



Superintendencia de Bancos y de
Otras Instituciones Financieras

Manual de Transacción del Nuevo Marco Contable

Intendencia de Seguros
Dirección de Tecnología de la Información

Febrero 2018
Versión 1.0.0.0.1
Managua, Nicaragua

Tabla de Contenido

1	MANUAL DE TRANSACCIÓN DEL MARCO CONTABLE	4
1.1	INTRODUCCIÓN.....	4
1.2	ASPECTOS CONCEPTUALES (FLUJO DE DATOS)	4
1.3	TIPOS DE ENVÍOS	5
1.3.1	<i>Envíos de las Compañías de Seguros a la SIBOIF.....</i>	<i>5</i>
1.3.2	<i>Formato de los archivos.....</i>	<i>5</i>
1.3.3	<i>Envíos de la SIBOIF a las Compañías de Seguros.....</i>	<i>6</i>
1.4	CONTACTOS	7
2	ANEXOS	8
2.1	ANEXO A: FORMATOS DE ARCHIVOS SEGÚN TIPO DE ENVÍO	8
2.1.1	<i>Anexo A.1: Tipo de envío: MUC – (MUC_Saldos).....</i>	<i>8</i>
2.2	ANEXO B: ARCHIVOS DE RESPUESTAS DE LA SIBOIF	8
2.2.1	<i>Anexo B.1: Incidencias</i>	<i>8</i>
2.2.2	<i>Anexo B.2: Estadísticas</i>	<i>8</i>
2.3	ANEXO C: CATÁLOGOS ANEXOS.....	9
2.3.1	<i>Anexo C.1: Catálogos generales</i>	<i>9</i>
2.3.2	<i>Anexo C.2: Catálogo de Validaciones.....</i>	<i>9</i>
2.3.2.1	<i>Anexo C.3.1: Tabla: MUC_Saldos.....</i>	<i>9</i>
2.4	ANEXO D: MANUAL DE USUARIO PARA LA CARGA DE LOS SALDOS CONTABLES	10
2.4.1	<i>Introducción.....</i>	<i>10</i>
2.4.2	<i>Descripción General del Sistema</i>	<i>10</i>
2.4.2.1	<i>Estructuración del Sistema</i>	<i>10</i>
2.4.2.1.1	<i>Inicio de Sesión.....</i>	<i>10</i>
2.4.2.1.2	<i>Gestión de Archivos</i>	<i>11</i>
2.4.2.1.3	<i>Envíos.....</i>	<i>11</i>
2.4.2.1.4	<i>Consulta de Envíos</i>	<i>13</i>
2.4.2.1.5	<i>Seguridad.....</i>	<i>15</i>
2.4.2.1.6	<i>Cambio de Clave</i>	<i>16</i>
2.5	ANEXO E: FORMATOS CON SUS INSTRUCTIVOS	17
2.5.1	<i>Anexo E.1: Intercambio de llaves públicas de GNUPG</i>	<i>17</i>
2.5.1.1	<i>Anexo E.1.1: Solicitud de intercambio de llaves públicas GNUPG</i>	<i>19</i>
2.5.1.1.1	<i>Anexo E.1.1.1: Formato de Solicitud de intercambio de llaves públicas GNUPG.....</i>	<i>19</i>
2.5.1.1.2	<i>Anexo E.1.1.2: Instructivo de Solicitud de intercambio de llaves públicas GNUPG</i>	<i>20</i>
2.5.1.2	<i>Anexo E.1.2: Acta de aceptación de intercambio de llaves públicas GNUPG.....</i>	<i>21</i>
2.5.1.2.1	<i>Anexo F.1.2.1: Formato del Acta de aceptación de intercambio de llaves públicas GNUPG</i>	<i>21</i>
2.5.1.2.2	<i>Anexo E.1.2.2: Instructivo del Acta de aceptación de intercambio de llaves públicas GNUPG</i>	<i>22</i>
2.5.2	<i>Anexo E.2 Solicitud de altas, bajas y cambios de cuentas de acceso.</i>	<i>23</i>
2.5.2.1	<i>Anexo E.2.1: Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo</i>	<i>23</i>
2.5.2.1.1	<i>Anexo E.2.1.1: Formato de la Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo</i>	<i>25</i>
2.5.2.1.2	<i>Anexo E.2.1.2: Instructivo de la Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo.....</i>	<i>26</i>
2.6	ANEXO F: MANUAL DEL GNUPG	27
2.6.1	<i>Introducción.....</i>	<i>27</i>
2.6.2	<i>Generación de las claves.....</i>	<i>27</i>
2.6.3	<i>Cifrar ficheros</i>	<i>29</i>
2.6.4	<i>Descifrar ficheros</i>	<i>29</i>
2.6.5	<i>Generar la llave pública.....</i>	<i>30</i>
2.6.6	<i>Importando una llave pública a su llavero</i>	<i>30</i>



2.6.7	<i>Automatización desatendida</i>	30
2.6.7.1	Compresión y Cifrado de archivos y Generación del Sha1	30
2.6.7.2	Descifrar ficheros	33
2.6.7.3	Generación del Sha1	33
2.6.7.4	Obtener todos los archivos del servidor de FTP a través de SSH.....	33

Lista de figuras

FIGURA 1	PROCESO GENERAL DE ENVÍO Y RECEPCIÓN DE DATOS	4
FIGURA 2	SERVIDOR DE FTP	6
FIGURA 3	PANTALLA DE INICIO DE SESIÓN	10
FIGURA 4	OPCIONES DEL MENÚ	11
FIGURA 5	PANTALLA DE ENVÍO DE INFORMACIÓN	12
FIGURA 6	VENTANA ELEGIR ARCHIVO	13
FIGURA 7	PANTALLA CONSULTA DE ENVÍO	13
FIGURA 8	CONSULTA DE ENVÍO - CALENDARIO	14
FIGURA 9	CONSULTA DE ENVÍO DETALLE.....	15
FIGURA 10	OPCIÓN DE CAMBIO DE CLAVE	15
FIGURA 11	PANTALLA DE CAMBIO DE CLAVE	16
FIGURA 12	PROCESO DE INTERCAMBIO DE LLAVES PÚBLICAS ENTRE LA SIBOIF E INSTITUCIONES FINANCIERAS	17
FIGURA 13	FORMATO DE SOLICITUD DE INTERCAMBIO DE LLAVES PÚBLICAS	19
FIGURA 14	FORMATO DEL ACTA DE ACEPTACIÓN DE INTERCAMBIO DE LLAVES PÚBLICAS	21
FIGURA 15	PROCESO DE SOLICITUD DE ALTAS, BAJAS Y CAMBIO A LAS CUENTAS DE ACCESO.....	23
FIGURA 16	FORMATO DE LA SOLICITUD DE ALTAS, BAJAS Y CAMBIO A LAS CUENTAS DE ACCESO	25

Lista de tablas

TABLA 1	TIPOS DE ENVÍOS DE LAS INSTITUCIONES FINANCIERAS A LA SIBOIF	5
TABLA 2	NOMENCLATURA DE LOS NOMBRES DE LOS ARCHIVOS A SER ENVIADOS POR LA SIBOIF	7
TABLA 3	CONTACTOS	7
TABLA 4	INSTRUCTIVO DE SOLICITUD DE INTERCAMBIO DE LLAVES PUBLICAS	20
TABLA 5	INSTRUCTIVO DE ACTA DE ACEPTACIÓN DE INTERCAMBIO DE LLAVES PUBLICAS.....	22
TABLA 6	INSTRUCTIVO DE SOLICITUD DE ALTAS, BAJAS Y CAMBIO A LAS CUENTAS DE ACCESO	26

1 Manual de Transacción del Marco Contable

1.1 Introducción

Este documento recopila todos los aspectos relacionados con el envío de Anexo de saldos contables.

1.2 Aspectos conceptuales (Flujo de datos)

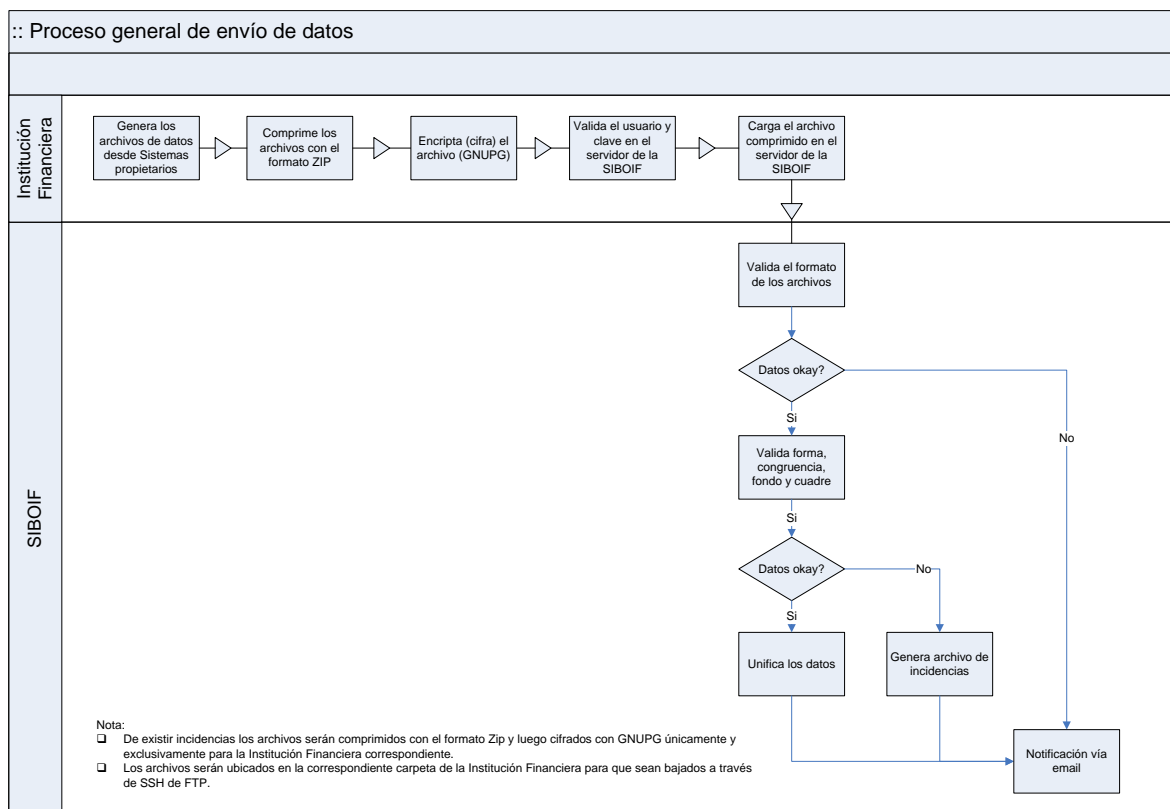


Figura 1 Proceso general de envío y recepción de datos

El flujo principal de envío de datos es mostrado en la “Figura 2: Proceso general de envío y recepción de datos.”:

1. Las Compañías de Seguros deberán generar los archivos pertinentes de sus sistemas propietarios.
2. Los archivos generados deberán de ser comprimidos en el formato Zip.
3. Una vez que se encuentran comprimidos el archivo deberá ser cifrado (encriptado) utilizando la llave publica de la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF).
4. Posteriormente se deberá de conectar a la página principal de la SIBOIF donde deberá de autenticarse con su usuario y clave.
5. Una vez conectado deberá de cargar el archivo cifrado.
6. La primera validación consiste en verificar los archivos enviados, se verifica que la cantidad de archivos y el formato este acorde con el tipo de envío. De no estar acorde con el estándar se notifica de forma automática vía e-mail.

