

Cabe recordar que en el segundo informe se desarrollo el modelo teórico de funcionamiento que consistía fundamentalmente de la cesión de la gestión de cobro de los Impuestos Provinciales a los municipios a través de un mecanismo de coparticipación inversa que respetara los actuales niveles de recaudación de cada una de las jurisdicciones.

Se incorpora, a partir de la firma del "Pacto de Saneamiento de los Municipios de la Provincia de Córdoba", organismos en formación, creados por dicho pacto, denominados Entes de Recaudación y Gestión, que serán los depositarios de la responsabilidad de gestionar y procurar el cobro de las correspondientes liquidaciones tributarias.

Se propone, además, que sea el Banco de la Provincia de Córdoba el que se encargue del efectivo cobro de los tributos.

Para comenzar debemos realizar una distinción entre datos e información.

Los datos consisten en hechos y cifras que tienen relativamente poco significado para el usuario. Por ejemplo, los datos podrían ser el número de horas laboradas por cada empleado. Si procesamos estos datos, podríamos convertirlos en información. Si multiplicamos las horas que cada empleado trabajó por el sueldo que recibe por hora, el producto será sus ingresos brutos. Si sumamos las cifras correspondientes a los ingresos brutos de todos los empleados, obtendremos el importe total de la nómina de la institución. Este importe de nómina seria información para los niveles de decisión. La información consiste en datos procesados, o datos con significado.

Los comerciantes en antigüedades y los operadores de mercados callejeros suelen decir que "Los cachivaches de una persona son el tesoro de otra". Si aplicamos la misma lógica a los datos y la información, podríamos decir que "Los datos de una persona son la información de otra". Las cifras de ingresos brutos de los empleados de una institución ilustran lo anterior. Las cifras individuales son información para cada uno de los empleados. Cada cifra les dice cuánto ganaron la semana pasada. Para el dueño de la compañía, en cambio, esa cifra son datos. El funcionario quiere saber a cuanto asciende la nómina total de la institución y es preciso procesar las cifras individuales (los datos) para producir esa cantidad. La transformación de datos en información corre por cuenta de un procesador de información. El procesador de información es uno de los elementos claves del sistema conceptual. El procesador de

información puede incluir elementos computacionales, elementos no computacionales o alguna combinación de los dos.

En el caso del presente sistema la idea es que los *datos* sean ingresados en forma distribuida, es decir que cada uno de las instituciones que participan del sistema tenga la responsabilidad de mantener actualizados y confiables a los datos que el mismo genera y recepta; ya sea por cercanía con el contribuyente o por que son de generación propia.

Por el lado de la *información* se pretende que este disponible, de acuerdo a cada necesidad para todos los que intervienen en el proceso de percepción de impuestos, según el esquema que se desarrolla mas abajo, comenzando por el contribuyente y terminando por la Provincia.

Se debe aclarar que cuando se hace mención a la Provincia como una entidad participante del sistema, se incluye a los organismos pertinentes en la temática: el Ministerio de Finanzas, la Dirección Provincial de Rentas y la Dirección Provincial de Catastro.

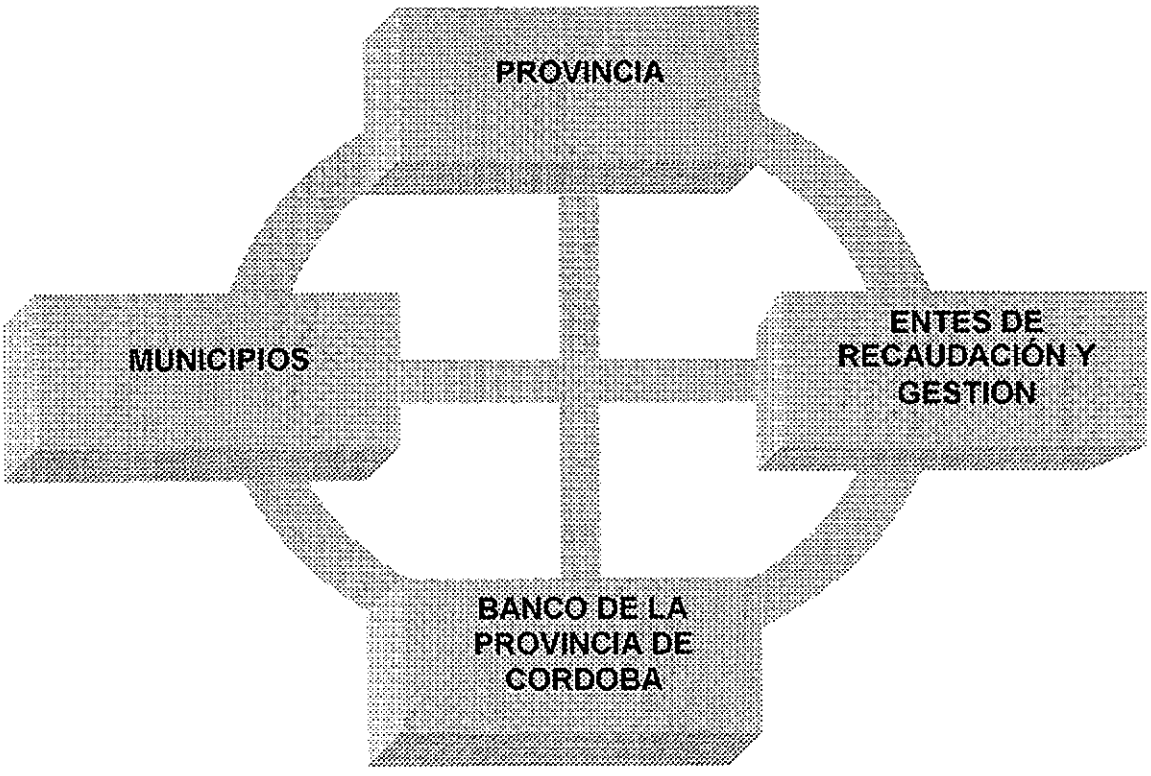
Es de destacar el rol que se le asigna a la Provincia dentro de este marco, siendo el de ente de control y rector de todo el sistema.

1.2. OBJETIVOS DE SISTEMA

Se plantean los siguientes objetivos:

- Mantener actualizada la información referida a la gestión completa de cobro de los tributos incluidos en el Sistema de Coparticipación Inversa.
- Brindar acceso, a los actores involucrados, a dicha información en tiempo y forma.
- Permitir por parte de las entidades participantes realizar las tareas de operación, gestión y control de todo el proceso de recaudación tributaria Provincial y Municipal.
- Permitir el acceso del contribuyente a su estado de cuenta para su tramitación y control.

1.3. ESQUEMA GENERAL DE FUNCIONAMIENTO DEL SISTEMA



El esquema propuesto pretende la participación de cuatro entidades que se dividirían funciones tomando provecho de las capacidades de cada una, tal y como se planteó en la etapa del modelo teórico y de diagnóstico del presente trabajo.

A fin de permitir un control cruzado y lograr la separación de funciones que se debe generar en todo sistema que administre dineros públicos, se prevé que quién mantenga los datos básicos para el cálculo del tributo, no sea quién sea responsable del cálculo y generación del mismo y procure su pago, mientras que este último no sea quién perfeccione el cobro.

Todos los actores se encontrarán comunicados permitiendo el acceso a la información en función de sus necesidades y atribuciones específicas de la manera que se desarrolla más adelante.

La comunicación planteada se realizará a través de una red informática desarrollada sobre Internet, a la vez que prevé un circuito de los documentos en soporte papel que darán validez legal a las operaciones y servirán de base para las tareas de control y auditoría.

Toda transacción será registrada en soporte papel o a través del sistema de firma digital permitiendo identificar al responsable de dicha transacción.

1.4. ACTORES QUE PARTICIPAN DEL SISTEMA

1.4.1. Municipalidad

En base a la características de cercanía y de mayor conocimiento de los cambios producidos por los contribuyentes en sus propiedades sujetas a impuestos.

Por otro lado existe una costumbre de parte de los contribuyentes de acercarse a las oficinas municipales a realizar los trámites.

Encargado del mantenimiento de la información referida a los contribuyentes y a los bienes sometidos a los tributos.

Toda modificación de datos básicos deberá ser autorizada por el Municipio, a fin de concentrar la responsabilidad de su integridad, estando sujeta a la inspección por parte de la Provincia.

1.4.2. Contribuyentes

Ya sea vía Internet o vía la tramitación personal, el contribuyente deberá poder realizar los siguientes trámites, en cualquiera de las oficinas provinciales, municipales o de los entes de recaudación y gestión cualquiera de los siguientes trámites:

- Solicitar estado de deuda.
- Solicitar refinanciaciones de deuda.
- Emitir comprobantes de pago.
- Solicitar altas, bajas o midificaciones de los datos referidos a sus bienes.
- Solicitar modificaciones de informaciónes referidas a sus datos personales.
- Formular cualquier tipo de reclamo.

La tramitación de dichos requerimientos se realizará por vía electrónica al organismo de competencia que recibirá una notificación electrónica de dicho pedido.

1.4.3. Provincia

Como organo rector y de control del modelo, deberá tener acceso a toda la información disponible en el sistema a fin de cumplir con dicho rol:

- Realizar inspecciones a los municipios y a los entes.
- Realizar auditorias contables e informáticas del sistema.

1.4.4. Entes de recaudación y gestión

Los entes serán los encargados, en base a la información provista por los municipios de realizar las siguientes tareas:

- Generar las liquidaciones de los tributos a su cargo.
- Emitir los recibos de pago.

- Mantener los estados de cuentas de los contribuyentes.
- Emitir la notificaciones de deuda e intimaciones de pago.
- Realizar la procuración del cobro por vía extrajudicial y/o judicial en los casos que esta facultad le haya sido delegada.
- Realizar el control de las rendiciones del banco.

Así como el Municipio será el responsable de mantener los datos básicos, fuente para la liquidación de los impuestos, los entes serán los únicos responsables del mantenimiento de los estados de cuenta y de la liquidación de los tributos, estando bajo la inspección de los organismos municipales y provinciales.

1.4.5. Banco de la Provincia de Córdoba

El banco será la entidad recaudadora por excelencia, debiendo preverse la posible incorporación de otras entidades financieras como entes recaudadores.

Entre las tareas que le corresponderán dentro del Sistema propuesto, se incluyen:

- Habilitar cajas para el cobro de los tributos.
- Realizar la distribución de fondos entre provincia y municipio. Esta tarea deberá ser automatizada dada la complejidad que supone el Modelo de Coparticipación Inversa.
- Acreditar en las respectivas cuentas Provinciales y Municipales.
- Enviar los talones de cobro, con listados resúmen y comprobantes de depósito.

1.5. ARQUITECTURA DEL SISTEMA

1.5.1. Introducción

Como ya sabemos, la comunicación de datos es el desplazamiento de información codificada de un punto a otro mediante sistemas de transmisión eléctricos u ópticos.

A tales sistemas se les denomina frecuentemente redes de comunicación de datos.

En general, estas redes se establecen para colectar datos provenientes de puntos remotos (por lo general terminales o microcomputadoras) y transmitir dichos datos a un punto central en el que se encuentra una computadora u otra terminal, o para realizar el proceso inverso, o alguna combinación de los dos.

Las redes de comunicación de datos facilitan el uso mas eficiente de las computadoras centrales y mejoran el control diario de los negocios al permitir un flujo de información más rápido.

También suministran servicios de conmutación de mensajes para hacer posible el intercambio de información entre terminales.

Mediante estas redes se logra un mejor y mas oportuno intercambio de datos entre usuarios, y el poder de las computadoras se pone a la disposición de más usuarios, siendo un objetivo central de este sistema poner a disposición de los contribuyentes información sobre sus estados de cuenta, por ejemplo.

Los objetivos de la mayoría de la red de comunicación de datos serán:

Reducir el tiempo y esfuerzo requeridos para realizar las diversas tareas operativas.

- Capturar los datos de contribuyentes en la fuente.
- Centralizar el control de los datos.
- Efectuar una rápida difusión de la información.
- Reducir el costo actual y futuro de la gestión de cobro.
- Apoyar la expansión de la capacidad de procesamiento con un incremento razonable en los costos, conforme crece el sistema.
- Apoyar los objetivos gubernamentales al centralizar o descentralizar sistemas de computo.
- Apoyar un mejor control administrativo de la recaudación.

1.5.2. Usos de la comunicación de datos.

Algunas de las características mas importantes detectadas en el relevamiento del Sistema que conducen a la necesidad de implementar una red de comunicación de datos eficiente son:

- Utilización extensiva de computadoras personales.
- Dispersión geográfica de los usuarios.
- Alto volumen de datos.
- Operaciones descentralizadas.
- Alto volumen de correo Inter-reparticiones, servicio de mensajería

- Oeraciones repetitivas en papel, como recreación o copiado de información
- Necesidad de actualización inmediata de la información en uso.
- Necesidad de celeridad y oportunidad de las funciones de las reparticiones.

1.5.3. El Modelo Internet

1.5.3.1. El Modelo Cliente / Servidor

Se propone la aplicación de un sistema cliente-servidor con replicación de los servidores de aplicaciones y de datos en cada una de las reparticiones, previendo la posibilidad de utilizar un servidor remoto en caso de caerse el servidor local en alguna repartición.

En toda comunicación entre dos computadoras existen varios esquemas de funcionamiento. Una comunicación entre computadoras no es mas que un intercambio de información, que, generalmente, suele ser bidireccional.

Estas formas de comunicación pueden seguir varios esquemas como son el jerárquico, el maestro/esclavo o el cliente/servidor.

Estos esquemas definen de forma genérica el modo en el que se intercambia la información.

Asi, por ejemplo, en un esquema jerárquico la transmisión de la información atraviesa los niveles de la jerarquía de menor a mayor, para después volver a descender en el árbol que la define hasta encontrar el nodo de destino. En un esquema maestro/esclavo, el comunicante, que actúa como esclavo, tiene que seguir los parámetros y momentos de la comunicación que impone el maestro.

Internet y, en general, las redes de comunicación modernas, utilizan el modelo cliente/servidor, que es el que se propone como solución para el Sistema motivo del presente.

El modelo cliente/servidor se basa en la asignación de roles a entidades que participan en la comunicación de manera que uno pide información (cliente) y el otro sirve (servidor), tal como a continuación se describe:

Cliente: es la maquina que solicita la comunicación. El que dicha máquina solicite la comunicación quiere decir que vaya a ser la destinataria de la misma ya que ésta es bidireccional y, por tanto, la información puede fluir en cualquier sentido. De todas formas, lo habitual es que la maquina cliente sea la que reciba la información.

Servidor: es el receptor de la solicitud de comunicación. Los servidores se caracterizan por tener unos programas en funcionamiento continuo denominados servicios o demonios, en función del sistema operativo del que se trate. Estos demonios (la palabra demonio viene acuñada del termino daemon utilizado por los sistemas operativos UNIX, aunque hay sistemas operativos como Windows que hablan de servicios por simplificar se utilizará la palabra demonio que es menos común que servicio y, por tanto, identifica mejor la funcionalidad descrita en los servidores) están "escuchando" constantemente por si hubiera peticiones de comunicación por parte de clientes. Se trata, pues, de un sistema de comunicación asíncrono donde un cliente puede solicitar el inicio de una comunicación en cualquier momento y el servidor

(teóricamente) está siempre en disposición de responder a la comunicación de cualquier cliente. Esto se producirá siempre que el servidor disponga de los servicios que el cliente solicita, ya que todos los servidores no contienen todos los servicios.

De cualquier manera las definiciones que se han dado con anterioridad deben ser matizadas para el modelo de Internet y para otros modelos de comunicación. En muchos tipos de protocolos de red las computadoras que desempeñan la misión de servidor tienen exclusivamente ese papel, al igual que ocurre con las maquinas que son clientes.

En el modelo de Internet esto no ocurre así y una computadora, que en un momento dado solicita una comunicación y, por tanto, desempeña el rol de cliente, puede desempeñar la función de servidor posteriormente cuando recibe una solicitud de inicio de comunicación. Para ellos es suficiente que tenga un demonio escuchando la solicitud de un servicio por parte de cualquier cliente. De cualquier manera, la posibilidad de actuar como servidor exige ciertos requerimientos en el sistema operativo, como, por ejemplo, la capacidad de realizar multiproceso.

En el caso del cliente, las exigencias para el sistema operativo son mucho menores y prácticamente es suficiente con disponer del protocolo de comunicaciones. En la actualidad suele ser un componente estándar de los sistemas operativos y los programas clientes, en muchas ocasiones se proporcionan directamente, o en su defecto, son de distribución publica como ocurre con los navegadores de World Wide Web.

Se puede decir que el servidor es una maquina más compleja, que tiene que estar constantemente escuchando la solicitud de clientes hacia cualquiera de los servicios que puede proporcionar. Cada servicio exigirá de la presencia de un demonio escuchando la llegada de posibles solicitudes de ese servicio.

A los fines de intentar una clasificación de las redes se utilizará la siguiente:

Intranet: Es la red interna, privada y segura de una organización, utilice o no medios de transporte de terceros.

Extranet: Es una red privada y segura, compartida por un conjunto de organismos, aunque utilice medios de transporte ajenos e inseguros, como pudiera ser Internet.

Internet: Es la red de redes, "metared" a donde se conecta cualquier red que se desee abrir al exterior, pública e insegura, de alcance mundial, donde puede comunicar cualquier pareja o conjunto de interlocutores, dotada además de todo tipo de servicios de valor añadido.

Un dispositivo especificamente dedicado a la protección de una Intranet ante una Extranet, y fundamentalmente ante Internet, es el cortafuegos (Firewall). Esta es una máquina dedicada en exclusiva a leer cada paquete que entra o sale de una red para permitir su paso o desecharlo directamente. Esta autorización o rechazo está basada en unas tablas que identifican, para cada pareja de interlocutores (bien sea basado en el tipo de interlocutor o inclusive en su identificación individual) los tipos de servicio que pueden ser establecidos. Para llevar a cabo su misión, existen diversas configuraciones, donde se pueden incluir encaminadores (routers), servidores de proximidad (proxy), zonas desmilitarizadas, bastiones y demás parafernalina, a veces copiada de modelos militares.

Para proteger la red interna "Intranet" del exterior se utilizará el esquema expuesto en la figura, o bien variaciones del mismo.

Se parte de la base de que la información que viaja entre la Intranet y el exterior ha de atravesar la "zona desmilitarizada" (DMZ de sus siglas inglesas), pasando por dos encaminadores.

Un encaminador protege los accesos desde la zona desmilitarizada hacia la Intranet (encaminador interno). En la zona desmilitarizada se instalarán aquellos servicios a los que haya que acceder desde el exterior y desde el interior, en una máquina especialmente segura, denominada bastión, que debe ser dedicada exclusivamente a este fin.

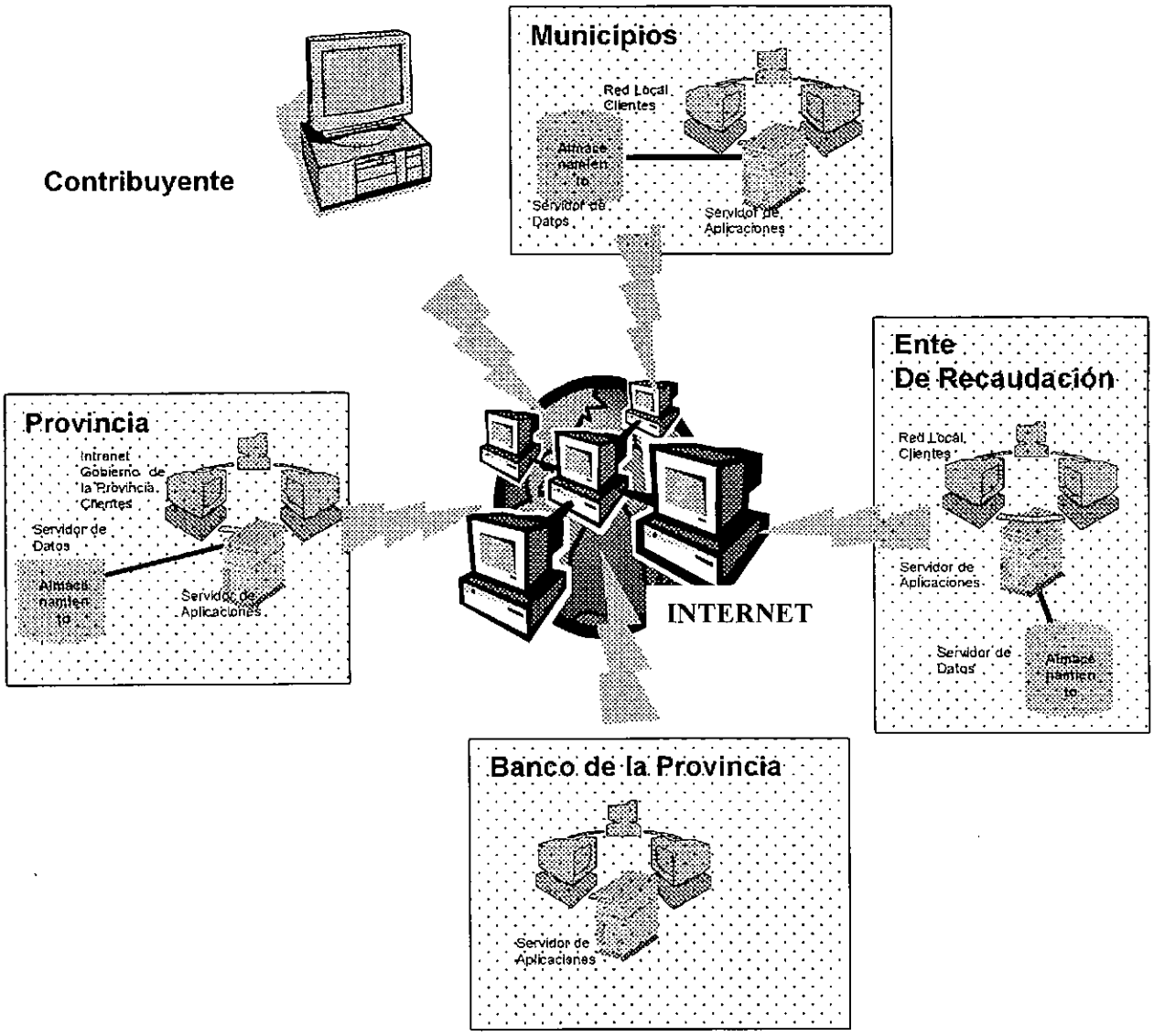
Por ejemplo, un servidor proxy accede a un servidor Internet, recuperando la información que haya solicitado un usuario interno, y almacenándola para que pueda ser recuperada desde la Intranet.

Del mismo modo, el correo electrónico podrá recibirse en un servidor instalado en la zona desmilitarizada y reexpedirse hacia el interior. El objetivo es evitar establecer sesiones directas entre una maquina Intranet y una máquina externa.

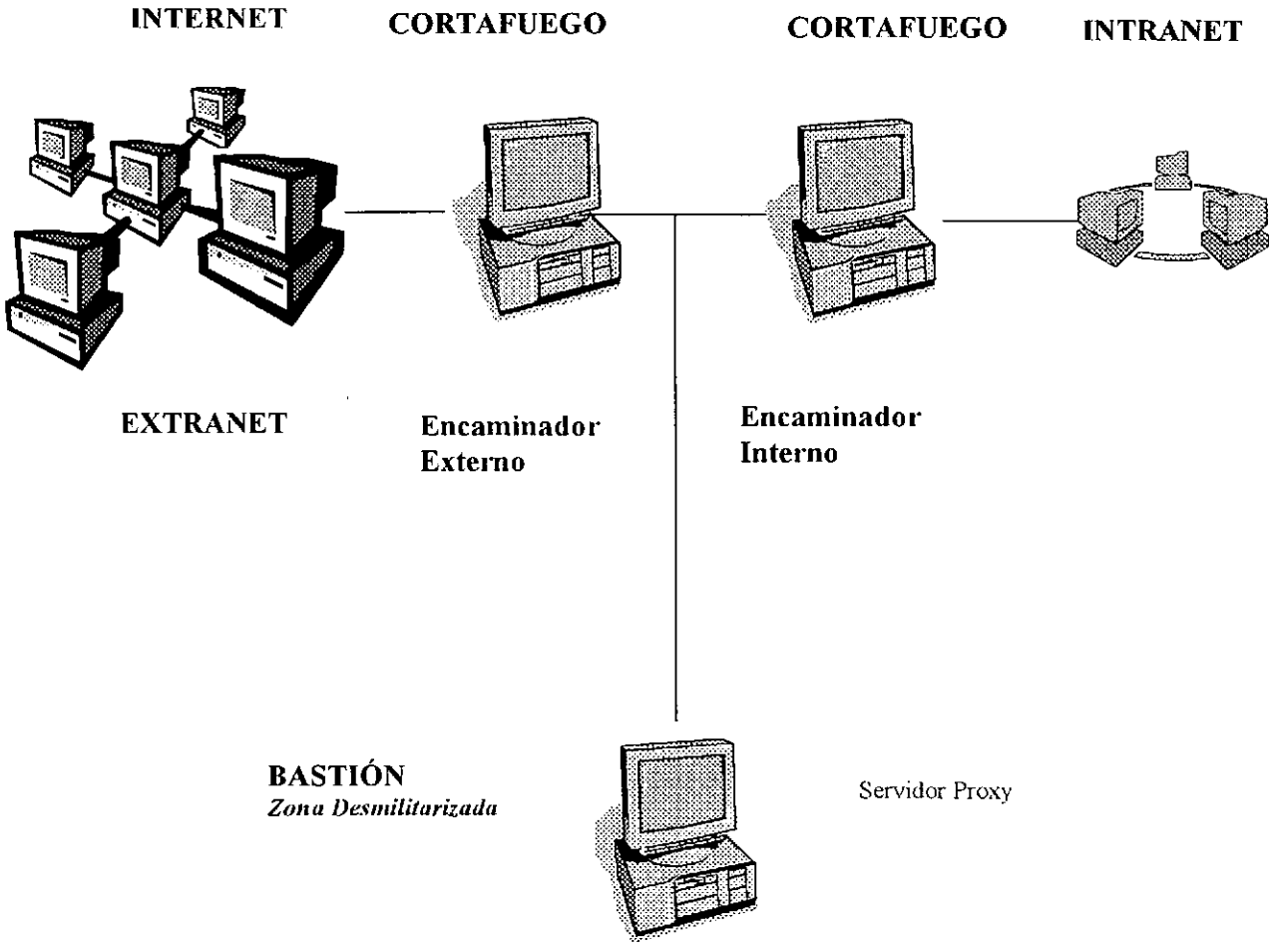
Los encaminadores impedirán que se establezcan conexiones de este tipo, salvo aquellas que específicamente se determinen. El encaminador externo solo permitirá que atraviese trafico autorizado entre el exterior y el bastión, y el encaminador interno hará lo propio con el trafico entre el bastión y la red interna.

Para este sistema se propone la instalación de una extranet que conecte la intranets de cada una de la reparticiones y organismos a vincular.

1.5.4. Arquitectura Física del Sistema

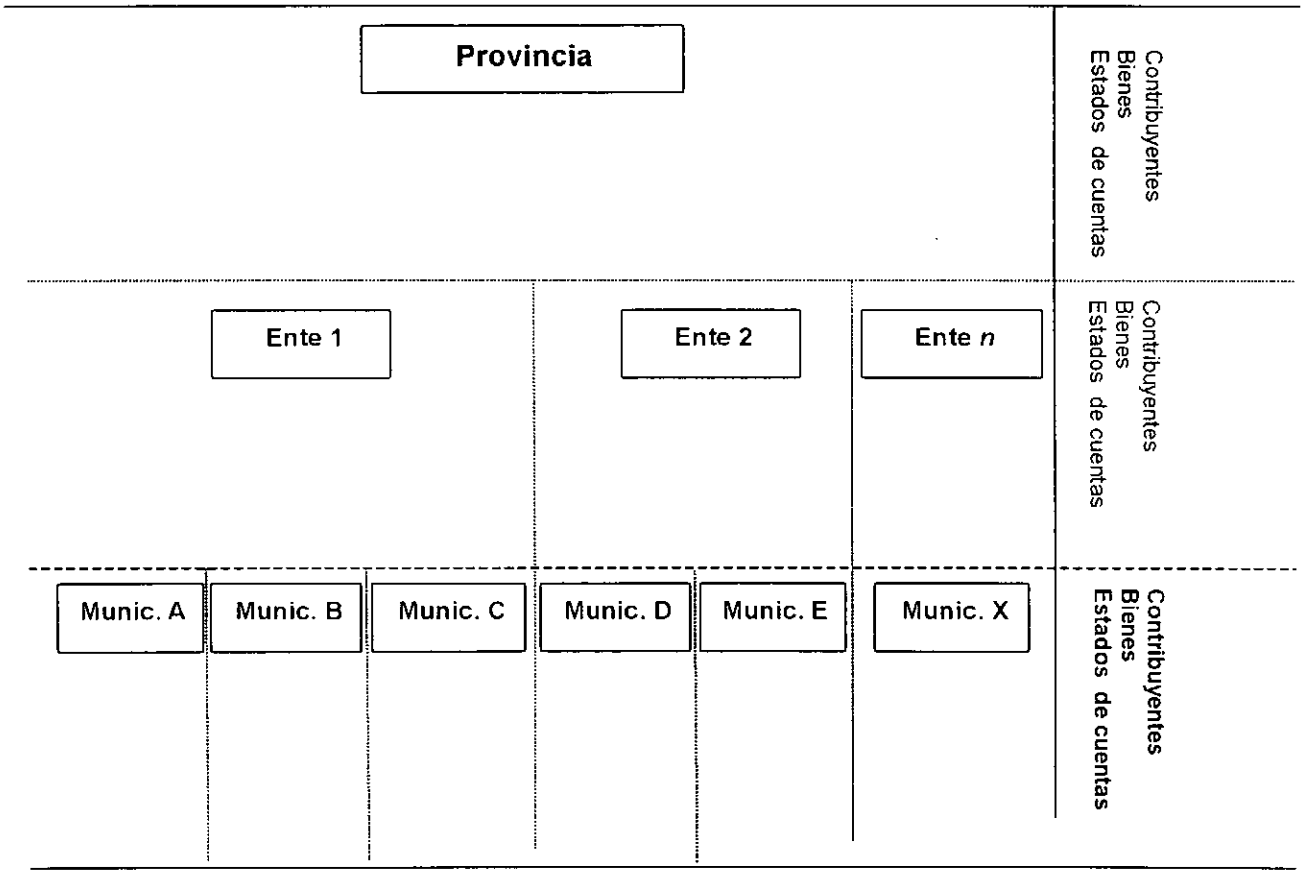


Se propone una arquitectura distribuida que interconecta, a través del soporte Internet, las distintas redes locales de la reparticiones que tienen acceso al mismo.



1.5.5. Arquitectura de Almacenamiento

A continuación se presente un cuadro con el modelo de almacenamiento propuesto:



Se plantea un esquema de Bases de Datos distribuida con copias de resguardo y consulta en cada nivel y superior.

Motiva la elección de esta arquitectura de almacenamiento razones de velocidad de acceso y procesamiento, por ejemplo, si la Provincia desea efectuar un proceso sobre todos los datos provinciales a fin de obtener indicadores de gestión, sería muy lento, sino imposible, intentar el rescate de los datos básicos de todos los municipios.

Otra de las razones es la de seguridad, ya que permitiría tener resguardos de información permanente por cualquier problema que pudiera surgir con algunos de los almacenamientos, esto permitiría que ante la caída de cualquiera de los servidores de datos de cualquier nodo del sistema, todas las oficinas podrían seguir trabajando mediante enlaces remotos a otro nodo.

En cada municipio se almacenará información referida a los contribuyentes y sus estados de deuda de su jurisdicción, contando con una base de datos en cada municipio.

Los Entes por su parte almacenarán la misma información pero referida a todos los municipios servidos por dicho Ente.

Por último la Provincia tendrá su Base de Datos general con información sobre todos los contribuyentes de la provincia.

La modificación de un dato por parte de alguno de los actores, traerá aparejada la actualización de ese dato en los otros almacenamientos de los diferentes niveles, ya on-line o mediante procesamiento diferido por lotes, según la calidad del vínculo y el volumen transportado.

Para ello será necesario contar con un software middleware que se encargue de sincronizar las actualizaciones y que realice un control de inconsistencias permanente.

En cuanto a la clave de los contribuyentes esta deberá ser única para todos los registros vinculados a dicho contribuyente, se propone adoptar el DNI para personas físicos y el CUIT para personas jurídicas.

En cada recibo de pago emitido por el ente se deberá consignar la distribución del monto entre la Provincia y el Municipio, esto se podría codificar en soporte óptico de modo que el banco sepa cuanto depositar para la provincia y cuanto para el municipio o bien se encuentre conectado on-line con el ente emisor para consultar la base de recibos.

1.6. ESTRUCTURA LÓGICA DEL SISTEMA

1.6.1. Relaciones externas del Sistema

A continuación se incluye el listado de las operaciones que se genera en cada uno de los organismos que participan del sistema.

Contribuyente

- Solicitar estado de deuda.
- Abonar una deuda.
- Solicitar alta de un bien.
- Solicitar baja de un bien.
- Solicitar modificación de datos de un bien.
- Solicitar transferencia de un bien.
- Solicitar Libre-Deuda.
- Solicitar refinanciaciones.
- Efectuar reclamos varios.

Municipio

- Dar de alta un contribuyente (se deberá consultar en la base de la Provincia para cerciorarse que ese contribuyente no exista en otra jurisdicción)
- Modificar datos de un contribuyente.
- Dar de alta un bien
- Dar de baja un bien
- Modificar datos de un bien.
- Transferir un bien.
- Ingresar pagos recibidos desde el Banco.

Provincia

- Ingresar pagos recibidos desde el Banco.
- Controlar concordancia entre registros de pagos, depósitos en la cuenta y talones de pago.
- Controlar liquidación y distribución.
- Controlar consistencia de datos básicos.

