



CONECTIVIDAD a SWIFTNet vía
“SERVICE BUREAU”
BCG, Business Computer Group





TABLA DE CONTENIDO

1. Introducción
2. Definición de “Service Bureau”
3. Características
4. Esquema de Conectividad
5. Servicios Ofrecidos
 - a. Conexión a SWIFTNet para nuevos usuarios
 - b. Conectividad a SWIFTNet para usuarios de SWIFTAlliance
6. Estadísticas de la Base Instalada de Clientes
7. Anexos
 - a. Aprobación del “Board” de SWIFT
 - b. “Service :Lavel Agreement”
 - c. “Service Bureau Policy”

INTRODUCCION

Como parte de su política corporativa **S.W.I.F.T.** se ha fijado el objetivo de triplicar a mediano plazo el número de usuarios conectados a la red SWIFTNet, y es la reducción de costos parte vital de esta estrategia que busca facilitar la incorporación de usuarios de tamaño mediano y pequeño con opciones mas competitivas para el acceso a la red. El “Service Bureau” es la respuesta de **SWIFT** que satisface esta necesidad, ya que su filosofía es la de eliminar el impacto a nivel operativo y de inversión asociado a la adquisición del Terminal de Financiero, sus cargos recurrentes de mantenimiento y la infraestructura de comunicaciones, ofreciendo en su lugar el servicio de conectividad a la red a través de alternativas complementarias que se apoyan en principios de economías de escala.



BCG, Business Computer Group, el Asociado de Negocios y Servicios de SWIFT para el Norte de Latinoamérica, alineado con la estrategia corporativa de **S.W.I.F.T.**, tiene la satisfacción de poner a su disposición la alternativa de conectividad a SWIFTNet, a través de su “Business Partner Service Bureau” el cual permite acceder a esta “extranet” financiera de manera rápida y segura. Cabe destacar que nuestro “Service Bureau” esta basado en la familia de productos SWIFTAlliance Access, Entry, Workstation, Webstation, Gateway y SWIFTNet Link.



Los servicios ofrecidos en esta propuesta satisfacen la operativa de instituciones cuya conexión primaria a SWIFT se realiza desde el “Service Bureau”; bien sea directamente como usuarios de SWIFTAlliance Access o indirectamente apoyándose en la funcionalidad RAHA de SWIFTAlliance Gateway, para aquellos bancos con licencias propias. Los servicios de conectividad ofrecidos son tolerantes a fallas técnicas y a desastres naturales e incluyen los procedimientos de contingencia exigidos por SWIFT.

Es importante destacar que el “Business Partner Service Bureau” de BCG ha sido debidamente aprobado por el “SWIFT Board of Directors”, asimismo es supervisado y auditado directamente por empresas independientes contratadas por SWIFT, cumpliendo con todos los criterios y condiciones especificados en el documento adjunto “Service Bureau Policy”. Cabe destacar que el mismo es operado y mantenido por el staff de ingenieros de **BCG**, el cual goza de las certificaciones de “Education y Service Partners Programs”, lo cual nos permite ofrecer un servicio que cumple con los mas altos estándares de la industria.

DEFINICION DE “SERVICE BUREAU”

Un “Service Bureau” es una unidad de servicios avalada por SWIFT, cuya finalidad es la de brindar a sus usuarios la posibilidad de acceder a los servicios interactivos de SWIFTNet InterAct, FileAct, Browse y FIN. Este último, SWIFTNet FIN, es el servicio de intercambio de mensajes financieros a través de la red MV SIPN (Multi Vendor Secure IP Network).

Adicional a los otros servicios de SWIFTNet, el “Service Bureau” de Business Computer Group ofrece conectividad a SWIFTNet FIN para aquellas instituciones que deseen intercambiar mensajes financieros con instituciones usuarias de la red.



CARACTERISTICAS DEL “SERVICE BUREAU”

Este centro de servicios interactivos distribuye su procesamiento en sus sedes, ubicadas en las ciudades de Panamá y Caracas, ofreciendo conectividad a SWIFTNet de manera independiente, complementaria y tolerante a fallas técnicas y a desastres naturales. Para cada una de ellas están disponibles ambientes redundantes de Producción, Respaldo y Pruebas.

En materia de Servidores cada una de sus sedes posee la siguiente configuración:

I) SWIFTAlliance Access Producción y Respaldo:

Dos servidores Marca Dell, PowerEdge 1600SC, Procesador Xeon, 2.0GHz, 1 GB RAM, 36 GB DD, HotSwap Raid 1.

II) SWIFTAlliance Gateway Producción y Respaldo: Dos servidores Marca Dell, PowerEdge 1600SC, Procesador Xeon, 2.0GHz, 1 GB RAM, 36 GB DD, HotSwap Raid 1.