7. Si el formato se encuentra bien, se procede a validar el contenido de los archivos. Si se encontrase alguna inconsistencia, se genera un archivo donde posteriormente es comprimido (zip) y cifrado (GNUPG). Se envía un e-mail automático de notificación para que las Compañías de Seguros a través de FTP descargue dicho archivo.
8. Si no existiesen problemas relevantes en la validación se procede a unificar los datos en el histórico.

1.3 Tipos de envíos

1.3.1 Envíos de las Compañías de Seguros a la SIBOIF

Tipo de envío	Archivos	Descripción
MUC	MUC (MUC_Saldos)	Corresponde al envío de los saldos contables mensuales de las Compañías de Seguros.

Tabla 1 Tipos de envíos de las Instituciones Financieras a la SIBOIF

1.3.2 Formato de los archivos

El formato de los archivos a ser utilizados para envío de datos a la SIBOIF es archivo de texto (ASCII). Los campos deberán de estar separados por el carácter "|" (pipeline) y el código de cuenta contable debe estar delimitados por comillas dobles.

Las cuentas, en el archivo de carga, podrán repetirse de acuerdo a las afectaciones en las diferentes monedas contenidas en el Anexo C.1.

Las cuentas reportadas con el código 3 del Anexo C.1 (moneda extranjera) deberán ser expresadas y reportada en dólares estadounidenses.

Por ejemplo, el archivo de MUC_Saldos está conformado por tres campos o columnas (ver Anexo A.1: Tipo de envío: MUC – MUC_Saldos). Un ejemplo del contenido de dicho archivo se muestra a continuación:

```
"110000000"|4|1207
"110100000"|4|200
"110101000"|4|0
"110102000"|1|200
"110102000"|4|200
"110200000"|4|1007
"110201000"|1|500
"110201000"|2|50
"110201000"|3|10
"110201000"|4|720
"110202000"|1|200
"110202000"|2|2
"110202000"|3|5
"110202000"|4|287
"120000000"|4|5500
"120100000"|4|3200
"120101000"|1|500
"120101000"|2|100
```

```
"120101000"|3|100  
"120101000"|4|2300  
"120102000"|1|400  
"120102000"|4|400  
"120103000"|1|500
```

El nombre del archivo a ser remitido deberá de tener el nombre que se encuentra entre paréntesis de la “Tabla 1 Tipos de envíos de las Instituciones Financieras a la SIBOIF” con la extensión .txt, es decir para este envío es muc_saldos.txt.

Los envíos deberán de estar comprimidos con el formato Zip. Luego deberán de ser cifrados con GPG con la extensión .dat

El nombre del archivo cifrado deberá de contener al final del mismo el símbolo de raya (underscore “_”) seguido del código generado por la función criptográfica Sha-1. Este código tiene como fin garantizar que el archivo remitido no ha sido alterado durante la transmisión. Por ejemplo: ACME200510_c477cd741fe913af75dc92ffd27ece78a7348760.dat

1.3.3 Envíos de la SIBOIF a las Compañías de Seguros

La SIBOIF pondrá a la disposición de las Compañías de Seguros una carpeta propia en un servidor FTP (File Transfer Protocol) para ubicar los archivos de incidencias, referencias crediticias, los consolidados, entre otros. A este sitio se accederá a través de SSH (Secure Shell). Cada Compañía de Seguros tendrá acceso único y exclusivamente a su carpeta, adicionalmente los archivos ubicados en dichas carpetas estarán cifrados única y exclusivamente para las Compañías de Seguros respectivas. La figura 2 muestra un ejemplo de la estructura del sitio.

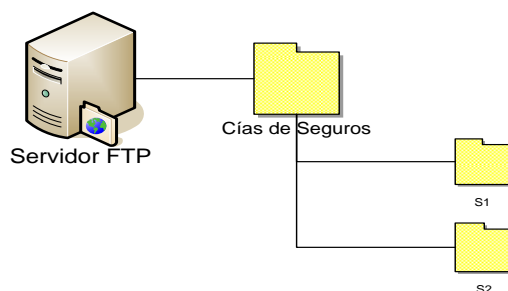


Figura 2 Servidor de FTP

La SIBOIF tiene un tipo de envíos a las Compañías de Seguros:

- **Incidencias (errores):** Cuando se identifique una incidencia (error de validación) en los archivos remitidos en los correspondientes lotes, se creará un archivo con el mismo nombre conteniendo los registros con problemas. Al final del registro se agregará el número del registro, así como un campo conteniendo todos los errores de validación. Los errores estarán codificados conforme el Catálogo de Validaciones (Anexo C.3: Catálogo de Validaciones). De igual forma se generará un archivo general de incidencias el cual contendrá todas las incidencias encontradas en la validación de cada uno de los archivos enviados.

El formato de dichos archivos será de texto (ASCII) según lo expuesto en el acápite (1.3.2 Formato de los archivos).

Los nombres de los archivos se encontraran comprimidos (Zip) y a su vez cifrados (GNUPG):

Nombre del archivo	Nomenclatura	
<u>Incidencias (errores)</u> yyyyymmdd_hh_mi_ss_mmm_[id_carga]_SiglasInstFin_ MUC_Errores_SHA1.dat Ejemplo: 20051104_16_41_14_030_[635]_ACME_ MUC_Errores_4578ecd09a2d0c8431bdd8cf3d5c5f3ddcdf c9.dat	Yyyy	Año
	Mm	Mes
	Dd	Día
	Hh	Hora
	Mm	Minutos
	Ss	Segundos
	Mmm	Milisegundos
	id_carga	Id de Carga
	SiglasInstFin	Siglas de la Compañía de Seguros
	MUC	Manual Único de Cuenta
	SHA1	Código generado por la función criptográfica Sha-1

Tabla 2 Nomenclatura de los nombres de los archivos a ser enviados por la SIBOIF

1.4 Contactos

Área	Nombre	Email	Extensión
Seguros	Horacio Rodriguez Caceres	hrodriguez@siboif.gob.ni	4401
	Luis Narváez Paredes	lnarvaez@siboif.gob.ni	4513
	Donald A. Montealegre Gómez	dmontealegre@siboif.gob.ni	4511
	Marieta Reyes Sequeira	mreyes@siboif.gob.ni	4506
Tecnología	Carlos Flores Román	cflores@siboif.gob.ni;	4701
	Carmen Isabel Prado	cprado@siboif.gobn.ni	4922
	David Marengo	dmarengo@siboif.gob.ni;	4927

Tabla 3 Contactos

Los números de la planta telefónica de la SIBOIF son los siguientes: 2298-2100 c y 7826-2900 m.

2 Anexos

2.1 Anexo A: Formatos de archivos según tipo de envío

2.1.1 Anexo A.1: Tipo de envío: MUC – (MUC_Saldos)

Orden	Campo	Tipo de dato	Descripción	Tabla Relacionada
1	id_cuenta	varchar(8)	Cuenta Contable. Corresponde al código de la cuenta contable establecida en el nuevo marco contable.	
2	id_moneda	int	Código de la moneda.	id_moneda
3	saldo	numeric(20, 2)	Saldo de la cuenta contable, siempre en positivo a excepción de aquellas cuentas que sea permitido por tener ambas naturalezas.	

2.2 Anexo B: Archivos de respuestas de la SIBOIF

2.2.1 Anexo B.1: Incidencias

Orden	Campo	Tipo de dato	Descripción	Tabla Relacionada
1	id_cuenta	varchar(8)	Cuenta Contable. Corresponde al código de la cuenta contable.	
2	id_moneda	int	Código de la moneda.	id_moneda
3	saldo	numeric(20, 2)	Saldo de la cuenta contable.	
4	Linea	Int	Línea original de remisión del archivo donde se encuentra la incidencia.	
5	Id_validacion	varchar(500)	Códigos de validaciones separados por comas de encontrarse más de un error en la línea indicada.	

Ejemplo:

```
"110101000"|2|200|13|"08.001.0017"
"120301001"|4|200|20|"08.001.0005"
"110200000"|4|107|40|"08.001.0012"
"110200000"|1|500|20|"08.001.0013"
```

2.2.2 Anexo B.2: Estadísticas

Orden	Campo	Tipo de dato	Descripción	Tabla Relacionada
1	Id_consecutivo	int	Consecutivo	
2	Id_validacion	Int	Código de validación.	

Orden	Campo	Tipo de dato	Descripción	Tabla Relacionada
3	Descripción	varchar(500)	Descripción de la validación que fué violada	

Ejemplo

1|"08.001.0007"|": La suma de los saldos de las cuentas deudoras ..."

Nota: Con el objetivo de ahorrar espacio los últimos dos mensajes fueron cortados. En la práctica aparecerá la descripción correspondiente al Catálogo de Validaciones (Anexo C.3).