Banco

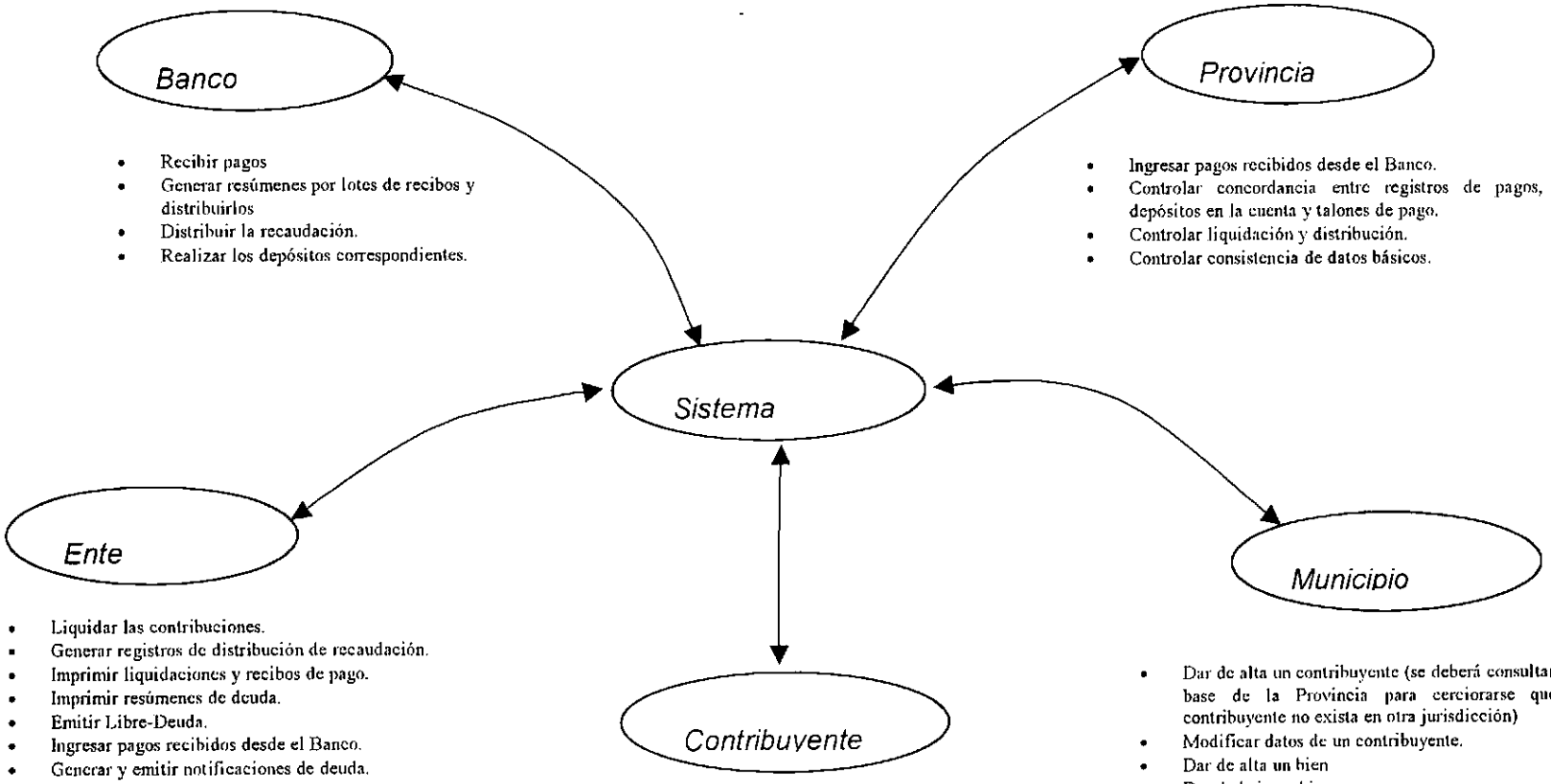
- Recibir pagos
- Generar resúmenes por lotes de recibos y distribuirlos
- Distribuir la recaudación.
- Realizar los depósitos correspondientes.

Ente de Recaudación y Gestión

- Liquidar las contribuciones.
- Generar registros de distribución de recaudación.
- Imprimir liquidaciones y recibos de pago.
- Imprimir resúmenes de deuda.
- Emitir Libre-Deuda.
- Ingresar pagos recibidos desde el Banco.

- Generar y emitir notificaciones de deuda.
- Generar y emitir intimaciones de deuda.
- Bloquear registros de deuda por paso a Área de Cobro Vía Judicial
- Generar y emitir refinanciaciones de deudas

Relaciones Externas del Sistema



- Recibir pagos
- Generar resúmenes por lotes de recibos y distribuirlos
- Distribuir la recaudación.
- Realizar los depósitos correspondientes.

- Ingresar pagos recibidos desde el Banco.
- Controlar concordancia entre registros de pagos, depósitos en la cuenta y talones de pago.
- Controlar liquidación y distribución.
- Controlar consistencia de datos básicos.

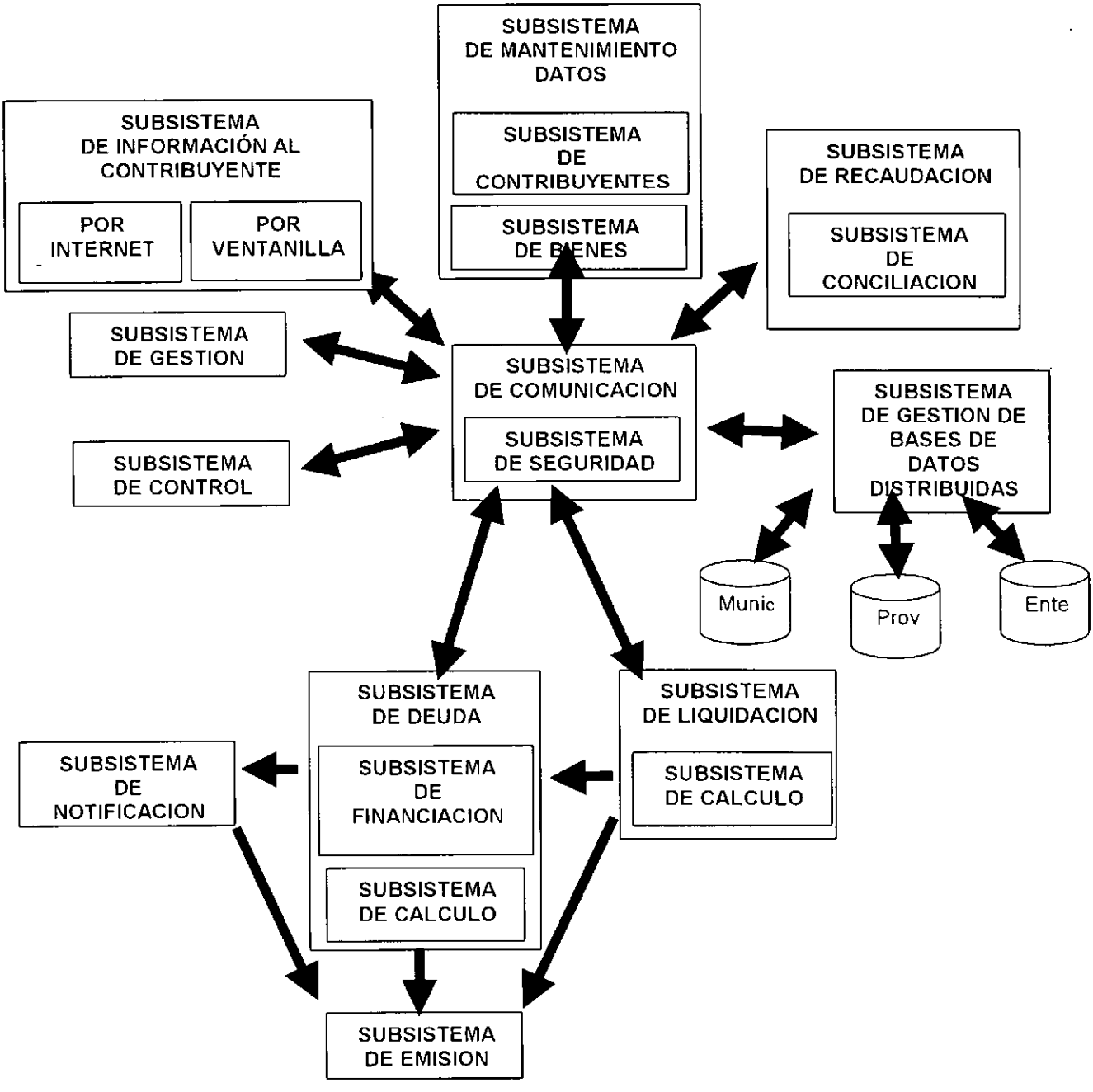
- Liquidar las contribuciones.
- Generar registros de distribución de recaudación.
- Imprimir liquidaciones y recibos de pago.
- Imprimir resúmenes de deuda.
- Emitir Libre-Deuda.
- Ingresar pagos recibidos desde el Banco.
- Generar y emitir notificaciones de deuda.
- Generar y emitir intimaciones de deuda.
- Bloquear registros de deuda por paso a Área de Cobro Vía Judicial
- Generar y emitir refinanciaciones de deudas

- Solicitar estado de deuda.
- Abonar una deuda.
- Solicitar alta de un bien.
- Solicitar baja de un bien.
- Solicitar modificación de datos de un bien.
- Solicitar transferencia de un bien.
- Solicitar Libre-Deuda.
- Solicitar refinanciaciones.
- Efectuar reclamos varios

- Dar de alta un contribuyente (se deberá consultar en la base de la Provincia para cerciorarse que ese contribuyente no exista en otra jurisdicción)
- Modificar datos de un contribuyente.
- Dar de alta un bien
- Dar de baja un bien
- Modificar datos de un bien.
- Transferir un bien.
- Ingresar pagos recibidos desde el Banco.

1.6.2. Componentes internos del sistema

1.6.2.1. Subsistemas



El sistema se compone de varios subsistemas que se tienen a su cargo la gestión completa de todas las operaciones vinculadas al proceso de recaudación, su control e información.

Los subsistemas y sus relaciones se encuentran esquematizados en la en la figura de arriba y son:

1.6.2.2. Subsistema de mantenimiento de datos:

Los datos básicos que se utilizan para el cálculo de los tributos se pueden dividir en dos categorías: los referidos a los contribuyentes y los referidos a los bienes sujetos a tributos.

El concepto de bienes a los fines del presente se refiere a aquellos objetos u entidades que constituyen la base imponible de los tributos y tasa a liquidar, por ej: automotores, comercios, inmuebles, etc.

Es posible asignarle a cada tributo un bien asociado, aun cuando este no sea bien en el sentido estricto de la palabra, según esto un bien podría ser una persona física o jurídica objeto de una multa.

Cada tributo se calcula en base a datos asociados al bien, por ejemplo en el caso de automotores, se calcula en base a la marca y modelo del móvil, entre otros; el impuesto inmobiliario se calcula en base a la valuación del inmueble como la suma del valor del terreno mas la valuación de las mejoras realizadas, según la ubicación del mismo y otros datos adicionales.

El mantenimiento de los datos referidos a los bienes será administrado por el subsistema de bienes.

El otro elemento que completa la liquidación del tributo es el contribuyente, que es quién se responsabiliza por el pago del mismo asumiendo la deuda generada. Del contribuyente se debe registrar información suficiente para individualizarlo de manera fehaciente y para ubicarlo (domicilio) para enviarle comunicaciones, otros datos importantes de registrar son aquellos que le permitirían acceder a algún tipo de exención por algún régimen especial.

Un contribuyente puede tener varios bienes, en distintas jurisdicciones, sujetas a tributación, por lo que es base en la conformación de este sistema que el contribuyente posea una única clave de identificación asociada a todos sus bienes y demás operaciones que efectúe, esta será DNI o pasaporte para personas físicas y CUIT para las jurídicas.

El mantenimiento de los datos referidos a los contribuyentes será administrado por el subsistema de contribuyentes.

La operación y mantenimiento de los subsistemas de mantenimiento de datos será responsabilidad de los municipios.

1.6.2.3. Subsistema de liquidación:

Este subsistema será el encargado de realizar la selección, cálculo y generación de la liquidaciones de los distintos vencimientos que operen en los tributos según el cronograma fijado por las autoridades de aplicación. Se deberá prever la generación de recibos por pago contado.

Uno de los problemas mas difíciles de solucionar en la liquidación de tributos es la movilidad frecuente en el tiempo de las formas y métodos de calculo de los tributos, según la dinámica impuesta por los órganos legislativos año tras año.

Para ello se deberá instalar un motor de cálculo parametrizable con registro histórico de las formas de cálculo para el cálculo retroactivo de tributos.

Dicho motor de cálculo configura un subsistema dentro del de liquidación.

El subsistema de liquidación permitirá la realización del proceso por lotes de bienes según parámetros de selección variados.

El motor de cálculo, según el modelo de coparticipación inversa, será el encargado de realizar el cálculo de la distribución entre municipio y provincia de lo liquidado.

1.6.2.4. Subsistema de deuda:

Encargado del mantenimiento de los registros de deuda, llevando el estado de cuenta por bien y por contribuyente.

Este subsistema constituye el corazón del sistema ya que registra los compromisos pagados, por vencer, vencidos, en procuración y/o financiados de cada bien.

Cuenta con dos subsistemas; el primero de cálculo, encargado de determinar intereses, recargos, punitorios, etc., mientras que el segundo de financiación, encargado de generar los registros de financiación, preparando la emisión de las chequeras de pago, modificando el estado de los registros de deuda refinanciados.

1.6.2.5. Subsistema de notificación:

Funcionará en estrecha relación con el Subsistema de deuda, y estará a cargo de preparar la emisión de las notificaciones o intimaciones por falta de pago según criterios indicados por el usuario.

Deberá prever la posibilidad de ingresar las novedades remitidas por el correo o agente de distribución en cuanto a la recepción o no de las notificaciones emitidas a fin de poder ser consultados a requerimiento de la asesoría legal.

Los organismos que manejará este sistema serán los Entes de Recaudación y Gestión.

1.6.2.6. Subsistema de recaudación:

Será el encargado de recibir la información referida a la recaudación enviada por el Banco recaudador.

La tarea del subsistema comenzará con la recepción del pago, por parte del Banco, del contribuyente , generando la extinción de la obligación y el registro de la misma.

Con los pagos recibidos el Banco informará al sistema de la confección de lotes de rendición, origen de los depósitos a las cuentas de la Municipalidad y la Provincia, a partir de las discriminaciones efectuadas al momento de la liquidación.

La remisión de los lotes y los respectivos resúmenes permitirán realizar la tarea de conciliación.

Comprenderá un sistema de conciliación que permitirá controlar en forma fehaciente la rendición efectuada por el Banco contra la imputación de pagos, según el subsistema de deuda.

1.6.2.7. Subsistema de información al contribuyente:

Este subsistema fue ideado con la finalidad de proveer al contribuyente de la información sobre sus datos y sobre su estado de cuentas y permitirle realizar algunos trámites y autogenerarse los recibos de pago.

El susbsistema se divide en dos modalidades que definen a su vez dos subsistemas.

La consulta por vía de una conexión a un site en Internet donde mediante una identificación y una palabra clave, estará a cargo del subsistema de consulta por Internet, el que deberá administrar los accesos y proveer la información al usuario en línea. Permitirá, además, la impresión de los recibos por parte del usuario.

Será a su vez un sistema de mensajería desde el contribuyente a las reparticiones debiendo establecer las rutas para la derivación de los mensajes de manera inteligente.

El subsistema de consulta por ventanilla será provisto a los puesto de atención al público de la Provincia, el Municipio y el Ente de Gestión y Recaudación correspondientes, a fin de que los contribuyentes que no utilicen Internet puedan realizar las consultas en las bocas de atención de las reparticiones.

1.6.2.8. Subsistemas de gestión y de control

Serán subsistemas de información a disposición de las Municipalidades y de la Provincia que a través de software de DataWarehousing y de Data Mining (Minería de Datos) permitirán por un lado a los funcionarios a cargo de tomar decisiones contar con la información sobre el estado de la recaudación de manera organizada, sistematizada y actualizada según sus necesidades.

Por otro lado permitirá a los auditores y a sus equipos de trabajo el acceso a las bases de datos históricas, a los registros de transacciones, a los diarios de accesos, en definitiva a todos los registros de información que se almacenan para definir el control sobre los diferentes elementos sujetos a auditoría.

1.6.2.9. Subsistema de seguridad y comunicación

El subsistema de comunicación tendrá la tarea de mantener las comunicaciones entre los distintos elementos de la red, generando los reportes de tráfico, controles de errores, etc., tal como se describe mas adelante en la parte de seguridad y control.

El subsistema de seguridad será el encargado de mantener el cifrado de las comunicaciones, controlar el acceso de conexión, controlar los accesos a las bases de datos y aplicaciones y de generar los archivos de auditoría de todo el sistema.

1.6.2.10. Subsistema de Gestión de Base de Datos Distribuida.

Tal como se planteó, se pretende lograr un replicación de los datos de manera distribuida, siendo este subsistema el encargado del mantenimiento de la consistencia de los datos en sus diversas ubicaciones físicas, administrando el control de transacciones,

detectando inconsistencia generadas por fallos. Será el encargado de realizar, además, la administración de la actualizaciones de información y del control de acceso a los datos según autorizaciones dispuestas por el Administrador.

1.6.2.11. Cuadro de usuarios de los distintos subsistemas

SUSBSISTEMA	USUARIO				
	Municipio	Provincia	Ente	B.P.C.	Contribuyente
MANTENIMIENTO DE DATOS	O				
CONTRIBUYENTES	O				
BIENES	O				
INFORMACIÓN AL CONTRIBUYENTE	O	O	O		O
POR INTERNET					O
POR VENTANILLA	O	O	O		
RECAUDACIÓN			O	O	
CONCILIACIÓN			O		
GESTION DE BASE DE DATOS	O	O	O		
COMUNICACIÓN	O	O	O	O	
SEGURIDAD	O	O	O	O	O
GESTION	O	O			
CONTROL	O	O			
LIQUIDACIÓN			O		
CALCULO			O		
DEUDA			O		
FINANCIACION			O		
NOTIFICACION			O		

1.6.3. Manual de Procedimientos

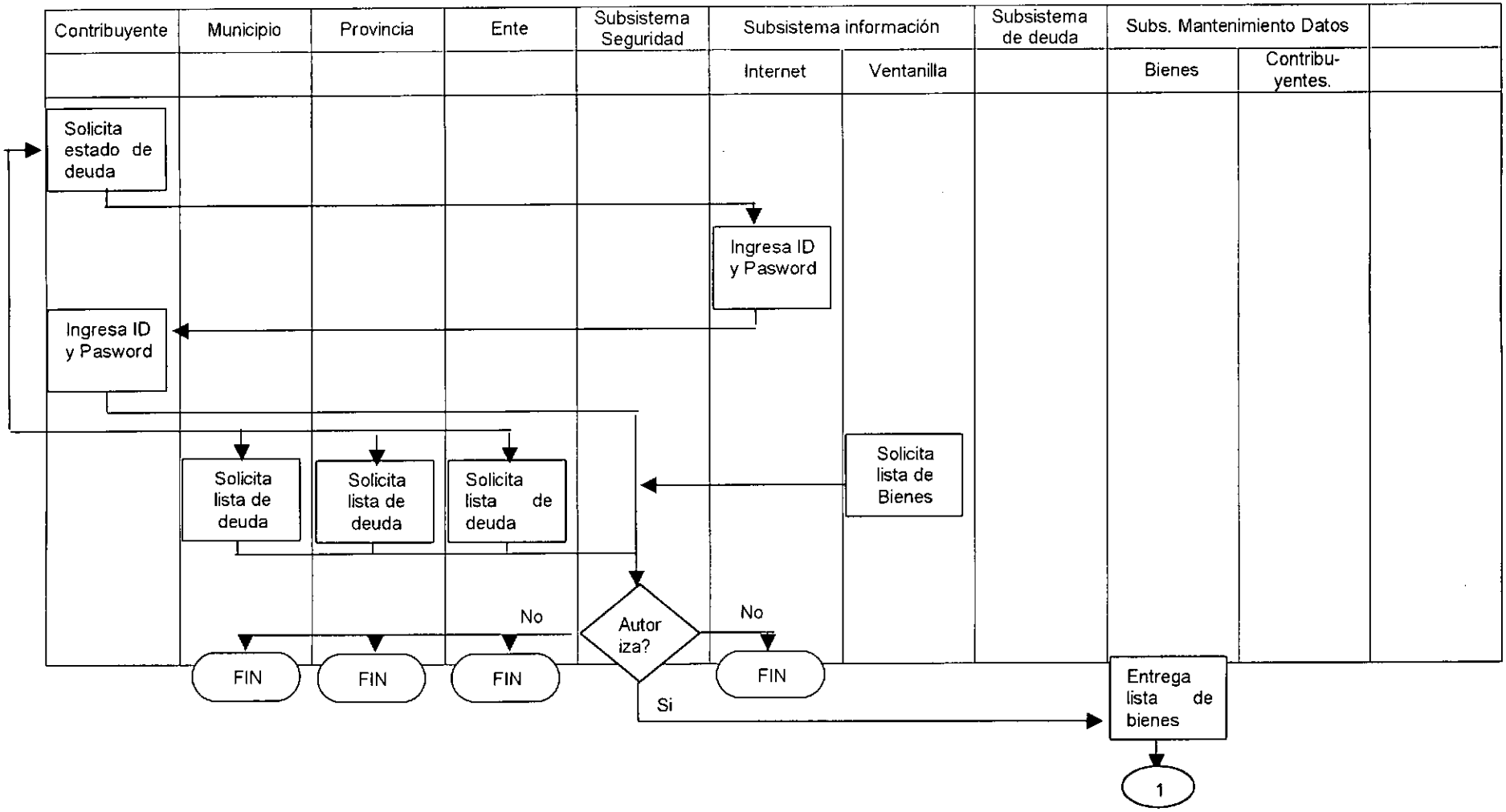
A continuación se incluyen los esquemas de procedimientos de las operaciones mas significativas del sistemas.

Dichos esquemas se inscriben dentro del alcance del presente trabajo, los que deberán ser ajustado al momento de la generación del sistema en forma definitiva, no obstante consideramos que a partir del relevamiento de las operaciones y procedimientos mas usuales se ha logrado una aproximación importante a los distintos procedimientos que se deberían implementar dentro del sistema.

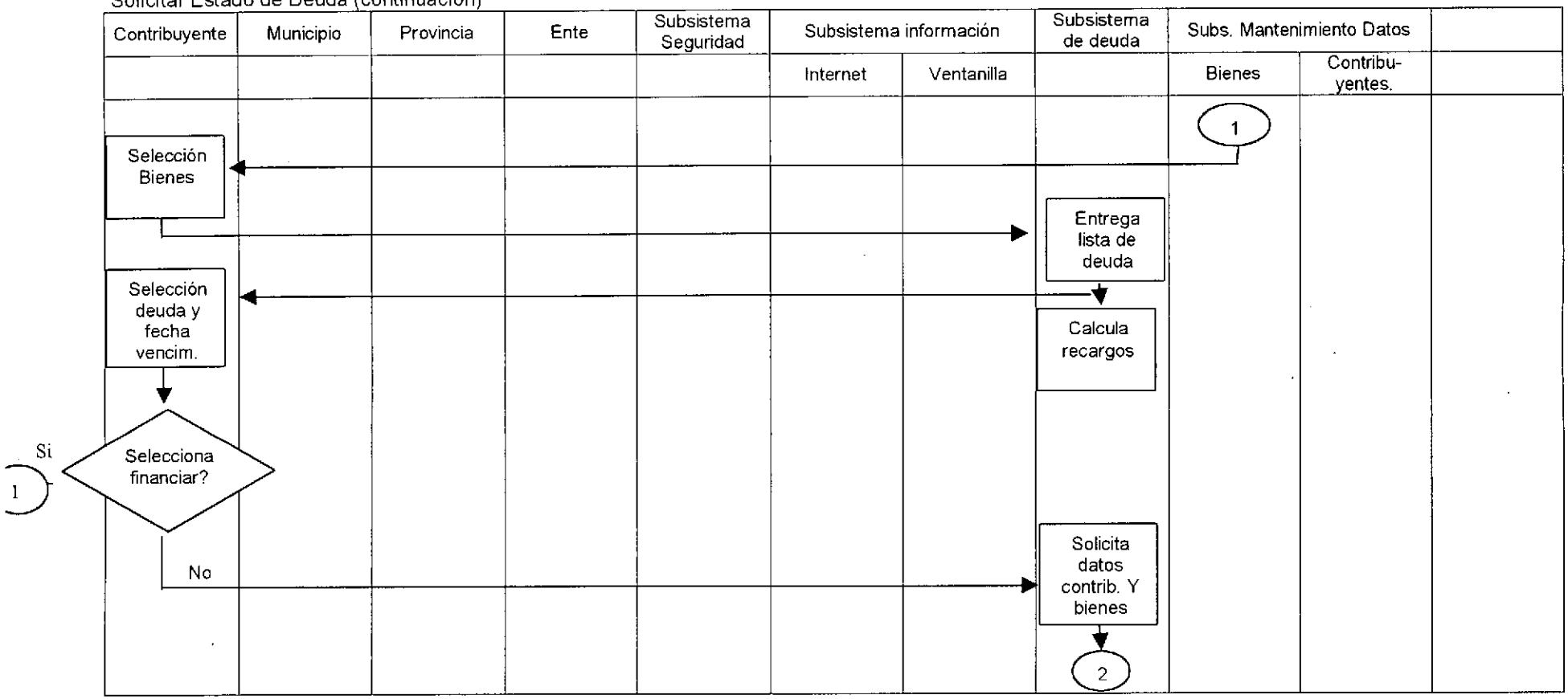
Es de destacar que se han incluido tanto los componentes externos como externos del sistema, a fin de lograr una visión completo de los procesos descritos.

En cuanto a la simbología empleada, se ha optado por los gráficos estándar para este tipo de representación, con el objeto de lograr esquemas autoexplicativos y de fácil comprensión

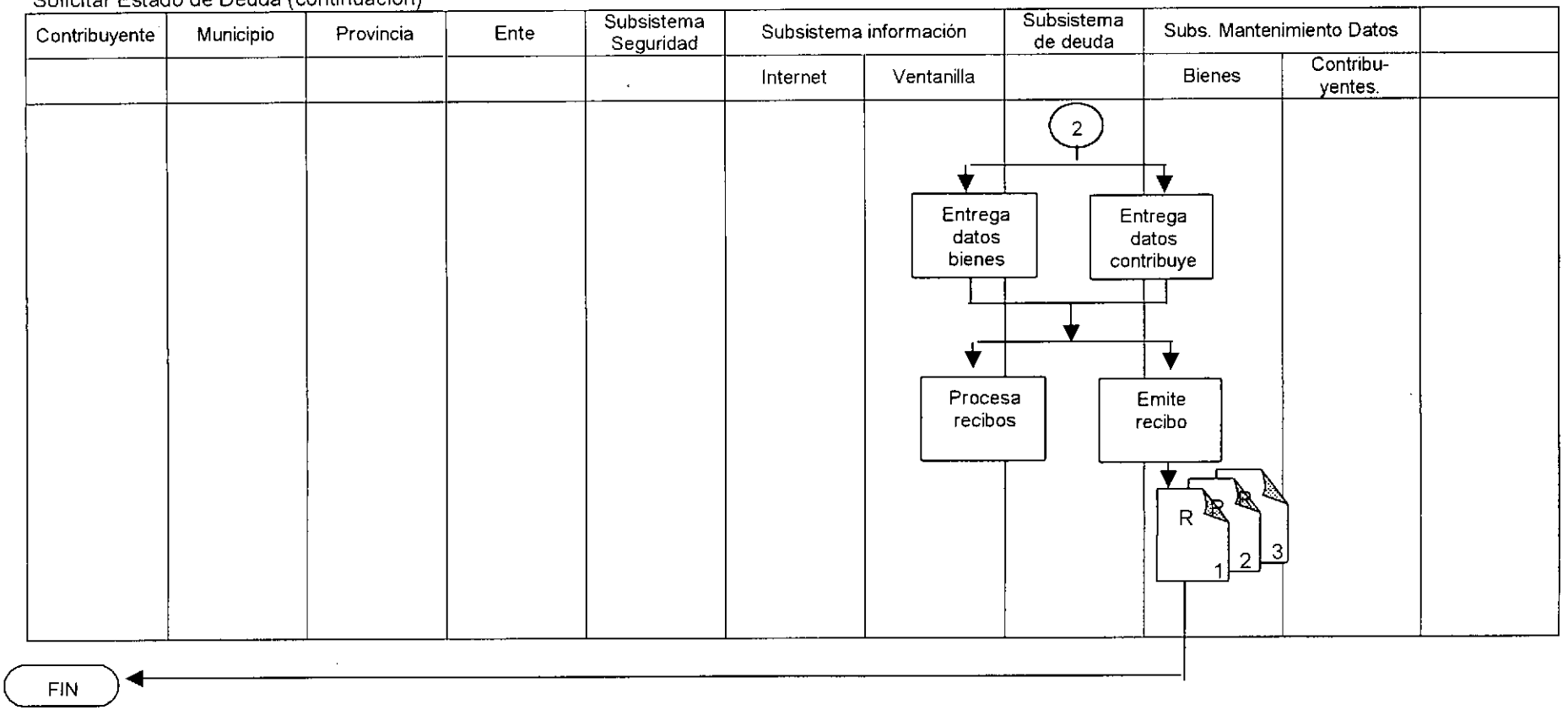
1.6.3.1. Solicitar Estado de Deuda



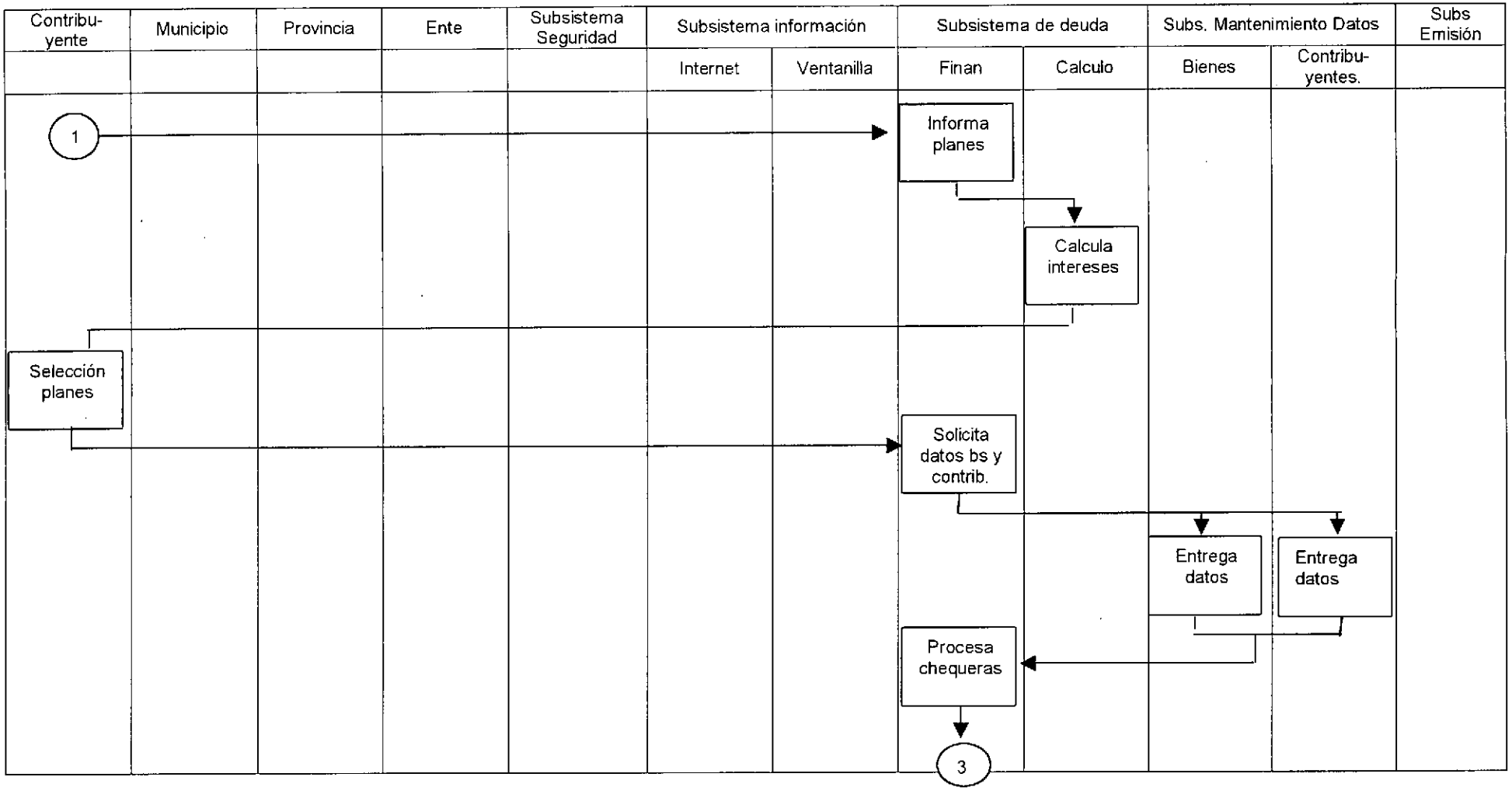
Solicitar Estado de Deuda (continuación)



Solicitar Estado de Deuda (continuación)

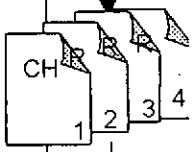


1.6.3.2. Solicitud de Financiación

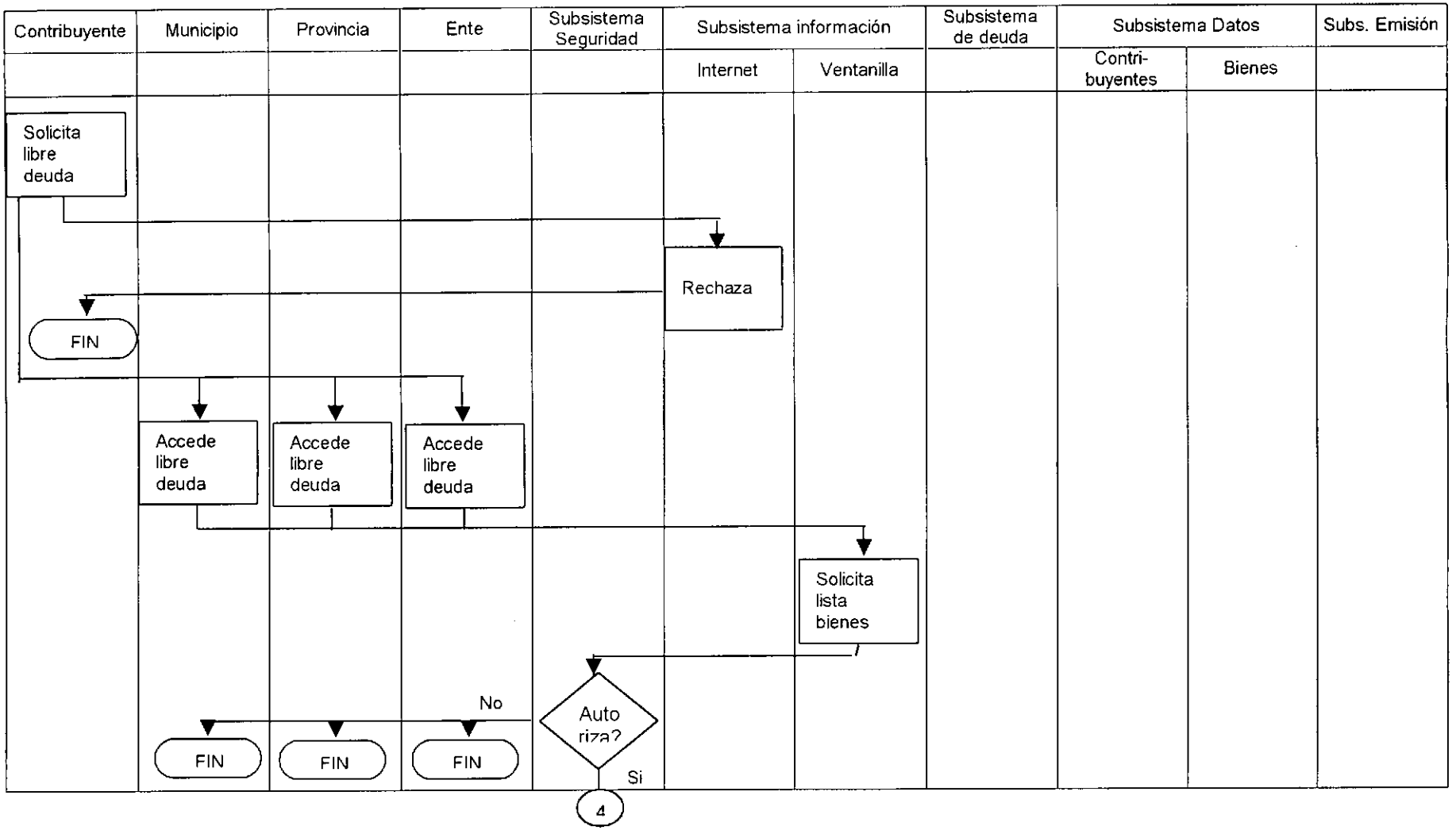


Solicitud de Financiación (continuación)