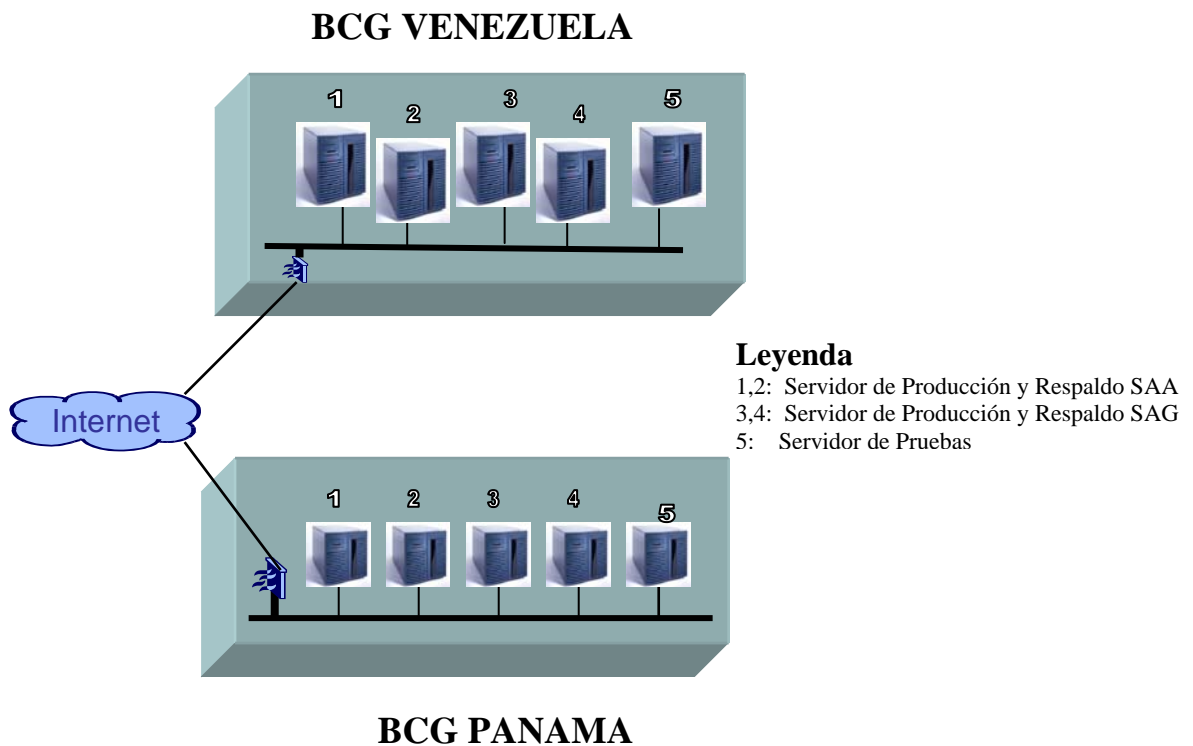
III) SWIFTAlliance Access y Gateway “Test and Trainig”: Un servidor Marca Dell, PowerEdge 1600SC, Procesador Xeon, 2.0GHz, 1GB RAM, 36 GB DD, HotSwap Raid 1.

Los discos están configurados con la facilidad de “Disk Mirroring”, lo cual robustece la recuperación a fallas en el disco principal, adicionalmente los discos poseen tecnología “Hot Swap” permitiendo ser removidos dinámicamente, flexibilizando el mantenimiento de la instalación, aumentando al mismo tiempo la capacidad de tolerancia y rapidez de recuperación a fallas.

Los Servidores están protegidos contra el acceso de usuarios no autorizados mediante una pareja de Firewalls/VPN's de alta disponibilidad, conectados en modalidad "Maestro/Esclavo" vía protocolo NSRP y que juntos generan una zona totalmente protegida cuyo único acceso será posible mediante túneles virtuales IPSEC.

En Panamá, el acceso a Internet se realiza a través de un enlace permanente con un ancho de banda de 1024K compartido entre 2 "Internet Service Providers" (ISP) distintos y a través de "Routers" conectados entre si usando el protocolo BGP para el balanceo dinámico de las sesiones, los cuales permiten su alta disponibilidad. En Caracas el acceso a Internet es reforzado por un tercer ISP adicional.

El "Service Bureau" esta localizado en edificios con suministro de energía propia y con capacidad de recuperación a fallas eléctricas externas en un máximo de 15 minutos, adicionalmente cada sede posee una unidad de suministro de energía (UPS) que garantiza la operativa por un lapso de dos horas, previendo así cualquier retardo en el suministro de las plantas eléctricas de los edificios.

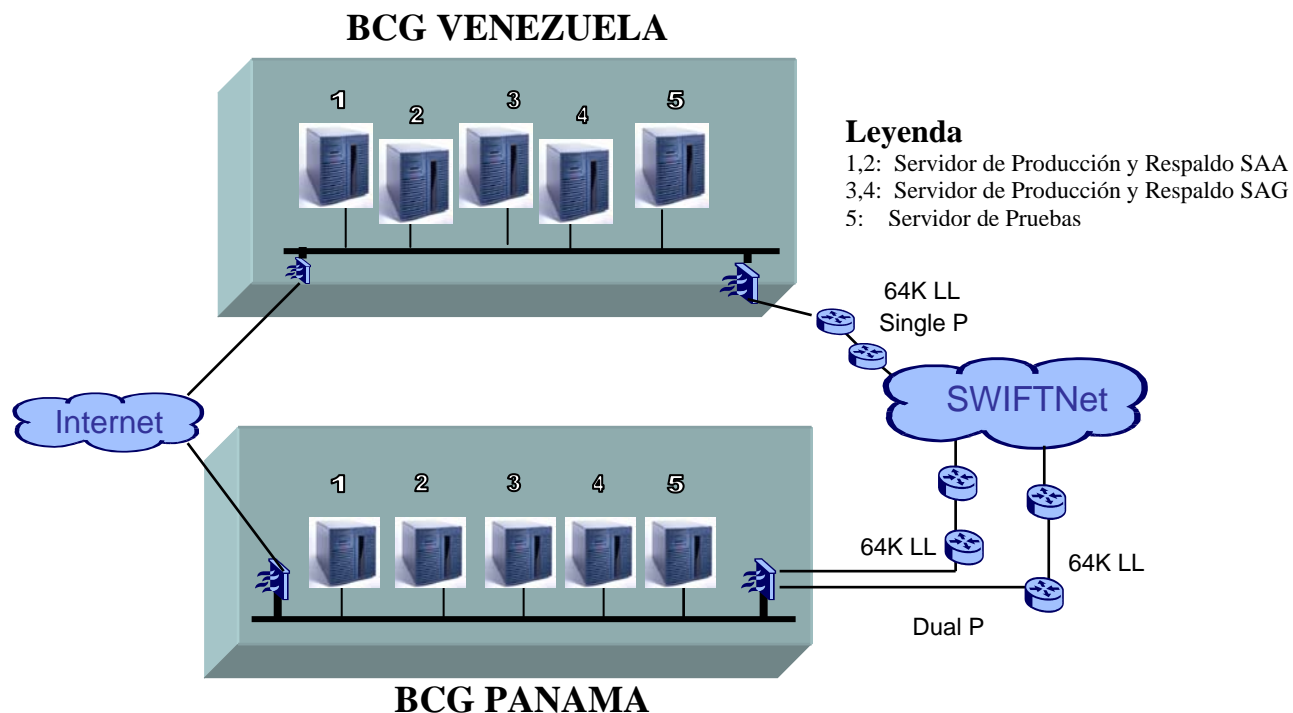


ESQUEMA DE CONECTIVIDAD A SWIFTNet

Como consecuencia de la migración a SWIFTNet, uno de los factores mas importantes a tomar en cuenta es la manera como se implanta la conectividad con la red, es por esto que es fundamental seleccionar configuraciones que toleren eventuales fallas en las líneas de comunicación. El modelo Dual P propuesto por SWIFT fue creado para soportar fallas tanto a nivel de los encriptadores de datos (VPN Box) como a nivel de líneas de comunicación; de manera complementaria el modelo Single P ofrece una conexión permanente a través de la cual se implanta la conectividad tipo MULTI LINE, diseñada para ser tolerante a Catástrofes Naturales.