2.3 Anexo C: Catálogos anexos

2.3.1 Anexo C.1: Catálogos generales

Id_moneda [1, 2]		
	1	Nacional sin Mantenimiento de Valor.
	2	Nacional con Mantenimiento de Valor.
	3	Extranjera.
	4	Total / Consolidado

2.3.2 Anexo C.2: Catálogo de Validaciones

2.3.2.1 Anexo C.3.1: Tabla: MUC_Saldos

Validación	Descripción
08.001.0001	El código de cuenta no puede ser nulo
08.001.0002	El código de moneda no puede ser nulo
08.001.0003	El saldo no puede ser nulo
08.001.0004	El código de cuenta no puede repetirse para la misma moneda
08.001.0005	El código de cuenta no existe en el Catálogo de Cuentas
08.001.0006	La moneda especificada no existe en el catálogo de monedas
08.001.0007	La suma de los saldos de las cuentas deudoras no coincide con la suma de los saldos de las cuentas acreedoras
08.001.0008	El total de activos no equivale al total del pasivo más el total del patrimonio en el Estado de Situación Financiera.
08.001.0010	No se enviaron saldos consolidados en moneda 4
08.001.0011	El total consolidado identificado con la moneda (4) no es igual a la sumatoria de los saldos de la moneda (1), (2) y (3); ésta última, multiplicada por el tipo de cambio oficial vigente a la fecha de corte que corresponda
08.001.0012	El saldo no coincide con la suma de las cuentas hijas
08.001.0013	Reportó una cuenta que no es afectada con saldos para la moneda 1, 2 y 3
08.001.0016	El saldo de la cuenta no puede expresarse en negativo, a menos que exista excepción
08.001.0017	El código de la moneda no aplica para la cuenta reportada
08.001.0021	No se enviaron saldos para la cuenta padre

Validación	Descripción
08.001.0025	Las cuentas con saldos en cero no deben ser reportadas

2.4 Anexo D: Manual de Usuario para la carga de los Saldos Contables

2.4.1 Introducción

El manual presenta una descripción general del sistema, así como las características de cada uno de los bloques de procesos. Por cada pantalla se da a conocer una breve descripción de las características y funcionalidad de la misma, se describen los campos de datos, valores de las listas en caso de que el campo tenga asociada una, e instrucciones de uso.

2.4.2 Descripción General del Sistema

El Sistema de envío de datos para los diferentes aplicativos y/o sistemas en un modo simplificado puede verse como una herramienta que permite realizar cargas de archivos de las Instituciones Financieras y luego consultar el progreso de las mismas cumpliendo con las validaciones establecidas por la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF).

2.4.2.1 Estructuración del Sistema

El **Sistema** se encuentra estructurado en los siguientes bloques de funciones: Gestión de Archivos y Seguridad.

- **Gestión de Archivos:** En este bloque de funciones se encuentran los procesos necesarios para la carga de archivos y estado de la misma en el transcurso de las validaciones del sistema, tal como: Envíos y Consulta de Envíos.
- **Seguridad:** En este bloque de funciones se encuentra el proceso relacionado al cambio de clave de usuario.

2.4.2.1.1 Inicio de Sesión

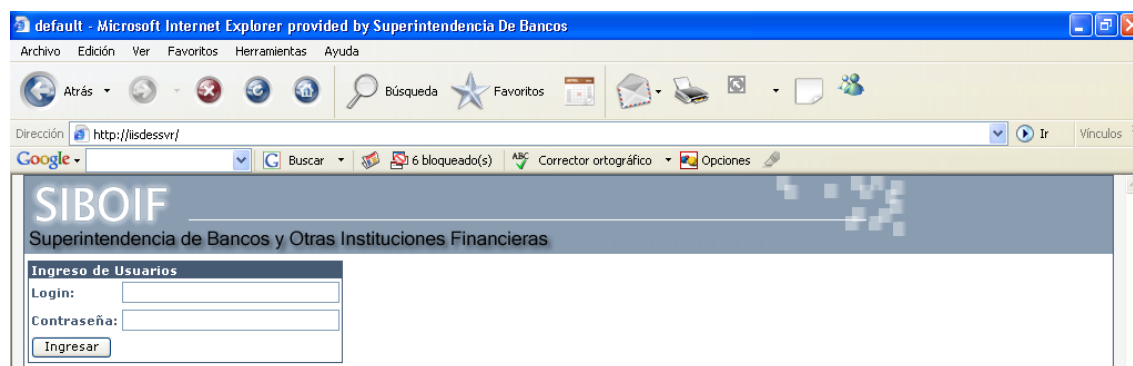


Figura 3 Pantalla de Inicio de Sesión

Descripción General

Esta opción debe de ser el primer paso que tiene que dar el usuario para empezar a utilizar el **Sistema de Envíos de Archivos**.

La pantalla contiene los siguientes campos:

Campos	Descripción
Login	Id del Usuario a ingresar
Contraseña	Clave del usuario.
Ingresar	Al presionar el botón de ingresar se válida que la clave exista y la contraseña sea válida.

Instrucciones de Uso	
1.	Ingresar el login de usuario.
2.	Ingresar la contraseña correspondiente.
3.	Presionar el botón de Ingresar para acceder al sistema.

2.4.2.1.2 Gestión de Archivos

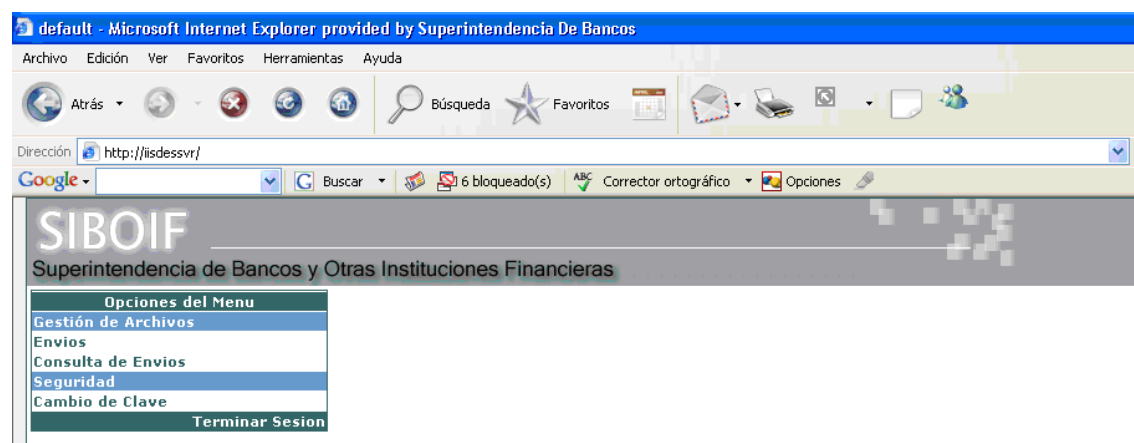


Figura 4 Opciones del Menú

El Bloque de funciones de Gestión de Archivos presenta las siguientes opciones:

- Envíos
- Consulta de Envíos

A continuación se exponen en detalle las opciones presentadas anteriormente.

2.4.2.1.3 Envíos

Figura 5 Pantalla de Envío de Información

Descripción General

A través de esta pantalla el usuario realiza la carga de archivos correspondiente a su institución Financiera.

La pantalla contiene los siguientes campos:

Campo	Descripción
Tipo de Envío	Lista de valores que permite especificar el tipo de envío a realizar. En este caso como el tipo de envío es para la carga de los saldos contables, el usuario deberá de seleccionar el tipo de envío ""
Fecha de Datos	Lista de fechas que permite al usuario especificar la fecha de corte de los datos enviados.
Archivo	Permite especificar el archivo que se desea cargar por medio de la ruta local, el campo de archivo posee un botón Browse (Examinar) para la carga de información.

Al hacer clic en **Browse** se accede al explorador de archivos:

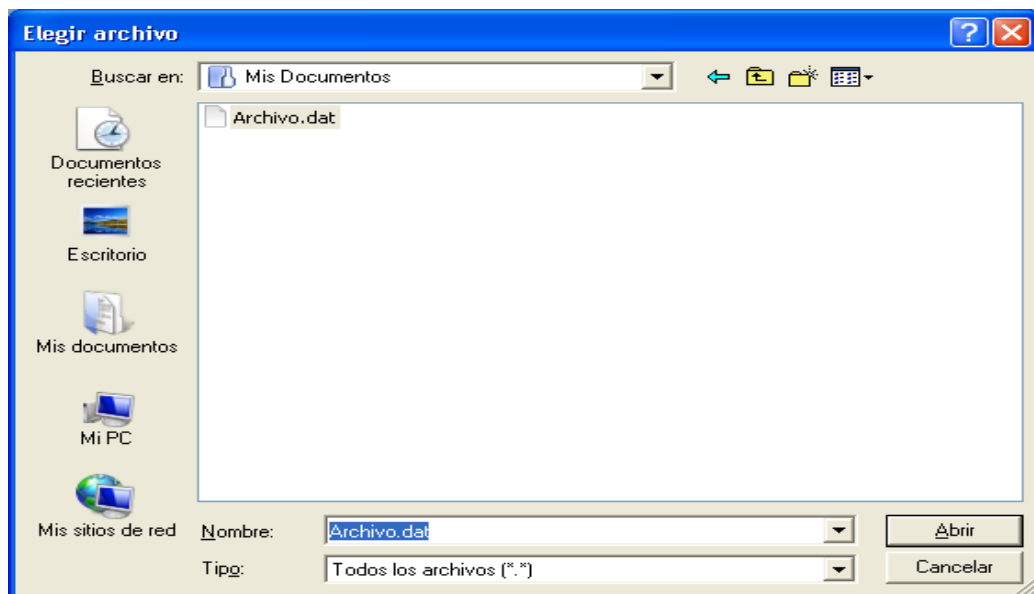


Figura 6 Ventana elegir archivo

En esta exploración de archivos se especifica el archivo a cargar en el sistema, la extensión de los archivos debe de ser .dat, una vez seleccionado el archivo se presiona el botón Abrir. En caso de presionar el botón Cancelar, la operación de selección de archivos se anula.

Instrucciones de Uso

1.	Especificar el Tipo de Envío
2.	Seleccionar el archivo a cargar al sistema, los archivos a cargar deben de ser de extensión .dat.
3.	Presionar el botón subir, y esperar la generación del número de Envío y el valor cifrado del archivo.