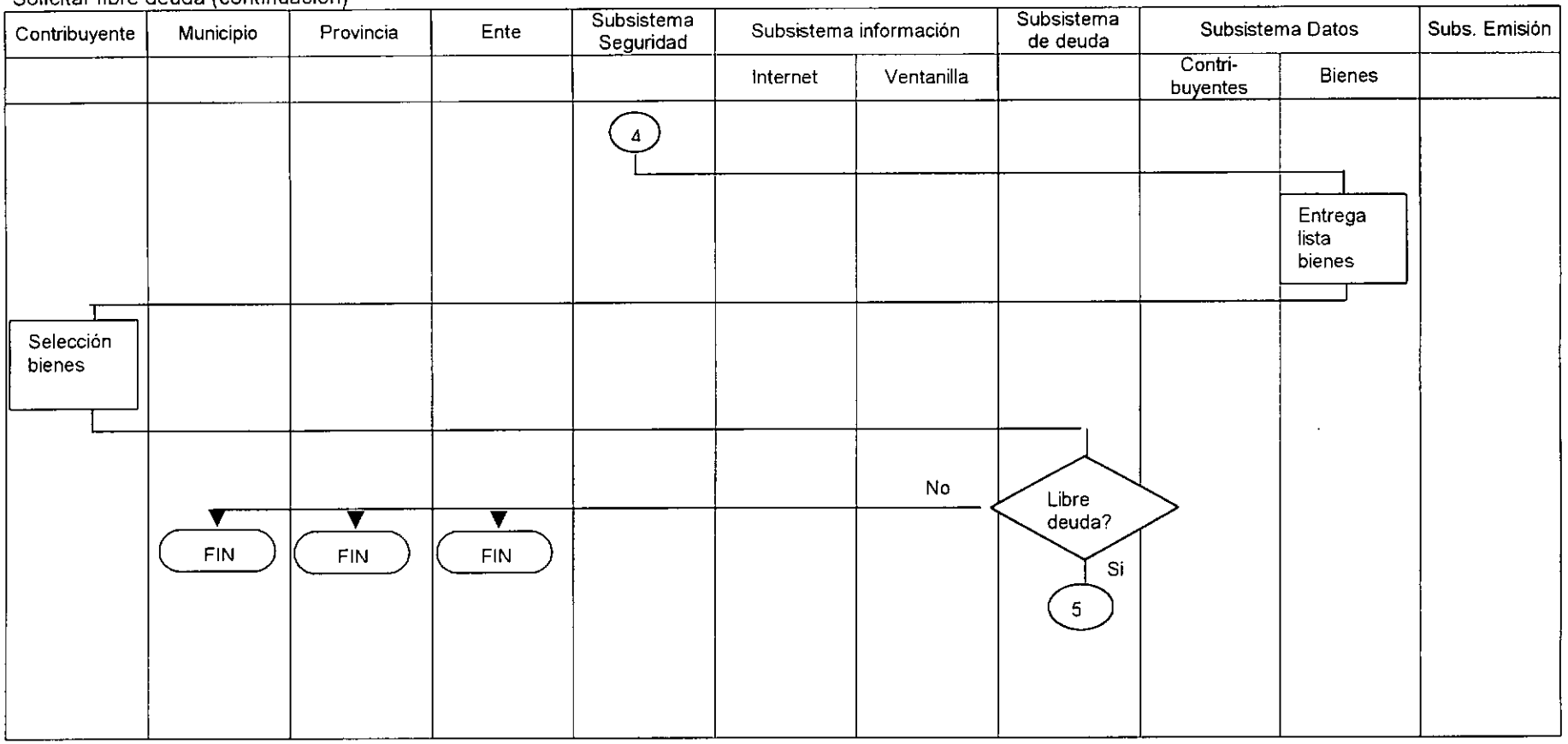
Contribu-yente	Municipio	Provincia	Ente	Subsistema Seguridad	Subsistema información		Subsistema de deuda		Subs. Mantenimiento Datos		Subs Emisión
					Internet	Ventanilla	Finan	Calculo	Bienes	Contribu-yentes.	
							3				Emite chequeras
FIN											



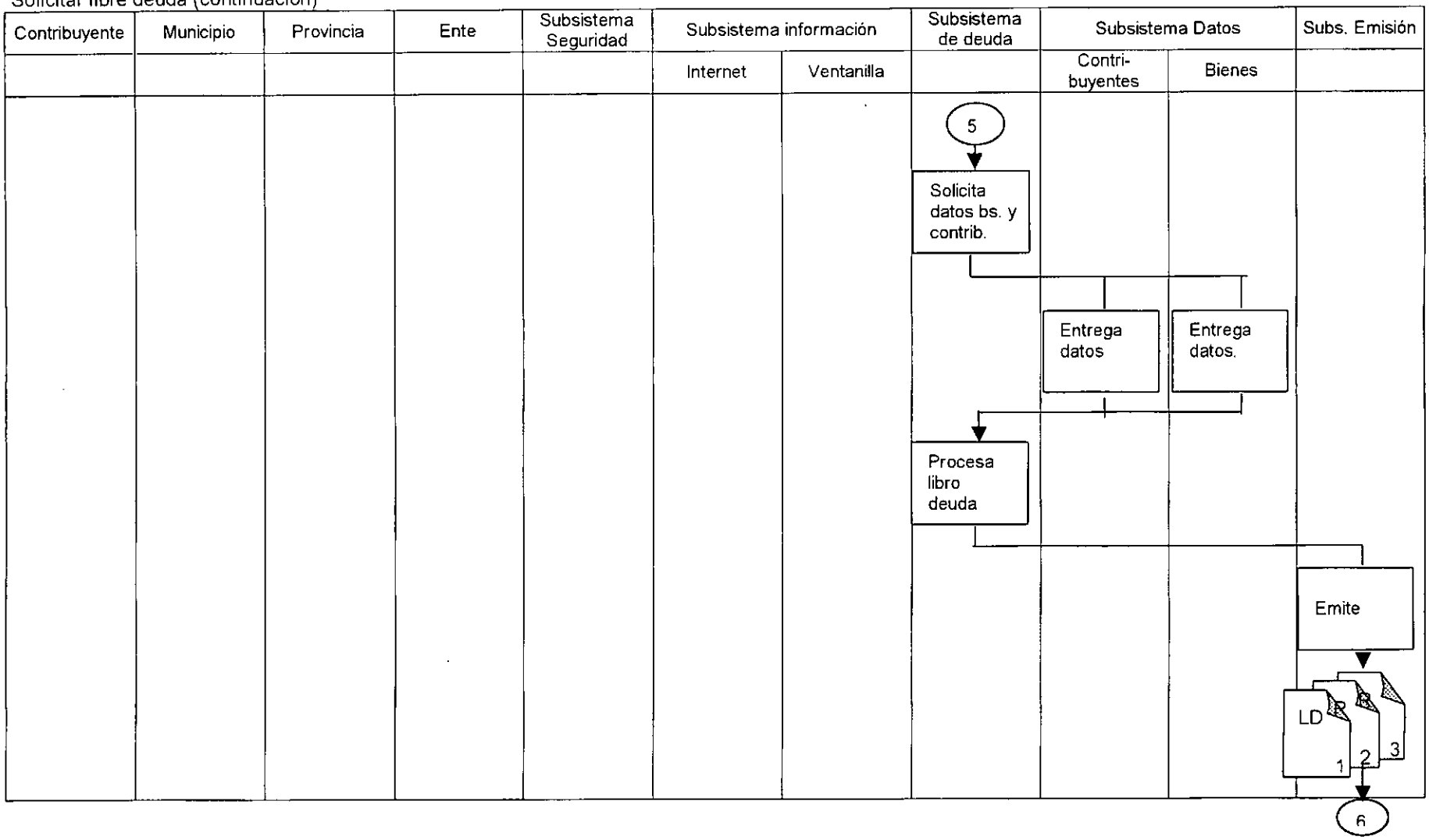
1.6.3.3. Solicitar libre deuda



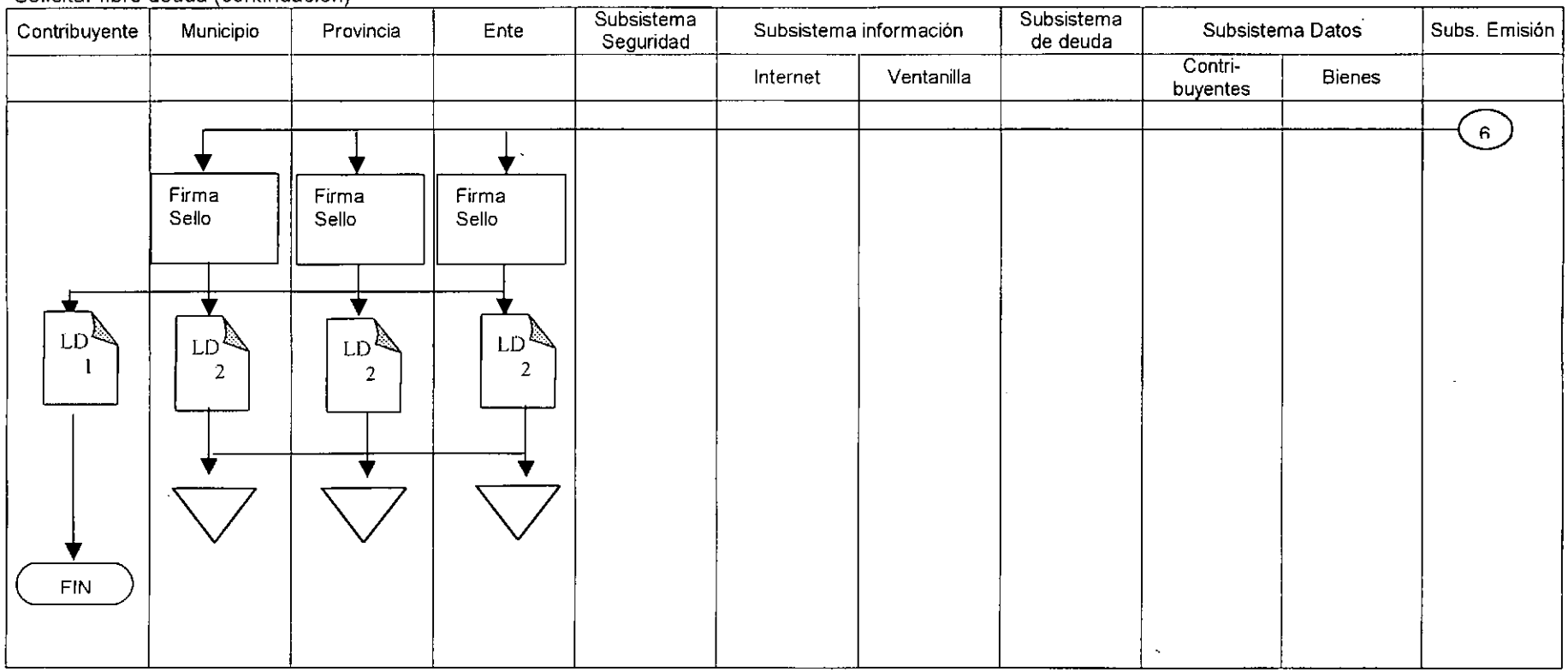
Solicitar libre deuda (continuación)



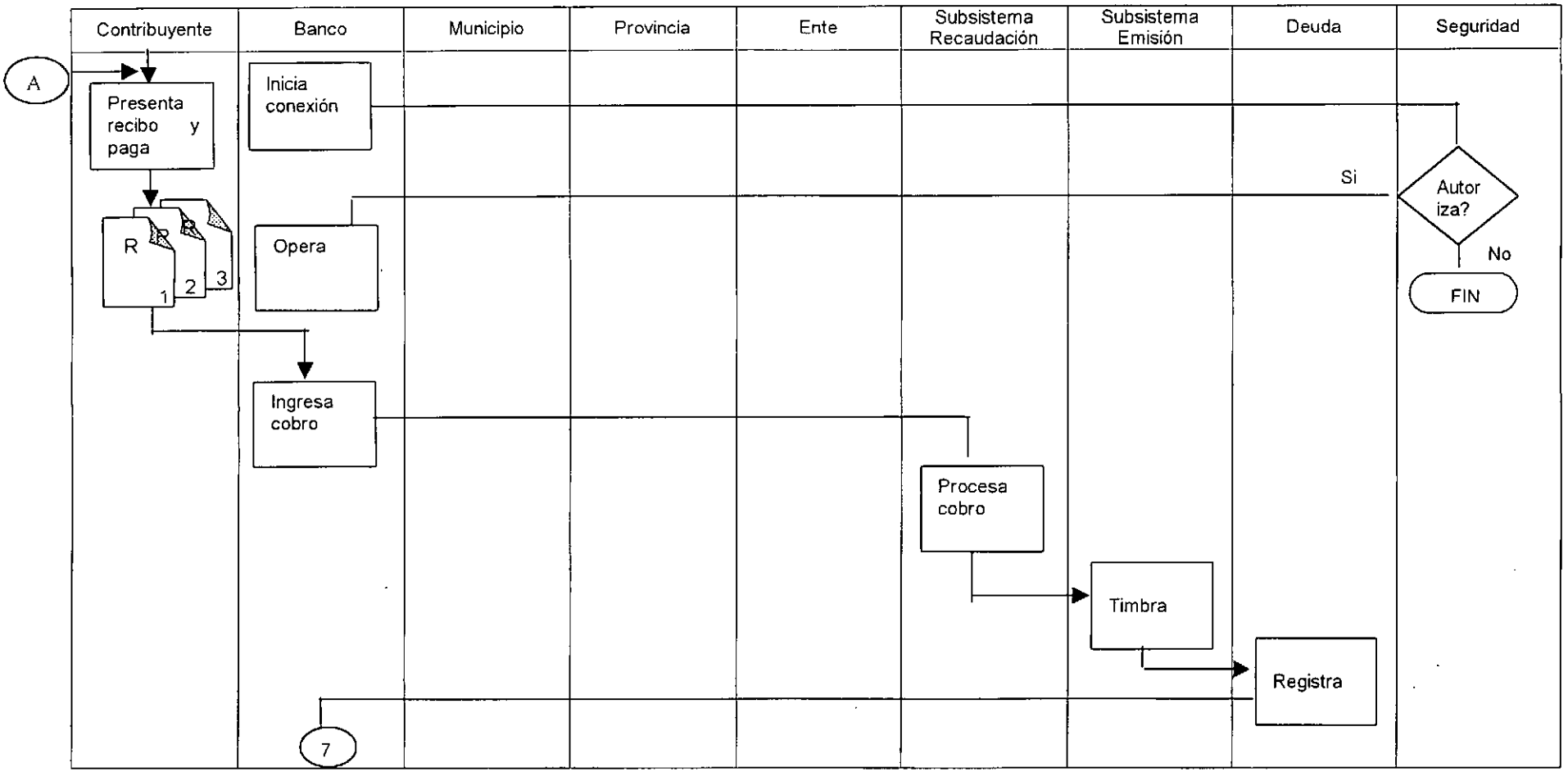
Solicitar libre deuda (continuación)



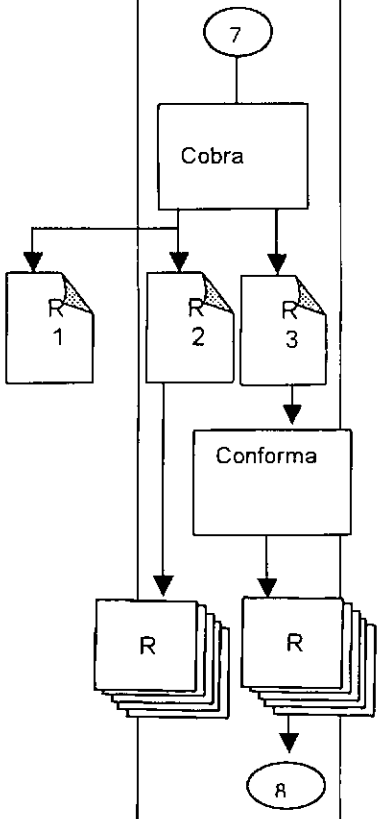
Solicitar libre deuda (continuación)



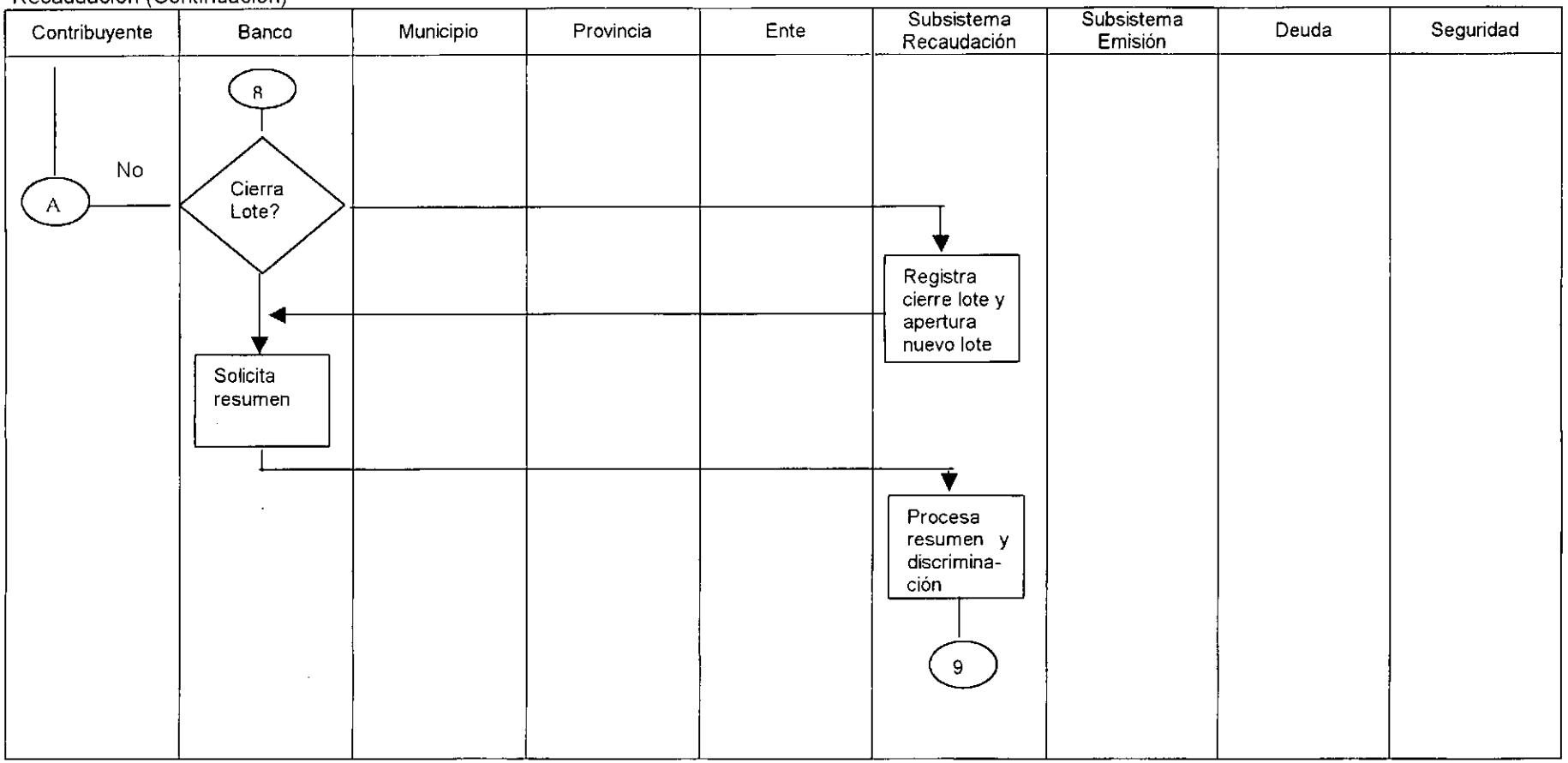
1.6.3.4. Recaudación



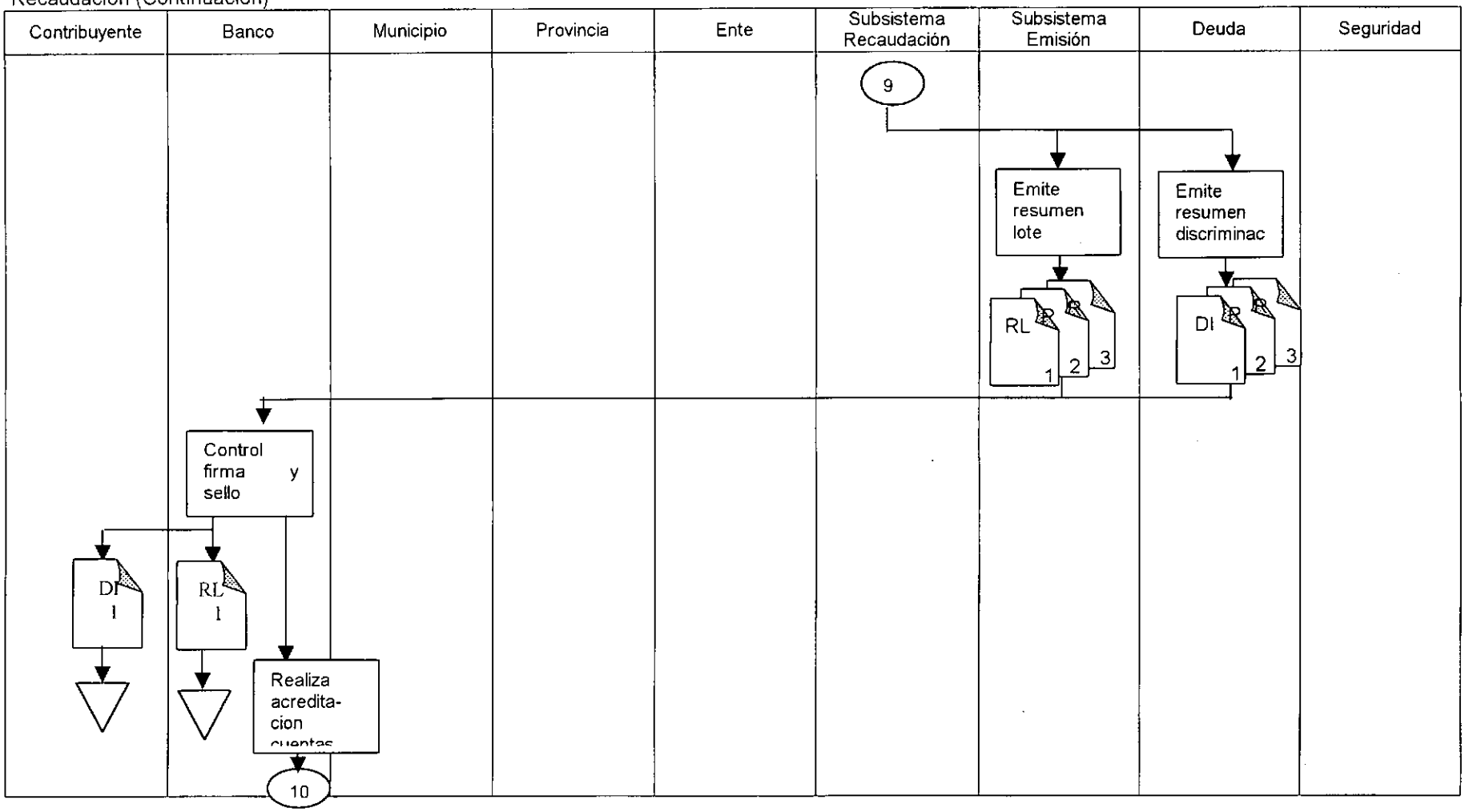
Recaudación (Continuación)

Contribuyente	Banco	Municipio	Provincia	Ente	Subsistema Recaudación	Subsistema Emisión	Deuda	Seguridad
								

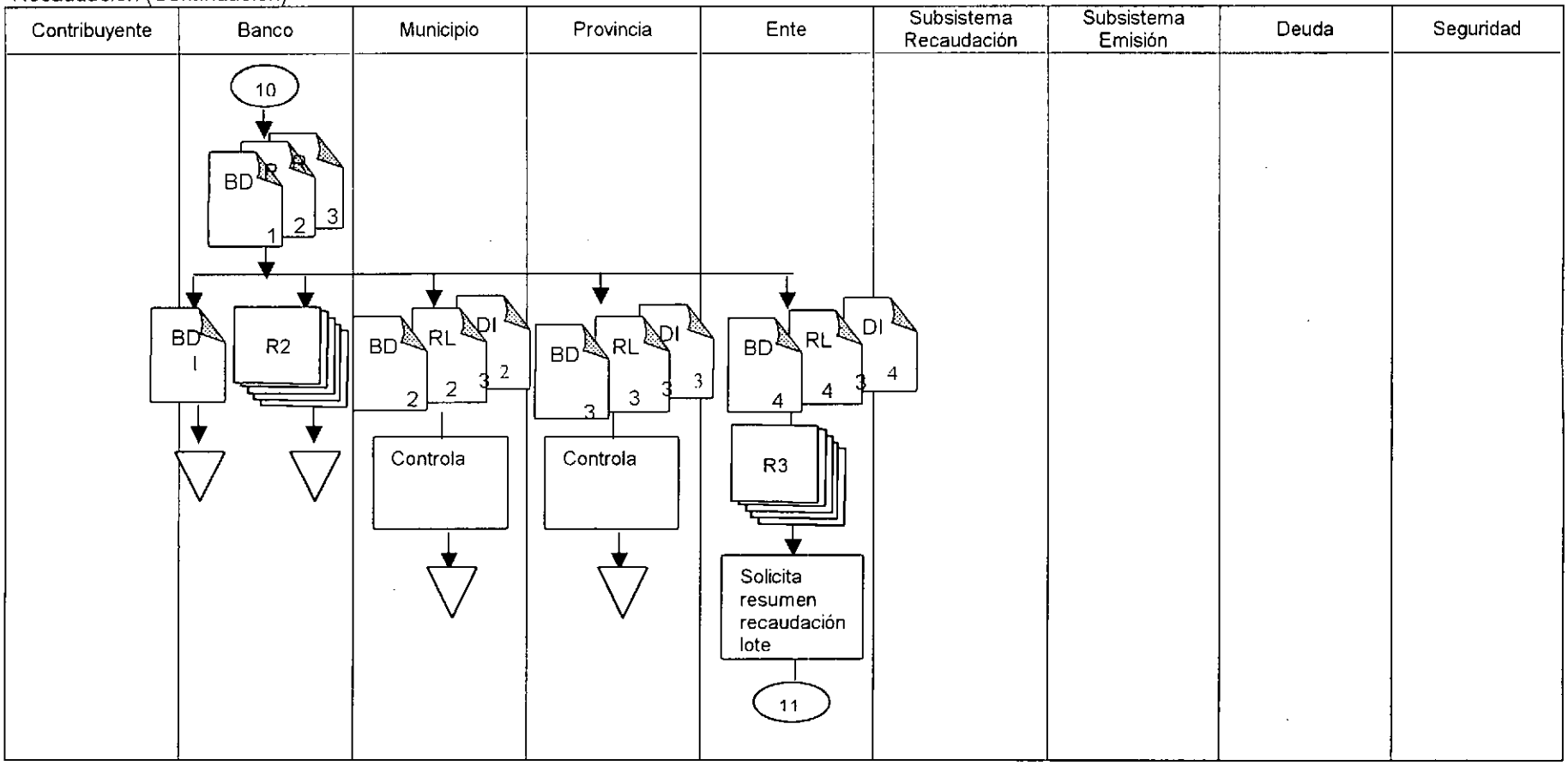
Recaudación (Continuación)



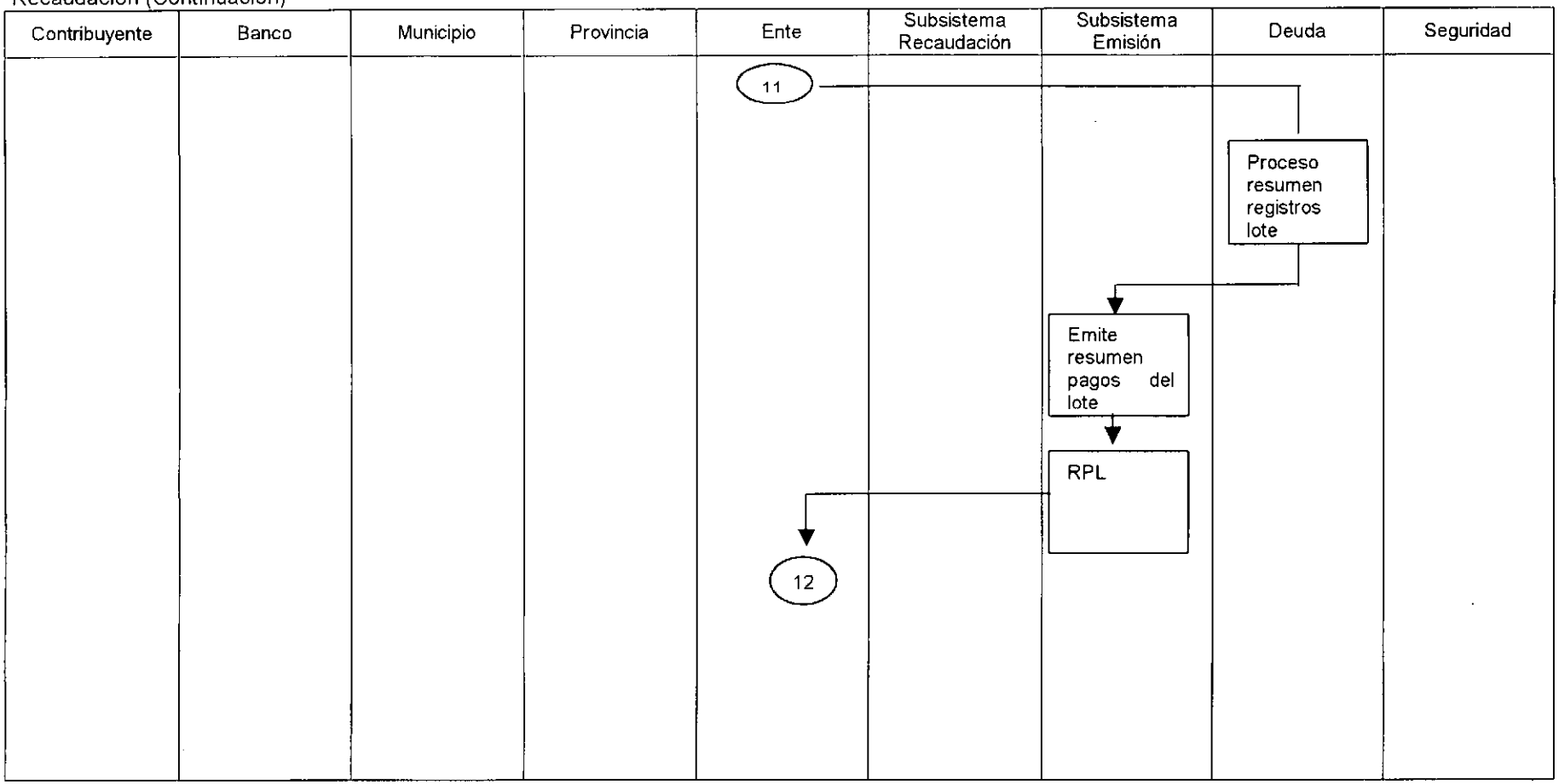
Recaudación (Continuación)