El “Service Bureau” utiliza los modelos Dual P y Single P en su conexión a SWIFTNet, manteniendo con SWIFT tres canales dedicados permanentes con anchos de banda de 64 K, “Routers”, “Firewalls” y “VPN Boxes” para la protección de los canales de comunicación. Es importante mencionar que los VPN Boxes de la opción Dual P están interconectados, por lo que en caso de alguna falla en la línea primaria, automáticamente se activa la línea de respaldo de forma transparente.

Ambas sedes del “Service Bureau” están conectadas a SWIFTNet de manera ACTIVE-ACTIVE a través de dos Network Partners diferentes, lo cual lo hace también tolerante a fallas ocurridas a este nivel; siendo concurrente el tráfico de mensajes en dichas sedes.

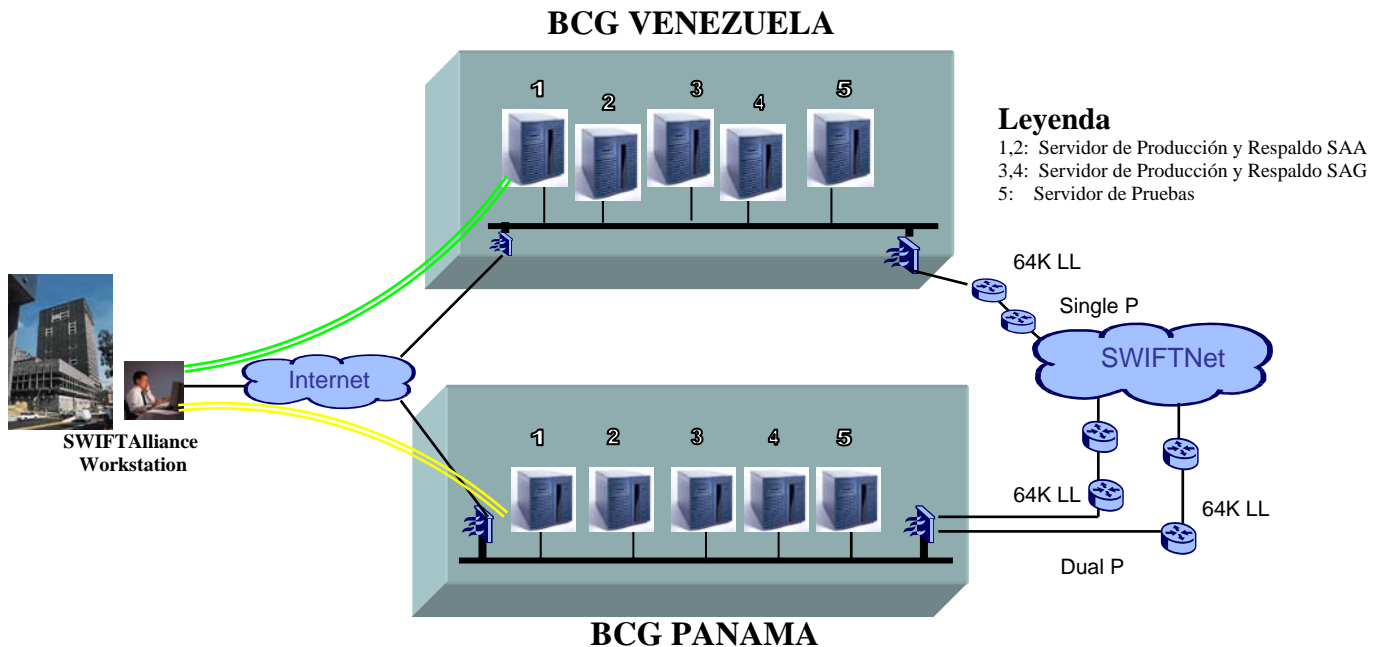


SERVICIOS OFRECIDOS

1. Conexión a SWIFTNet FIN para nuevos usuarios

SWIFTAlliance Workstation: En esta modalidad la institución tiene en sus instalaciones una estación de trabajo conectada permanentemente vía Internet al “Service Bureau” mediante la cual realizara los procesos de creación, verificación, autorización, impresión de mensajes, Login/Select a SWIFTNet FIN, creación, eliminación, modificación de preacuerdos de corresponsales, envío y recepción de mensajes SWIFT. La preparación del ambiente de BKE para la autenticación de los mensajes, así como también la administración de los certificados debe ser realizada desde el servidor del “Service Bureau”. Es importante destacar que entre los servidores de BCG de Panamá y BCG de Venezuela diariamente se realiza un proceso de replicación asincrónica de los servidores de Alliance, de manera que todas las noches las Bases de datos son actualizadas de manera recurrente y después del cierre de operaciones; esto permite que en caso de una falla en una de sus sedes, sea posible reactivar desde la otra la comunicación con SWIFTNet FIN y continuar con la operación.

Para proteger los puntos de acceso al “Service Bureau” cada usuario tiene instalado a su estación de trabajo de SWIFTAlliance Workstation dos Firewalls/VPN Box para crear Túneles Virtuales de protección. Adicionalmente el “Service Bureau” cuenta con tres conexiones seguras a Internet proporcionadas por proveedores diferentes lo cual hace mas robusta la conexión al ofrecer canales alternos y redundantes de comunicación entre el Servidor del SWIFTAlliance Access y la estación de SWIFTAlliance Workstation. De cara al banco y con la finalidad de reforzar su conexión a Internet, recomendamos contratar los servicios dos enlaces a Internet con ISP independientes.