2.4.2.1.4 Consulta de Envíos

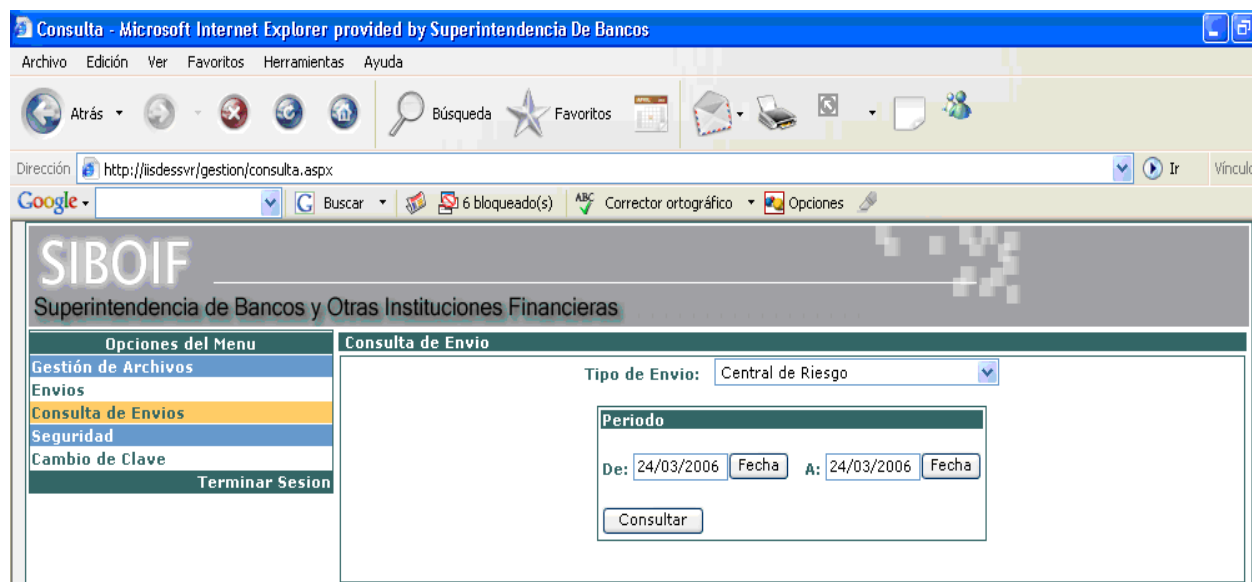


Figura 7 Pantalla Consulta de Envío

Descripción General

A través de esta pantalla el usuario realiza la consulta de los archivos cargados previamente en el Sistema. La pantalla de Consultas de Envío cuenta con un rango de Fechas para mostrar las cargas deseadas, al mismo tiempo se limitan los resultados al tipo de Envío seleccionado.

La pantalla contiene los siguientes campos:

Campo	Descripción
Tipo de Envío	Es una lista de valores que permite especificar si el archivo es de CDR, MUC, Solicitud de Referencias de Crediticias y/o Equivalencias de Personas o de los Anexos de la Intendencia de Seguros.
Fecha Inicial	Punto inicial en la que se quiere iniciar la consulta
Fecha Final	Punto Final en el cual se desea finalizar la consulta
Consultar	Gestiona las cargas realizadas en el rango de fechas previamente establecidas.

Al hacer click sobre el campo Fecha Inicial o Fecha Final se muestra el siguiente Calendario:

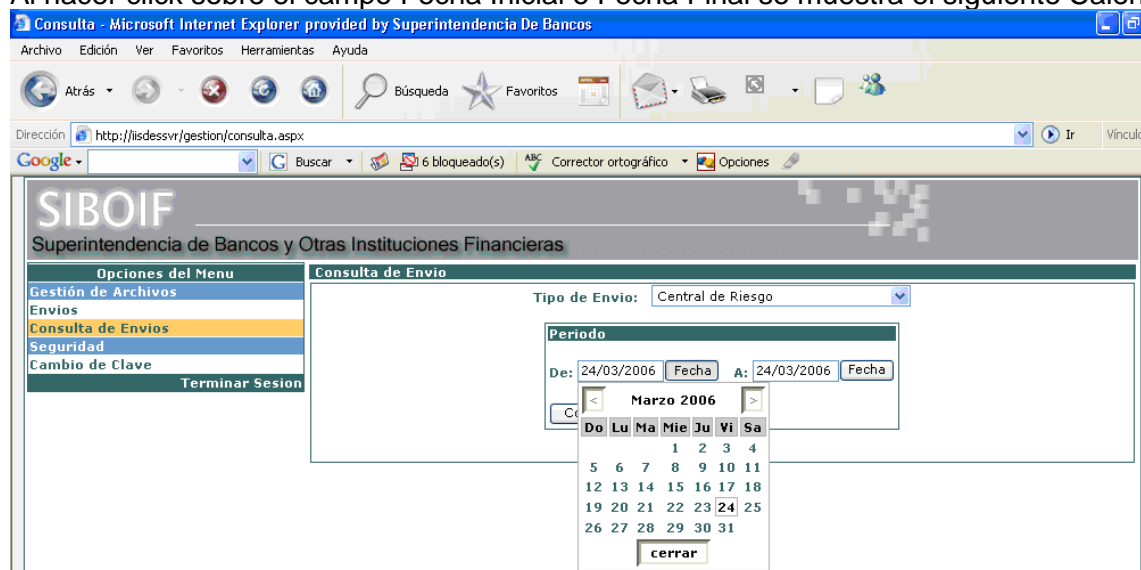
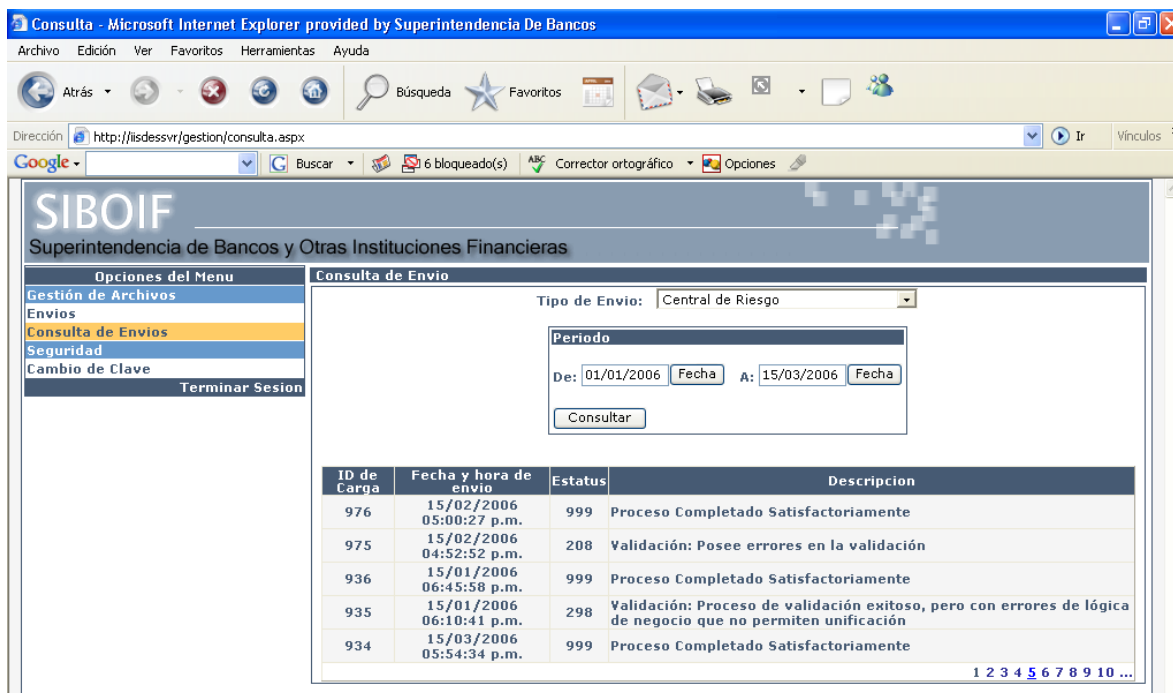


Figura 8 Consulta de Envío - Calendario

Con el cual el usuario tendrá la flexibilidad de seleccionar la fecha de una forma exacta y precisa, evitando así la digitación de la misma.

Al hacer clic en el botón Consultar se muestran los siguientes resultados en pantalla:



ID de Carga	Fecha y hora de envío	Estatus	Descripción
976	15/02/2006 05:00:27 p.m.	999	Proceso Completado Satisfactoriamente
975	15/02/2006 04:52:52 p.m.	208	Validación: Posee errores en la validación
936	15/01/2006 06:45:58 p.m.	999	Proceso Completado Satisfactoriamente
935	15/01/2006 06:10:41 p.m.	298	Validación: Proceso de validación exitoso, pero con errores de lógica de negocio que no permiten unificación
934	15/03/2006 05:54:34 p.m.	999	Proceso Completado Satisfactoriamente

Figura 9 Consulta de Envío Detalle

Instrucciones de Uso	
1.	Especificar el Tipo de Envío
2.	Se establece la fecha inicial
3.	Se establece la fecha final
4.	Presionar el botón Consultar y se mostrarán las cargas realizadas en el período seleccionado en caso de existir alguna.

2.4.2.1.5 Seguridad

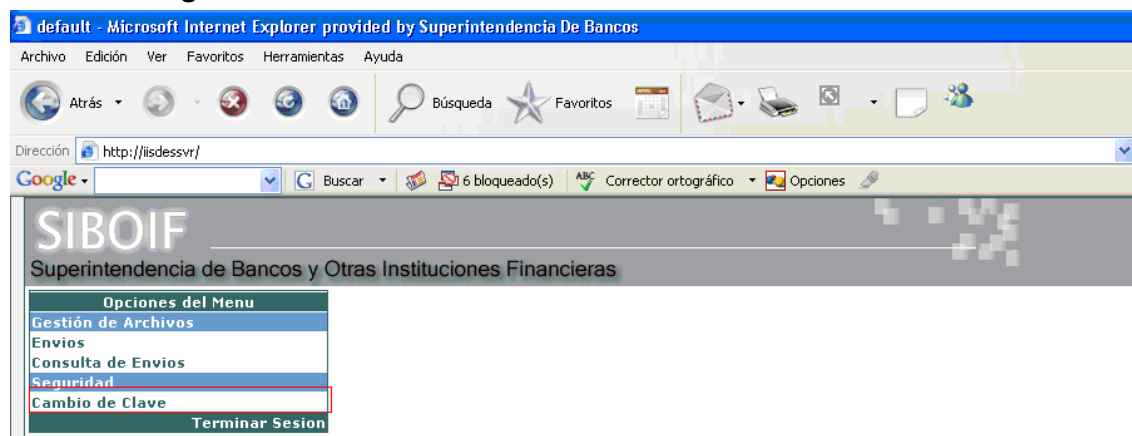


Figura 10 Opción de Cambio de Clave

El Bloque de funciones de Seguridad presenta las siguientes opciones:

- Cambio de Clave

A continuación se expone en detalle la opción listada anteriormente.