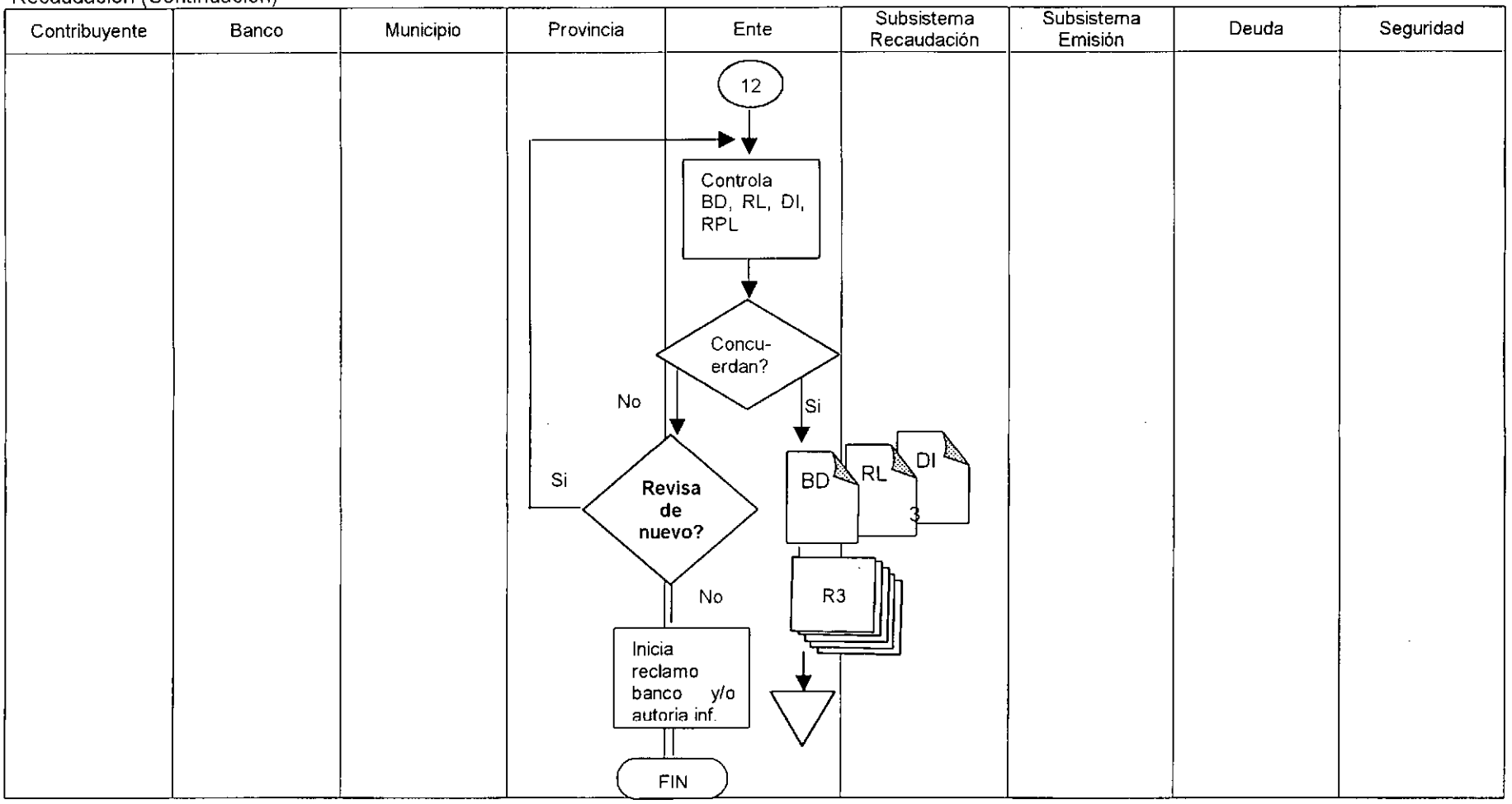
Recaudación (Continuación)



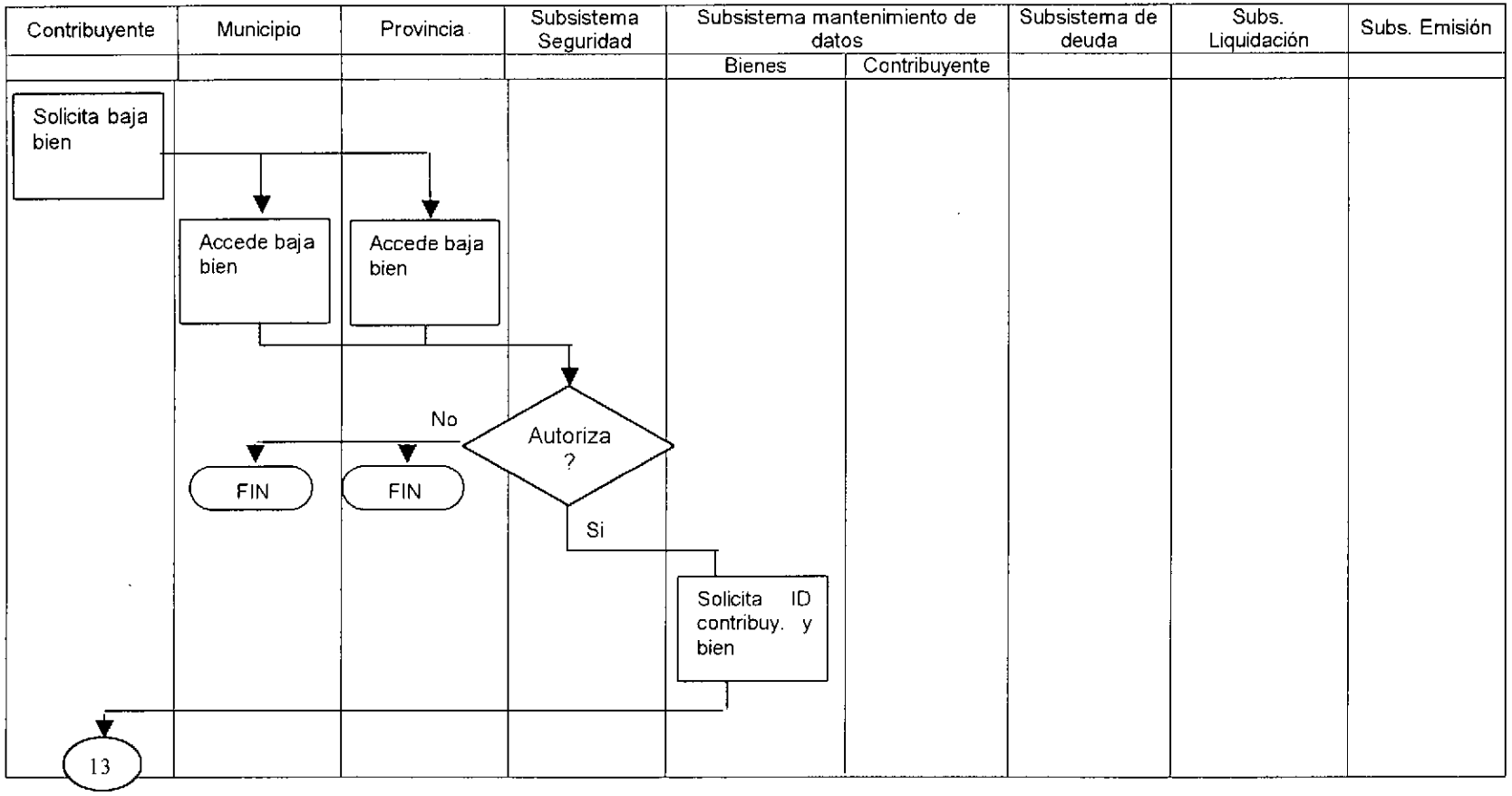
Recaudación (Continuación)



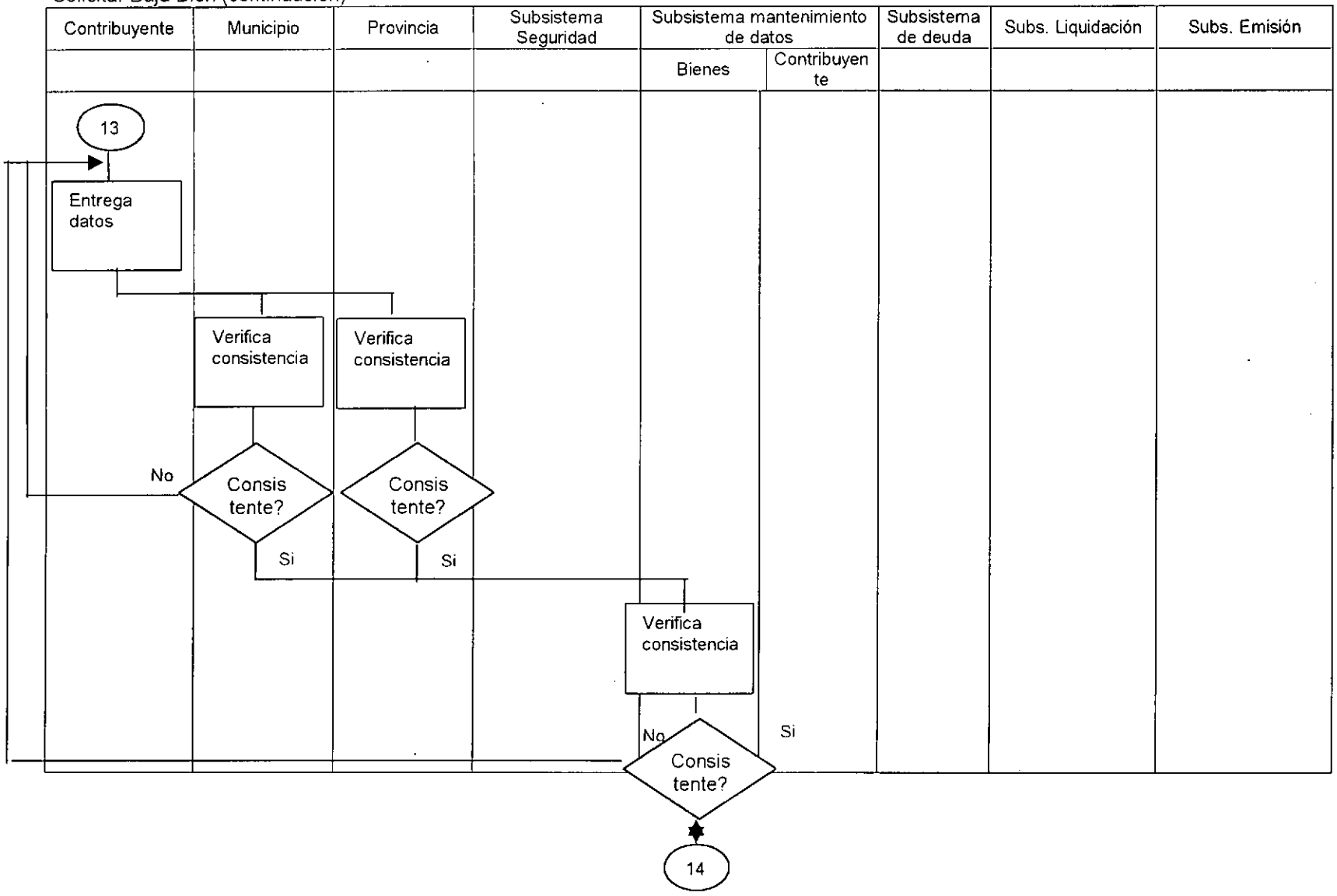
Recaudación (Continuación)



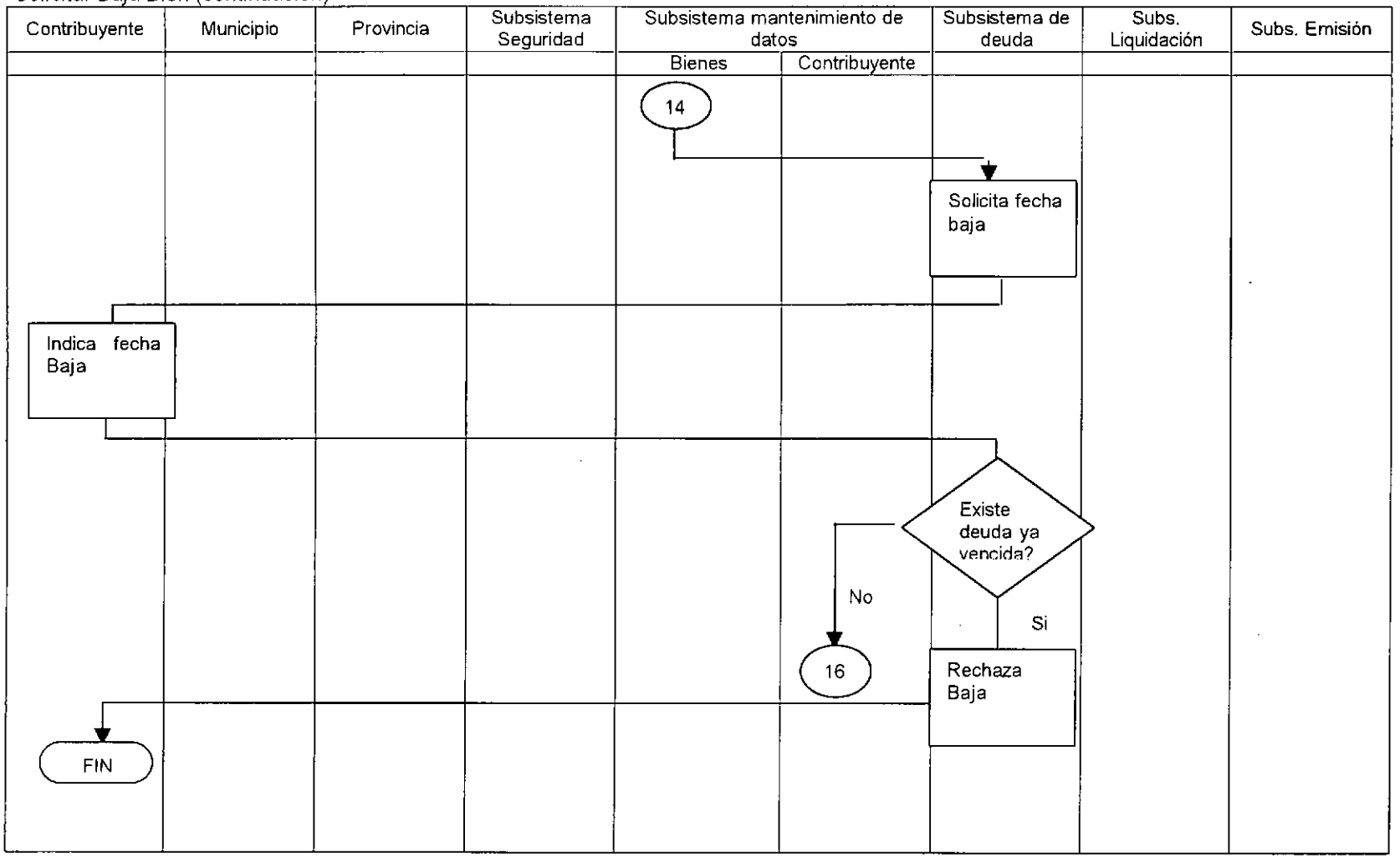
1.6.3.5. Solicitar Baja Bien



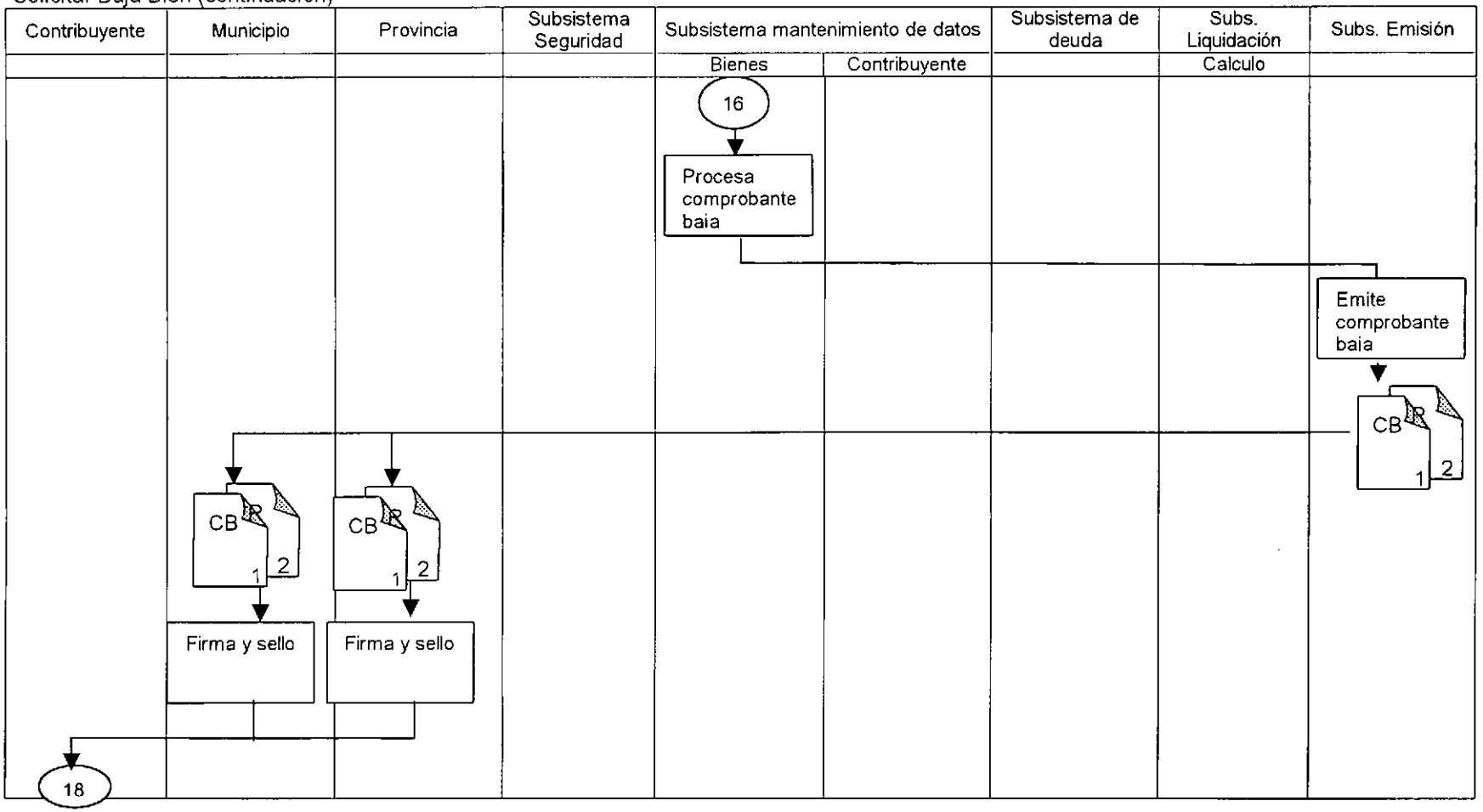
Solicitar Baja Bien (continuación)



Solicitar Baja Bien (continuación)

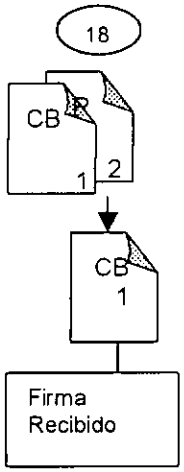


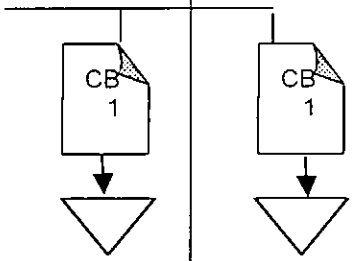
Solicitar Baja Bien (continuación)



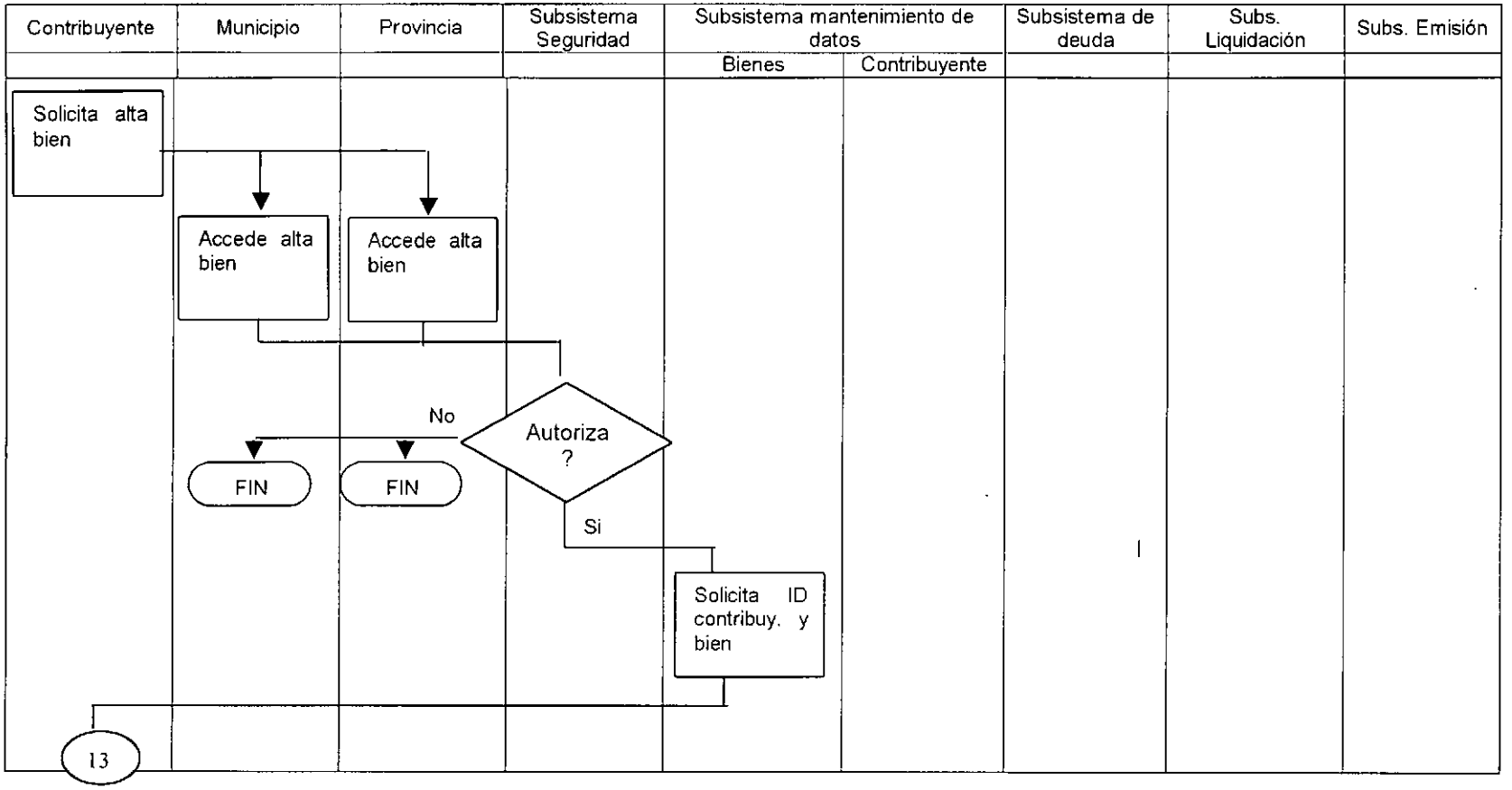
Solicitar Baja Bien (continuación)

Contribuyente	Municipio	Provincia	Subsistema Seguridad	Subsistema mantenimiento de datos		Subsistema de deuda	Subs. Liquidación	Subs. Emisión
				Bienes	Contribuyente		Calculo	

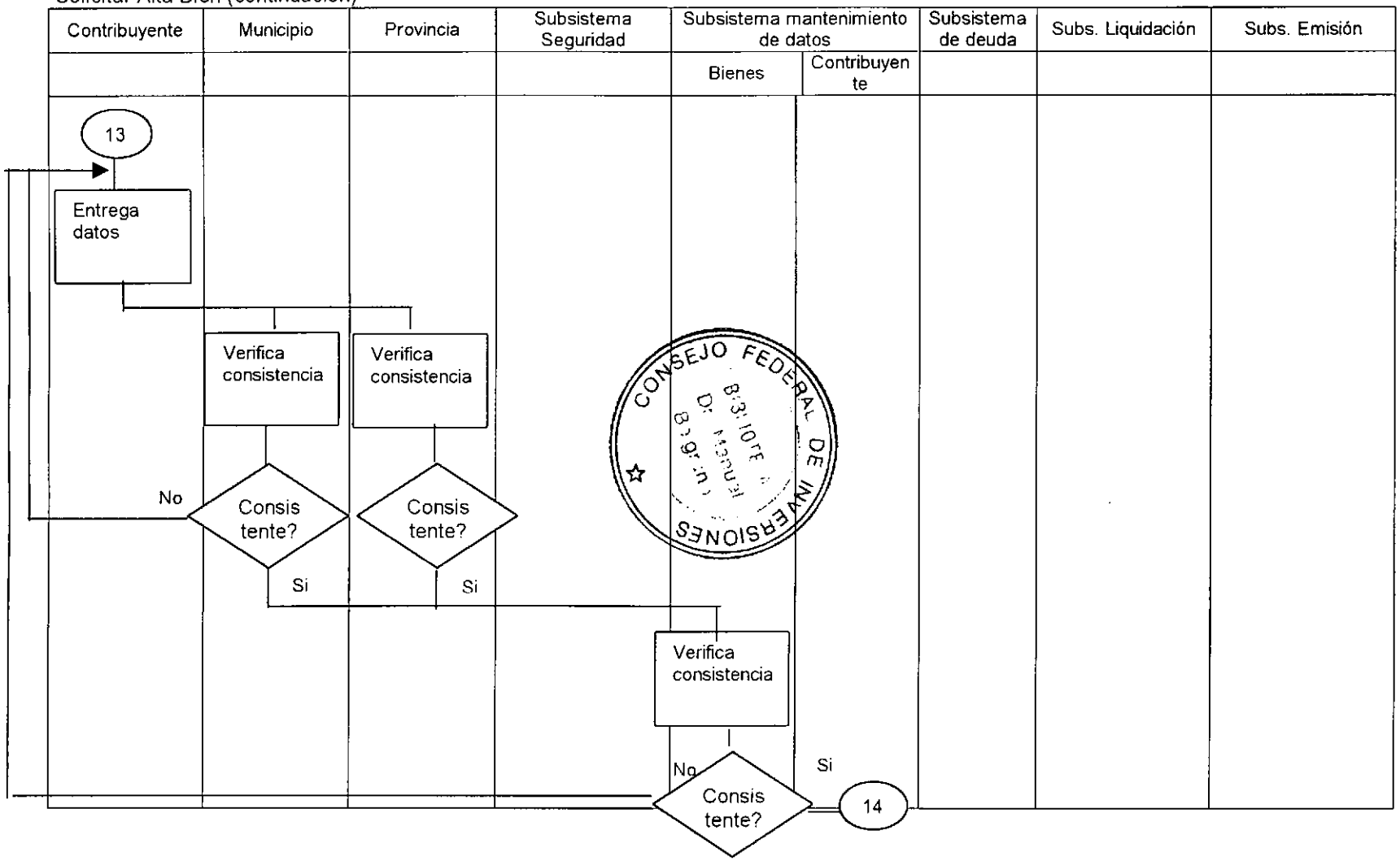




1.6.3.6. Solicitar Alta Bien

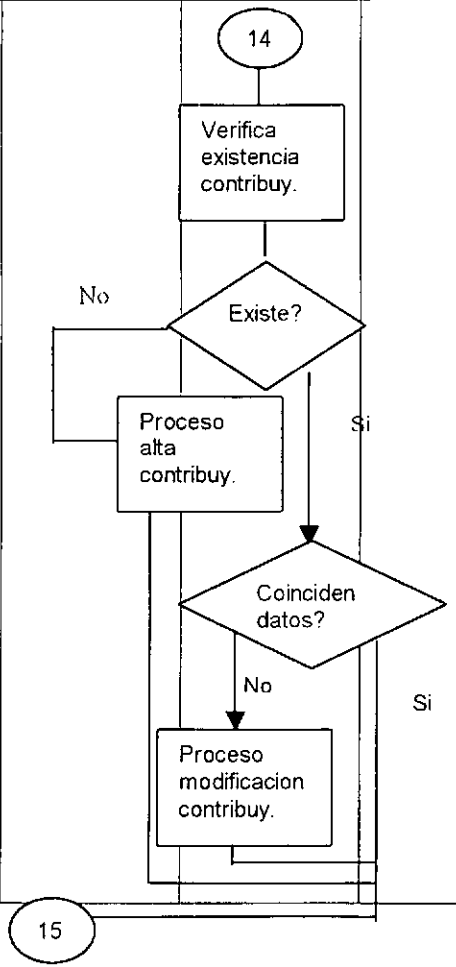


Solicitar Alta Bien (continuación)

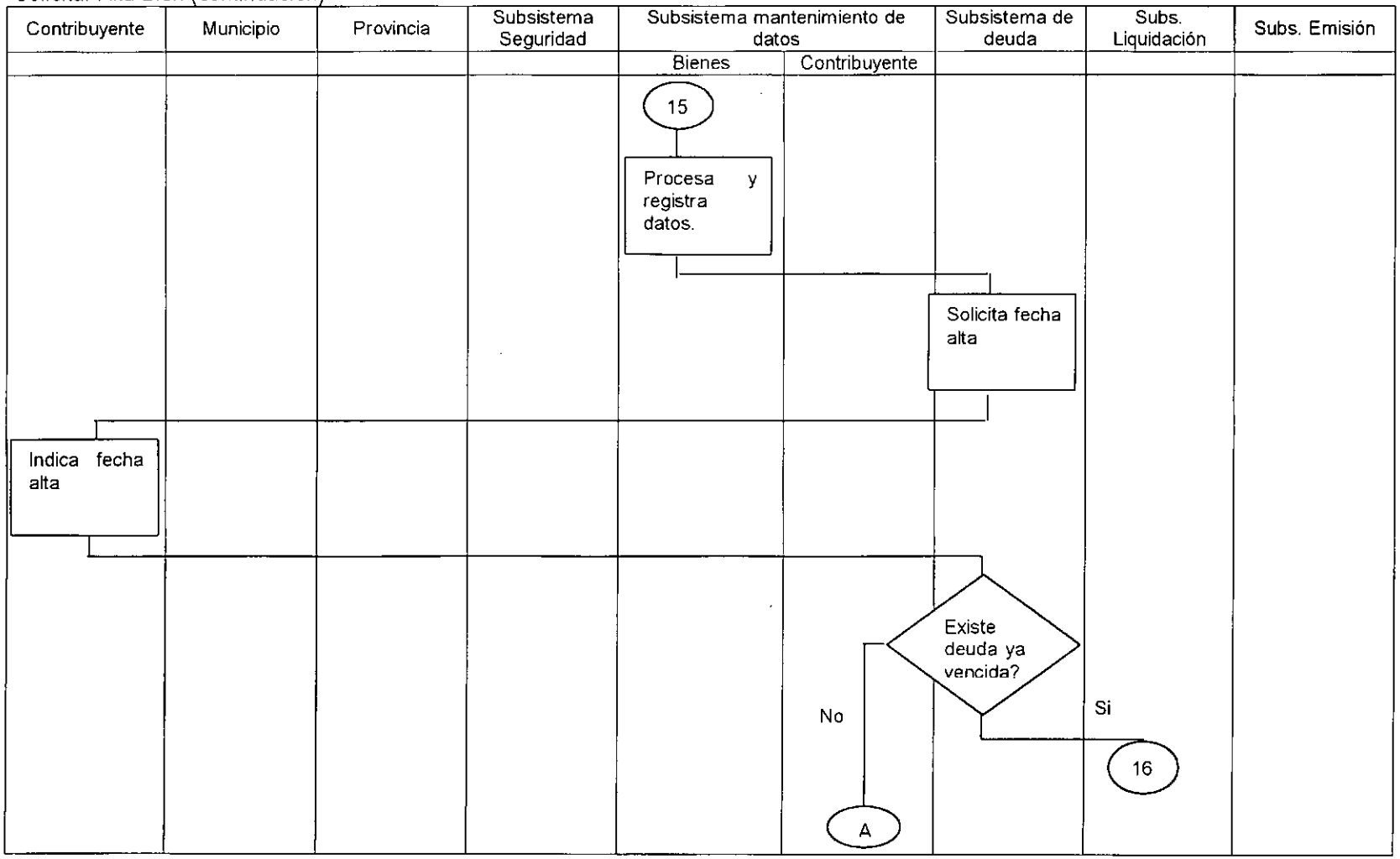


Solicitar Alta Bien (continuación)

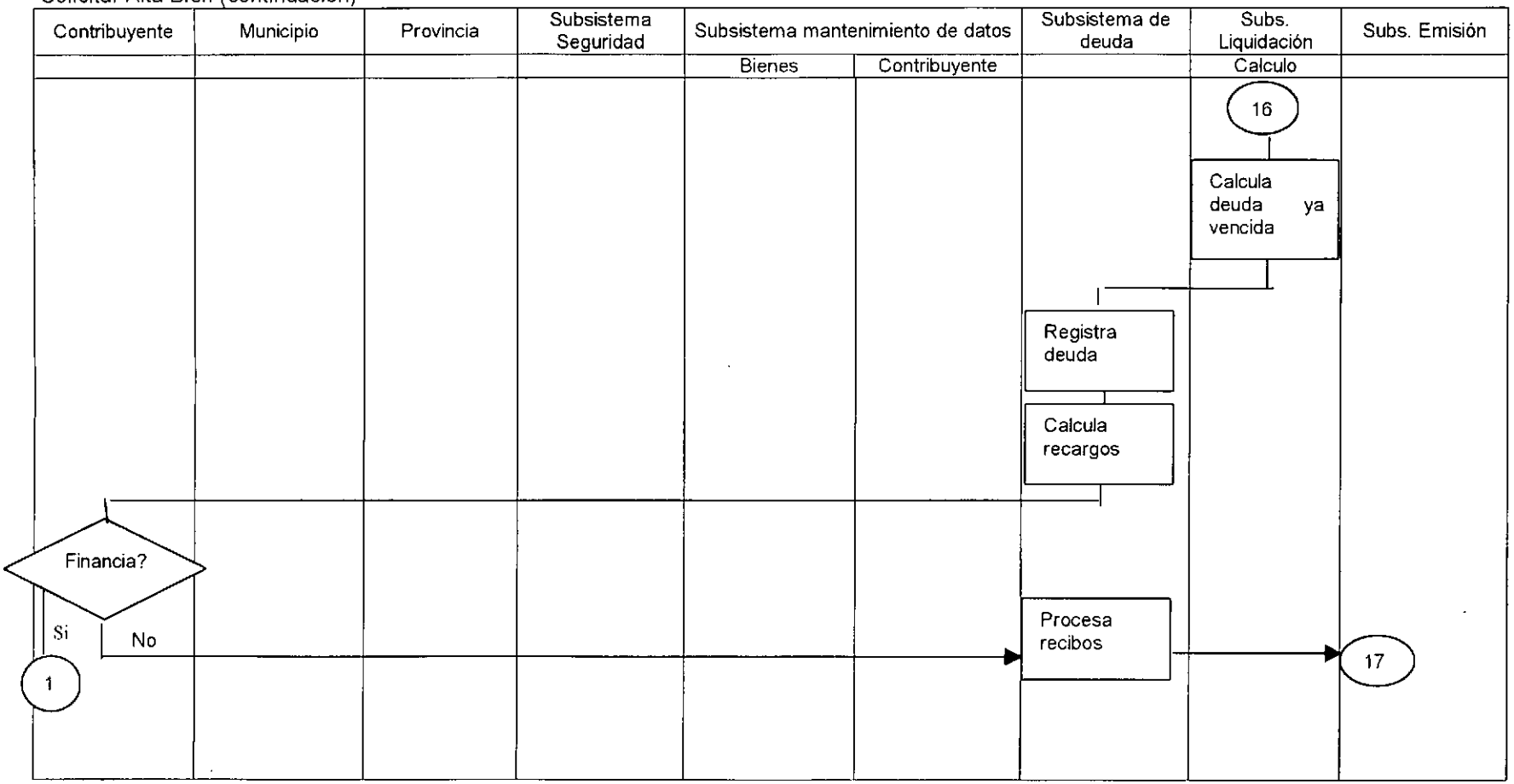
Contribuyente	Municipio	Provincia	Subsistema Seguridad	Subsistema mantenimiento de datos		Subsistema de deuda	Subs. Liquidación	Subs. Emisión
				Bienes	Contribuyente			