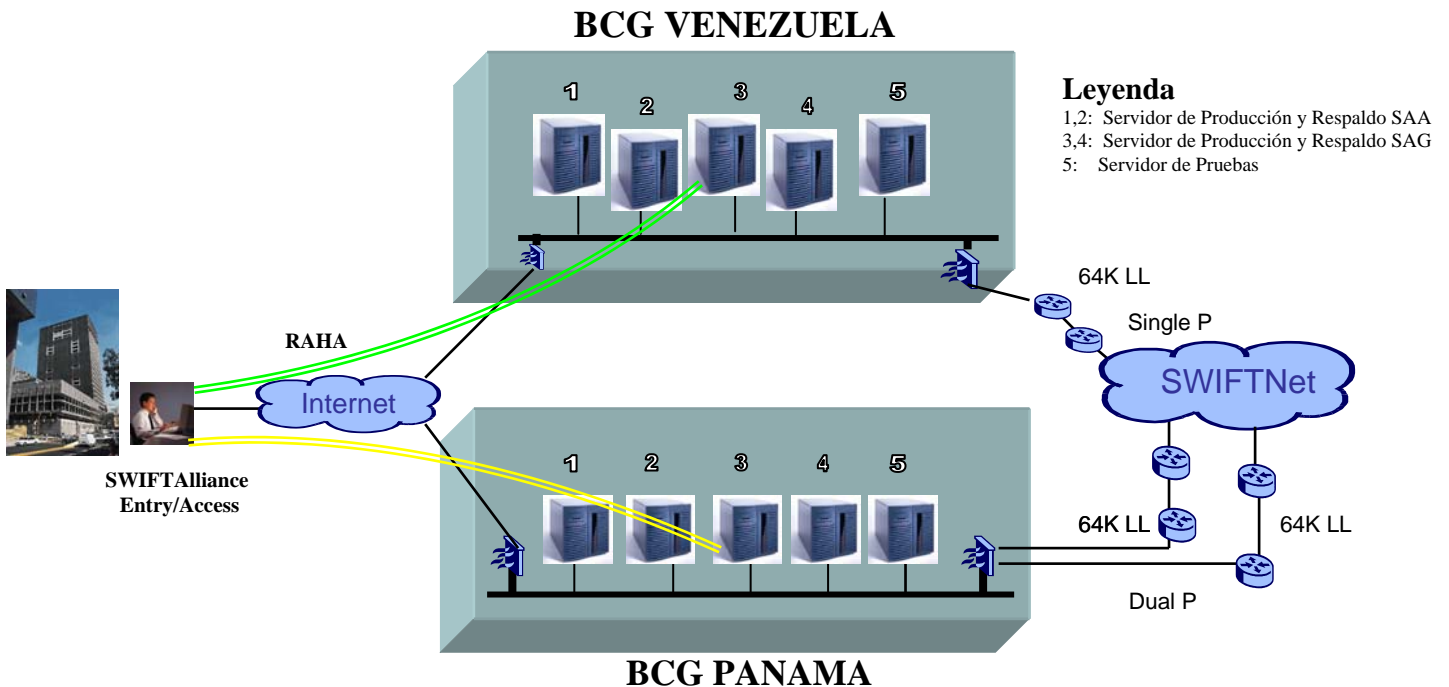


2. Conectividad a SWIFTNet FIN para usuarios de SWIFTAlliance Entry/Access

Esta modalidad se recomienda para aquellos usuarios que deseen conectar su servidor de SWIFTAlliance Entry/Access a la red SWIFTNet para acceder a la aplicación financiera FIN, prescindiendo del componente SWIFTNet Link y del puerto de acceso al “Back Bone” de SWIFTNet, y se apoya en la funcionalidad “Remote API Host Adapter” RAHA ofrecida por el producto SWIFTAlliance Gateway que habilita el intercambio bidireccional de mensajes entre el servidor de SWIFTAlliance de la institución financiera y el “Service Bureau”. Dicho servidor se conecta permanentemente vía Internet a los servidores de SWIFTAlliance Gateways de Panama y Caracas a través de túneles virtuales de protección generados por dos VPN Boxes. De cara al banco y con la finalidad de reforzar su conexión a Internet, recomendamos contratar los servicios dos enlaces a Internet con ISP independientes.

Los procesos de creación, verificación, autorización, impresión de mensajes; creación, eliminación, modificación de preacuerdos de corresponsales, Login/Select a SWIFTNet FIN, envío y recepción de mensajes SWIFT, la preparación del ambiente de BKE para la autenticación de los mensajes son realizados en el servidor de SWIFTAlliance de la institución. El enrutamiento de mensajes hacia el servidor SWIFTAlliance de cada institución financiera es responsabilidad del “Service Bureau”.

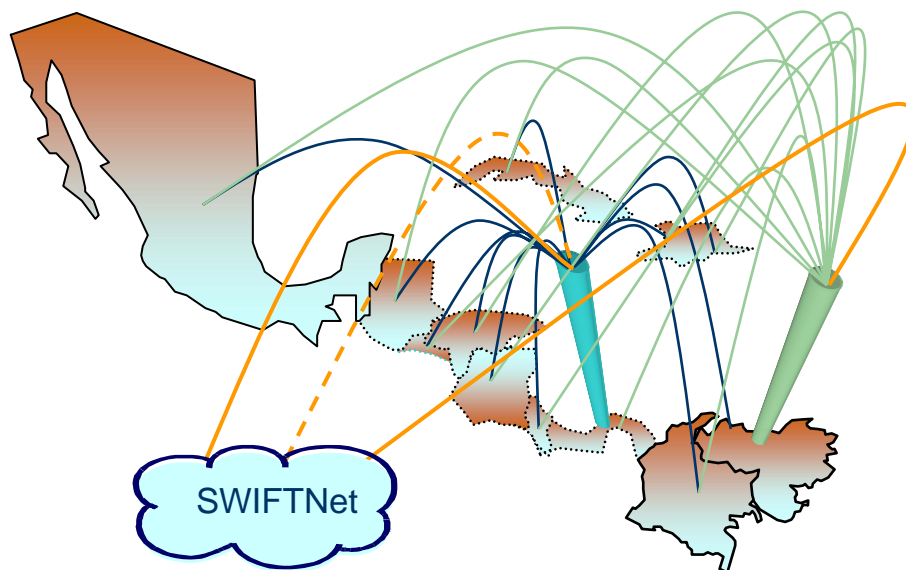
Es muy importante destacar que el intercambio de mensajes entre el servidor SWIFTAlliance y el SWIFTAlliance Gateway está protegido a través del uso de VPN Boxes y “Firewalls” que garantizarán el acceso solamente a usuarios autorizados.