2.4.2.1.6 Cambio de Clave

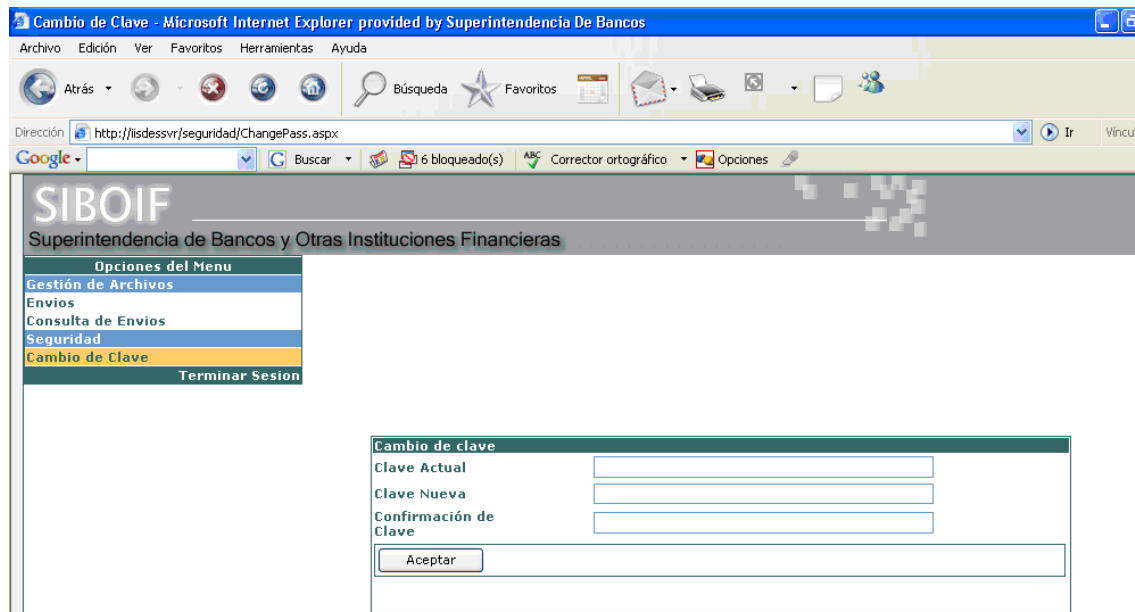


Figura 11 Pantalla de Cambio de Clave

Descripción General:

El formulario Web de cambios de clave tiene el propósito de cambiar la contraseña del usuario que está en línea en ese momento. El cambio de contraseña tomará efecto hasta el próximo inicio de Sesión.

La pantalla contiene los siguientes campos:

Campo	Descripción
Clave Actual	Contraseña Actual del usuario en línea.
Clave Nueva	Contraseña nueva a introducir.
Confirmación de Clave	Confirma la contraseña ingresada en el campo anterior.
Botón Aceptar	Sustituye la contraseña anterior por la nueva.

Instrucciones de Uso	
1.	Digitar la contraseña actual.
2.	Digitar la nueva contraseña.
3.	Confirmar la nueva contraseña especificada en el campo anterior.
4.	Presionar el botón de Aceptar para que los cambios surtan efectos.

2.5 Anexo E: Formatos con sus Instructivos

2.5.1 Anexo E.1: Intercambio de llaves públicas de GNUPG

Este procedimiento, sirve de guía para las actividades relacionadas con el intercambio de llaves públicas entre las Instituciones Financieras y la SIBOIF, con el objetivo de proteger la información que se transmite entre ellas. Para esto se encriptarán los archivos de datos a intercambiar utilizando la herramienta de encriptación GNUPG.

Las solicitudes de intercambio de llaves públicas en las instituciones financieras serán elaboradas por el oficial de seguridad o cargo similar, autorizadas por su gerente de operaciones o similar y enviadas a la SIBOIF para que la intendencia propietaria del sistema y el director de informática las aprueben y estas serán intercambiadas directamente con el Administrador de Bases de Datos (DBA) de la SIBOIF.

Este procedimiento se realizará tomando en consideración que la validez de las llaves públicas tendrá una duración de un año de vigencia y deberán ser regeneradas por cada una de las partes involucradas e intercambiadas nuevamente. El intercambio se realizará en un medio de almacenamiento físico en las instalaciones de las SIBOIF.

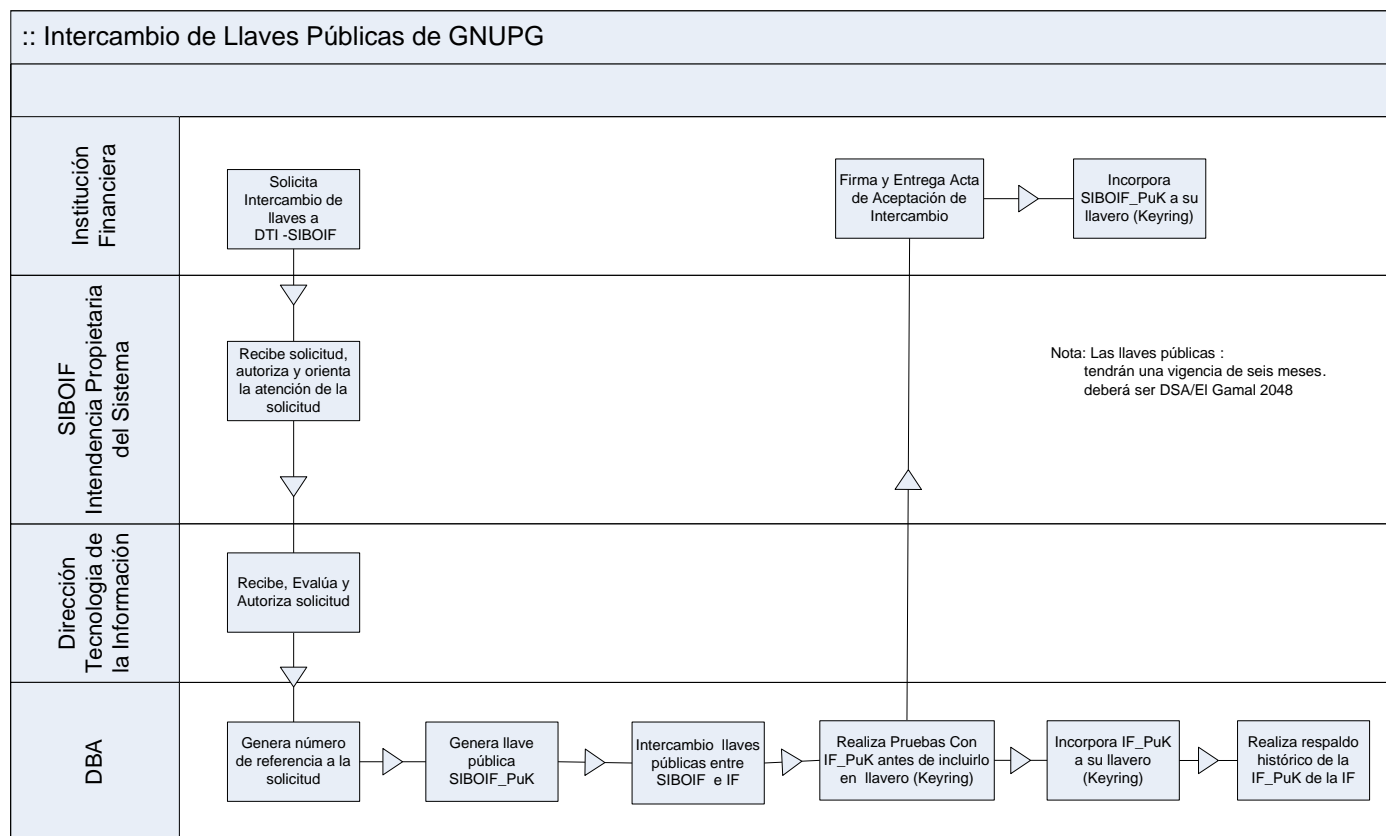


Figura 12 Proceso de intercambio de llaves públicas entre la SIBOIF e instituciones Financieras

Este procedimiento se ejecutará cada vez que las partes involucradas necesiten actualizar los llaveros (keyring) debido al periodo de caducidad de las llaves públicas establecido por la SIBOIF o bien por cambios anticipados en las llaves por cualquiera de los involucrados. En caso de caducidad se deberá de realizar una semana antes de la fecha de vencimiento establecida por la SIBOIF. Para los cambios en las llaves públicas se hará en el momento que sea necesario.

- ❑ El Oficial de Seguridad de la Institución Financiera en conjunto con el gerente de operaciones o similar emiten una “Solicitud de intercambio de llaves publicas GNUPG” (Anexo F.1.1) y la envían a la intendencia dueña del sistema en la SIBOIF.
- ❑ La intendencia dueña del sistema recibe la “solicitud de intercambio de llaves publicas GNUPG”
- ❑ La intendencia dueña del sistema en conjunto con el director de informática autorizan la solicitud.
- ❑ El director de informática orienta al Administrador de Bases de Datos y sistemas para que atienda dicha solicitud.
- ❑ El Administrador de Bases de Datos y sistemas recibe la solicitud, la evalúa y le asigna a la solicitud un número de referencia consecutivo por institución. Este número deberá de ser generado de la siguiente forma:

SiglasDeInstitucion_yyyy_999

SiglasDeInstitucion	Siglas de la Institución Financiera
yyyy	Año actual
999	Consecutivo de tres dígitos

- ❑ El Oficial de Seguridad de la Institución Financiera procede a generar la llave pública de intercambio y la copia en un CD.
- ❑ El Administrador de Bases de Datos y sistemas de la SIBOIF procede a generar la llave pública de intercambio y la copia en un CD.
- ❑ El Administrador de Bases de Datos y sistemas de la SIBOIF intercambian los CD de llaves públicas con el Oficial de Seguridad de la Institución Financiera en las instalaciones de la SIBOIF.
- ❑ El Administrador de Bases de Datos y sistemas de la SIBOIF realiza pruebas con el archivo de llave pública de la institución financiera antes de pasarlo a producción.
- ❑ Si las pruebas fueron satisfactorias el Administrador de Bases de Datos y sistemas de la SIBOIF le orienta al Oficial de Seguridad de la Institución Financiera que llene el “Acta de aceptación de intercambio de llaves publicas GNUPG” (Anexo F.1.2).
- ❑ El Oficial de Seguridad de la Institución Financiera llena dicha acta aceptando la transacción realizada y se la entrega al Administrador de Bases de Datos y sistemas de la SIBOIF.
- ❑ Ambas partes una vez intercambiadas y probadas las copias proceden a incorporarlas en sus respectivos llaveros (keyring).

