

Instrucciones para la Transmisión y Recepción de la Información Tecnológica

1. Introducción

El presente anexo tiene el objetivo de definir como será enviada la información, la seguridad que se establecerá para la transportación de los datos hacia esta Superintendencia, el medio físico que se utilizará a fin de proveer el canal adecuado para la recepción, la actualización y notificación de la información recibida.

2. Medio Físico a Utilizar

- Sitio Web de apoyo

El sitio Web de apoyo para la transferencia de datos será el <http://209.198.203.111> el cual levantará una página que le solicitará los datos respectivos a fin de que pueda enviar la información requerida. Para efectuar el proceso de transferencia de datos podrá usar el Internet Explorer v5.0 en adelante, utilizará la dirección del servidor mostrada y se le presentará la hoja que le guiará, de manera simple, a ejecutar el envío de la información.

- Estándares a usar en el manejo de la información

Las convenciones a utilizar para la creación de los usuarios y los nombres de los archivos serán las siguientes:

Los nombres de los archivos a enviar tendrán el siguiente formato:

Tanto los anexos como la información que no está en éstos deberá de adoptar las reglas a continuación

Nombre: **Dxxyddmmaaaax.ext**, donde

D:	Denota documento
xx:	Es un correlativo de identificación tomado de los códigos de documentos mostrados en el cuadro No. 1
yy:	es un correlativo que inicia de 00 y aumenta dependiendo de cuantos documentos se creen para el Dxx
ddmmaaaa:	Corresponde a la fecha en que se envía el documento
x:	Corresponde a un correlativo, si el documento ha sido enviado más de una vez para el mismo día, el valor por defecto es 1.
ext:	Corresponde a la extensión del tipo de plataforma en que ha sido creado el archivo: doc, rtf, pdm, cdm, pdf, etc

SUPERINTENDENCIA DEL SISTEMA FINANCIERO
SAN SALVADOR, EL SALVADOR, C.A.

- Ejemplos: D0604300920011.doc: son las “Políticas de Seguridad del Sistema” de Clientes y Depósitos en MSWord enviadas una vez el 30 de Septiembre de 2001.
D0201031020012.cdm: es el modelo conceptual de la Base de Datos, de cuentas corrientes, en power designer, enviado por segunda vez el 3 de octubre de 2001.
D0202031020011.cdm: es el modelo conceptual de la Base de datos, de cuentas de ahorro, en power designer, enviado por primera vez el 3 de octubre de 2001.

- Ubicación en el Servidor de la SSF

Para ubicar los archivos recibidos se utilizarán las siguientes convenciones en nuestros directorios:

El nivel raíz identificará a la SSF

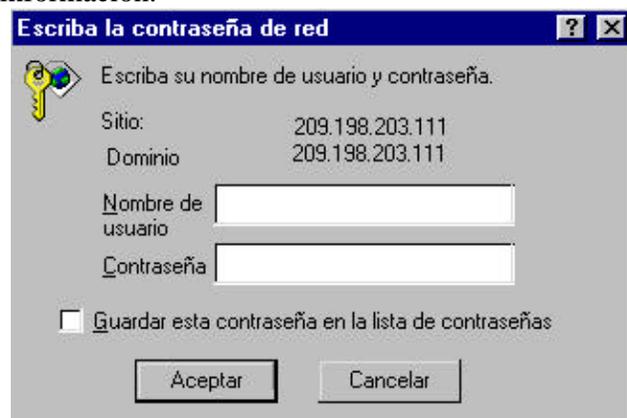
El nivel 2 identificará al sistema de Depósitos

El nivel 3 identificará a las entidades bancarias en donde se ubicarán los archivos y se almacenarán históricamente basados en las convenciones de nombres

En la siguiente estructura de directorios se muestra como se asociarán los directorios de cada institución con los correspondientes usuarios, de manera que cuando se requiera enviar un archivo por medio de la página Web mencionada, el nombre del usuario (UserID) le indicará donde deberá colocarlo en el servidor de la SSF y la única selección que hará el usuario, será el escoger el archivo a enviar.

3. Seguridades en el transporte de datos

Posteriormente a que invoque el IP del Web Site el primer nivel de seguridad que deberá de pasar será el ingreso del nombre del usuario y la contraseña asignada por la SSF para que pueda enviar la información.



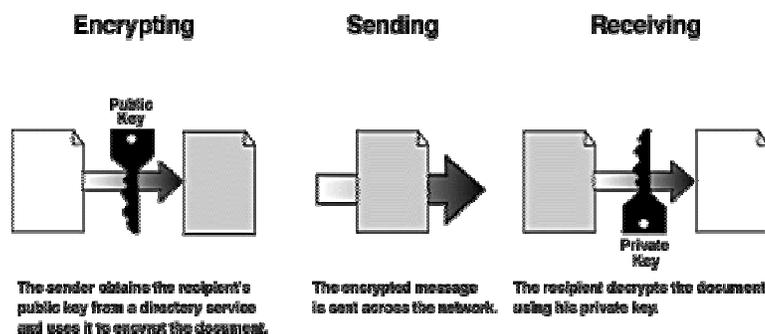
- Uso de la llave pública y llave privada

El segundo nivel de seguridad a utilizar para asegurar el transporte de datos será el uso de llaves públicas y privadas, para lo cual la SSF contratará el servicio con una AC (autoridad Certificadora) del uso de las llaves publicas con 128 bits para encriptación de la información.

CONCEPTO

Mediante un programa de cómputo cualquier persona puede obtener un par de números, matemáticamente relacionados, a los que se denomina llaves. Una llave es un número de gran tamaño, que se puede conceptualizar como un mensaje digital, como un archivo binario, o como una cadena de bits o bytes.

Las llaves pública y privada tienen características matemáticas, su generación es siempre en parejas, y están relacionadas de tal forma que si dos llaves públicas son diferentes, entonces, las correspondientes llaves privadas son diferentes y viceversa. En otras palabras, si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es la de que cada individuo genere un par de llaves: pública y privada. El individuo debe de mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer a los demás individuos.



La criptografía de llave pública ofrece algoritmos de encriptación y desencriptación. Si un documento se encripta con una llave pública, entonces, solo se desencripta con la correspondiente llave privada.

- La Autoridad Certificadora (CA) a utilizar para nuestro proceso de transferencia de información será VerySign

4. Tipos de formatos para los archivos

- Para los Anexos H, I, J, K, L, M

Todos los formatos de estos anexos podrán ser enviados en Excel, Lotus o en Word

- Información complementaria (que no están en los anexos)

Para la información que no está contenida en los anexos serán utilizados los tipos de plataformas expresados en el Cuadro No. 1, en donde se establece el formato sugerido de envío

**Aprobado en la Sesión de Consejo Directivo de la Superintendencia del Sistema Financiero CD 52/01
del 01 de noviembre de 2001**