ESTADISTICAS DE LA BASE INSTALADA DE CLIENTES DICIEMBRE 2006

- a. Número de Bancos Conectados: **111**
 - i. Producción: **105**
 - ii. Implantación: **6**
- b. Tráfico Diario x Banco:
 - i. Nivel Inferior: **100 msg x día**
 - ii. Nivel Superior: **2,000 msg x día**
- c. Tráfico Diario del Service Bureau: **10,500 mensajes**
- d. Bancos Centrales Conectados: **5**
- e. Países Conectados: **16**
 - i. Norte América: **2**
 - ii. Centro América: **7**
 - iii. Sur América: **2**
 - iv. Caribe: **5**

Belice	Cuba	Guatemala	México	Republica Dominicana	Venezuela
Colombia	Curacao	Haití	Nicaragua	Saint Marteen	
Costa Rica	El Salvador	Honduras	Panamá	USA	



ANEXOS



SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION

10 July 2003
BS-bm


BCG, Business Computer Group
Panama, S.A.
Mr. Felipe Rios
Executive Manager
World Trade Center, 53 Rd. Street
6th Floor, Office 605
PANAMA CITY
Panama

Dear Sir

We are pleased to advise you that the Board of Directors approved on 10 July 2003 the application of BCG as a not majority owned Service Bureau. However, please advise the name of the users to whom you will offer services, as these have to be communicated to our Audit Department.

Yours faithfully


Brigitte Moens
Board Secretariat


Martine Loosen,
Manager, Board Secretariat

copy: Mr. H. Quintero, User Group Chairman, Banco Internacional de Costa Rica S.A.
Commercial Operations Services

S.W.I.F.T. SCRL

Avenue Adèle 1 - B-1310 La Hulpe - Belgium
Tel.: +32 2 655 31 11 - Fax: +32 2 655 32 26 - SW11Q BE BB - www.swift.com
VAT: BE 413.330.856 - RC Nivelles: 51367

BCG Business Partner Service Bureau

SERVICE LEVEL AGREEMENT

Service Bureau Rules & Guidelines :

1. Introduction

The creation and use of a Service Bureau stems from the trend towards outsourcing of data processing to increase operational efficiency and global cost savings. This trend has been re-enforced by the evolution of telecommunication and computer technologies; the development of facilities management services and integrated banking solutions; the increasing specialisation of Financial Institutions and the engagement of the IT industry in the financial sector. Furthermore, groups of smaller Users also want to share the hardware and operating costs of their S.W.I.F.T. connections.

However, by placing S.W.I.F.T. interface operations with a Service Bureau, Users are potentially putting at risk one of their mission-critical business functions. Furthermore, the use of a Service Bureau may also jeopardise S.W.I.F.T.'s contractual commitments to other, directly connected Users for message confidentiality, integrity, availability, and system reliability.

For there to be complete confidence in Service Bureaux, the related areas of risk must be controlled to ensure secure and timely transmission and secure storage of information. To assist its Customers, S.W.I.F.T. has therefore defined a range of control measures to ensure adequate security in the relationship between Users and Service Bureaux.

According to the Service Bureau Policy, Service Bureaux must sign Service Level Agreements (SLA) with all Users to whom they provide services.

Topics to be included in such a Service Level Agreement are, amongst others:

- availability, including contingency planning
- capacity requirements
- documentation requirements
- functionality
- installation services
- performance
- procedures for fixing functional, performance or security problems
- quality
- reliability
- security
- support
- training

Auditable metrics for each of these areas should be specified. Since Service Bureaux act on behalf of their Users in managing access to S.W.I.F.T. and because of the need to maintain the integrity of S.W.I.F.T.'s network, it is imperative that Service Bureaux provide levels of service that are consistent with S.W.I.F.T.'s overall operations. This is particularly true, if a Service Bureau provides shared access to a wide variety of Users with divergent needs. If minimum service levels are not maintained, Users will not receive the service quality they expect and this will ultimately reflect poorly on S.W.I.F.T. itself.

2. Security Rules and Guidelines

The Security Rules & Guidelines detailed below are derived from S.W.I.F.T.'s own security policy, standards and practices and form an integral part of the Service Level Agreement.

In line with an expert's conclusion that technology is unlikely to provide a fool-proof solution to the risks involved with Service Bureaux, emphasis is placed on procedurally based control measures rather than technology-driven ones.

The areas of control covered are primarily:

- personnel;
- physical security, including network resilience, Uninterruptible Power Supply, selection of operating locations, and disaster recovery planning;
- data security;
- software controls.

2.1 General Controls

Processing activities for different Users utilising the same Service Bureau will be segregated.

- all data, encryption/authentication keys, cards, and other S.W.I.F.T.-related materials physically and logically separate for each of the Users utilising the same Service Bureau will be kept separate.

Implement a set of systematic, auditable processes for delivering services to the User

- an audit trail and evidence of work done will be created for each trade and be available through Service Bureau View – History Reports. The SWIFT acknowledgment will be available in this report.

Notify immediately breaches of confidentiality, integrity and availability to the User and SWIFT

Examples of such security breaches are:

- accidental or malicious disclosure of S.W.I.F.T. traffic and other sensitive data;
- accidental or malicious modification, destruction, loss of traffic or other sensitive data;
- unavailability of services.

The Service Bureau agrees to:

- notify S.W.I.F.T. of any problems which render the User's part of the network inoperative;
- identify, in consultation with the S.W.I.F.T. Customer Support Centre, whether the fault lies in the User's part of the network;
- correct the fault, if it lies in the User's part of the network;
- notify S.W.I.F.T. when the fault has been rectified and the User's part of the network is again functioning normally;
- respond correctly, if necessary, to recovery procedures initiated by S.W.I.F.T. to eliminate a fault in the S.W.I.F.T. part of the network;
- react correctly to fallback operations initiated by S.W.I.F.T. to bypass a failure in the S.W.I.F.T. network;
- perform the necessary procedures to revert from fallback operation to normal operation when the failure is cleared by S.W.I.F.T.