El Administrador de Bases de Datos y sistemas de la SIBOIF realiza un respaldo histórico de las llaves públicas caducadas (Instituciones Financieras y SIBOIF).



2.5.1.1 Anexo E.1.1: Solicitud de intercambio de llaves públicas GNUPG

Este formato es para el uso del área de informática de las instituciones financieras y para el consumo de los especialistas en informática de la SIBOIF.

2.5.1.1.1 Anexo E.1.1.1: Formato de Solicitud de intercambio de llaves públicas GNUPG

Superintendencia de Bancos y Otras Instituciones Financieras (SIBOIF) Dirección de Tecnología de la Información (DTI) Área de Soporte Técnico Solicitud de Intercambio de Llaves publicas GNUPG					
			No. Referencia:		
Datos Generales					
A:					
	Nombre y Apellido	Cargo	Firma		
De:					
Autoriza:					
Institución:					
Fecha:					
Datos Solicitud					
Descripción:					
Observaciones:					
Firmas Autorizadoras					
Estado	Nombre	Cargo	Fecha	Hora	Firma
Recepcionada					
Autorización Intendencia					
Autorización DTI					
Recibida					
Elaborada					

Figura 13 Formato de Solicitud de intercambio de llaves públicas

2.5.1.1.2 Anexo E.1.1.2: Instructivo de Solicitud de intercambio de llaves públicas GNUPG

Instructivo del formato de Solicitud de Intercambio de Llaves Publicas GNUPG							
A	Dirija la solicitud al coordinador del sistema de la intendencia dueña en la SIBOIF.						
De / Autoriza	Escriba quien es el que solicita y autoriza los cambios (Oficial de Seguridad o cargo similar de la institución Financiera y Gerente Administrativo Financiero o cargo similar de la institución Financiera).						
Institución	Anote el nombre de la institución la cual está solicitando la actualización del nuevo conjunto de llaves						
Fecha Elaboración	Anote la fecha en que se elabora la solicitud en la Institución Financiera con el formato dd/mm/yyyy.						
No. Referencia	Este número será llenado por el DBA. <ul style="list-style-type: none"> SiglasDeInstitucion_yyyy_999 <table border="1"> <tr> <td>SiglasDeInstitucion</td> <td>Siglas de la Institución Financiera</td> </tr> <tr> <td>yyyy</td> <td>Año</td> </tr> <tr> <td>999</td> <td>Consecutivo de tres posiciones</td> </tr> </table>	SiglasDeInstitucion	Siglas de la Institución Financiera	yyyy	Año	999	Consecutivo de tres posiciones
SiglasDeInstitucion	Siglas de la Institución Financiera						
yyyy	Año						
999	Consecutivo de tres posiciones						
Descripción de la solicitud	Explique de forma clara y concisa para ayudar a explicar el cambio, en qué consiste el servicio que requiere. Si es por vencimiento de las llaves públicas, cambio imprevisto en su llavero o por un nuevo requerimiento, etc.						
Observaciones	Observaciones que señala el coordinador del sistema, director de informática o el DBA de la SIBOIF de ser estas necesarias.						
Firmas	Esta sección es utilizada exclusivamente por la SIBOIF para llevar la traza o pista del estado de la solicitud en cuanto a su atención por medio de la firma de las diferentes personas involucradas en este proceso: Recepcionada Autorización Intendencia Autorización DTI Recibida Elaborada						

Tabla 4 Instructivo de Solicitud de Intercambio de llaves publicas

2.5.1.2 Anexo E.1.2: Acta de aceptación de intercambio de llaves públicas GNUPG

Este formato es para el uso y consumo del área de soporte técnico de la DTI en la superintendencia de bancos y es el comprobante en la transacción de intercambio de llaves públicas entre el oficial de seguridad y el administrador de bases de datos (DBA).

2.5.1.2.1 Anexo F.1.2.1: Formato del Acta de aceptación de intercambio de llaves públicas GNUPG

Superintendencia de Bancos y Otras Instituciones Financieras (SIBOIF)				
Dirección de Tecnología de la Información (DTI)				
Área de Soporte Técnico				
Acta de aceptación de intercambio de llaves publicas GNUPG				
		No. Referencia		
A				
De				
Institución				
Fecha Intercambio		Hora Intercambio		
Situación Actual		Resultado del Proceso		
<input type="checkbox"/> Llaves Expiradas <input type="checkbox"/> Llaves Por Expirar <input type="checkbox"/> Requerimientos nuevos <input type="checkbox"/> Modificaciones en los llaveros <input type="checkbox"/> Otros		<input type="checkbox"/> Llaves Regeneradas <input type="checkbox"/> Llaves Modificadas <input type="checkbox"/> Llaves Intercambiadas <input type="checkbox"/> Otros		
Pasa a producción		<input type="checkbox"/> Si	<input type="checkbox"/> No	
Firma Oficial de Seguridad o Similar				
Nombre Especialista				
Observaciones				

Figura 14 Formato del Acta de aceptación de intercambio de llaves públicas

2.5.1.2.2 Anexo E.1.2.2: Instructivo del Acta de aceptación de intercambio de llaves públicas GNUPG

Instructivo del formato del Acta de Aceptación de intercambio de llaves publicas GNUPG	
A	Escriba el Nombre del Funcionario y el cargo que ocupa. Esta solicitud debe ser dirigida DBA de la SIBOIF.
De	Escriba el Nombre del Funcionario y el cargo que ocupa. Para este formato en particular quien envía es el oficial de seguridad de la institución financiera o cargo similar, como autoridad que aprueba el intercambio.
Fecha Intercambio	Anote la fecha en la que se acepta el intercambio con el formato dd/mm/yyyy.
Hora Intercambio	Anote la hora en que se acepta el intercambio con el formato HH:MM; a.m ó p.m.
Institución	Anote el nombre de la institución la cual solicito la actualización del nuevo conjunto de llaves
No. Referencia	Corresponde al No. De referencia de la solicitud de intercambio que corresponda a la institución.
Situación actual	Indique cuál de las opciones indicadas representa la situación actual en el sistema de la institución financiera. Llaves Vencidas Llaves Por vencer Requerimientos nuevos Modificaciones en los llaveros Otros
Resultados del proceso	Indique cual fue el resultado de los procesos que elaboró Llaves Regeneradas Llaves Modificadas Llaves Intercambiadas Otros
Pasa a producción	El DBA indica si el procedimiento de intercambio de llaves finalizó de forma exitosa. Escriba si acepta pasar a producción o no, esto estará en dependencia de las pruebas que realice el DBA. Si todo está como se solicitó debe aceptar para poder ver reflejado el cambio en los sistemas.
Observaciones	Si considera incluir alguna observación, o en el caso de que la categoría sea Otros.
Nombre Especialista	Nombre del administrador de sistemas y bases de datos o encargado de realizar los cambios de la SIBOIF.
Firma	Cualquier acta de intercambio debe ser firmada por ambas partes, tanto por el oficial de seguridad o cargo similar que es quien solicita el intercambio así como por el administrador de sistemas y bases de datos que es quien administra los llaveros de la SIBOIF.

Tabla 5 Instructivo de Acta de aceptación de Intercambio de llaves publicas

2.5.2 Anexo E.2 Solicitud de altas, bajas y cambios de cuentas de acceso.

Este procedimiento, es la guía base a utilizar en las actividades de creación, eliminación y/o modificación de cuentas de acceso (usuarios) a los sistemas de la SIBOIF. A través de este se documenta y controla cada acción que se realiza en el módulo global de seguridad de sistemas en cuanto a la administración de usuarios y accesos a módulos específicos por medio de la asignación de roles.

Estas solicitudes son utilizadas tanto en la creación como en la administración de usuarios internos o externos y son elaboradas en dependencia del tipo y ubicación del usuario, ya sea para una Institución Financiera o bien por una intendencia específica a lo interno de la SIBOIF.

2.5.2.1 Anexo E.2.1: Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo

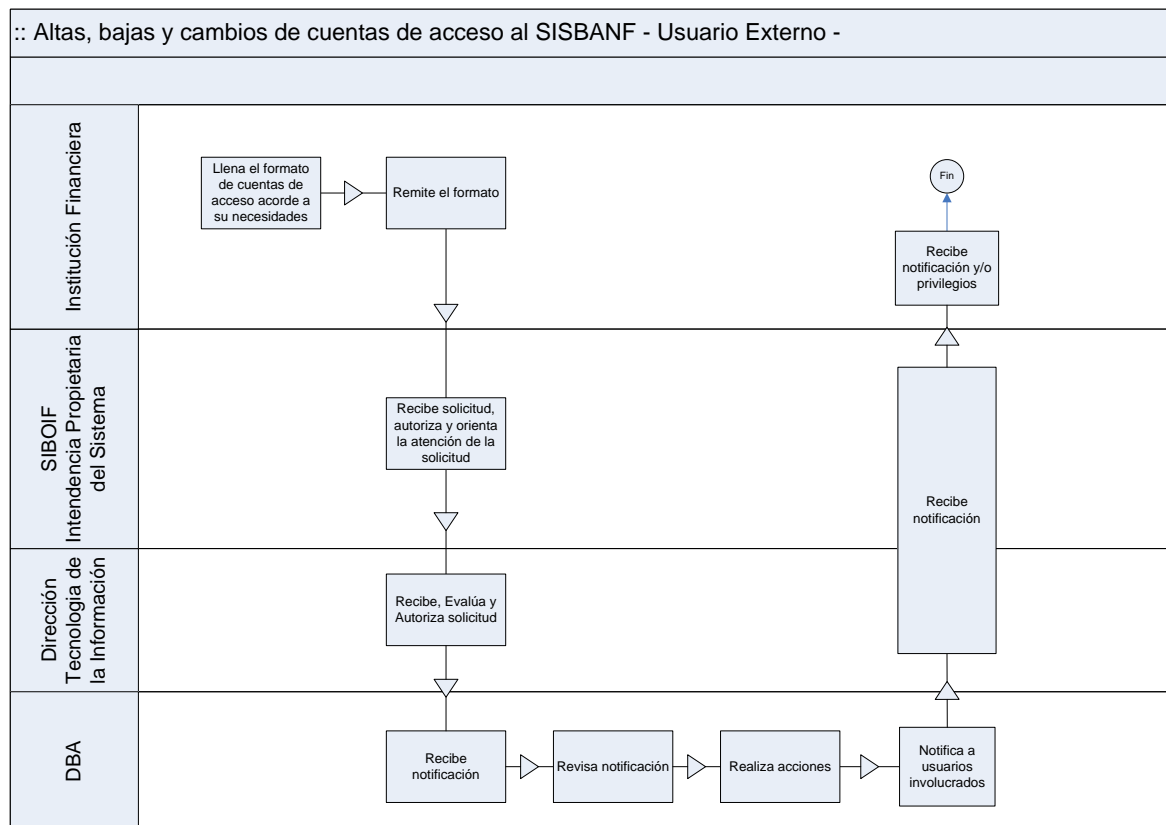


Figura 15 Proceso de solicitud de altas, bajas y cambio a las cuentas de acceso

Este proceso ocurre cuando una Institución Financiera a la cual se le ha otorgado acceso a utilizar uno o más sistemas de la SIBOIF, desee crear o bien modificar una cuenta de acceso existente.