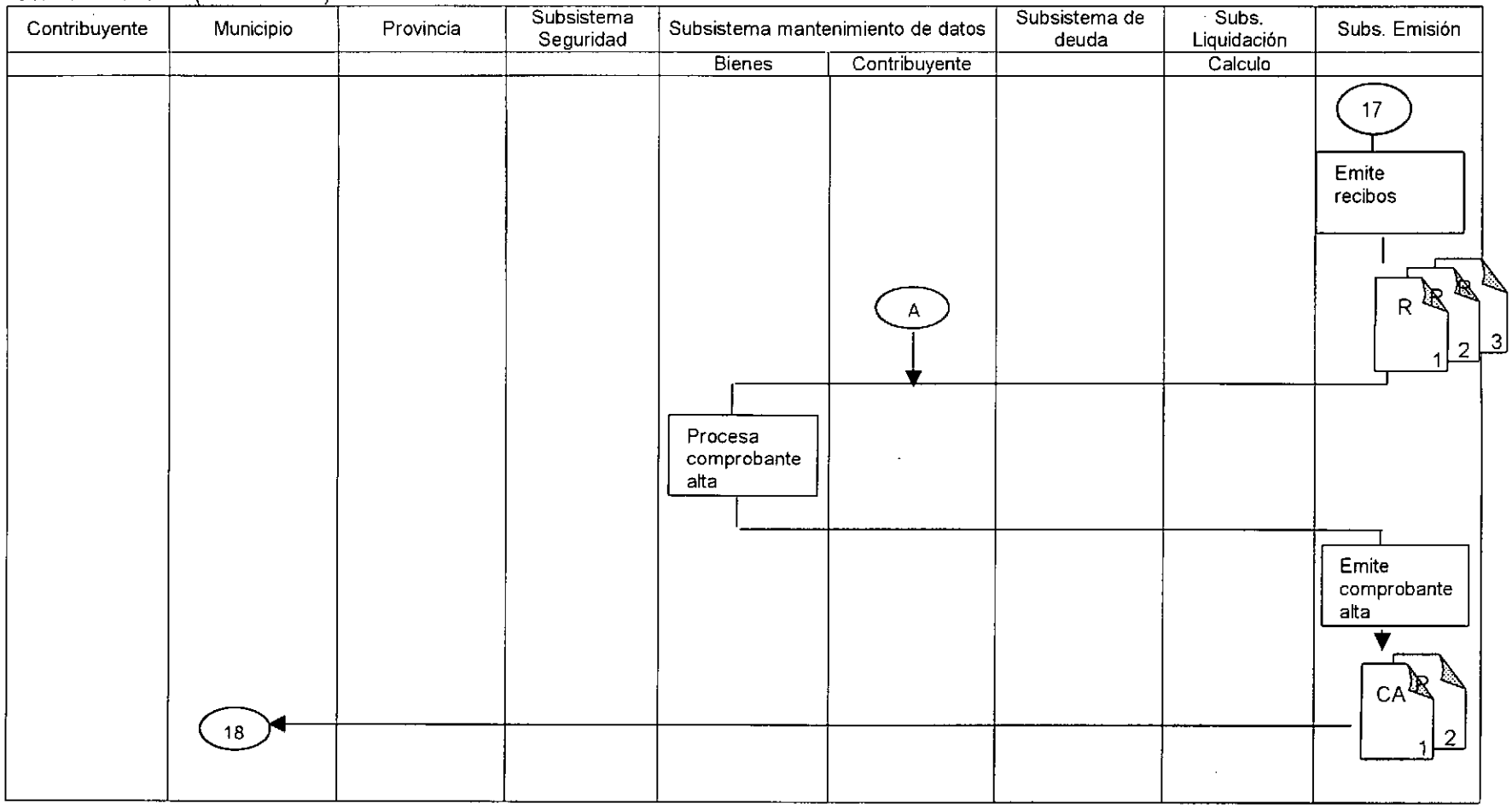
Solicitar Alta Bien (continuación)



Solicitar Alta Bien (continuación)

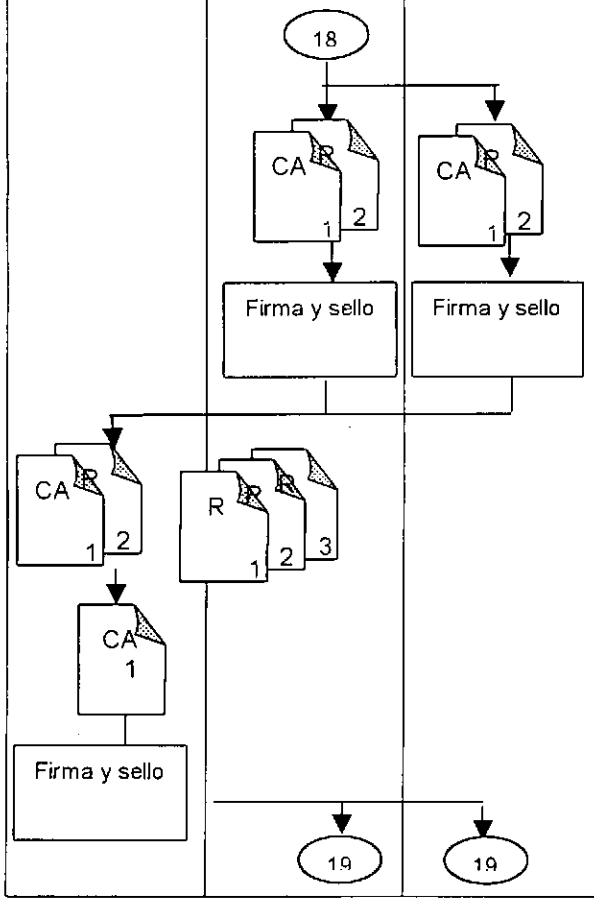


Solicitar Alta Bien (continuación)



Solicitar Alta Bien (continuación)

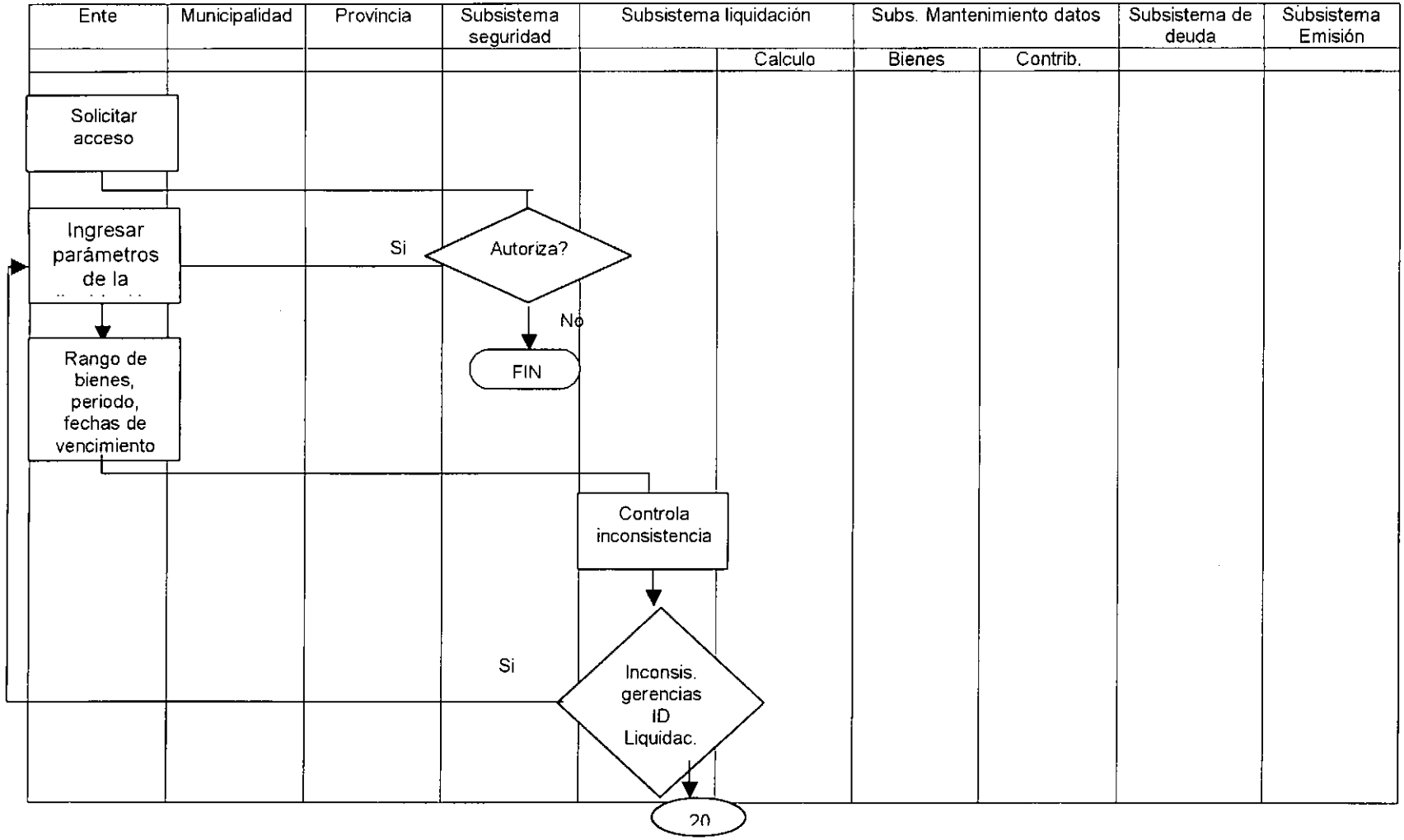
Contribuyente	Municipio	Provincia	Subsistema Seguridad	Subsistema mantenimiento de datos		Subsistema de deuda	Subs. Liquidación	Subs. Emisión
				Bienes	Contribuyente		Calculo	



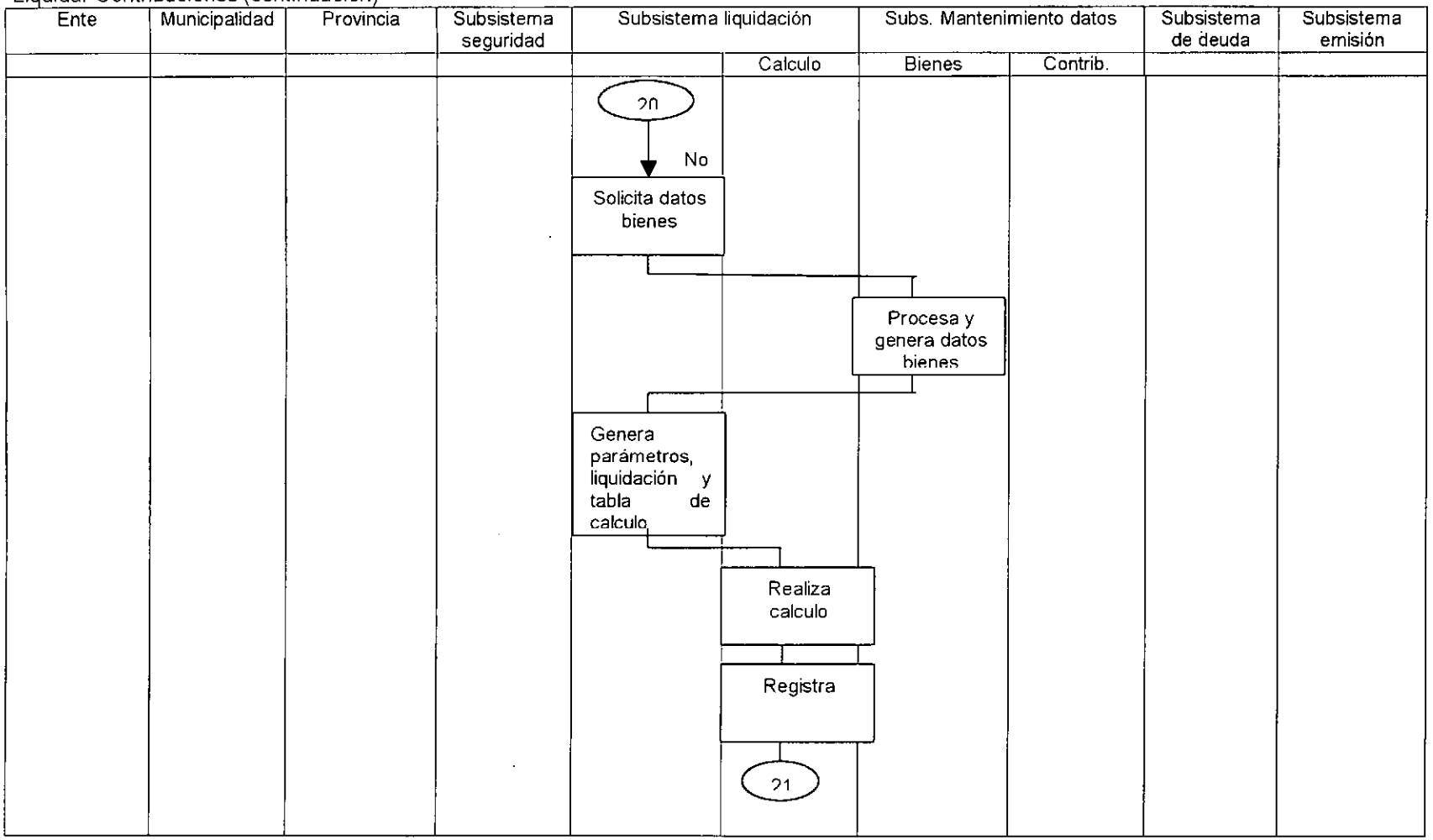
Solicitar Alta Bien (continuación)

Contribuyente	Municipio	Provincia	Subsistema Seguridad	Subsistema mantenimiento de datos		Subsistema de deuda	Subs. Liquidación	Subs. Emisión
				Bienes	Contribuyente		Calculo	

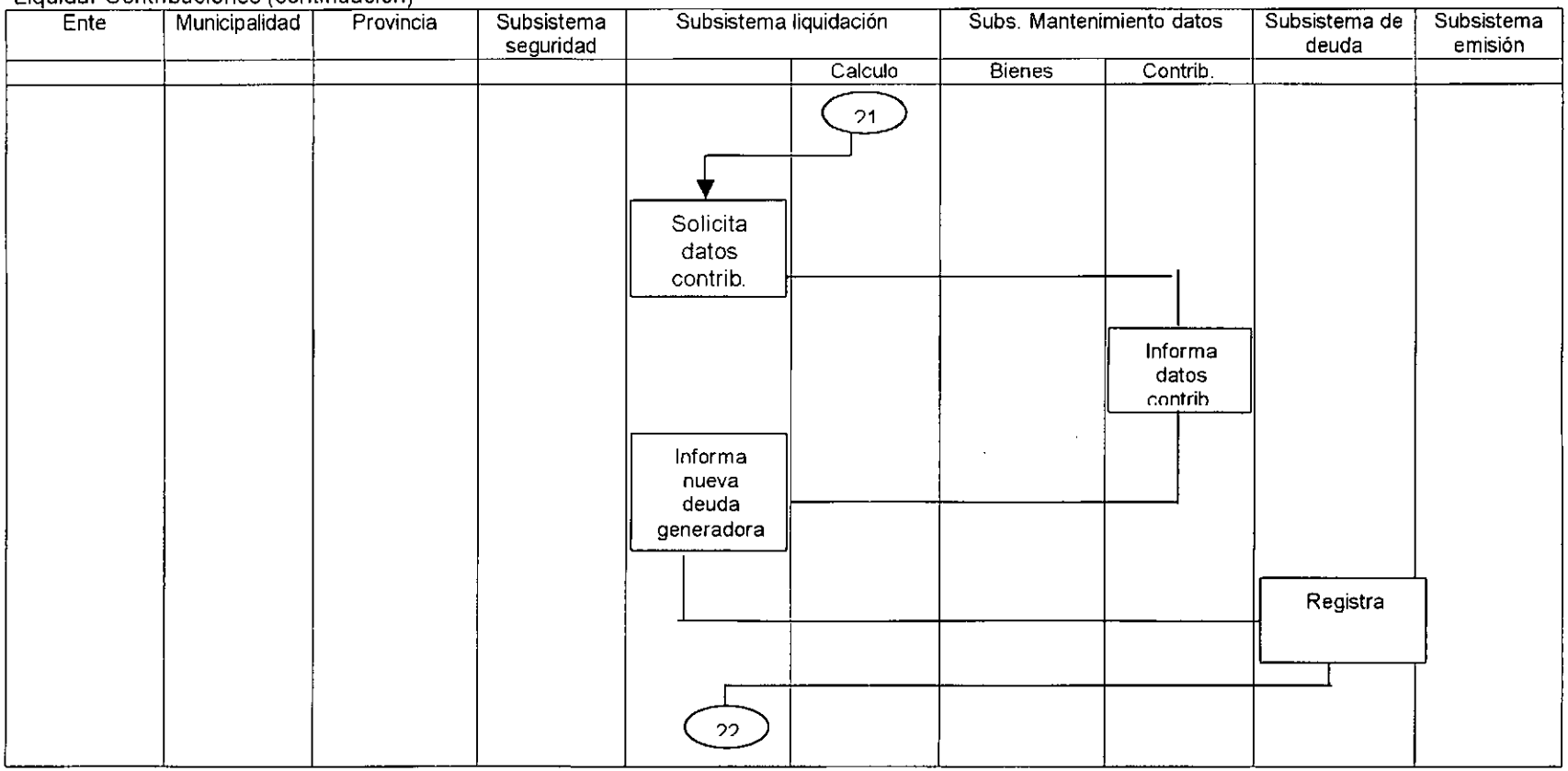
1.6.3.7. Liquidar Contribuciones



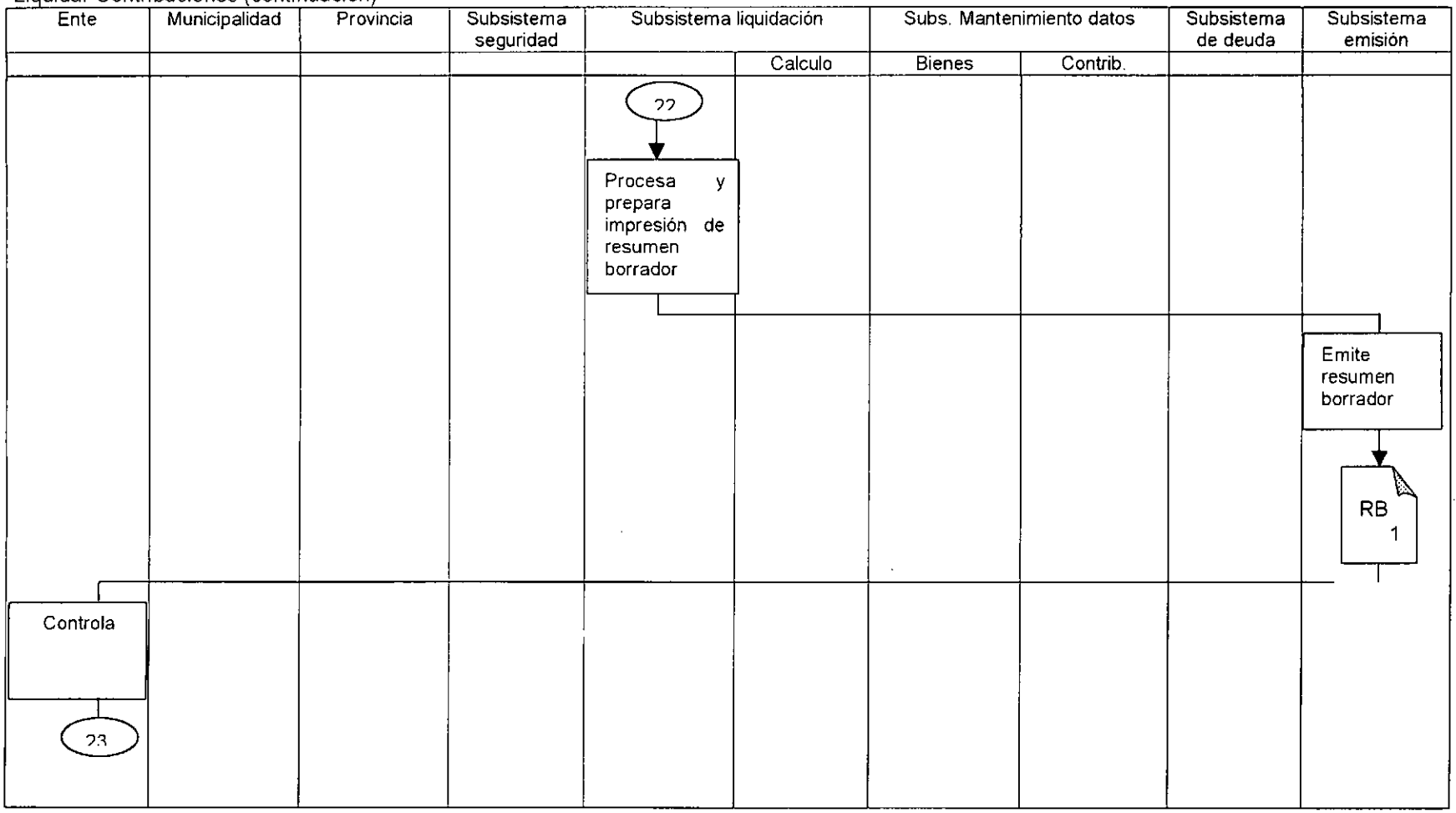
Liquidar Contribuciones (continuación)



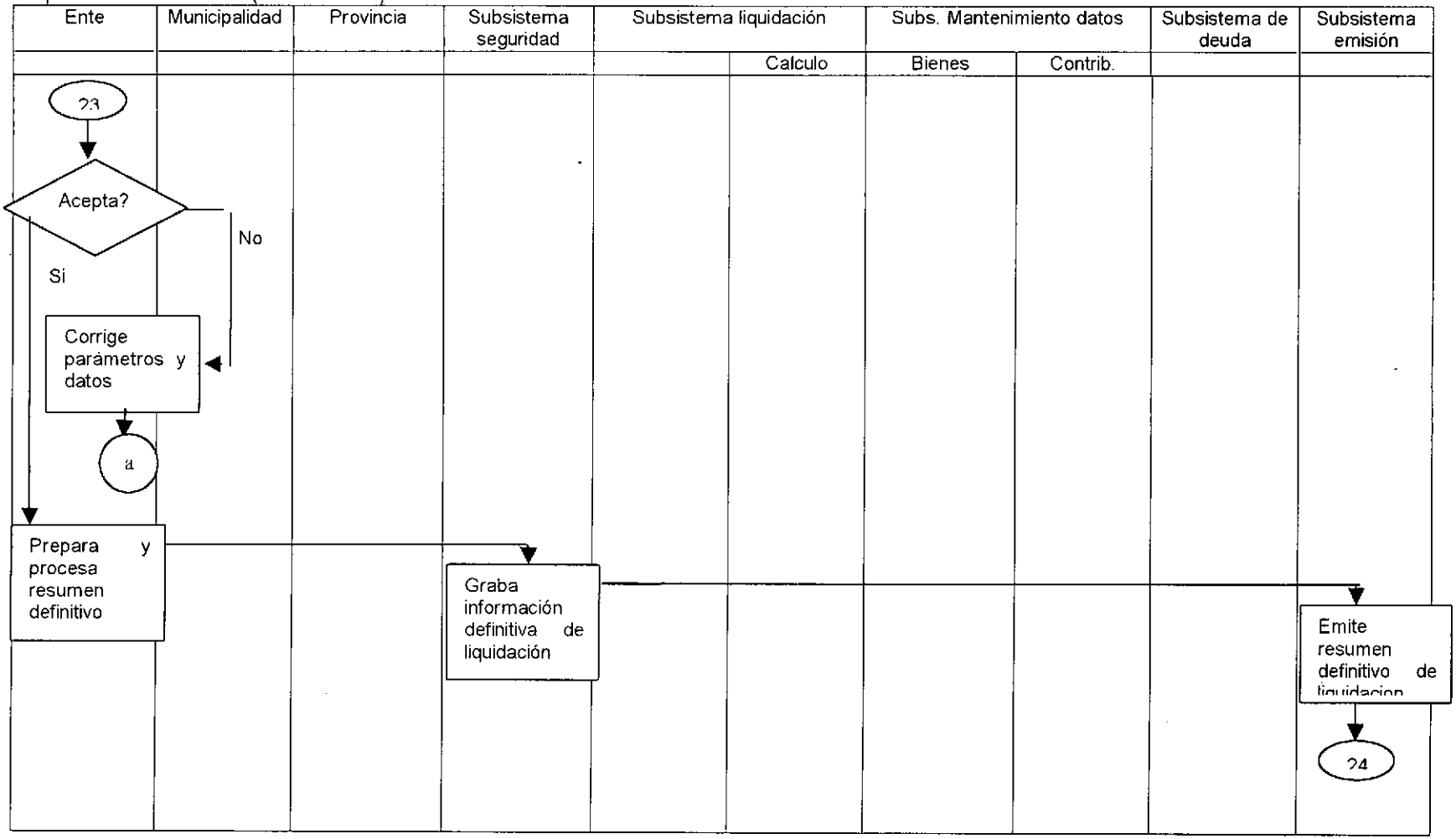
Liquidar Contribuciones (continuación)



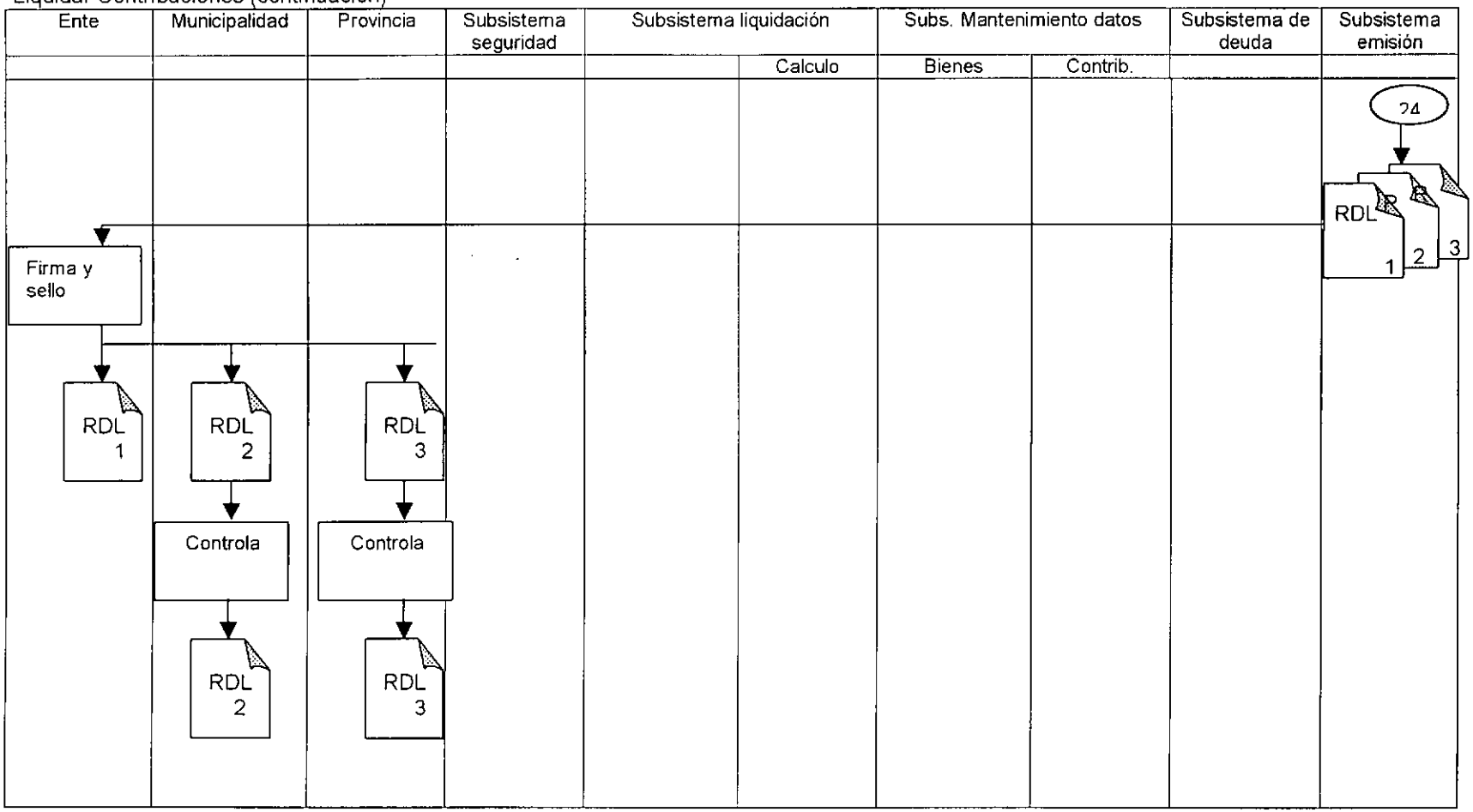
Liquidar Contribuciones (continuación)



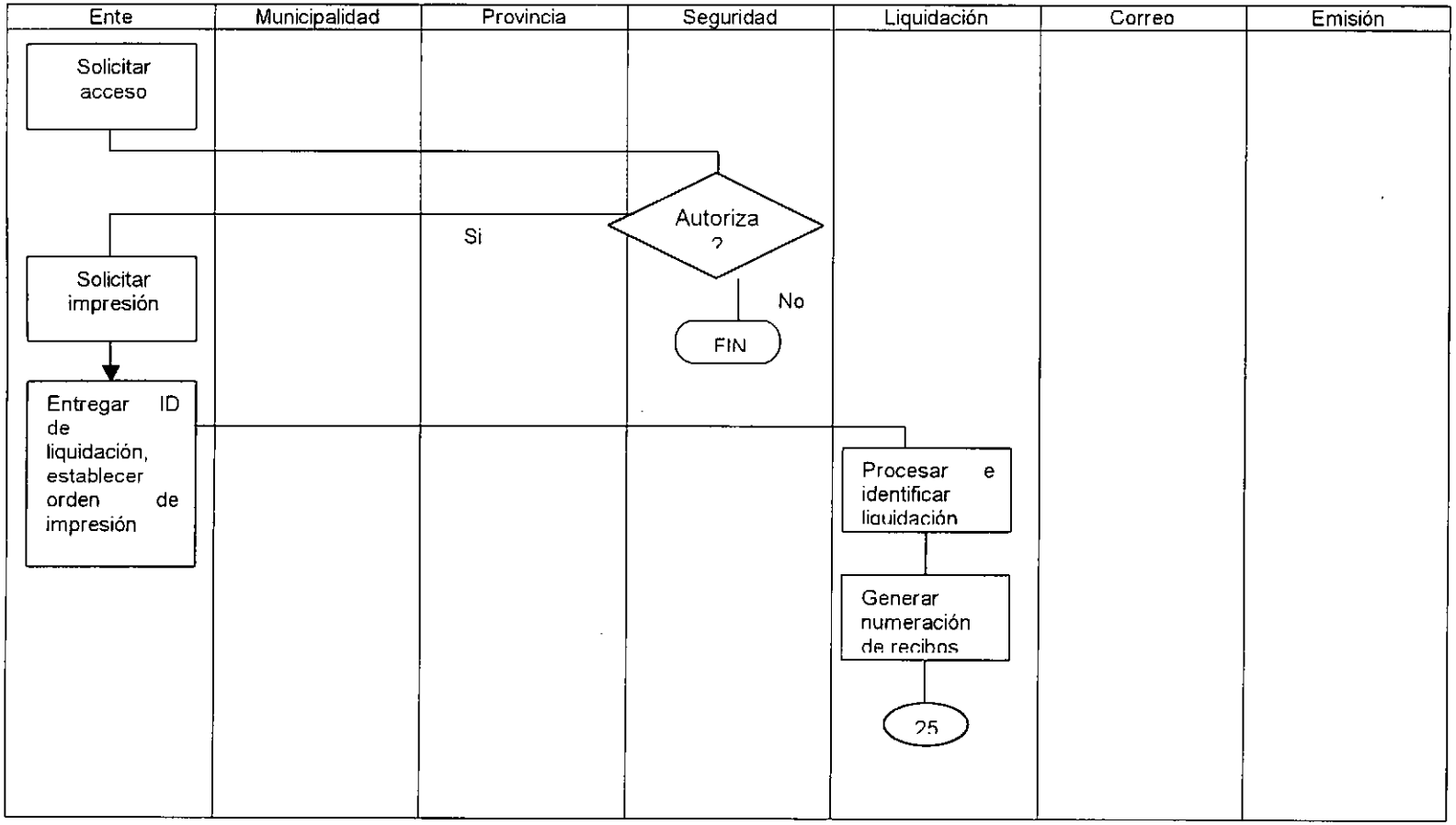
Liquidar Contribuciones (continuación)