2.2 Confidentiality

2.2.1. General

Establish a Non-Disclosure Agreement (NDA) between the User and the Service Bureau

- the NDA contained in the the Service Bureau Participant Agreement will also encompass all SWIFT activity. In addition, no User will know about traffic statistics, authentication and encryption keys, pins, passwords, computer and network configurations, of another User of the Service Bureau.

Unless otherwise indicated, the SLA will be made available to S.W.I.F.T.'s Security Auditors

Establishment and management (modifications/termination) of bilateral authentication key exchange arrangements (pre-agreements) between correspondents is to be performed directly by the Service Bureau. BKE's will be exchanged within 24 hours of receipt of authorization from the User via e-mail.

Restrict access to authentication keys

- these keys will never be disclosed to operators or to non-owners of the keys.

Service Bureau staff will be granted only those privileges that are strictly necessary for the performance of their duties

- this 'least privilege', 'need to know,' or 'need to have' principle applies not only to computerised systems but also to any other written or oral information;
- segregation of duties is the division of responsibilities for actions between at least two individuals;
- in any act or transaction that is susceptible to fraud, major operational impact or other security risk, processes are segregated so that no single individual can act alone.

2.2.2. FIN specific

The Service Bureau will obtain their own SCR directly from S.W.I.F.T.

The Service Bureau will maintain the encryption keys between the SCR and the Service Bureau and the encryption key for storage of the authentication keys

2.3 Integrity

2.3.1. General

Guarantee integrity of traffic stored locally or awaiting processing at all times and under all circumstances

- the Service Bureau is able to provide supporting documentation for all processing, so that any transaction processed can be traced back to instructions originating from a User as per time periods documented in the Service Bureau Participant Agreement.

Formal procedures will ensure that all User messages are processed accurately and timely

This includes formal reporting to the User of all S.W.I.F.T.-related system activity obtained via S.W.I.F.T. reporting features so that:

- the sending User can verify that all messages sent are acknowledged by S.W.I.F.T
- the sending User can respond appropriately to abnormal circumstances such as negative acknowledgements.
- the sending and receiving Users can verify the proper management of system acknowledgements

2.3.2. FIN specific

USE Security Officer (USOF) functions will be maintained directly under the control of the Service Bureau
USE Key Management Officer (UKMO) functions will be maintained directly under the control of the Service Bureau

The Service Bureau will inform Users of the request for a Certificate and the blacklisting of a Certificate or SCR within 24 hours

- authentication keys must be renewed and activated according to formal, current procedures provided to the Service Bureau by the User;
- the procedures referred to must agree with the USE pre-agreement forms exchanged between Users.

Procedures are in place to ensure that all User messages are processed accurately, timely, once and only once

2.4 Availability

- the Service Bureau will ensure terminal availability; hence, terminals must be capable of handling peak traffic (incoming and outgoing) to be expected under normal conditions;
- procedures are in place that require both local and off-site data back-up and hardware redundancy where deemed necessary;
- access to sufficient back-up terminal capacity adequate to handle at least the urgent traffic (incoming and outgoing) in the event of failure of the main terminal(s) is in place;
- back-up of the prime terminal link can be provided through a leased line.

Notify Users if normal availability cannot be provided

- S.W.I.F.T. notifications regarding situations in S.W.I.F.T.'s realm of responsibility that could endanger timely delivery, enhanced with Service Bureau messages indicating local processing problems, must be forwarded to the User in due time.
- The User must know about and use the appropriate methods in both normal and abnormal operating conditions. In any determination of liability, consideration will be given to a User's responsibility for checking acknowledgements, delivery of messages and any notifications that another User or any part of the S.W.I.F.T. network is or will be down, and to their responsibility to take appropriate alternative action.

3. Installation, Operation, Training & Support Guidelines

3.1 Central Infrastructure

The Service Bureau will provide and maintain the required infrastructure

- The Service Bureau shall provide and maintain the required infrastructure to install and operate the central S.W.I.F.T. Interface on behalf of its customers in a secure environment, in line with S.W.I.F.T.'s criteria. This infrastructure will include : site provision, communication lines to customer site, modems, and other required peripheral devices.

3.2 Operations

Coordinate the central S.W.I.F.T. interface

- The Service Bureau will be responsible for the co-ordination of the central S.W.I.F.T. Interface installation and configuration on behalf of its customers.

Carry out daily operations

- The Service Bureau will agree with its S.W.I.F.T. customers on the responsibility and execution of customer-related data and security definitions and maintenance, daily procedures and operations of the central S.W.I.F.T. interface, as well as operations required on a regular basis (backups, reporting, updates, etc.).

3.2 Customer Installation and Training

Provide first-line support

- The Service Bureau will be responsible to provide first-line support to its S.W.I.F.T. customers to allow them to process S.W.I.F.T. transactions in a way that is in line with the responsibilities and liabilities that S.W.I.F.T. imposes on all its customers. This support typically includes minimum guarantees regarding :
 - ongoing customer training regarding interface changes & updates
 - provision of expert resource access to support customers' operations during office hours
 - first level contact for technical & operational assistance, problem investigation and analysis, provision of temporary solutions within required timeframe
 - direct liaison with S.W.I.F.T. help desk on behalf of customers for 'connectivity' problems (interface and/or comms).

1. Definition and General Principles

A “Service Bureau” for the purpose of this Policy is a non-S.W.I.F.T. organisation that provides facilities management and/or data processing services to one or more S.W.I.F.T. Users including operation of a S.W.I.F.T. interface for prime connection to the network and/or for disaster recovery.

A “Service Bureau” may only act on behalf of Users to use S.W.I.F.T. products and services.

A “Service Bureau” may not send or receive messages through the S.W.I.F.T. network for its own account and accordingly is not entitled to a S.W.I.F.T. address.