Las solicitudes de creación o cambio en las cuentas de acceso son elaboradas por el jefe de área de la institución financiera la cual tiene acceso al sistema y autorizadas por el gerente de operaciones o similar de la Institución Financiera, enviadas a la SIBOIF para su revisión y aprobación por la

intendencia dueña del sistema y el director de informática y ejecutadas directamente por el Administrador de Bases de Datos (DBA).

- ❑ La Institución Financiera crea una “Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo” (Anexo F.2) y la envía al dueño del sistema en las instalaciones de la SIBOIF.
- ❑ La intendencia dueña del sistema en conjunto con el director de informática, reciben la solicitud, evalúan la factibilidad y la aprueban.
- ❑ El director de informática envía la solicitud al DBA, para que este la ejecute.
- ❑ El DBA recibe la solicitud y le asigna un número de referencia consecutivo por sistema. Este número deberá de ser generado de la siguiente forma:

- SiglasDelSistema_yyyy_999

SiglasDelSistema	CdR	Central de Riesgo (CdR)
	MUC	Manual Unico de Cuentas (MUC)
	LdD	Lavado de Dólares (LdD)
	MAR	Modelo de Análisis de Riesgo (MAR)
	ANXSEG	Anexos de la Intendencia de Seguros
yyyy	Año actual	
999	Consecutivo por sistema de tres dígitos	

- ❑ El DBA procede a ejecutar la solicitud, según lo indicado en ésta.
 - Para el caso de alta de usuarios cuando estos son creados, se debe de seguir la siguiente nomenclatura.

NombreInstitucion_NombreUsuario_999

Nombre_Institucion	El nombre corto o siglas de la Institución Financiera
NombreUsuario	El nombre del usuario al cual se le otorga el acceso, este estará compuesto de: Primer letra del primer nombre + primer Apellido Pedro Pérez = pperez
999	Consecutivo de tres posiciones por usuario con el mismo nombre y apellido

- ❑ El DBA notifica vía correo electrónico la conclusión del proceso.
- ❑ Fin del procedimiento.

2.5.2.1.1 Anexo E.2.1.1: Formato de la Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo

Superintendencia de Bancos y Otras Instituciones Financieras (SIBOIF) Dirección de Tecnología de la Información (DTI) Área de Soporte Técnico					
Solicitud de altas, bajas y cambio a las cuentas de acceso					
		No. Referencia:			
Datos Generales					
A:					
	Nombre y Apellidos	Cargos	Firmas		
De:					
Autoriza:					
Institución:					
Fecha:					
Datos Solicitud					
Acciones a Realizar		Información del Usuario			
<input type="checkbox"/> Creación de Nuevo Usuario <input type="checkbox"/> Modificar un perfil Existente <input type="checkbox"/> Eliminar Usuario Existente		Nombres y Apellidos del Usuario:			
		Nombre Usuario:			
Información del Perfil					
1 Central de Riesgo 1.1 Carga de Datos <input type="checkbox"/> 1.1.1 Central de Riesgo <input type="checkbox"/> 1.1.2 Equivalencias Personas 1.2 Referencias Crediticias <input type="checkbox"/> 1.2.1 Por Lote <input type="checkbox"/> 1.2.2 Web Services		2 Manual Único de Cuentas 2.1 Carga de Datos <input type="checkbox"/> 2.1.1 MUC <input type="checkbox"/> 2.1.2 Estratificaciones <input type="checkbox"/> 2.1.3 Anexos 3 Lavado de Dinero <input type="checkbox"/> 3.1 Carga de Datos 4. Otros 4.1 Descarga de información			
Observaciones:					
Firmas Autorizadoras					
Estado	Nombre	Cargo	Fecha	Hora	Firma
Recepcionada					
Autorización Intendencia					
Autorización DTI					
Recibida					
Elaborada					

Figura 16 Formato de la Solicitud de altas, bajas y cambio a las cuentas de acceso

2.5.2.1.2 Anexo E.2.1.2: Instructivo de la Solicitud de altas, bajas y cambio a las cuentas de acceso para usuario externo

Instructivo del formato de Solicitud de altas, bajas y cambio a las cuentas de acceso							
A	Dirija la solicitud al coordinador de la intendencia dueña del sistema						
Remitentes	Escriba quien es el que solicita y autoriza los cambios (Jefe de área de la institución Financiera y Gerente Administrativo Financiero o cargo similar de la institución Financiera).						
Institución	Anote el nombre de la institución la cual está realizando la solicitud						
Fecha Elaboración	Anote la fecha en que se elabora la solicitud en la Institución Financiera con el formato dd/mm/yyyy.						
No. Referencia	Este número será llenado por el DBA. <ul style="list-style-type: none"> SiglasDeInstitucion_yyyy_999 <table border="1"> <tr> <td>SiglasDeInstitucion</td> <td>Siglas de la Institución Financiera</td> </tr> <tr> <td>yyyy</td> <td>Año</td> </tr> <tr> <td>999</td> <td>Consecutivo</td> </tr> </table>	SiglasDeInstitucion	Siglas de la Institución Financiera	yyyy	Año	999	Consecutivo
SiglasDeInstitucion	Siglas de la Institución Financiera						
yyyy	Año						
999	Consecutivo						
Acciones a Realizar	Indique cuál de las opciones indicadas representa la acción o acciones a realizar en su solicitud de acuerdo a sus necesidades: Creación de Nuevo Usuario Modificar un perfil Existente Eliminar Usuario Existente						
Datos de Usuario	Escriba el nombre completo del usuario sobre el cual se realizará la acción, así como su username para el sistema						
Información del Perfil	Indique cuál de las opciones indicadas representa las funciones o perfiles que el usuario deberá de poseer dentro del sistema: Central de Riesgo Ref. Cred. En Línea Ref. Cred. Por Lote Anexos Descarga de información (Consolidada, Errores, etc.) Manual Único de Cuentas Lavado de Dinero						
Firmas	Esta sección es utilizada exclusivamente por la SIBOIF para llevar la traza o pista del estado de la solicitud en cuanto a su atención por medio de la firma de las diferentes personas involucradas en este proceso: Recepcionada Autorización Intendencia Autorización DTI Recibida Elaborada						
Observaciones	Observaciones que señala el coordinador del sistema, director de informática o el DBA de la SIBOIF de ser estas necesarias.						

Tabla 6 Instructivo de Solicitud de altas, bajas y cambio a las cuentas de acceso

2.6 Anexo F: Manual del GNUPG

2.6.1 Introducción

GNUpg es la implementación del mundo de software libre de PGP, este es un sistema de cifrado asimétrico, es decir se compone de una llave pública y una llave privada, con este sistema se pueden realizar tanto cifrado de datos (con la llave pública), como firmado de ficheros para asegurar la autenticidad (usando la llave privada y el destinatario a firmar). Este documento pretende ser sólo una breve guía para cifrar y descifrar ficheros, para consultas exhaustivas:

<http://www.gnupg.org/gph/es/manual/book1.html>

<http://www.gnupg.org/gph/es/manual/book1.html>

2.6.2 Generación de las claves

Lo primero de todo necesitamos un equipo que cuente con el paquete GNUpg.

El programa de instalación se ubica en la página principal de GnuPG.

<http://www.gnupg.org/>

<http://www.gnupg.org/download/>

El archivo de instalación para Windows puede ser ubicado directamente en la siguiente liga:

<ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.1.exe>

Una vez que el programa se ha descargado debe presionar doble clic y por si solo se instalara (gnupg-w32cli-1.4.1.exe).

Modificar el c:\autoexec.bat con la siguiente instrucción:

SET PATH=%PATH%;C:\Archivos de programa\GNU\GnuPG

Una vez hecho esto generamos el par de claves, la pública y la privada con el comando:

```
gpg --gen-key
```

Si es la primera vez que lo ejecutamos nos creará el fichero "**C:/Documents and Settings/jperez/Datos de programa/gnupg/pubring.gpg**" donde se guardan las configuraciones y las claves, y habrá que ejecutarlo de nuevo para que se lance el proceso de creación el cual es un sistema de menús que a continuación se muestran y comentan.

```
gpg --gen-key
```

```
gpg (GnuPG) 1.4.1; Copyright (C) 2005 Free Software Foundation, Inc.
```

```
This program comes with ABSOLUTELY NO WARRANTY.
```

```
This is free software, and you are welcome to redistribute it  
under certain conditions. See the file COPYING for details.
```

```
gpg: keyring `C:/Documents and Settings/pparamo/Datos de programa/gnupg\secren  
g.gpg' created
```

```
gpg: keyring `C:/Documents and Settings/pparamo/Datos de programa/gnupg\pubrin  
g.gpg' created
```

```
Please select what kind of key you want:
```



(1) DSA and ElGamal (default)
(2) DSA (sign only)
(5) RSA (sign only)
Your selection? **1**

Seleccionamos el tipo de llave por defecto, ElGamal.