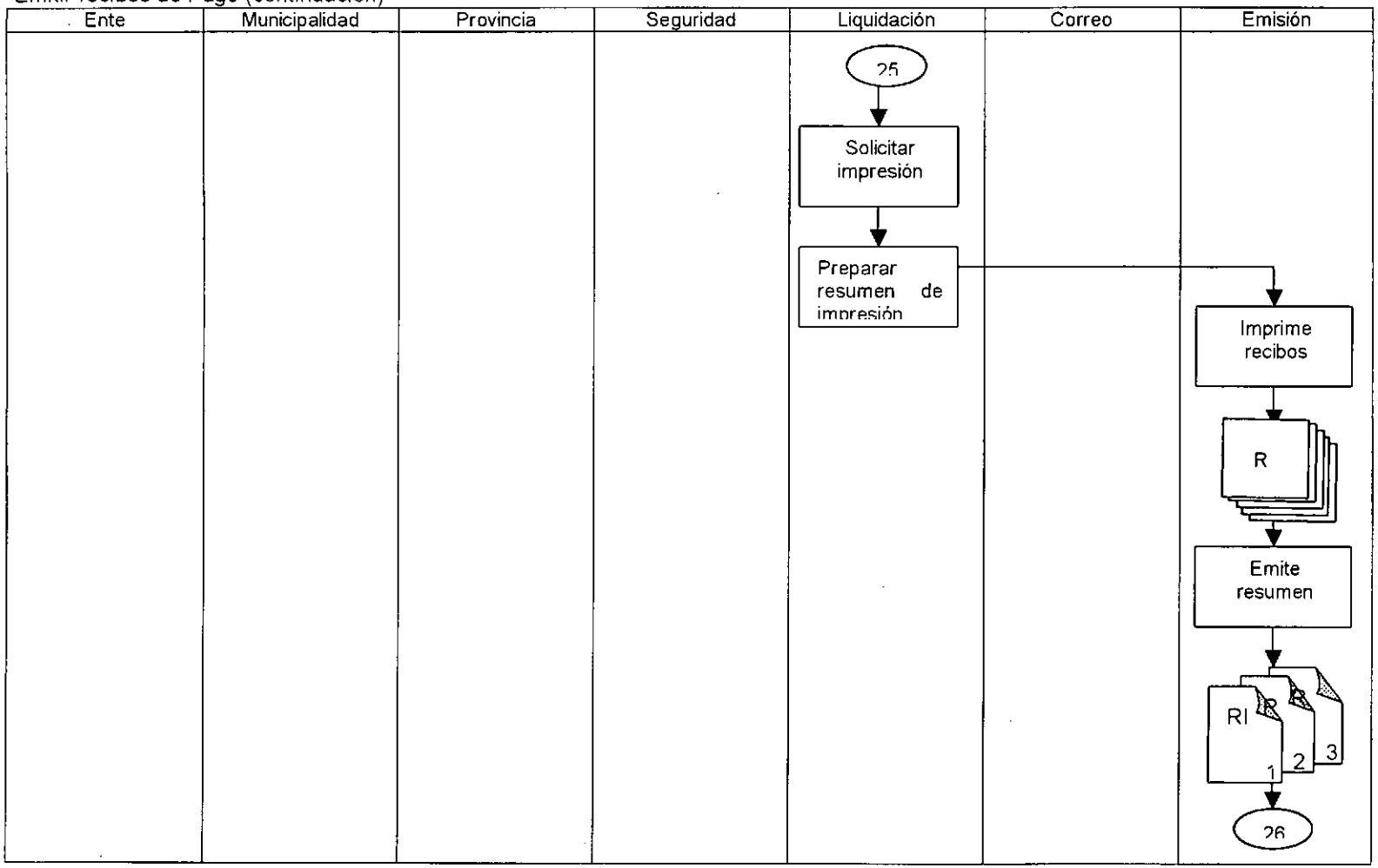
Liquidar Contribuciones (continuación)



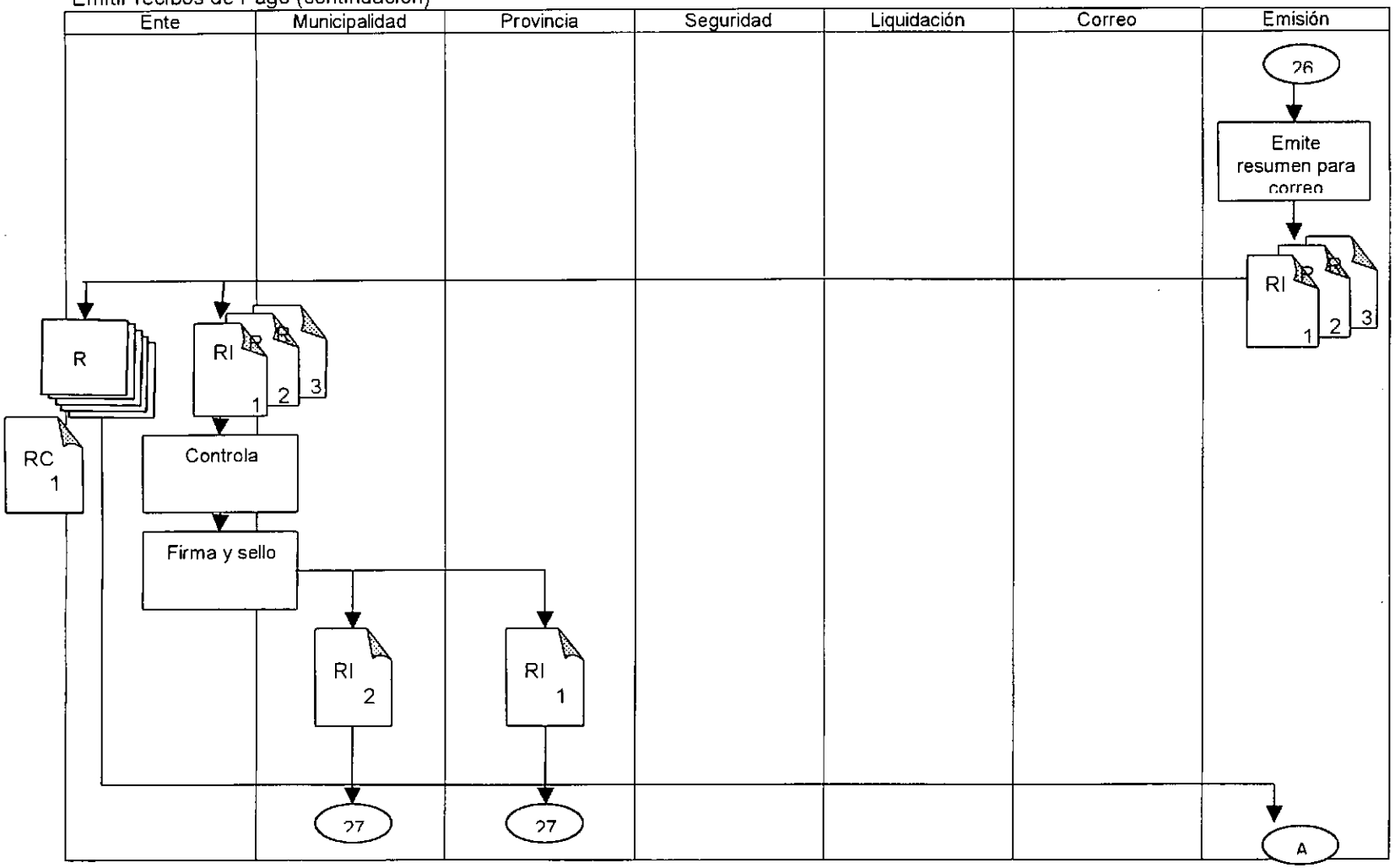
1.6.3.8. Emitir recibos de Pago



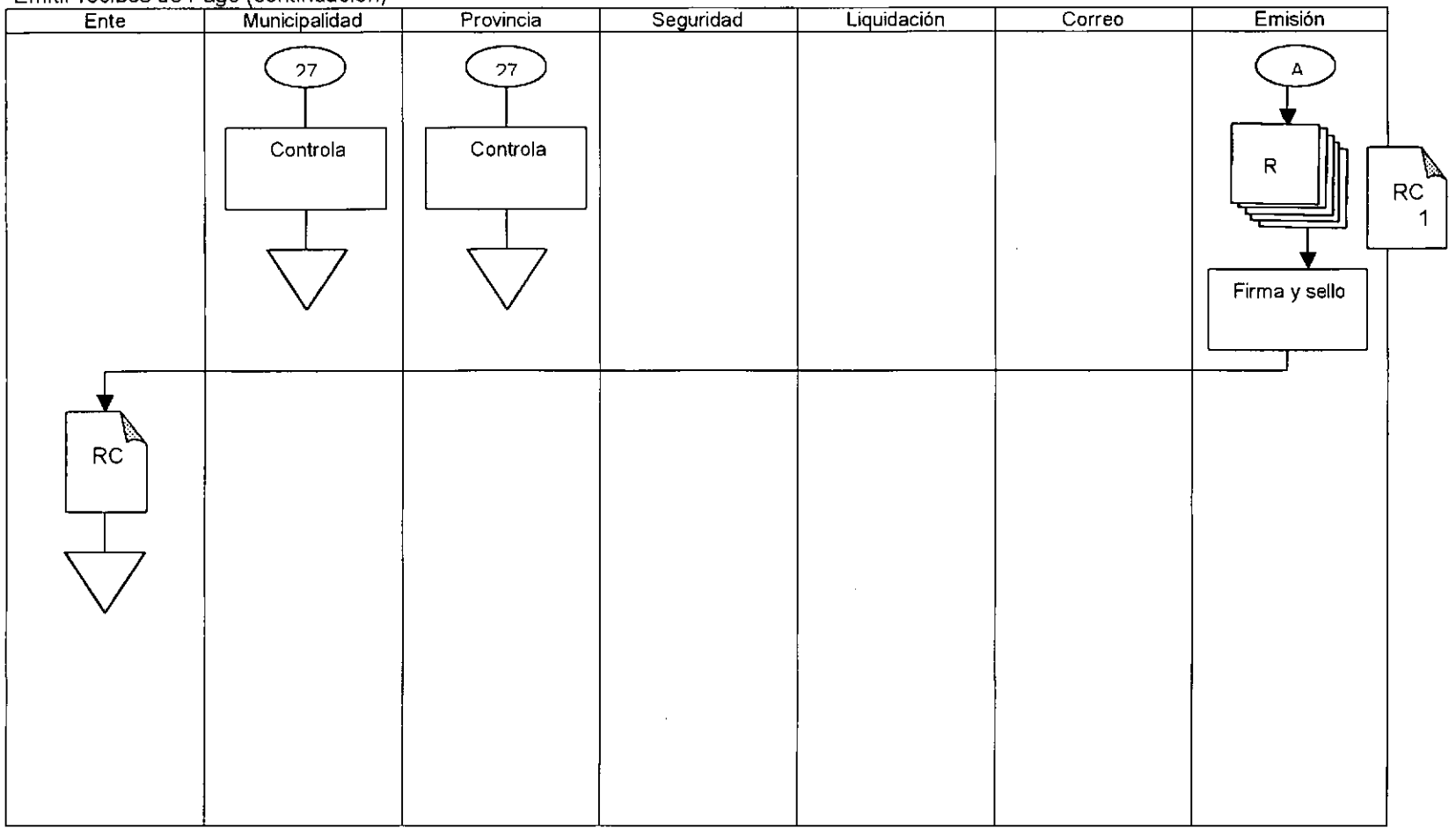
Emitir recibos de Pago (continuación)



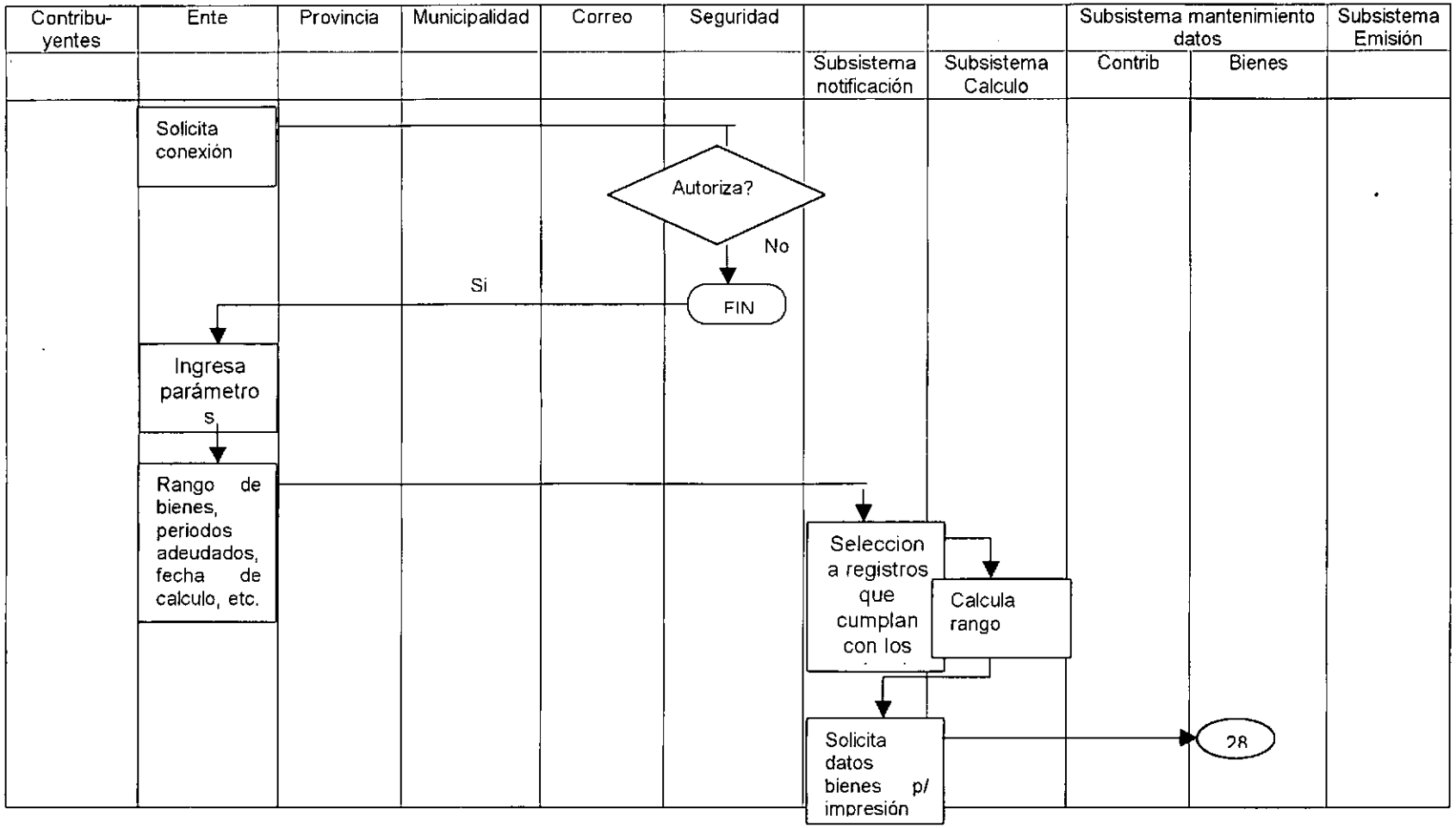
Emitir recibos de Pago (continuación)



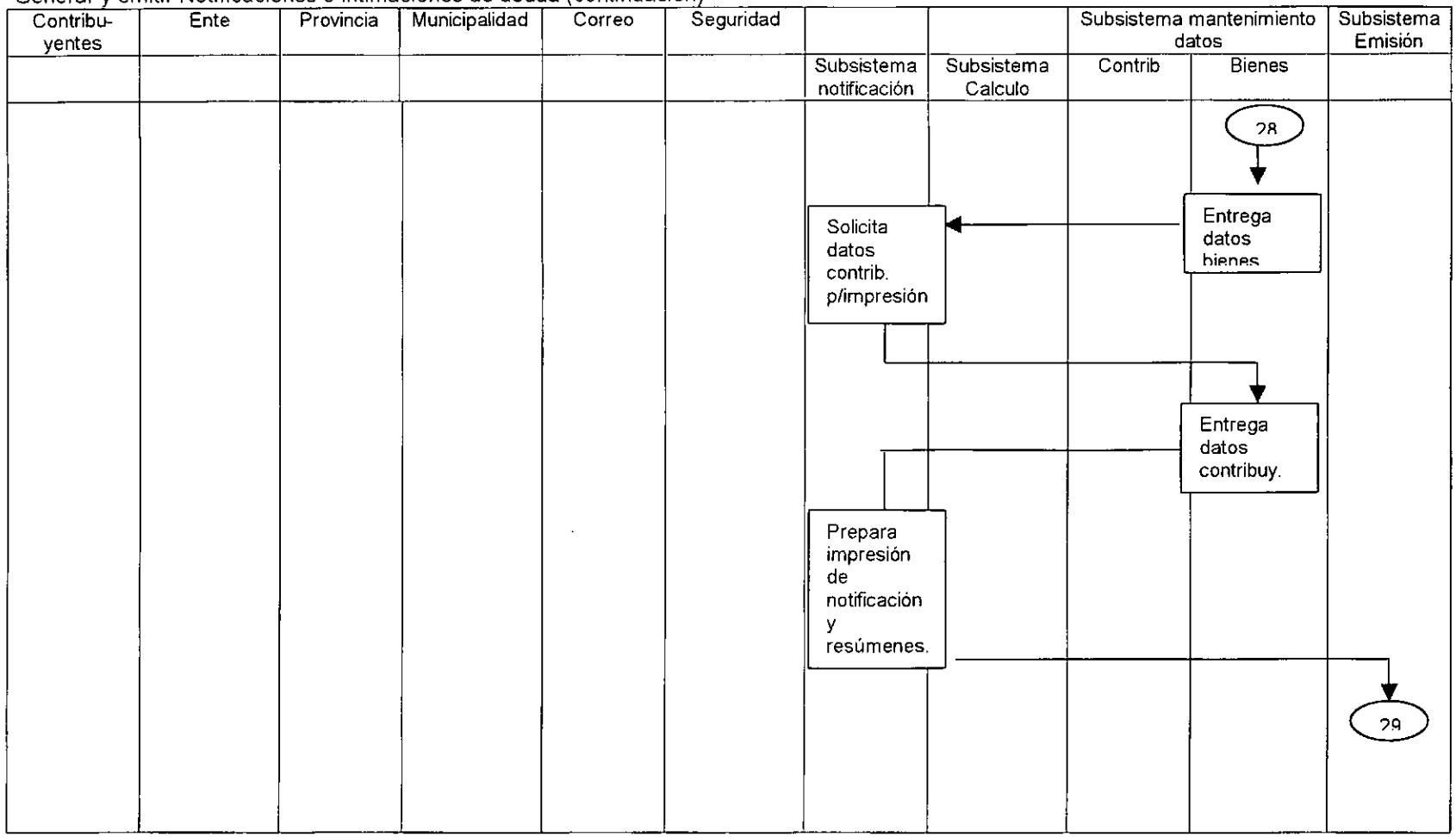
Emitir recibos de Pago (continuación)



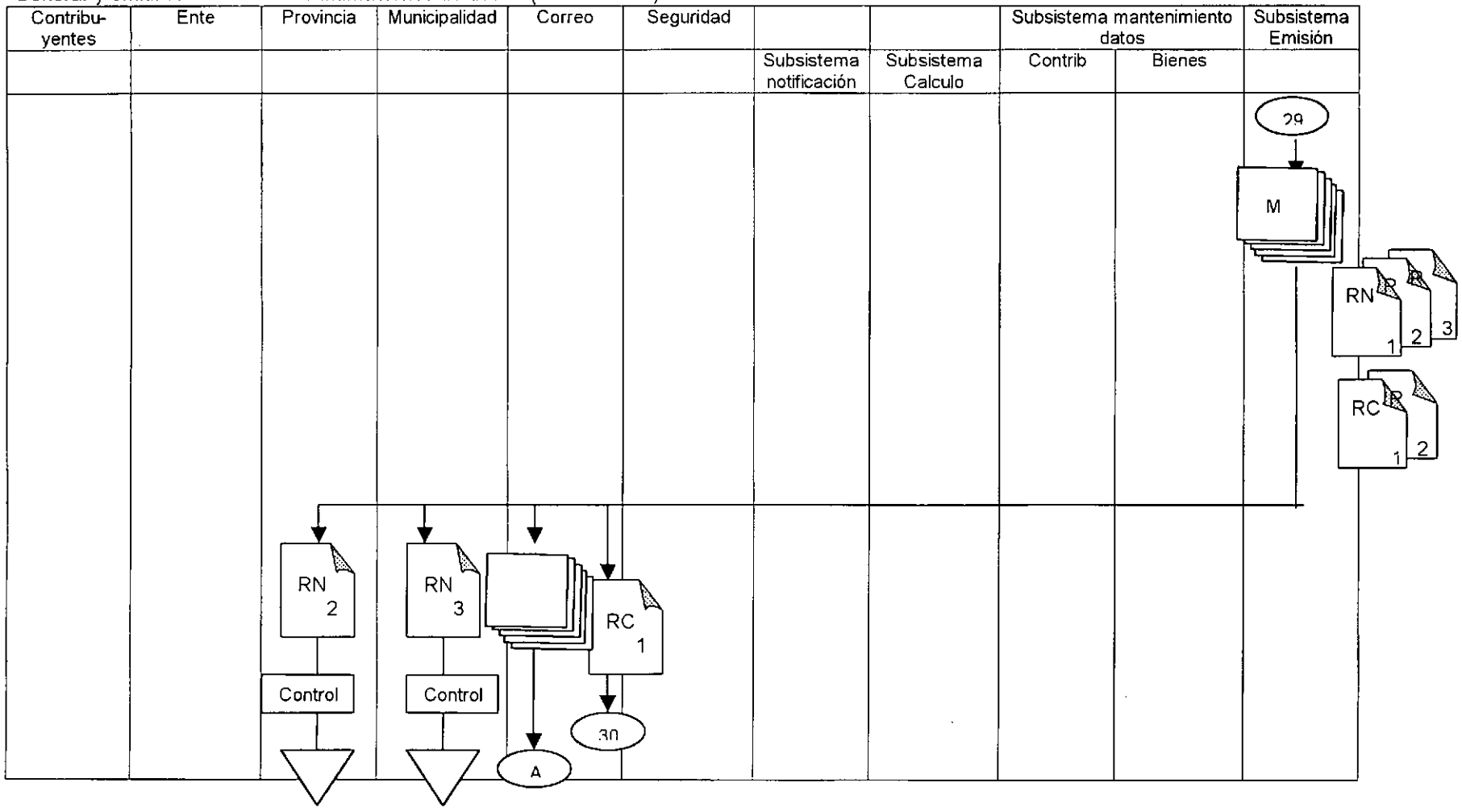
1.6.3.9. Generar y emitir Notificaciones o intimaciones de deuda



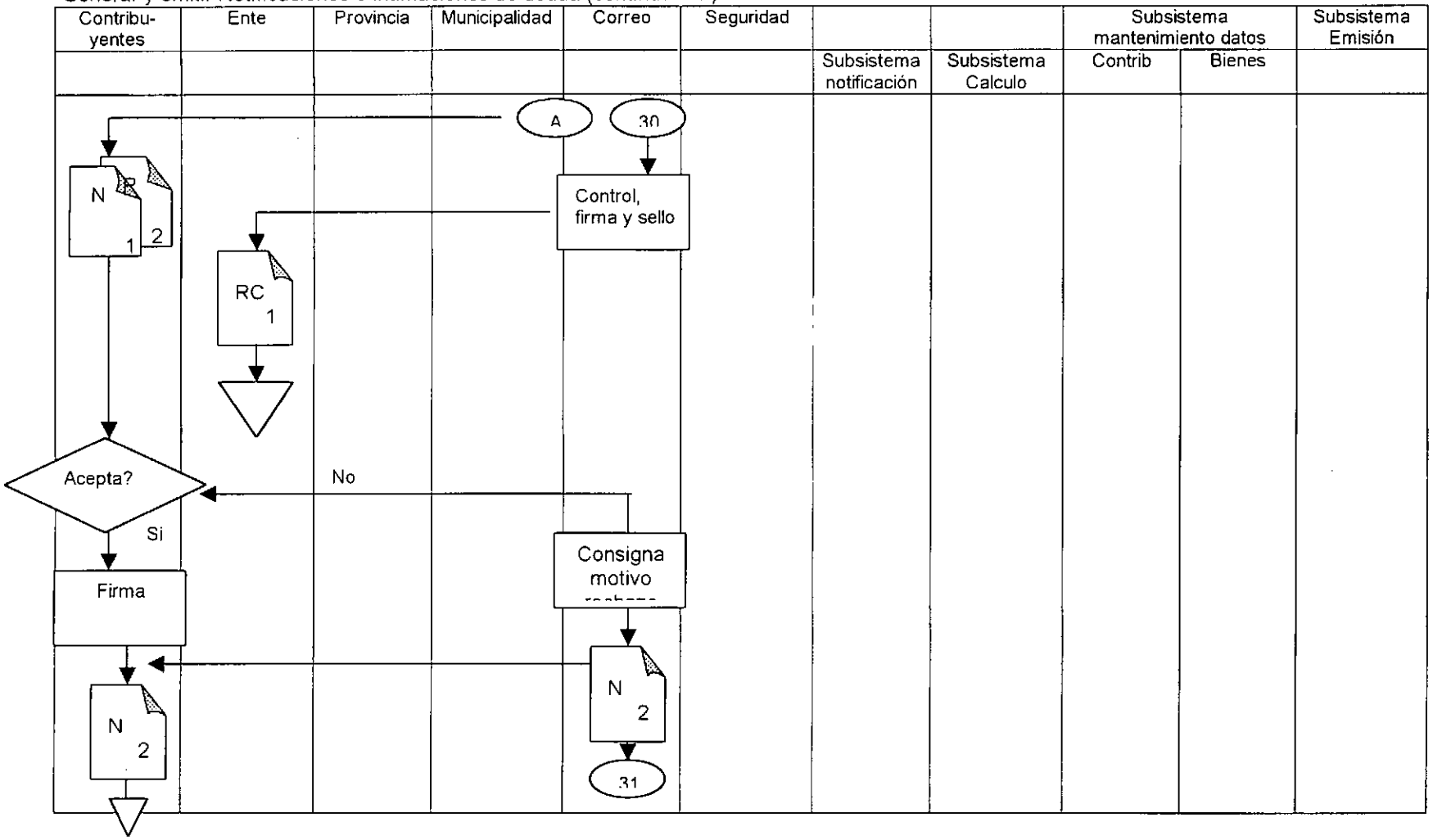
Generar y emitir Notificaciones o intimaciones de deuda (continuación)



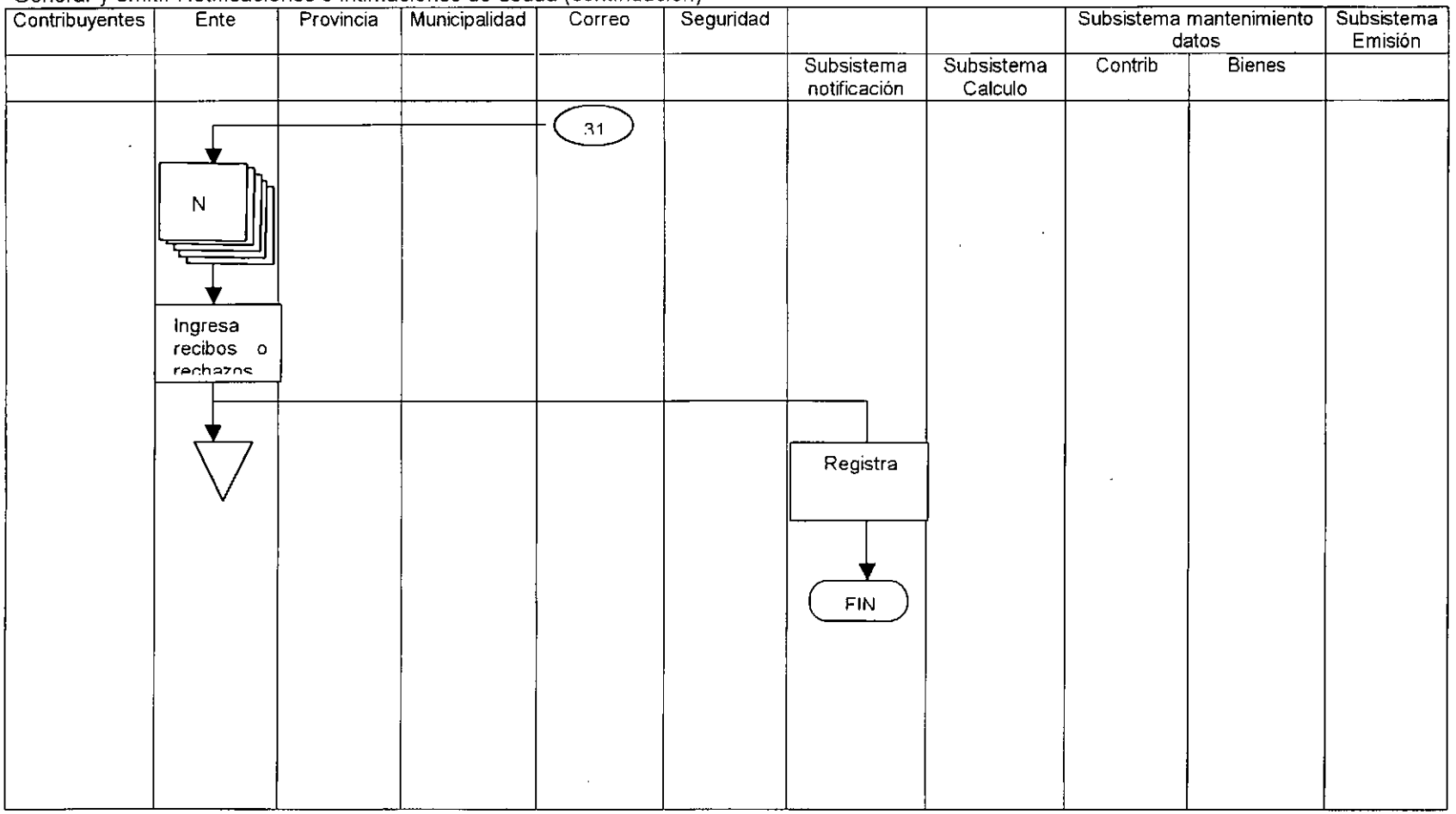
Generar y emitir Notificaciones o intimaciones de deuda (continuación)



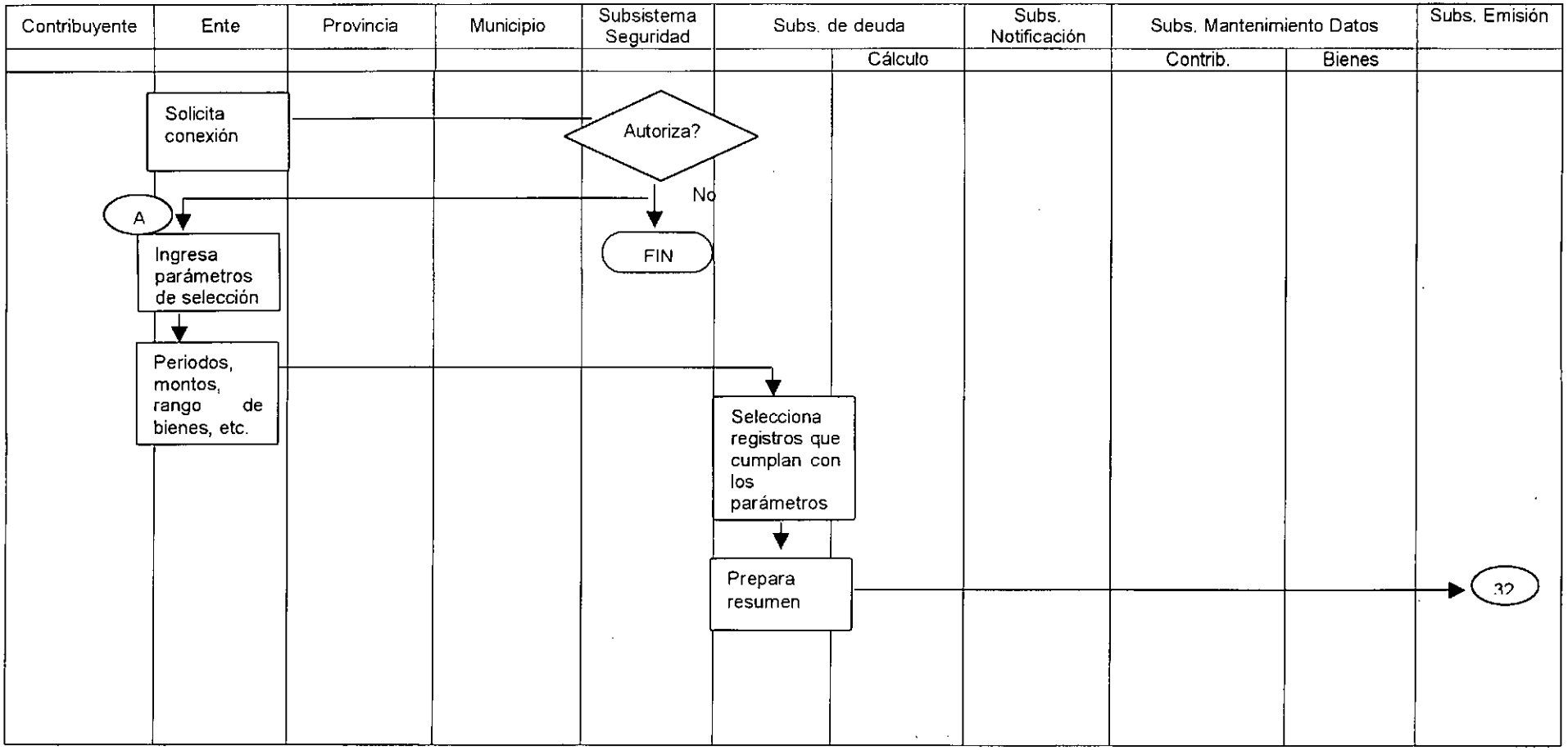
Generar y emitir Notificaciones o intimaciones de deuda (continuación)



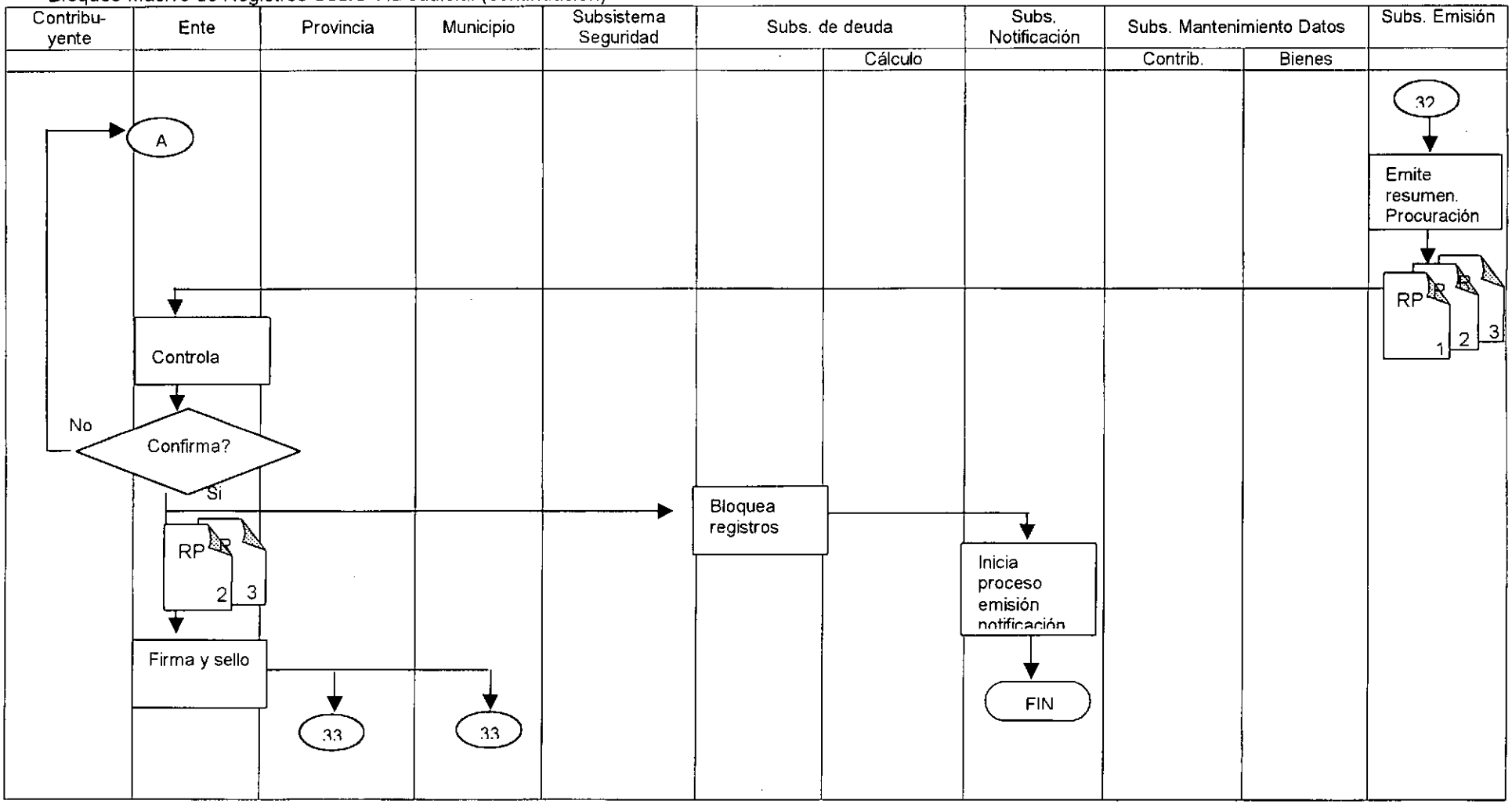
Generar y emitir Notificaciones o intimaciones de deuda (continuación)



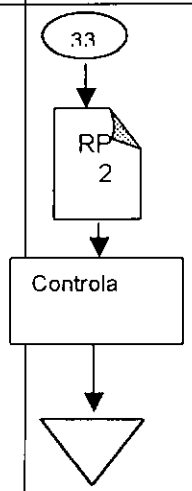
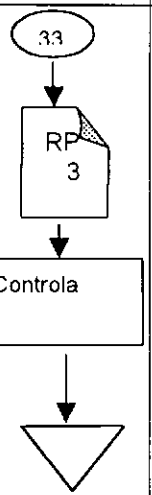
1.6.3.10. Bloqueo Masivo de Registros Cobro Vía Judicial



Bloqueo Masivo de Registros Cobro Vía Judicial (continuación)



Bloqueo Masivo de Registros Cobro Vía Judicial (continuación)

Contribu-yente	Ente	Provincia	Municipio	Subsistema Seguridad	Subs. de deuda		Subs. Notificación	Subs. Mantenimiento Datos		Subs. Emisión
						Cálculo		Contrib.	Bienes	
										

1.7. EQUIPO DE ESPECIALISTAS A CARGO DEL SISTEMA

Muchos sistemas fracasan por falta de un equipo capacitado de seguimiento, mantenimiento y adaptación permanente del mismo.