A “Service Bureau” connection should not diminish the security either of S.W.I.F.T.'s or of a User's systems.

2. Users Responsibilities

A User choosing to be connected via a “Service Bureau” is responsible for:

- a) Ensuring that the security features to access the S.W.I.F.T. system remain under its control so as to restrict access to authorised Users;
- b) Controlling how access to S.W.I.F.T. is managed by the “Service Bureau”;
- c) Ensuring that the “Service Bureau” does not act in a way contrary to that User's obligations and responsibilities towards S.W.I.F.T. and other Users;

- d) Ensuring that the same level of security standards for message confidentiality, integrity and systems availability applicable to it as a S.W.I.F.T. User is maintained by the “Service Bureau” to minimise the potential impact of an operational failure of the “Service Bureau”;
- e) Ensuring that the “Service Bureau” complies with all ownership, operational and security requirements;
- f) Ensuring that the “Service Bureau” complies with all User Handbook obligations incumbent upon Users;
- g) Defining the scope of its “Service Bureau”'s functions and obligations in an agreement with its “Service Bureau”;
- h) Notification of any non-compliance with and breach of the conditions specified in this “Service Bureau” Policy.

Users accept full responsibility for messages sent or received in their name through a “Service Bureau” connection; they recognise that delivery of a message to a S.W.I.F.T. interface operated by their “Service Bureau” is deemed to equate to delivery of that message to them. Users also recognise that they are responsible for any message passing through a S.W.I.F.T. interface at their “Service Bureau” and which thereby purports to emanate from them.

Users connected through the same “Service Bureau” shall be jointly and severally liable in case of breach of any of their above obligations. They agree to indemnify S.W.I.F.T. for any claims for losses or damages resulting from failure to comply with this “Service Bureau” Policy.

Failure to adhere to all obligations mentioned in this Policy may result in revocation of the “Service Bureau” connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.

3. “Service Bureau” General Operational and Security Requirements

- a. A “Service Bureau” may only act on behalf of their User(s) in establishing a connection to S.W.I.F.T. and may not send or receive messages through the S.W.I.F.T. network for their own account.
- b. A “Service Bureau” may not allow non-S.W.I.F.T. Users to connect to or otherwise use a S.W.I.F.T. interface.
- c. A “Service Bureau” may not disclose any information related to S.W.I.F.T. operations, including but not limited to the contents of messages passing through the S.W.I.F.T. system, S.W.I.F.T. technical documentation, S.W.I.F.T. security tokens and S.W.I.F.T. network information, without the prior written consent of S.W.I.F.T. and the User(s) to whom they provide services.

- d. The interface used by a “Service Bureau” to access the S.W.I.F.T. network must be qualified and capable of supporting all features of the respective S.W.I.F.T. service.
- e. All S.W.I.F.T. FIN messages sent from one S.W.I.F.T. User to another S.W.I.F.T. User through a “Service Bureau” must be transmitted over the S.W.I.F.T. network.
- f. A “Service Bureau” may not sub-contract any of their obligations specified in this “Service Bureau” Policy to any third party without prior written consent of their User(s) and S.W.I.F.T.
- g. A “Service Bureau” must sign Service Level Agreements with all S.W.I.F.T. Users to whom they provide services. The Service Level Agreement between the “Service Bureau” and its Users must include the conditions specified herein. In addition, it must contain security arrangements, operations and availability requirements, back-up facilities and disaster recovery mechanisms, based upon the “Service Bureau” Rules and Guidelines document provided by S.W.I.F.T.
- h. A “Service Bureau” must acknowledge that failure to adhere to all obligations mentioned in this Policy may result in revocation of the “Service Bureau” connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.
- i. A “Service Bureau” must annually confirm in writing that it is in compliance with all criteria and conditions specified in the “Service Bureau”x Policy.

4. Specific Rights and Obligations

Considering the above definitions, principles, responsibilities and requirements, the following distinctions shall apply:

4.1 “Service Bureau”x not majority owned and controlled by Users

For “Service Bureau”x not meeting the ownership criteria specified above, National Member Group approval is first required from every country where the “Service Bureau” plans to provide the service, as determined by the country code of the BIC of the User(s) receiving the service.

In addition, the “Service Bureau” application for connection to S.W.I.F.T. shall be submitted to the S.W.I.F.T. Board of Directors for their approval.

Approval by the National Member Group as well as by the S.W.I.F.T. Board of Directors shall be based upon the provision by the “Service Bureau” of genuine services to Users and its adherence to the following additional conditions:

The “Service Bureau” must agree to be audited by S.W.I.F.T. on an annual basis at their own expense to ensure compliance with all criteria and conditions specified in the “Service Bureau” Policy and Service Level Agreement. This Service Level Agreement shall be made available to the S.W.I.F.T. Security Auditors upon request.

4.2 "Service Bureau"x for Disaster Recovery Facilities

Independent of ownership, "Service Bureau"x are permitted to have access to S.W.I.F.T. solely for disaster recovery purposes. A specific agreement between a "Service Bureau" and its User(s) must govern activation of this connection which has to remain under the operational control of S.W.I.F.T.

4.3 Other facilities

Approved "Service Bureau"x will have access to the S.W.I.F.T. products and/or services necessary to ensure the connection of their User(s) to the S.W.I.F.T. network according to this "Service Bureau" Policy.

Admitted "Service Bureau" will thus have the right to:

- a) acquire - on behalf of their User(s) - S.W.I.F.T. products and/or services necessary for the connection to the S.W.I.F.T. network;
- b) call - on behalf of their User(s) - the S.W.I.F.T. Customer Support Centre for support related issues;
- c) use S.W.I.F.T. Vendor Testbed facilities.

SERVICE BUREAU POLICY

1. Definition and General Principles

A Service Bureau for the purpose of this Policy is a non-S.W.I.F.T. organisation that provides facilities management and/or data processing services to one or more S.W.I.F.T. Users including operation of a S.W.I.F.T. interface for prime connection to the network and/or for disaster recovery.

A Service Bureau may only act on behalf of Users to use S.W.I.F.T. products and services.

A Service Bureau may not send or receive messages through the S.W.I.F.T. network for its own account and accordingly is not entitled to a S.W.I.F.T. address.