DSA keypair will have 1024 bits.
ELG-E keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) **2048**

Con esto seleccionamos la longitud de la llave. La longitud de la llave requerida por la SIBOIF para este proceso es de 2048 bits.

Requested keysize is 2048 bits
Please specify how long the key should be valid.
0 = key does not expire
<n> = key expires in n days
<n>w = key expires in n weeks
<n>m = key expires in n months
<n>y = key expires in n years
Key is valid for? (0) **1y**
Key expires at 06/06/06 10:35:53
Is this correct? (y/N) **y**

A continuación se nos solicita el tiempo para el cual la llave pública tendrá validez. Para nuestro ejemplo consideramos suficiente un año. Contestamos que sí y seguimos.

You need a user ID to identify your key; the software constructs the user ID from the Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: **Pedro Páramo**
Email address: **pparamo@siboif.gob.ni**
Comment: **SIBOIF_DTI_Soporte Técnico.**

Se rellenan los campos con los identificadores que vamos a usar.

You are using the 'CP850' character set.
You selected this USER-ID:
"Pedro Páramo (SIBOIF_DTI_Soporte Técnico.) <pparamo@siboif.gob.ni>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? **o**
You need a Passphrase to protect your secret key.

Si está bien pulsamos O y continuamos.

You need a Passphrase to protect your private key.

Enter passphrase:

Necesitamos una clave para proteger nuestra llave privada, es conveniente elegir una lo más larga y compleja posible, ya que el punto débil del cifrado asimétrico es la protección de esta llave.

Repeat passphrase:

Repetimos la clave.

Con este proceso ya tenemos generadas las claves y podemos firmar y encriptar documentos, para comprobar que todo está bien, miramos si se han generado las claves.

gpg --list-keys

2.6.3 Cifrar ficheros

Para cifrar documentos procedemos de la siguiente forma: buscamos el fichero que queremos encriptar y ejecutamos el siguiente comando:

gpg -o fichero_cifrado -e fichero_original

You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID. End with an empty line: jperez@siboif.gob.ni

Current recipients:

2048g/2B993C22 2005-06-02 "Pedro Páramo <pparamo@siboif.gob.ni>"

Enter the user ID. End with an empty line:

Es conveniente borrar el fichero sin cifrar, una vez nos aseguremos que el fichero cifrado ha sido creado.

2.6.4 Descifrar ficheros

Para descifrar el fichero que previamente habíamos cifrado:

gpg -o fichero -d fichero_cifrado

You need a passphrase to unlock the secret key for

user: "José Pérez <jperez@siboif.gob.ni>"

2048-bit ELG-E key, ID 7C4D8652, created 2005-06-03 (main key ID A216DAED)

gpg: encrypted with 2048-bit ELG-E key, ID 7C4D8652, created 2005-06-03

"José Pérez <jperez@siboif.gob.ni>"

Nos pedirá la clave que le pusimos cuando creamos las claves, con esto nos aseguramos que sólo quien la conozca pueda descifrarla.

Con este breve documento se ha pretendido dar una rápida descripción de cómo cifrar y descifrar ficheros de forma sencilla y rápida.

2.6.5 Generar la llave pública

Para enviar la clave pública a un tercero deberá de dar el siguiente comando:

```
gpg --armor --export pparamo@siboif.gob.ni > pparamo_pk
```

Para ver el contenido de la llave pública:

```
type pparamo_pk
```

2.6.6 Importando una llave pública a su llavero

Para importar una llave pública deberá de dar el siguiente comando:

```
gpg --import jperez_pk
gpg: key 9104CDDA: public key "José <jperez@siboif.gob.ni>" imported
gpg: Total number processed: 1
gpg:          imported: 1
```

2.6.7 Automatización desatendida

2.6.7.1 Compresión y Cifrado de archivos y Generación del Sha1

```
Cls
+-----+
::| Nombre   : gpg_all.bat
::| Version  : 1.0.0.1.01
::| Institución: SIBOIF
::| Descripción: Llama a la rutina de comprimir y cifrar
::|
::| Parametros : N/A
::|
::| Autor    : Carlos Flores <emartinez@siboif.gob.ni>;
::|           Enrique Martinez <emartinez@siboif.gob.ni>;
::|
::| Fecha    : 2006.09.21 Jueves
::|
::| Nota     : Recordar cambiar el siguiente camino (PATH)
::|
::|           C:\Temp\CdR_Cargas\Ba\Datos
::|           CdR_Ba
```

```
:: | C:\TempTools\Sha1sum
:: |
:: |
:: +-----+
:: -

ECHO OFF
CLS
ECHO Por favor espere ...

:: +-----+
:: | Definiendo las variables de ambiente
:: +-----+
SET V_PATH_ORIGINAL=%PATH%
SET V_PATH_WORK="C:\Temp\Tools"
SET V_PATH_DATA="C:\Temp\CdR_Cargas\Ba\Datos"
SET V_FILENAME_OUTPUT=CdR_Ba

SET V_SHA1_CMD=C:\TempTools\Sha1sum

SET PATH=%PATH%;%V_PATH_WORK%
SET PATH=%PATH%;"C:\Archivos de programa\WinRAR\"
SET PATH=%PATH%;"C:\Archivos de programa\GNU\GnuPG\"

IF NOT EXIST %V_PATH_DATA%\*. * GOTO ERROR

CD %V_PATH_DATA%

:: +-----+
:: | Llamando a la sub rutina que se encargara del proceso
:: +-----+
CALL gpg_cifrar

GOTO FIN

:: +-----+
:: | Controlando los errores
:: +-----+
:ERROR
ECHO.
ECHO.
ECHO Debe crear el directorio donde se encuentren los archivos de carga
ECHO.

:: +-----+
:: | El proceso ha finalizado con exito
:: +-----+
:FIN
SET PATH=%V_PATH_ORIGINAL%
```



CD %V_PATH_WORK%

ECHO.

ECHO Proceso finalizado con exito.

ECHO.

ECHO ON

```
:: -
:: +-----+
:: | Nombre : gpg_cifrar.bat
:: |
:: | Version : 1.0.0.1.01
:: |
:: | Institución: SIBOIF
:: |
:: | Descripción: Comprime y cifra un archivo texto
:: |
:: | Parametros : %1 Nombre del archivo a procesar (nombre sin extensión)
:: |
:: | Autor : Carlos Flores <emartinez@siboif.gob.ni>;
:: | Enrique Martinez <emartinez@siboif.gob.ni>;
:: |
:: | Fecha : 2006.09.21 Jueves
:: |
:: | Nota : Recordar cambiar el siguiente camino (PATH)
:: | C:/Documents and Settings/???????/Datos de programa/gnupg/pubring.gpg
:: +-----+
:: -

:: +-----+
:: | Comprimiendo en el formato ZIP
:: +-----+
ECHO.
ECHO [1/3] Comprimiendo ...
IF EXIST %V_FILENAME_OUTPUT%.zip DEL %V_FILENAME_OUTPUT%.zip
Winrar a -afzip -ibck -ep %V_FILENAME_OUTPUT% *.txt

:: +-----+
:: | Cifrando (Encriptando)
:: +-----+
ECHO [2/3] Cifrando ...
IF EXIST %V_FILENAME_OUTPUT%.dat DEL %V_FILENAME_OUTPUT%.dat
gpg --always-trust --keyring "C:/Documents and Settings/emartinez/Datos de
programa/gnupg/pubring.gpg" -r sisbanf@siboif.gob.ni -o %V_FILENAME_OUTPUT%.dat -e
%V_FILENAME_OUTPUT%.zip

:: +-----+
```



```
:: | Aplicando el algoritmo SHA1
:: +-----+
ECHO [3/3] Aplicando el codigo SHA1 ...
SET LOCAL_CMD=%V_SHA1_CMD% %V_FILENAME_OUTPUT%.dat
SET V_Sha1_Tmp=
For /F "Tokens=1" %%i in ('%LOCAL_CMD%') Do SET V_Sha1_Tmp=%%i
IF EXIST %V_FILENAME_OUTPUT%.dat RENAME %V_FILENAME_OUTPUT%.dat
%V_FILENAME_OUTPUT%_%V_Sha1_Tmp%.dat
```

2.6.7.2 Descifrar ficheros

Si desea que el descifrado sea desatendido primero necesita guardar su frase en un archivo. Definitivamente el lugar y el archivo mismo deben ser cuidadosamente seleccionados.

Notepad C:\LugarUltraSecreto\Nombrearchivo.scr

Luego pueden construir un bat con las siguientes instrucciones:

```
REM %1 Archivo de destino
REM %2 Archivo de origen

cd c:\

SET PATH=%PATH%;"C:\Archivos de programa\GNU\GnuPG"
gpg --keyring "C:/Documents and Settings/USERNAME/Datos de programa/gnupg/pubring.gpg" --
secret-keyring "C:/Documents and Settings/USERNAME/Datos de programa/gnupg/pubring.gpg" --
passphrase-fd 0 < C:\LugarUltraSecreto\ArchivoUltraSecreto.scr -o %1 -d %2
```

2.6.7.3 Generación del Sha1

Existen varias alternativas:

- Puede ser generado de forma automática con la **clase SHA1CryptoServiceProvider** de .Net y el namespace es: **System.Security.Cryptography**
- **A través del programa SHA1SUM.EXE**
- **Utilizando los .bat detallados en el punto 2.7.7.1**

2.6.7.4 Obtener todos los archivos del servidor de FTP a través de SSH

Servidor	ns2.siboif.gob.ni
Usuario	BancoA_pparamo_001
Clave	cl@v#_s#gur@&12345
Formas de acceder	SSH; http://www.ssh.com/ PuTTY Download Page: http://the.earth.li/~sgtatham/putty/latest/x86/putty-0.60-installer.exe Nombre de Archivo a descargar: putty-0.60-installer.exe o la versión mas actual



Superintendencia de Bancos y de Otras Instituciones Financieras

Si desea automatizar la bajada del archivo es conveniente utilizar el PuTTY a través del siguiente comando:

```
pscp -pw cl@v#_s#gur@&12345 BancoA_pparamo_001@ns2.siboif.gob.ni:*.dat c:\temp\putty
```

Donde:

cl@v#_s#gur@&12345	Clave
BancoA_pparamo_001@ns2.siboif.gob.ni	Usuario en ns2.siboif.gob.ni
*.dat	Las extensiones de los archivos a bajar
c:\Temp\putty	Donde se bajaran los archivos en computadora local