Para el logro de los objetivos planteados, se propone la formación de un equipo de especialistas en información que tendría a su cargo mantener operativo y actualizado al sistema.

Usamos el término especialistas en información para describir a cualquiera de los empleados de una organización que tiene responsabilidades de tiempo completo en cuanto al desarrollo y mantenimiento de los sistemas.

Hay seis categorías principales de especialistas en información: profesionales en administración, analistas de sistemas, administradores de bases de datos, especialistas en redes, programadores y operadores.

En la figura se muestra la forma en que estos especialistas se trabajado tradicionalmente unos con otros y con el usuario en la creación de sistemas basados en computadoras.

Las flechas representan flujos de comunicación, e incluyen el flujo final de información de la computadora al usuario.

La figura ilustra la cadena de comunicación tradicional que conecta al usuario, los especialistas en información y la computadora. El usuario puede ser un funcionario, un empleado de un organismo o un contribuyente.

Los profesionales en administración realizarán el diagnóstico permanente y detectarán las fallas que el Sistema presente mediante técnicas de monitoreo permanente, relevando y analizando indicadores de satisfacción de los usuarios.

A partir de los diagnósticos formularán estrategias para mejorar la calidad de funcionamiento del Sistema.

Los analistas de sistemas trabajaran con los usuarios en la creación de nuevos sistemas y en el mejoramiento de los sistemas existentes.

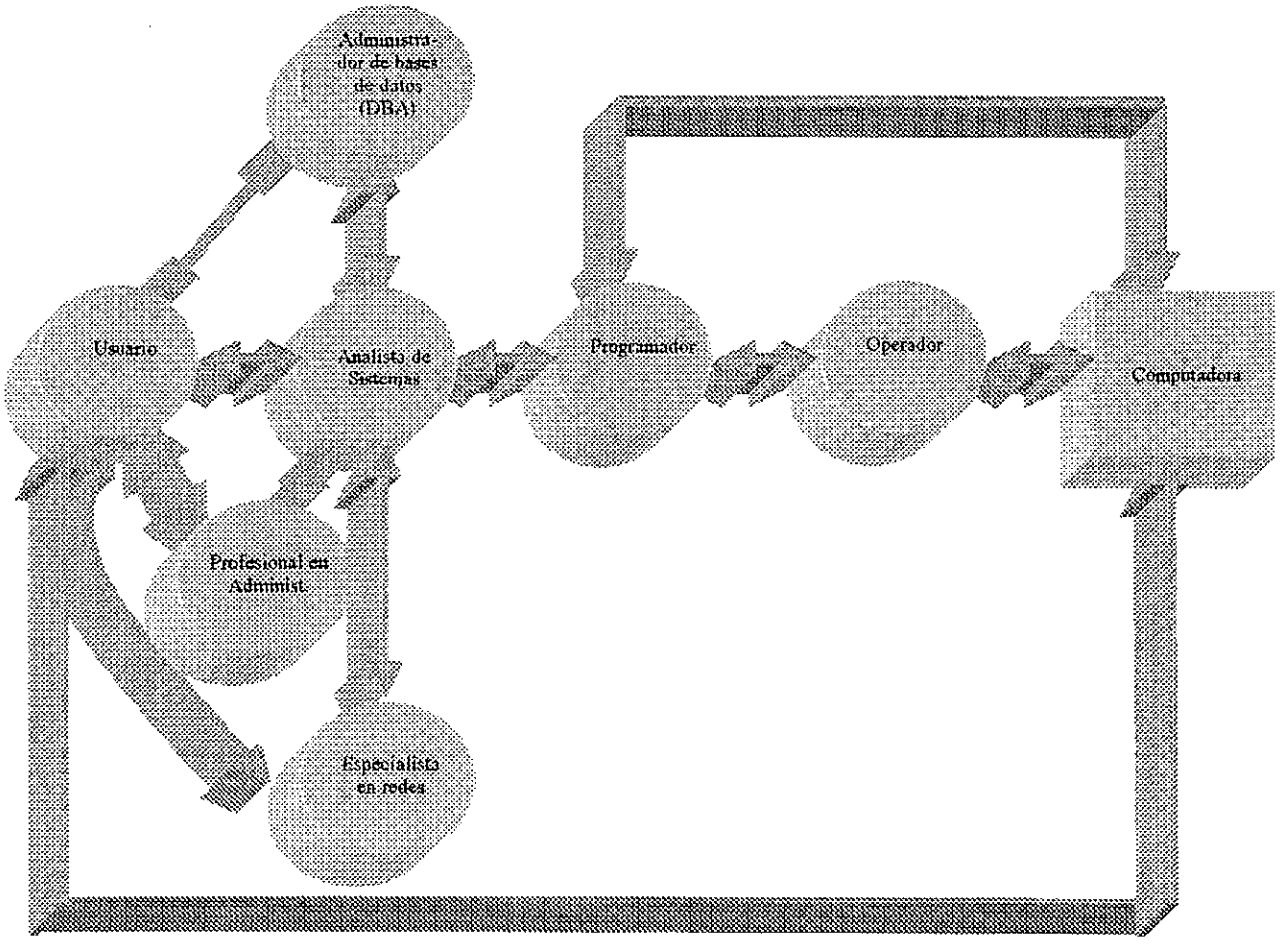
Los analistas de sistemas son expertos en la definición de problemas y en la preparación de documentación escrita que describe la forma en que la computadora ayudará a resolver los problemas.

Los administradores de bases de datos (DBA, database administrators) trabajarán con los usuarios y analistas de sistemas para crear las bases de datos que contienen los datos necesarios para producir la información de usuario. Una base de datos es una colección integrada de datos de computadora, organizados y almacenados de una manera que facilita su recuperación.

Una vez creadas las bases de datos, es común que los administradores de bases de datos controlen estos importantes recursos.

Los especialistas en redes trabajarán con analistas de sistemas y usuarios para establecer la red de comunicación de datos que vincula entre si los recursos de computación dispersos. Los especialistas en redes deberán tener profundos conocimientos en los campos de computación y de telecomunicaciones e Internet.

Los programadores usarán la documentación preparada por los analistas de sistemas para codificar las instrucciones que hacen que la computadora transforme los datos en la información que los usuarios necesitan.



1.8. SEGURIDAD Y CONTROL

Las actividades gubernamentales ya preocupaban por la seguridad mucho antes de que se reconociera que era necesaria en el campo de las computadoras. Siempre se han interesado en la protección física de bienes por medios tales como cerraduras, barreras y guardianes.

La introducción de procesamiento computarizado, técnicas centralizadas de almacenamiento de bases de datos y redes de comunicación ha incrementado la necesidad de la seguridad.

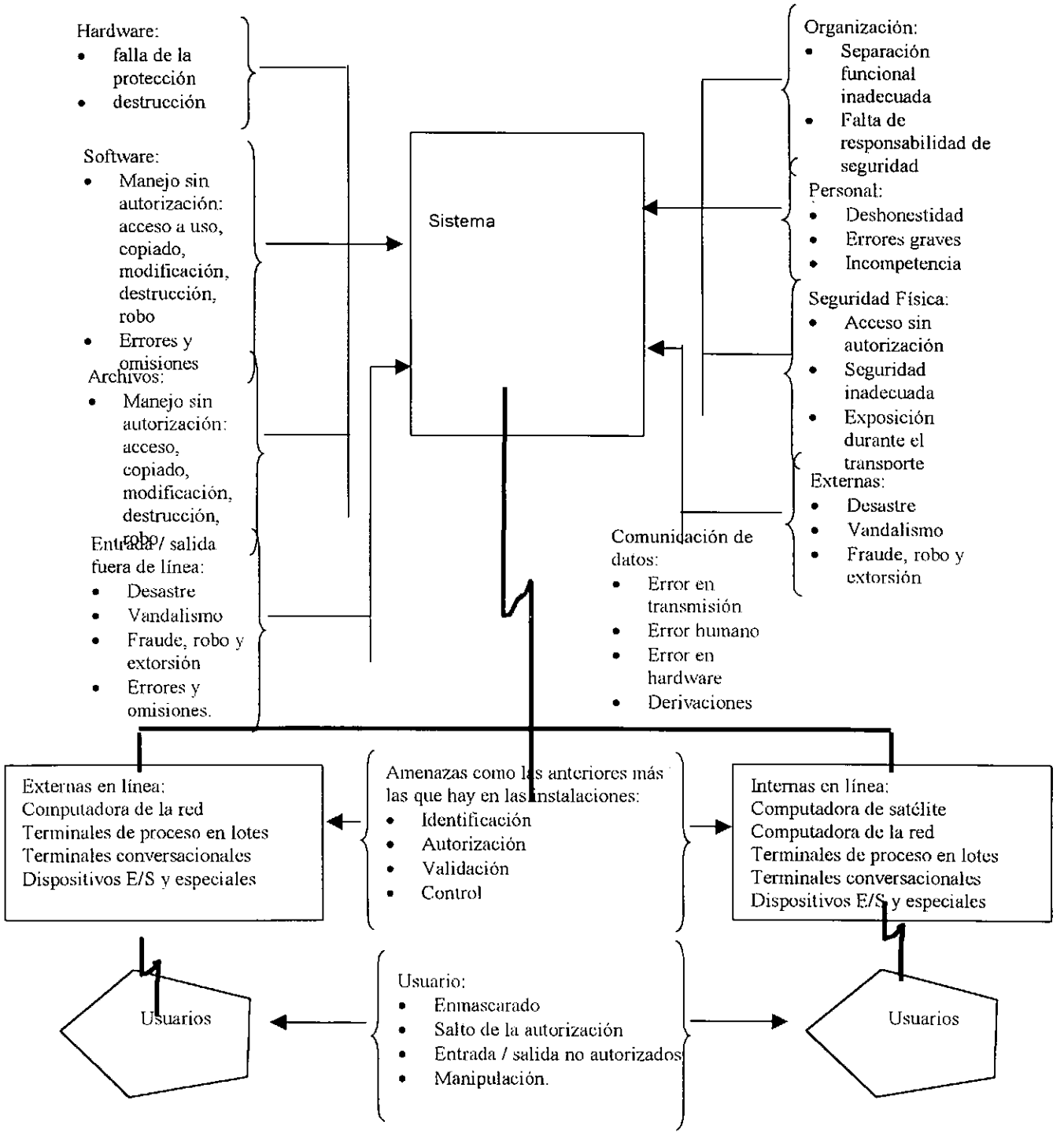
El interés por la seguridad se encuentra ahora enfocado directamente en las áreas relacionadas con la computación de las áreas de las agencias empresariales o gubernamentales.

Este énfasis se manifiesta en la existencia de controles para impedir, detectar y corregir, cualquier cosa que pueda suceder a la organización a través de las amenazas que deben enfrentar sus sistemas basados en computadoras.

En la figura se muestran los componentes del sistema, como hardware, software, organización, personal, comunicación de datos, etc.

Debajo de cada componente se observan unos cuantos ejemplos típicos de las amenazas enfrentadas por los componentes en cuestión.

Por ejemplo, las amenazas tipicas para el componente Comunicaciones de datos son errores de transmisión, errores humanos, errores de hardware y derivaciones ilegales.


Hardware:
• falla de la protección
• destrucción
Software:
• Manejo sin autorización: acceso a uso, copiado, modificación, destrucción, robo
• Errores y omisiones
Archivos:
• Manejo sin autorización: acceso, copiado, modificación, destrucción, robo
Entrada/ salida fuera de línea:
• Desastre
• Vandalismo
• Fraude, robo y extorsión
• Errores y omisiones.
Sistema
Organización:
• Separación funcional inadecuada
• Falta de responsabilidad de seguridad
Personal:
• Deshonestidad
• Errores graves
• Incompetencia
Seguridad Física:
• Acceso sin autorización
• Seguridad inadecuada
• Exposición durante el transporte
Externas:
• Desastre
• Vandalismo
• Fraude, robo y extorsión
Comunicación de datos:
• Error en transmisión
• Error humano
• Error en hardware
• Derivaciones
Externas en línea:
Computadora de la red
Terminales de proceso en lotes
Terminales conversacionales
Dispositivos E/S y especiales
Amenazas como las anteriores más las que hay en las instalaciones:
• Identificación
• Autorización
• Validación
• Control
Internas en línea:
Computadora de satélite
Computadora de la red
Terminales de proceso en lotes
Terminales conversacionales
Dispositivos E/S y especiales
Usuarios
Usuario:
• Enmascarado
• Salto de la autorización
• Entrada / salida no autorizados
• Manipulación.
Usuarios

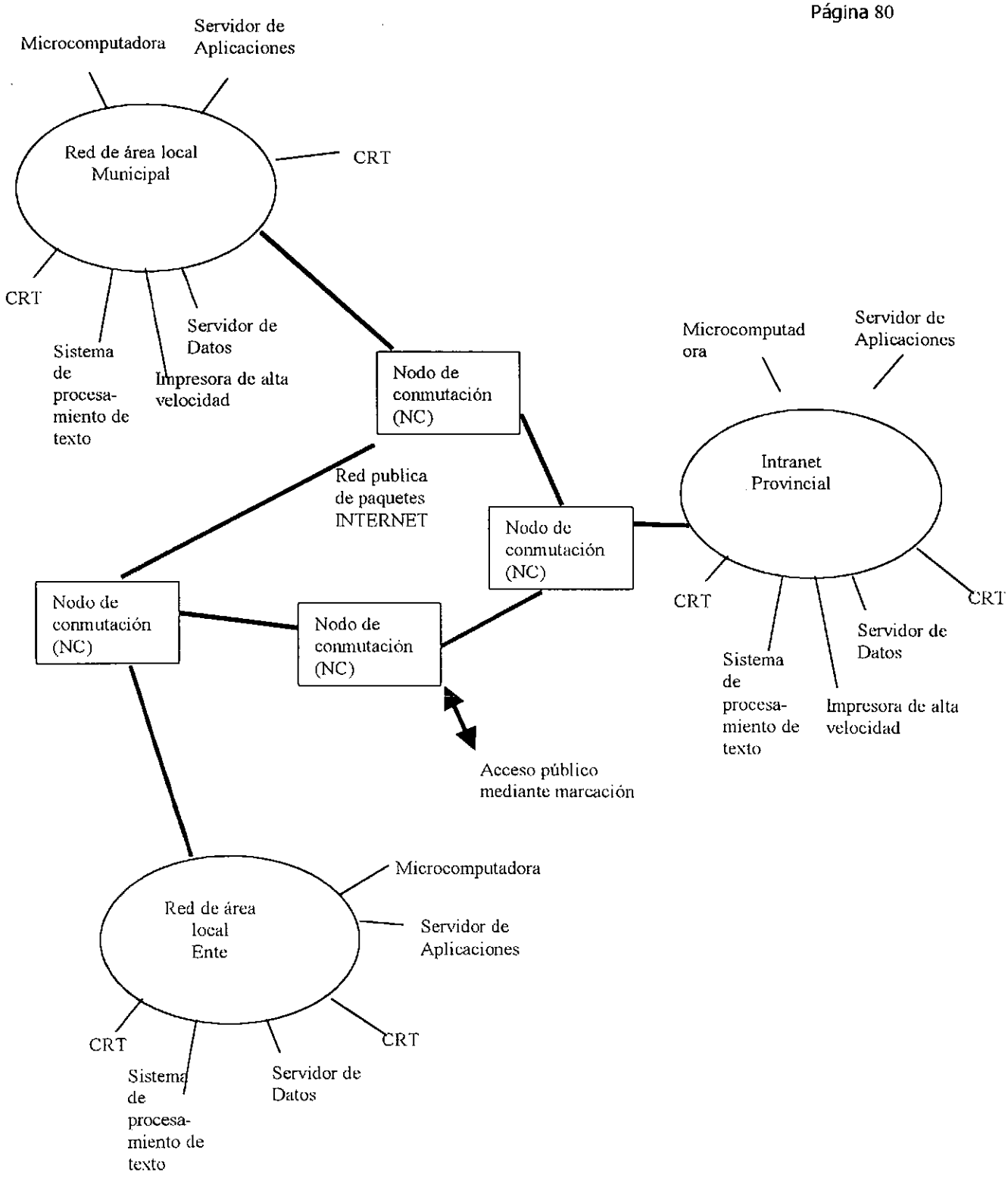
1.8.1. Seguridad en la Red

En años recientes las organizaciones gubernamentales se han vuelto cada vez mas dependientes de las redes de comunicación de datos para las comunicaciones diarias de sus transacciones, la recuperación de bases de datos y el procesamiento de datos distribuidos, tal como se plantea para este Sistema.

Este compromiso con comunicaciones / teleprocesamiento de datos ha cambiado la vulnerabilidad potencial de los bienes de la organización estatal.

Tal cambio se ha dado debido a que la seguridad, el control y los mecanismos de revisión tradicionales asumen una forma nueva y diferente en los sistemas basados en la comunicación de datos.

El incremento en la dependencia respecto de las comunicaciones de datos, la consolidación en sistemas computarizados de muchas operaciones previamente manuales, el uso de sistemas de administración de bases de datos, y el hecho de que los sistemas de tiempo real en línea corten muchas líneas de responsabilidad, han aumentado el interés de la administración por la idoneidad de mecanismos actuales de control y seguridad utilizados en el medio de la comunicación de datos.


Microcomputadora
Servidor de Aplicaciones
Red de área local Municipal
CRT
CRT
Sistema de procesa-miento de texto
Servidor de Datos
Impresora de alta velocidad
Nodo de conmutación (NC)
Red publica de paquetes INTERNET
Nodo de conmutación (NC)
Nodo de conmutación (NC)
Nodo de conmutación (NC)
Microcomputad ora
Servidor de Aplicaciones
Intranet Provincial
CRT
CRT
Sistema de procesa-miento de texto
Servidor de Datos
Impresora de alta velocidad
Acceso público mediante marcación
Red de área local Ente
Microcomputadora
Servidor de Aplicaciones
CRT
CRT
Sistema de procesa-miento de texto
Servidor de Datos

También ha habido un énfasis creciente sobre la seguridad de la red de computación debido a las numerosas acciones legales que implican a funcionarios y directores de organizaciones, a los pronunciamientos de agencias gubernamentales reglamentarias, y a que las perdidas asociadas con fraudes de computación son mucho mas grandes por incidente que las de los fraudes no relacionados con computadoras. Estos factores han hecho aumentar la vigilancia con respecto a la protección de los bienes de información de las organizaciones gubernamentales contra muchos riesgos potenciales como fraudes, errores, perdidas de datos, violaciones de privacia y desastres que pueden ocurrir en una red de comunicación de datos estatal.

Con respecto a las redes de comunicación de datos, la organización debe ser capaz de implementar mecanismos adecuados de control y seguridad dentro de sus instalaciones, incluyendo edificios, terminales, redes de área local, líneas de abonados locales, centros de conmutación, unidades de interfaz de red (accesos), redes de paquetes, hardware (modems, multiplexores, dispositivos de cifrado, etc), protocolos de redes, software de la arquitectura de redes, equipo de prueba y control de la administración de la red.

En la figura se muestra un esquema de la red que se pretende implementar, donde el protocolo de comunicaciones a utilizar será el TCP/IP protocolo de Internet.

El mayor peligro que representa un acceso TCP/IP no autorizado viene precisamente por la mayor virtud del TCP/IP: su amplia disponibilidad de utilidades. Dada la estandarización de las utilidades TCP/IP, es muy razonable suponer que cada máquina con acceso TCP/IP tenga "puertos abiertos" , que a su vez tiene direcciones normalizadas donde encontrar transmisores de ficheros, servidores de correo, terminales virtuales y todo tipo de servicios de utilidad. Una ausencia de protección significaría que un tercero puede utilizar estos servicios normalizados, de común existencia en cualquier maquina, en beneficio propio.

En tal red todas las áreas antes mencionadas requieren una decisión positiva (políticas y procedimientos) en cuanto a seguridad y control. Con este tipo de red la organización es vulnerable en muchos puntos de entrada para algún intruso no autorizado.

Se analizara cada una de las porciones mas importantes de la red de comunicaciones de datos, como hardware software y se describirán los diversos controles que podrían usarse para evitar, detectar o corregir amenazas en el área especifica correspondiente.

Por ultimo, se presentara una metodología de matriz de control para identificar las amenazas y sus controles asociados.

Dicha matriz proporciona al administrador de la red de comunicación de datos un panorama adecuado de las amenazas del momento y cualesquiera controles oportunos para reducir tales amenazas.

Puntos de Control de la Red.

Para implementar un programa de seguridad aceptable en el medio de una red de comunicación, primero es necesario identificar todos los puntos en los que es necesario establecer el control.

Tales puntos se denominan puntos de control.

Una vez que se ha determinado en dónde se deben ubicar estos controles, entonces es posible identificar que controles individuales son realmente necesarios en la red.

Se han identificado puntos de control (es decir, áreas en las que es necesario implementar mecanismos de control y seguridad) para la red de comunicación.

El administrador de la red, el personal de auditoria informática o el oficial de seguridad deberán analizar tales áreas a fin de tener la certeza de que se implementen controles idóneos y que funcionen correctamente.

En esta lista se define el punto de control y se describe el tipo de seguridad general en cada uno de los puntos.

Como primer punto de control debe evaluarse la seguridad física de los edificios que alojan a cada uno de los circuitos de hardware, software o de comunicación.

Tanto las instalaciones locales como remotas deben asegurarse adecuadamente y contar con controles propias.

La seguridad del operador y demás personal implica la implementación de controles de acceso adecuados, de modo que solamente personal autorizado pueda entrar a áreas cerradas en las que se encuentra equipo de la red, o acceder a la red en si.

En esta área se incluyen adiestramiento adecuado en cuanto a seguridad, verificaciones de fondo e implementación de controles contra errores / fraudes.

Las terminales constituyen un área esencial en la que deben reforzarse los tipos físico y lógico de controles de seguridad.

Por seguridad física, es necesario revisar los cables conectores locales y los pares de alambre y tendidos a lo largo de las instalaciones de la repartición.

Los dispositivos locales de control de información que controlan grupos de terminales se deben revisar mediante controles programados físicos y lógicos.

El cifrado de hardware constituye un punto crucial de control, especialmente porque se relaciona con la seguridad de los mensajes.

Los módem se deben revisar, ya que se relacionan con el control y la seguridad en este punto de la red.

Los multiplexores, en caso de utilizarse en la red, se deben asegurar para evitar ingresos no autorizados, y además deben contar con circuitos de respaldo. Puede ser necesario contar con seguridad física y energía eléctrica de respaldo en un sitio remoto.

Se deben revisar las líneas de abonado locales que van de la repartición a la instalación de conmutación de la empresa de comunicaciones.

Es necesario evaluar la seguridad física y de apoyo de la instalación de conmutación en la empresa de comunicaciones (ofician de la central telefónica). Si esta instalación fuese destruida, se perderían todos los circuitos. Esta revisión podría incluir tanto oficinas centrales en alguna ciudad como estaciones terrenas para la transmisión vía satélite.

Los mecanismos de seguridad / control en el sitio mismo deben revisarse con respecto a los circuitos del canal intercentral (IC)

Un punto esencial de control es el sistema de bitácora, mediante el cual se registran todos los mensajes de entrada y salida.

El procesador de comunicación de entrada es otro punto esencial de control que se debe revisar.

En nodo de conmutación (NC) por paquetes, se debe revisar por seguridad y control.

Es necesario revisar todos los controles integrados al software de la computadora principal.

También dentro de la computadora principal, es necesario revisar todos los controles diseñados en los mecanismos/arquitectura del hardware.

Otro punto crucial de control, aunque solamente en los sistemas de bases de datos, es el soporte de registro de entrada de la base de datos antes y después de la imagen.

Otro punto de control es el sistema de administración de bases de datos (SABD) en si mismo.

El software del sistema de administración de bases de datos deberá contar con algunos controles que ayuden con respecto a la seguridad de la red de comunicación de datos y al control del flujo de datos / información.

El ultimo punto de control es el centro de control de la red en si.

Esta área tiene controles que se relacionan con administración y operación, equipo de prueba utilizado, informes, documentación, etc.

Los puntos de control mencionados constituyen las áreas especificas en las cuales es posible implementar y mantener características de control dentro de la red de comunicación de datos

Cada uno de los tres aspectos: técnico, software, seguridad de la red, se encuentra localizado a lo largo de toda la longitud de la red.

1.8.1.1. Cifrado

El cifrado, es el proceso de disfrazar información mediante el empleo de muchas reglas matemáticas posibles conocidas como algoritmos.

El descifrado es el proceso de restituir la información a una forma legible.

Por supuesto, no tiene sentido contar con un proceso sin el otro.

Cuando la información está en forma legible, se denomina texto claro o llano, cuando está cifrada, se denomina texto cifrado.

El arte de la criptografía es muy antiguo, y hasta hace poco, casi siempre fue utilizado en aplicaciones militares y políticas. Sin embargo, para las normas actuales de precisión tales códigos son inseguros y por lo tanto obsoletos.

El interés en la protección criptográfica alcanza su máxima expresión en el mundo de las comunicaciones.

De todas las rutas y lugares de descanso de la información, la mas vulnerable de revelar es la información comunicada.

Los datos almacenados en cintas magnéticas o en discos y en la memoria de la computadora pueden protegerse en gran medida mediante seguridad física, contraseñas y otros sistemas de control de acceso al software.

En las comunicaciones de datos modernas se aprovechan recursos ya existentes como circuitos telefónicos, transmisiones de microondas y relevadores vía satélite. Como resultado, la información comunicada está altamente expuesta de varias maneras.

Puede ser capturada con un mínimo de riesgo y costo para el ladrón de datos, y con una perdida máxima para la organización.

El sistema de cifrado consta de dos partes: el algoritmo en si, que es el conjunto de reglas para transformar la información, y la llave, que personaliza el uso de algoritmo al hacer única la transformación de los datos del usuario. Dos partes de información idéntica cifradas con el mismo algoritmo pero con llaves diferentes producen textos cifrados completamente diferentes. Cuando se utilizan la mayoría de los sistemas de cifrado, las partes en comunicación también deben compartir esta llave.

Si el algoritmo es adecuado y la llave se mantiene en secreto, entonces la adquisición del texto cifrado por parte de una persona no autorizada no tiene consecuencias para las partes en comunicación.

La llave es un valor numérico relativamente pequeño (en números de bits) que debe ser fácilmente transportable de un nodo de comunicación a otro.

La llave es como suena, se trata de algo pequeño, portátil y que con la ayuda de un buen cerrojo o cerradura, el algoritmo, mantiene los valores donde deben estar.

Los buenos sistemas de cifrado no dependen de la manutención en secreto del algoritmo. Solamente deben mantenerse en secreto las llaves.

El algoritmo debe ser capaz de aceptar un gran número de llaves, cada una de las cuales produce diferentes textos cifrados a partir del mismo texto llano.

Este gran "espacio para la llave" protege el texto cifrado contra quienes tratan de violarlo intentando todas las llaves posibles, de modo que una investigación computarizada exhaustiva consuma una cantidad excesiva de tiempo o cueste mucho mas que el valor de la información cifrada.

Los algoritmos de cifrado pueden implementarse en software o en hardware.

El software presenta más ventajas para la protección de archivos de datos y datos almacenados en la memoria de la computadora principal. Sin embargo, las implementaciones en hardware presentan las ventajas de velocidad de procesamiento mucho mas alta, independencia de los protocolos de comunicación, y mayor protección de la llave debido a que se encuentra fisicamente encerrada en la caja de cifrado. Los intentos no autorizados para forzar la caja provocan el borrado de las llaves y de información relacionada con ellas.

Las implementaciones de hardware han sido reducidas al nivel de pastilla porque son simplemente microprocesadores especializados alojados en pequeñas cajas de hardware.

Para la implementación del Sistema se recomienda la utilización de cifrado mediante criptosistemas de llaves públicas que se describe a continuación.

Los criptosistemas de llaves públicas son inherentemente distintos de los sistemas de llaves privadas, como la DES. Aquellos se basan en funciones de un solo sentido (unidireccionales).

En los algoritmos de llaves públicas, aun cuando originalmente se conozca el contenido de un mensaje y la llave de cifrado pública, una vez que se unen (cifran) por medio del algoritmo de función unidireccional ya no es posible separarlos, a menos que se cuente con la otra llave (privada).

Las funciones unidireccionales, que son relativamente fáciles de calcular en un sentido, son computacionalmente imposibles de "descalcular" en el sentido opuesto.

El remitente del mensaje debe buscar la función de cifrado en un sentido del destinatario en el directorio de llaves públicas y utilizarla para cifrar el mensaje. Los receptores mantienen sus propias llaves secretas o los algoritmos de descifrado complementarios (llaves publicas) para esta función unidireccional.

La diferencia esencial entre un sistema de llaves públicas (asimétrico) y un sistema de llaves privadas (simétrico) como la DES es que en aquel no se intercambian llaves secretas entre las partes comunicantes. Sin embargo, los sistemas de llaves públicas no eliminan el problema de distribución de las llaves, pero dicha distribución cuesta menos de la décima parte de lo que cuesta para la clase simétrica de algoritmo como la DES. Durante el inicio del sistema sigue siendo necesario distribuir las llaves. Un directorio público que contiene la función de cifrado unidireccional de cada participante es compartido por la comunidad. La fortaleza de tales sistemas radica en mantener el secreto de la función de descifrado y la capacidad del algoritmo para resistir el criptoanálisis. Si alguna persona resuelve la función unidireccional de la llave pública, entonces se compromete el sistema. La función unidireccional está basada en la dificultad de factorizar números primos bastante grandes. La solución a este problema ha escapado a los matemáticos durante años.

En los sistemas de cifrado de llaves públicas, la llave necesaria para descifrar un mensaje es diferente de la utilizada para cifrarlo. Las dos llaves están lejanamente relacionadas en un sentido matemático. La seguridad de los sistemas asimétricos depende de la dificultad extrema (imposibilidad analítica o imposibilidad computacional) de deducir una llave a partir de la otra.

Los algoritmos asimétricos pueden reducir bastante el problema de administración de llaves. Cada nodo receptor cuenta con su llave disponible al publico (de aquí el nombre "llaves publicas"), que es utilizada para cifrar mensajes enviados por cualquier miembro de la red a tal nodo. Estas llaves públicas pueden enumerarse en un directorio al estilo del telefónico. Además, cada usuario tiene una llave privada que descifra solamente los mensajes cifrados por su llave publica. El resultado neto es que si dos partes desean comunicarse entre si, entonces no hay necesidad de intercambiar llaves de antemano. Cada una de las partes conoce la llave publica de la otra parte gracias al directorio y puede comunicar de inmediato información cifrada. El problema de administración de llaves puede reducirse a que cada usuario se preocupe solo por la protección in situ de su llave privada.

En los algoritmos de llave pública se implementará el sistema de firma digital, que garantiza el origen del mensaje y no puede ser desconocido por el emisor.

De esta manera quién va ha emitir un mensaje con firma digital primero cifra su nombre y otros datos claves del mensaje a manera de firma con su propia llave privada, lo incorpora al resto del mensaje y lo cifra con la llave pública del destinatario.

El destinatario cuando recibe el mensaje lo descrifa con su llave privada, quedando cifrado la parte de la firma, lo que descifra con la llave pública del emisor, si

este proceso funciona correctamente garantiza que el emisor fue el indicado, ya que el único que pudo generar Un texto descifrable con la llave pública del emisor, es el emisor mismo con el uso de su llave privada.

De esta manera, el sistema de llaves pública cifra mensajes y también ofrece identificación electrónica de firma sin que haya ningún intercambio de llaves entre quienes se comunican.

El directorio público solamente requiere ser actualizado tanto como sea necesario. Es posible cifrar con una llave publica y descifrar con una llave privada, o viceversa.

Los algoritmos para los sistemas de llaves públicas son bastantes diferentes de los algoritmos simétricos como la DES, aunque en la practica sus textos cifrados son semejantes cuando se consideran desde el punto de vista de la comunicación de datos. Cada uno produce textos cifrados que constan de patrones de bits aleatorizados.