A Service Bureau connection should not diminish the security either of S.W.I.F.T.'s or of a User's systems.

2. Users Responsibilities

A User choosing to be connected via a Service Bureau is responsible for:

- a) ensuring that the security features to access the S.W.I.F.T. system remain under its control so as to restrict access to authorised Users;
- b) controlling how access to S.W.I.F.T. is managed by the Service Bureau;
- c) ensuring that the Service Bureau does not act in a way contrary to that User's obligations and responsibilities towards S.W.I.F.T. and other Users;
- d) ensuring that the same level of security standards for message confidentiality, integrity and systems availability applicable to it as a S.W.I.F.T. User is maintained by the Service Bureau to minimise the potential impact of an operational failure of the Service Bureau;
- e) ensuring that the Service Bureau complies with all ownership, operational and security requirements;
- f) ensuring that the Service Bureau complies with all User Handbook obligations incumbent upon Users;
- g) defining the scope of its Service Bureau's functions and obligations in an agreement with its Service Bureau;
- h) notification of any non-compliance with and breach of the conditions specified in this Service Bureau Policy.

Users accept full responsibility for messages sent or received in their name through a Service Bureau connection; they recognise that delivery of a message to a S.W.I.F.T. interface operated by their Service Bureau is deemed to

equate to delivery of that message to them. Users also recognise that they are responsible for any message passing through a S.W.I.F.T. interface at their Service Bureau and which thereby purports to emanate from them.

Users connected through the same Service Bureau shall be jointly and severally liable in case of breach of any of their above obligations. They agree to indemnify S.W.I.F.T. for any claims for losses or damages resulting from failure to comply with this Service Bureau Policy.

Failure to adhere to all obligations mentioned in this Policy may result in revocation of the Service Bureau connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.

3. Service Bureau General Operational and Security Requirements

- a. A Service Bureau may only act on behalf of their User(s) in establishing a connection to S.W.I.F.T. and may not send or receive messages through the S.W.I.F.T. network for their own account.
- b. A Service Bureau may not allow non-S.W.I.F.T. Users to connect to or otherwise use a S.W.I.F.T. interface.
- c. A Service Bureau may not disclose any information related to S.W.I.F.T. operations, including but not limited to the contents of messages passing through the S.W.I.F.T. system, S.W.I.F.T. technical documentation, S.W.I.F.T. security tokens and S.W.I.F.T. network information, without the prior written consent of S.W.I.F.T. and the User(s) to whom they provide services.
- d. The interface used by a Service Bureau to access the S.W.I.F.T. network must be qualified and capable of supporting all features of the respective S.W.I.F.T. service.
- e. All S.W.I.F.T. FIN messages sent from one S.W.I.F.T. User to another S.W.I.F.T. User through a Service Bureau must be transmitted over the S.W.I.F.T. network.
- f. A Service Bureau may not sub-contract any of their obligations specified in this Service Bureau Policy to any third party without prior written consent of their User(s) and S.W.I.F.T.
- g. A Service Bureau must sign Service Level Agreements with all S.W.I.F.T. Users to whom they provide services. The Service Level Agreement between the Service Bureau and its Users must include the conditions specified herein. In addition, it must contain security arrangements, operations and availability requirements, back-up facilities and disaster recovery mechanisms, based upon the Service Bureau Rules and Guidelines document provided by S.W.I.F.T.
- h. A Service Bureau must acknowledge that failure to adhere to all obligations mentioned in this Policy may result in revocation of the Service Bureau connection to the S.W.I.F.T. network and accordingly result in the User's deactivation.
- i. A Service Bureau must annually confirm in writing that it is in compliance with all criteria and conditions specified in the Service Bureaux Policy.

4. Specific Rights and Obligations

Considering the above definitions, principles, responsibilities and requirements, the following distinctions shall apply:

4.1. Service Bureaux majority owned and controlled by Users

Service Bureaux majority owned (directly or indirectly) and controlled by S.W.I.F.T. Users are permitted by right to connect to S.W.I.F.T.

Prior to the connection, and annually thereafter, the User(s) controlling the Service Bureau shall provide S.W.I.F.T. with a certificate confirming the ownership situation.

The User(s) controlling the Service Bureau must immediately inform S.W.I.F.T. when its ownership situation changes. Should this mean that the Service Bureau is no longer eligible under the above provision, then the conditions listed in 4.2 hereunder shall apply. The Service Bureau's User(s) must ensure compliance with the conditions listed in 4.2. within 90 days from effect of the ownership changes.

4.2. Service Bureaux not majority owned and controlled by Users

For Service Bureaux not meeting the ownership criteria specified above, National Member Group approval is first required from every country where the Service Bureau plans to provide the service, as determined by the country code of the BIC of the User(s) receiving the service.

In addition, the Service Bureau application for connection to S.W.I.F.T. shall be submitted to the S.W.I.F.T. Board of Directors for their approval.

Approval by the National Member Group as well as by the S.W.I.F.T. Board of Directors shall be based upon the provision by the Service Bureau of genuine services to Users and its adherence to the following additional conditions:

The Service Bureau must agree to be audited by S.W.I.F.T. on an annual basis at their own expense to ensure compliance with all criteria and conditions specified in the Service Bureau Policy and Service Level Agreement. This Service Level Agreement shall be made available to the S.W.I.F.T. Security Auditors upon request.

4.3. Service Bureaux for Disaster Recovery Facilities

Independent of ownership, Service Bureaux are permitted to have access to S.W.I.F.T. solely for disaster recovery purposes. A specific agreement between a Service Bureau and its User(s) must govern activation of this connection which has to remain under the operational control of S.W.I.F.T.

4.4. Other facilities

Approved Service Bureaux will have access to the S.W.I.F.T. products and/or services necessary to ensure the connection of their User(s) to the S.W.I.F.T. network according to this Service Bureau Policy.

Admitted Service Bureau will thus have the right to:

- a) acquire - on behalf of their User(s) - S.W.I.F.T. products and/or services necessary for the connection to the S.W.I.F.T. network;
- b) call - on behalf of their User(s) - the S.W.I.F.T. Customer Support Centre for support related issues;
- c) use S.W.I.F.T. Vendor Testbed facilities.