Casi siempre existe algún grado de error de propagación, por consiguiente, los aspectos prácticos en cuanto al manejo de comunicación de ambos tipos de textos cifrados son casi idénticos.

El mundo del cifrado está lleno de controversias y debates, provocados parcialmente por la tensión entre los gobiernos y los cifrados académicos independientes.

El asunto es siempre la seguridad nacional. Sin embargo, la razón subyacente a este debate es el hecho de que el cifrado es un arte mas que una ciencia. Quitando algunas excepciones dignas de atención, es matemáticamente imposible demostrar si puede quebrantarse un algoritmo de cifrado / descifrado. Así, la única ruta para quebrantar algo cifrado es un método hábil (y quizá tardado y costoso) de ensayo y error.

1.8.1.2. Controles de Hardware

El hardware de la red se analiza aquí en términos de los controles que se relacionan con él. Se analizarán los controles que se relacionan con procesadores de entrada, controladores de conmutación de paquetes, módems, multiplexores, controladores de información remotos, terminales y seguridad de voz por teléfono.

Procesadores de entrada: el procesador de entrada que controle la red de comunicación de datos regulada centralmente puede ser una de las áreas mas importantes de la seguridad y el control. Se trata solamente de una parte del hardware, pero dentro de ella se encuentran programas / protocolos de software que controlan los métodos de acceso para el flujo de datos.

Algunos de los controles específicos que es posible alojar en el interior del procesador de comunicación de entrada son:

- Exploración de terminales para asegurar que en la red solamente haya terminales autorizadas
- Registro de todos los mensajes que entran y salen por razones históricas y para recuperación inmediata en caso de falla del sistema
- Detección de errores y retransmisión de mensajes que llegan con error.

- Conmutación de mensajes, lo que reduce la posibilidad de perder mensajes (también puede haber conmutación de circuitos o conmutación de paquetes)
- Técnicas de almacenamiento y envío que ayudan a evitar la perdida de mensajes (aunque estas técnicas abren la posibilidad de que un programador de la red copie mensajes del disco de almacenamiento)
- Números de serie para todos los mensajes entre todos los nodos.
- Rellamada automática en instalaciones de marcación, a fin de evitar que la computadora principal se conecte a una terminal con marcación no autorizada
- Edición de sistemas, como reenrutamiento de mensajes y activación de alarmas remotas si se exceden ciertos parámetros o si sucede algo anormal
- Recopilación de estadísticas del trafico de la red para el control a largo plazo de toda la red.

Controladores de conmutación de paquetes: Un contralor de conmutación de paquetes o nodo de conmutación (NC) es semejante a un procesador de conmutación de entrada, pero cuenta con características mas especializadas relativas a la operación de una red de paquetes. El contralor de conmutación de paquetes puede efectuar cualquiera de las funciones de control ya mencionadas para los procesadores de entrada. Además, realiza otras funciones especificas de control como las siguientes:

- Sigue el registro de mensajes entre diferentes nodos de la red
- Controla la numeración de cada paquete para evitar la perdida de paquetes o mensajes, o inserciones ilegales.
- Enruta todos los mensajes. Puede enviar paquetes diferentes, con partes del mismo mensaje, por circuitos diferentes (trayectoria desconocida del circuito). Esto suele evitar que algún usuario/perpetrador no autorizado reciba todas las partes de un mensaje confidencial.
- Contiene bases de datos globales, locales o ambos con direcciones y otros datos confidenciales relativos a cada nodo. Estas bases de datos pueden guardar referencias cruzadas con otros documentos escritos cuando los nodos de la red se revisan por seguridad.
- Mantiene la pista del emisor de cada mensaje entregado en redes de paquetes con marcación, para fines de control y facturación.

Restringe a los usuarios la marcación o permite el empleo de circuitos arrendados en la red de paquetes.

Modems: El módem puede ser una unidad de interfaz ya sea para circuitos de comunicación de banda ancha (analógicos) o circuitos de comunicación de banda base (digitales). No importa para cuales, ya que estas unidades de hardware pueden efectuar cualesquiera de los controles que se mencionan enseguida, dependiendo de las características instaladas por cada fabricante.

Algunos controles del módem con marcación consisten en cambiar los números telefónicos del modem periódicamente, preservar confidenciales los números telefónicos tanto en el sitio del usuario como en el punto central de datos, posiblemente impedir la recepción automática de llamadas en el centro de datos (mediante el empleo de personal para interceptar las llamadas), eliminar números telefónicos de modems con marcación tanto locales como remotos, y solicitar el uso de terminales que tienen un circuito de identificación electrónica para todos los puertos con marcación. Por ultimo,

podría ser aconsejable utilizar un medio con marcación sólo hacia fuera, con el cual el acto de marcar hacia la red y proporcionar una contraseña activa automáticamente una desconexión, el procesador de entrada o la computadora principal marcan entonces el numero telefónico "aprobado" que corresponde a la contraseña utilizada durante la marcación original. En otras palabras, la marcación hacia dentro activa una marcación hacia fuera.

Multiplexores: Dado que muchos sitios de multiplexaje se encuentran en lugares remotos, un control elemental es impedir el acceso físico al multiplexor. Otra consideración es si el multiplexor debe contar con circuiteria doble o con energía eléctrica de apoyo (o con ambas cosas), ya que la perdida de un sitio de multiplexaje remoto puede desconectar a cientos de terminales. Debido a que los multiplexores estadísticos por división en el tiempo cuentan con espacio de memoria interna, y algunos tienen almacenamiento en disco facilitan el copiado ilegal de los mensajes. Otros controles son alojar todos los mensajes en el sitio del multiplexor remoto antes de su transmisión a la computadora principal y registrar manualmente todas las visitas de servicio de los proveedores.

Prevención de errores humanos en terminales: Con respecto al control de terminales o microcomputadoras en la red de comunicación de datos será necesario considerar sus áreas básicas. La primera implica mitigar los errores humanos mientras se están ejecutando sistemas con aplicaciones, y la segunda es proporcionar seguridad para terminales.

Serán necesarios controles para evitar, detectar y corregir errores humanos porque, de las dos áreas mencionadas, los errores humanos provocan la mayor perdida económica. Primero se presentará un listado de controles para prevención de errores humanos, y luego se procederá a pasar a la segunda área, que es el establecimiento de controles de restricción para la seguridad en terminales/microcomputadoras remotas.

Deberá proporcionarse capacitación adecuada a los operadores, mediante manuales autodidácticos y la actualización periódica de tales manuales.

El dialogo entre el operador y el sistema de aplicación debe mantenerse sencillo.La utilización de las terminales debe ser fácil, y éstas deben contar con tableros funcionales.

Las instrucciones deben estar programadas y disponibles para su reutilizacion cuando algún operador necesite ayuda.

Una excepción podrían constituirla los sistemas asegurados, en los cuales debe ser más difícil obtener ayuda.

Los operadores deben contar con procedimientos de rearranque que sea posible utilizar para la recuperación de errores durante una transacción.

Para que los operadores reduzcan al mínimo los errores, entonces será necesario minimizar los extremos en el área de trabajo en cuanto a iluminación, ruido, temperatura, etc.

Los tiempos de respuesta razonablemente breves reducen los errores, porque mayores tiempos de respuesta producen frustración causante de errores en los operadores. Los grandes tiempos de respuesta también reducen la productividad.

Las terminales inteligentes pueden editar errores administrativos lógicos y verificar los datos antes de su transmisión.

1.8.1.3. Controles de seguridad en terminales:

La terminal o la computadora personal remotas pueden ser el punto más importante para controlar la seguridad, los controles específicos deben reforzarse ahí. Existen tres formas generales para restringir el acceso a sistemas de computo o bases de datos, basadas en algo que se sabe, en algo que se tiene, o en algo que se es.

Primero, restringir el acceso mediante algo que se sabe implica el empleo de alguna tipo de código o contraseña de identificación secreto / restringido. Estos códigos / contraseñas se emiten a usuarios autorizados del sistema, que deben mantener la confidencialidad de ellos. Para ingresar al sistema, los usuarios solamente requieren introducir su ID/contraseña.

Segundo, el acceso puede restringirse mediante algo que se tiene, como una llave. Esta puede ser una llave física como las que se utilizan para abrir la puerta de una casa o encender un automóvil, o puede ser una llave electrónica

(números secretos cifrados contenidos en una pequeña pastilla de circuito). Un producto así es la ACCESS KEY (llave de acceso), del tamaño de una ficha de domino, que añade autentificacion del usuario a la seguridad existente en la red. Con esta ACCESS KEY el usuario introduce su ID/contraseña y, si es valida, entonces el sistema central genera un patrón intermitente en la pantalla de la microcomputadora o de la terminal. Por tanto, una ACCESS KEY no funcionara sin una ID/contraseña valida. El usuario que desea tener acceso sostiene la ACCESS KEY contra el patrón intermitente y aquella genera una contraseña única (que solamente es posible utilizar una vez) la cual debe teclearse y transmitirse de vuelta al sistema central. El sistema central conecta al usuario remoto sólo si esta contraseña única es correcta.

Esta ACCESS KEY está compuesta por sensores ópticos un circuito integrado, un reloj de tiempo real hecho de cristal de cuarzo, una pantalla de cristal liquido y una batería de litio que dura cinco años. En la pastilla electrónica se integran detección óptica y técnicas de codificación de datos (cifrado) patentadas a fin de impedir que el dispositivo sea duplicado. Además, la contraseña generada por la ACCESS KEY es única para cada acceso, y el reloj de tiempo real cambia automáticamente cada tres días la llave de cifrado contenida en la ACCES KEY del usuario. Debido a que cada ACCESS KEY es única para una ID/contraseña especifica de un usuario, hay identificación positiva para que el usuario entre al sistema. Esto significa que a los usuarios puede permitírseles acceso limitado una vez que han logrado entrar a la red.

Tercero, para restringir el acceso "por algo que se es ", se utilizan una o varias de las características físicas del usuario como identificador único que le permita la entrada al sistema. Esto puede ser una huella digital, la huella de una mano, la impresión de la retina de un ojo, una impresión de la voz, la verificación de una firma, etc. Actualmente estas técnicas pueden ser demasiado costosas, pero en el futuro serán la norma.

Para el caso del presente sistema se propone la utilización de los dos primeros tipos de identificación, según las exigencias de seguridad de cada caso.

Los siguientes son algunos controles específicos de seguridad que podrían implementarse en la localización de la terminal / computadora remota.

- Asegurarse de que las terminales cuenten con una pastilla electrónica única integrada que proporcione identificación positiva. Con las pastillas,

el procesador de entrada o la computadora principal pueden identificar electrónicamente a cada terminal.

- Asegurar físicamente los conmutadores de encendido/apagado de la terminal, o contar con cerrojos que inutilicen la pantalla y el tablero.
- Mantener las terminales en un sitio seguro físicamente.
- Cerrar todos los circuitos de comunicación después de las horas de oficina (inutilizar positivamente los circuitos de comunicación)
- Codificar por transacción cada terminal. Con esto se evita cualquier transacción que no este relacionada con el área de trabajo en que se encuentra localizada la terminal. En otras palabras, la terminal se hace especifica en cuanto a transacciones.
- Desarrollar un perfil de seguridad de los tipos de datos que se estén introduciendo y de los procedimientos de entrada al sistema del usuario. Si ocurre una violación, es posible apagar automáticamente la terminal que estaba siendo utilizada. Además, al día siguiente debe entregarse un informe de seguridad de terminales al administrador del área de trabajo del usuario.
- Restringir las terminales a funciones solo de lectura
- Numerar secuencialmente, y sellar registrando la fecha y hora de todos los mensajes.
- Asegurarse de que las contraseñas, no se impriman cuando se tecleen.
- Asegurarse de la eliminación adecuada de la salida de la impresora.
- Permitir que las terminales inteligentes editen las transacciones antes de su transmisión.

Cuando se busque el control y la seguridad de las terminales de marcación, revisar los controles para los modems con marcación enumerados previamente en la sección sobre modems.

1.8.1.4. Controles de los Circuitos.

Algunos de los circuitos de comunicación que deben revisarse son los pares de alambre y los cables colocados a lo largo de toda la instalación del usuario, las líneas de abonado locales que van de la instalación del usuario a la compañía telefónica, y los circuitos intercentral (IC) entre ciudades.

Los pares de alambre y los cables en el interior de la instalación del usuario deben hacerse lo mas seguros físicamente que sea posible debido a que es aquí por donde debe entrar cualquier persona que desee derivar el sistema. Es 100 veces mas fácil derivar una línea de abonado local que un canal intercentral. Es necesario tener la certeza de que las líneas están aseguradas detrás de las paredes y por encima de los techos, que el equipo telefónico y los recintos de conmutación (armarios de alambres) se encuentren bajo llave, y que las puertas cuenten con alarmas.

Con respecto a los cables internos en una instalación del usuario, deberá considerarse el empleo de fibras ópticas.

Tales dispositivos ofrecen seguridad gracias a su inmunidad al ruido generado eléctricamente, resistencia a derivaciones, aislamiento y tamaño pequeño. También proporcionan algunas ventajas muy especiales cuando se les utiliza en medio adverso.

Debe tenerse otra precaución con respecto al control y la seguridad de los cables de conexión contra derivaciones subrepticias.

1.8.1.5. Controles de las Computadoras Personales

La fuerza impulsora detrás del empleo de la computadora personal, especialmente de las conexiones de micro a macro y de las redes de área local, es el deseo de los usuarios terminales de utilizar datos de macrocomputadora con sus propias computadoras personales, que están localizadas en sus propios departamentos.

Los usuarios desean manipular tales datos y tener la capacidad de actualizar bases de datos de la macrocomputadora en tiempo real, así como interactuar con sistemas centralizados de aplicación de macrocomputadoras principales.

Como resultado, la seguridad de las computadoras personales es una cuestión en extremo importante en los medios actuales empresariales, gubernamentales y científicos.

La seguridad de una computadora personal como estación de trabajo puede dividirse en tres áreas principales.

Primero, todas las características de seguridad física que pueden instalarse en el sitio de una macrocomputadora principal central también deben considerarse en la ubicación de la computadora personal remota. Muchas de tales características de seguridad deben reducirse a escala debido al costo o a la pequeñez de la computadora personal. Por ejemplo, en el sitio donde se encuentra una macrocomputadora principal es posible instalar un gran sistema de supresión de incendios, pero en el sitio de una computadora personal remota deberá contarse con un pequeño extinguidor manual.

Segundo, la seguridad de los datos es la protección de datos y programas en el sitio central, durante la transmisión, y en el sitio de la computadora personal.

La seguridad para el acceso a la red es el tercer aspecto relacionado con la conexión de la computadora personal. No importa si la computadora personal está siendo utilizada en un enlace de micro a macro, una red de área local o un enlace de marcación a través de una red publica de conmutación de paquetes. La seguridad de acceso a la red es critica en cualquiera de tales utilizaciones.

La seguridad de la red implica restringir el acceso a los datos/información y a los programas. Para conseguir esta seguridad de la red con respecto a la computadoras personales, los objetivos generales de protección deben ser los siguientes:

- Verificación del origen y destino del mensaje
- Verificación de la secuencia de un mensaje
- Detección, por parte del receptor, de cualquier modificación al mensaje, a la secuencia de mensaje o a ambos.
- Detección por parte del emisor de un reconocimiento fraudulento de la recepción o no recepción de un mensaje.
- Prevención de la revelación no autorizada de mensajes para cualquier persona que no posea identificación única, como contraseña o llaves de cifrado.
- Aceptación positiva de los mensajes. Una vez que el sistema proporciona evidencia de aceptación, nunca se debe perder, distorsionar o duplicar sin autorización apropiada
- Requisitos especiales para la seguridad de la red que se encuentren vigentes para evitar una entrada ilegal en el instante de rearranque de la

red una vez que el sistema se ha caído o si ha estado parcialmente fuera de servicio.

- Aviso al personal de operación y elaboración de informes especializados de control como seguimiento, cuando ocurren errores en transmisión, enrutamiento y formateo del mensaje, o si ocurre otra anomalía.
- Control de acceso a la red y sus instalaciones, de modo que solamente el personal autorizado pueda entrar. Los seguimiento de auditoria completos deben mostrar quien tuvo acceso a qué y cuándo ocurrió el acceso.
- Detección y notificación rápidas y automáticas del tipo y localización de cualquier violación a la seguridad.
- Almacenamiento seguro de todos los mensajes en una bitácora del sistema de procesador de entrada/computadora principal.

El empleo de este método matricial se recomienda como medio conveniente para identificar las amenazas especificas relacionadas con las computadoras personales.

Tales amenazas se correlacionan después con los diversos componentes de cada sitio de computadora personal. Finalmente, los controles necesarios se correlacionan con las amenazas y con los controles previamente identificados a fin de construir una matriz bidimensional en la que se observen los controles requeridos en el lugar de cada computadora personal.

1.8.1.6. Controles de las bases de datos.

En la sección anterior se analizaron tres clases primordiales de seguridad relacionadas con las computadoras personales.

El tema es tan importante que se considera oportuno añadir más material acerca de la seguridad de los datos. Los expertos en seguridad sostienen que no existe forma infalible alguna para proteger los datos de una computadora personal. De todas maneras, es necesario proteger las bases de datos, por lo que enseguida se presentan algunas orientaciones para asegurarlas.

Utilizar las características de seguridad del software de administración de la macrocomputadora principal central. Junto con ellas, utilizar las características de cerradura de volumen, de archivo y de registro que pudieran estar disponibles en el servidor de archivos o en servidor de la red instalado en la computadora personal. Por ultimo, utilizar todas las características de seguridad contenidas en el en el "paquete de software de seguridad" que está instalado en la macrocomputadora principal.

Restringir la entrada al sistema con base en algo que sabe el usuario (contraseña), y en algo que tiene el usuario (llave).

Una vez que un usuario se encuentra en la base de datos, definir los limites de aquél, como la capacidad de leer, escribir, crear, borra, buscar, modificar, etc.,

Nombrar un administrador de bases de datos que pueda otorgar o revocar diversos privilegios de seguridad y también actuar como interfaz entre diversos usuarios con respecto a la base de datos. Esta persona será el custodio de la base de datos y también asegura procedimientos idóneos de respaldo y recuperación.

Utilizar dispositivos de seguridad de rellamada a fin de restringir la entrada.

Utilizar el cifrado de datos. Además de cifrar los datos para su transmisión por la red, para los datos de alta seguridad cifrarlos antes de su almacenamiento y luego descifrarlos cuando sean leídos de éste.

Monitorear y limitar la descarga de datos a las computadoras personales y su carga de vuelta a la macrocomputadora principal. Cuando los datos se encuentran en la base de datos de la macrocomputadora principal es posible protegerlos adecuadamente, pero una vez que llegan a la computadora personal remota, se pierden muchos de los controles con los que podrían evitarse errores y otra corrupción de los datos.

No mantener en línea datos extremadamente sensibles.

Desplegar en pantalla y clasificar tanto a los usuarios como a los datos.

No todo el mundo debe ver todo. Asignar diferentes niveles de acreditación de seguridad a los usuarios y también a los datos, permitiendo así que los usuarios vean solamente "lo que necesitan saber".

Crear un entorno físico seguro en el área alrededor de la estación de trabajo de la base de datos / computadora personal.

1.8.1.7. Controles de Protocolos

Los protocolos son simplemente las reglas por medio de las cuales dos maquinas se comunican entre si. La palabra "protocolo" proviene del griego protokollon, que fue la primera hoja adherida a un rollo de papiro, se trataba de la tabla (índice) de contenido.

La Organización Internacional para la Normalización (ISO) elaboro un modelo de siete capas (modelo OSI) para los protocolos.

Enseguida se describen brevemente las tareas realizadas por cada capa, junto con los controles que debe haber en cada capa. El modelo OSI es el modelo de protocolos mas popular aprobado por las organizaciones internacionales para el establecimiento de normas.

Capa1: Control de enlaces físicos. Esta capa es la circuiteria física de cables y modems. Está relacionada con la transmisión de una secuencia en serie de bits de datos a través del circuito de comunicación. Esta capa es incapaz de interpretar y no sabe que los datos pueden estar en forma de paquetes/tramas, y tampoco sabe nada acerca de verificación de errores, etc. Es el enlace físico por el que se desplazan los datos.

Se requieren controles para proteger físicamente cable de conexión, modems y circuitos de comunicación. El objetivo mas importante en esta capa es controlar el acceso físico de empleados o proveedores a los cables de conexión y a los modems. Esto incluye restringir su acceso a los gabinetes de conductores en los cuales están conectados todos los alambres y cables de comunicación. Todas las líneas de abonado locales que salen del edificio deberán asegurarse físicamente y colocarse fuera de alcance, para evitar daño físico o una fácil derivación telefónica. Deberán aplicarse procedimientos formales para ayudar a identificar amenazas a la seguridad o entradas ilegales al sistema cuando se efectúen en la capa física. Por ultimo, la protección física de los circuitos telefónicos (canales IC) es responsabilidad de la empresa de comunicaciones (compañía telefónica). No puede hacerse mucho al respecto, excepto revisar los procedimientos de seguridad física de la compañía telefónica y cifrar los datos antes de que abandonen el edificio del usuario para introducirse en la red publica.

Capa 2: Control de enlace de datos. Esta capa se encarga del empaquetamiento de datos en tramas o paquetes y hacerlos pasar por el cable de modo que puedan llegar a la capa 1. También se encarga de calcular el polinomio de comprobación de errores (CRC) y de insertar direcciones, etc. en la trama o paquete.

Los controles en esta capa deben contar con características como conteo secuencial de tramas, capacidades para la detección y retransmisión de errores, identificación de perdida de tramas y reducción a cero de posibles transmisiones duplicadas. Debe resolver problemas provocados por tramas dañadas/perdidas/duplicadas, impedir que un transmisor rápido ahogue a un receptor lento, proporcionar capacidades de rearranque limitadas en caso de situaciones de terminación anormal, asegurar que algunos de los datos transmitidos no se malinterpreten como caracteres de control en la línea, incrementar la eficiencia del control de flujo para asegurar que se envíe la mayor cantidad de tramas sin necesidad de reconocimiento, terminar una sesión de manera apropiada, etc.

Capa 3: Control de red. Esta capa se encarga de convertir direcciones lógicas (nombres) en direcciones físicas (nodos o dispositivos) También elige la mejor ruta del circuito en caso de que haya disponible mas de una y empaqueta el mensaje original en las longitudes designadas de paquete (que suelen ser de 128 caracteres).

Los controles por cuestionar en esta capa implican quien debe asegurar que todos los paquetes sean recibidos correctamente y en su orden apropiado en los destinos.

Esta capa de protocolo debe aceptar mensajes de la principal, convertirlos en paquetes, y asegurar que éstos se dirijan hacia su destino. Asimismo, en esta capa puede haber algunas bases de datos globales o locales que deben mantenerse seguras. El control de los congestionamientos, como la existencia de demasiados paquetes en un canal, se debe efectuar en esta capa. Esta capa también contendrá las rutinas para la emisión de cuentas para los usuarios y debe revisarse en cuanto a posibles problemas como errores, robo de tiempo o cargos incorrectos por mensajes.

Capa 4: Control de transporte: La capa 4 es la encargada del establecimiento y mantenimiento de la conexión, e inicia la solicitud de retransmisión cuando la capa 2 le notifica que un paquete/trama llegó con degradación. Algunas veces se denomina capa de principal a principal.

Los controles que es necesario comprobar en la capa 4 están relacionados con las conexiones de la red, porque la capa de transporte podría tener que crear conexiones múltiples en la red a fin de obtener el número necesario de trayectorias de circuitos.

En esta capa podría invocarse el multiplexaje, por lo que es necesario revisar los controles de esta función.

También en esta capa un programa en una maquina fuente dialoga con un programa similar en la maquina destino mediante el empleo de encabezados y mensajes de control, de este modo, algunos de los controles deberán ubicarse en los programas de aplicación. En las capas inferiores (capa 1 a 3) los protocolos son ejecutados en cada maquina y sus vecinas inmediatas, y no en las maquinas extremas de fuente y destino, que pueden estar separadas por muchos dispositivos de hardware y enlaces de circuitos.

Otro control necesario es el que determina si el software a este nivel es capaz de decir qué maquina pertenece a qué conexión.

Otros controles que se realizan en este nivel, aun cuando también sea posible aplicarlos en otra parte, son el direccionamiento de la maquina fuente/destino y el control de flujo (que aquí significa flujo de mensajes en vez de flujo de paquetes), de modo que una maquina no puede ahogar a otra.

Capa 5: Control de sesión. Esta capa apoya la sesión del usuario y enciende y apaga la comunicación entre dos estaciones de trabajo. Si la suspensión eléctrica temporal en la red interrumpe el circuito, entonces a menudo puede ser necesario descender a las capas inferiores (capas 1 a 4) para establecer la conexión antes de que el programa de aplicación o el operador se enteren del problema.

Los controles que se deben analizar en esta capa son los típicos que se relacionan con una terminal (especializada o de marcación), como contraseñas, procedimientos de entrada, direccionamiento terminal, autentificacion de terminales o de usuarios (o de ambos), y la entrega correcta de una cuenta.

Otro control se ejerce cuando las conexiones del control de transporte (capa 4), no son confiables, puede requerirse que la capa de sesión trate de recuperar las conexiones de transporte rotas.

En sistemas de administración de bases de datos, como el presente, es crucial que una transacción complicada contra la base de datos jamas aborte a la mitad de la rutina, porque entonces la base de datos quedaría en estado inconsistente.

La capa de sesión constituye el medio por el cual es posible hacer a un lado un conjunto de mensajes, de modo que ninguno de ellos sea entregado al usuario remoto sino hasta que se hayan completado todos los mensajes. Este mecanismo asegura que la falta de hardware o de software dentro de la subred nunca provoque el aborto de una transacción a la mitad de su procesamiento.

La capa de sesión también proporcionará secuenciacion de mensajes cuando la capa de transporte no lo haga.

Capa 6. Control de presentación.

Esta capa traduce ordenes de la capa de aplicación (la superior a ella), proporcionando una sintaxis (lenguaje) a comprendida por todos los dispositivos a través de la red.

Los controles en esta capa serán cifrado de software, comprensión de textos, reducción de textos y conversión de archivos y formatos de archivos incompatibles, de modo que sea posible la comunicación entre dos sistemas.

Esta capa también puede tomar terminales incompatibles y modificar la longitud de línea o de pantalla, las convenciones de fin de línea, el modo manuscrito contra el de imprenta, conjunto de caracteres y el direccionamiento del cursor para hacerlos compatibles.

Capa 7: Control de aplicación. Esta capa no efectúa la aplicación en si. Realiza funciones como transferencia de archivos y correo electrónico. Establece la interfaz entre el programa de aplicación del usuario y la red.

Los controles en esta capa están relacionados con los programas de aplicación de los sistemas administrativos utilizados en la organización.

Estos controles de la capa de aplicación consistirán en las tareas que aseguran una conexión valida entre cualquier programa de aplicación que se este utilizando en la

organización y el direccionamiento o transmisión de los mensajes requeridos por esta aplicación.

Debido a que el objetivo de la capa 7 es aislar los programas de aplicación de la detallada tarea técnica de transmitir mensajes, los controles deben asegurar que esta capa de software no pierda, dirija erróneamente o modifique incorrectamente ningún mensaje.

Muchos de los controles que se requieren aquí son los típicos controles lógicos que se encuentran integrados en el sistema mismo de la aplicación, aunque la capa 7 también debe contener controles internos dentro del software de comunicación.

1.8.1.8. Controles de Administración:

La administración de la red implica el establecimiento de una filosofía de control central para el manejo de las funciones globales de la red. El administrador de la red debe ser independiente de los demás administradores en el ámbito del procesamiento de datos e inclusive del departamento de sistemas de información en si.

Algunas de las responsabilidades generales de esta función laboral son diseño y análisis, operaciones de la red, control de fallas y administración de verificaciones/problemas.

Algunos de los controles de administración de la red son los siguientes: El equipo de administración de la red debe poseer una cuenta con la empresa de comunicaciones. Debe haber un numero central al cual llamar para registrar todos los problemas relacionados con quién, qué, dónde, cuándo, por qué, número telefónico, fecha y hora del problema. El grupo de control de fallas debe reunir estadísticas para su hardware, como el tiempo medio entre fallas (TMEF).

El proveedor de hardware de la red a deberá proporcionar tales datos.

El personal de administración de la red también debe contar con estadísticas acerca del tiempo desde la falla hasta la recuperación. En su forma mas detallada, esto consiste en el tiempo medio para diagnosticar (TMPD) mas el tiempo medio de respuesta (TMR) mas el tiempo medio de compostura (TMC)

Además del control central para informar problemas en la red, el grupo de administración de la red debe llevar otras estadísticas como tiempo de inactividad acumulativo de la red, tiempo de inactividad de la subred, informes de utilización de los circuitos, análisis del tiempo de respuesta, descripciones de la longitud de la fila, histogramas del uso diario (como numero de caracteres transmitidos por día por circuito), frecuencias de fallas en los circuitos (como numero de mensajes restransmitidos), estadísticas sobre la actividad de la computadora principal y los archivos, actividades relativas a errores de dispositivos locales, fallas de los accesos de la red, distribución de caracteres y volumen de los paquetes, distribución del trafico por hora del día y localización, volúmenes pico, y perfil estadístico de todo el trafico de la red relacionado con el tiempo. Estos informes, u otros similares, deben estar disponibles para administrar la red.

Con respecto a la documentación de la red (parte de la cual puede verificarse en forma cruzada en cuanto a actualidad en la base de datos global o local), la administración de la red debe contar con lo siguiente: registro de la disposición del circuito, mapas de la red, referencias cruzadas de hardware/software, todos los registros

de mantenimiento del proveedor de la red, listados de software por tareas y componente de la red, todos los números telefónicos de las ubicaciones de los usuarios y los nombres de las personas por llamar, registro del historial del mantenimiento del componente de interfaz, índice telefónico controlado por el circuito, historial de mantenimiento de cada componente, inventario por número de serie de los componentes de la red, localizaciones redundantes de la red y criterios de conmutación, contratos con el proveedor y una lista actualizada del personal que trabaja en el centro de la red.

Mediante la revisión del control de la administración de la red debe comprobarse la existencia de manuales de operación idóneos y de una descripción exhaustiva del funcionamiento de la red. Debe haber procedimientos de recuperación adecuados, procedimientos de apoyo y planes en caso de desastres.

No se pueden hacer mucho para controlar al equipo de prueba de comunicación, pues éste se encuentra en uso continuo. La administración de la red debe aceptar que el abuso puede conducir a violaciones de la privacia o la inserción de mensajes ilegales.

Cuando no se utiliza el equipo es necesario apagar la cerradura y retirar la llave. Con lo anterior se impide que la gente curiosee los datos al pasar por la red de comunicación de datos.

Para diagnosticar la ubicación y causa de los problemas es necesario utilizar equipo de prueba hacia atrás.

Los analizadores de redes basados en microprocesadores permiten la verificación de los tiempos de exploración a exploración o de exploración para responder. Tales comprobaciones ayudan a la administración de la red a evaluar la eficiencia de exploración.

El principal control para el equipo de prueba es asegurar que solamente personal calificado utilice este equipo y que además lo use sólo cuando es necesario.

1.8.1.9. Controles para recuperación / respaldo / desastres

A fin de crear la capacidad de recuperación en caso de desastres es necesario concebir procedimientos de recuperación y respaldo para todo el entorno (edificio) y para hardware, software, datos redes de comunicación. Un plan de recuperación para desastres extremadamente detallado y amplio puede hacer que la organización funcione de nuevo en caso de presentarse casi cualquier clase de desastre. Este plan global debe contemplar varios niveles de respuesta a diferentes posibles desastres y debe permitir la recuperación parcial o total en las áreas de:

- El edificio (medio)
- Software del sistema y las instalaciones
- Programas de aplicación
- Hardware del centro de datos.
- Computadoras Personales / Terminales remotas
- Formas manuales
- Apoyo para la entrada de datos
- Almacenamiento/retención de archivos de bases de datos en el sitio mismo y en lugares remotos
- Procedimientos del sistema operativo en el centro de datos y en áreas de usuarios remotos

- Asignación de personal y responsabilidades para casos de desastre
- Actualización y mantenimiento adecuados del plan para desastres

Los controles de recuperación y respaldo dentro de la red de comunicación de datos abarcan muchas áreas.

La persona que revise estos controles puede empezar en cualquier extremo de la red (terminales remotas o computadora principal central). El objetivo es comprobar los procedimientos de recuperación y el hardware de respaldo a lo largo de toda la red.¿Existen procedimientos de software para la recuperación de archivos de datos, bases de datos de la red, software de la red, etcétera?

Una consideración importante es el respaldo de los circuitos de comunicación. Una opción es alquilar dos circuitos por separado (que hayan sido enrutados de manera alternada) para que uno sea de respaldo. Otra opción es utilizar circuitos de marcación como respaldo para los circuitos rentados. Por supuesto, una alternativa más es contar con procedimientos manuales que sea posible utilizar durante un periodo muy corto si el circuito se cae, tal vez como máximo por unas horas.

Deberá haber capacidades de recuperación y rearranque en caso de falla del hardware o del software. Entre los medios de respaldo debe contemplarse energía eléctrica de apoyo, quizá en sitios tanto locales como remotos.

El plan para desastres en una red de comunicación de datos deberá incluir un plan por separado para cada una de las siguientes áreas: 1) el centro de control de la red de comunicación, 2) los circuitos de comunicación, 3) controladores remotos de conmutadores/concentradores/terminales inteligentes, 4)instalaciones de la empresa de comunicaciones (compañía telefónica), y 5) energía eléctrica para las instalaciones de la comunicación de datos y las terminales/luces de los usuarios.

En el plan para desastres en una red de comunicación de datos deben considerarse los siguientes detalles:

El administrador que toma decisiones y está a cargo de la operación de , recuperación del desastre. En caso de que el primer administrador esté indisponible, es necesario nombrar un segundo administrador.

Disponibilidad y capacitación de personal de apoyo con suficiente conocimiento, y experiencia en la comunicación de datos.

Procedimientos de recuperación para las instalaciones de la comunicación de datos. Esto es información sobre la ubicación de los circuitos, de a quién debe localizarse para apoyar los circuitos de datos y la documentación y prioridades preestablecidas acerca de cuáles circuitos de datos deben reconstruirse en primer lugar.

Cómo sustituir el hardware y software dañados de comunicación que son proporcionados por los proveedores.

Es necesario delinear que puede esperarse de parte de los proveedores, junto con el nombre y número telefónico de la persona que debe contactarse.

Localización de instalaciones alternativas de comunicación de datos y de equipo como cables de conexión, líneas de abonados locales, CIC, medios de conmutación de la empresa de comunicaciones, y otras redes públicas.