Javier Cascante E.
Superintendente

SP-A-094

Se reforma el Acuerdo SP-A-067 de fecha 12 de setiembre de 2005, *"Disposiciones sobre el uso de contraseñas para el uso del sistema para transferencia, carga y validación remota de archivo o consulta"*

Superintendencia de Pensiones, Despacho del Superintendente, al ser las quince horas del día veintiséis de junio del dos mil siete.

Considerando que,

1. De conformidad con lo dispuesto en los artículos 36, inciso d), y 38, inciso r), de la *Ley N° 7523, Régimen Privado de Pensiones Complementarias*, reformada por el artículo 79 de la *Ley N° 7983, Ley de Protección al Trabajador*, corresponde a la Superintendencia de Pensiones definir el contenido, la forma y la periodicidad con que las entidades supervisadas deben proporcionar información sobre su situación jurídica, económica y financiera, sobre las características y los costos de sus servicios, las operaciones activas y pasivas, y cualquier otra información que considere de importancia; todo con el fin de que exista información suficiente y confiable sobre la situación de las entidades supervisadas.

2. El artículo 180 de la *Ley Reguladora del Mercado de Valores*, señala que: "*La Superintendencia General de Entidades Financieras, la Superintendencia General de Valores y la Superintendencia de Pensiones Complementarias podrán utilizar medios electrónicos o magnéticos de transmisión y almacenamiento de datos, para solicitar información a las entidades fiscalizadas y para mantener sus archivos, actas y demás documentos. La información así mantenida tendrá valor probatorio equivalente al de los documentos para todos los efectos legales*".

3. El artículo 38 inciso f) de la ley N° 7523 atribuye al Superintendente la facultad de adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de autorización, regulación, supervisión que le competen a la Superintendencia.

4. La Superintendencia de Pensiones ejerce gran parte de la supervisión por medios automatizados con el fin de que la fiscalización se realice con la oportunidad requerida. Por ello es conveniente y oportuno que el suministro de la información sobre saldos contables, inversiones, afiliados, información cualitativa, operaciones únicas o múltiples y otras se dé en un marco de adecuada seguridad y confiabilidad.

Por tanto,

Artículo 1. Contraseñas de acceso a los sistemas de SUPEN por parte de las entidades supervisadas.

Las entidades supervisadas tienen derecho a un máximo de siete (7) cuentas de usuarios para acceder a todos los sistemas de la Superintendencia de Pensiones.

Es responsabilidad del Gerente, o el Presidente del Órgano de Dirección, realizar las solicitudes de creación y eliminación de las cuentas de usuarios según sus requerimientos. Dicho tramité deberá ser gestionado a través de un oficio firmado por el Gerente o el Presidente de su Órgano de Dirección, según corresponda, adjuntando el Formulario anexo a esta resolución (Anexo 1).
Las personas a las que se les otorgue una clave de acceso a los sistemas de SUPEN deberá firmar una carta de compromiso mediante la cual se establezcan las responsabilidades sobre el uso de la misma.

Artículo 2. Dispositivo Electrónico "TOKEN" para el acceso a la Red Privada Virtual (VPN) de la SUPEN.

La Superintendencia de Pensiones facilitará a cada entidad supervisada un único dispositivo de acceso a la red privada virtual, denominado "TOKEN", el cual genera un "password" diferente cada cinco segundos permitiendo, en combinación con el PIN y el código de acceso, el ingreso a aquella.

El dispositivo es un *"SafeWord Token",* Cisco Compatible, y será entregado únicamente al Gerente o el Presidente de su Órgano de Dirección, el cual deberá firmar una carta de compromiso en la cual se establezcan las condiciones para uso del dispositivo.

Aquellas entidades que deseen disponer de más de un dispositivo electrónico (Token) deberán adquirirlo por su cuenta en el mercado y entregar el número de serie que en el producto adquirido se identifica como SafeWord Software Serial Number y el identificador grupal de los dispositivos etiquetado como Token Group ID Number a la Superintendencia de Pensiones para la autorización de su uso. La SUPEN autorizará estos "Token" de conformidad a la cantidad de usuarios que tenga autorizados la entidad.

Artículo 3. Cambio de contraseña a una cuenta de usuario existente.

Las entidades supervisadas deberán remitir a la Superintendencia un oficio firmado por el Gerente o Presidente del Órgano de Dirección, según corresponda, solicitando formalmente una nueva contraseña para un usuario ya existente. Dicha gestión procederá en aquellos casos en que la cuenta de usuario se encuentre bloqueada por vencimiento de contraseña o porque se haya

excedido el número de intentos fallidos para conectarse. El oficio deberá incluir la siguiente información sobre el usuario:

- Cuenta de usuario (asignada por la SUPEN al funcionario de la entidad)
- Nombre completo (nombre y dos apellidos)
- Número de identificación (cédula de identidad)

Artículo 4. Eliminación de una cuenta de usuario existente.

En caso de que la entidad no requiera contar con la cuenta de un determinado usuario aquella estará en la obligación de remitir a la Superintendencia un oficio firmado por el Gerente o el Presidente del Órgano de Dirección, según se trate, solicitando expresamente la eliminación de la cuenta. La solicitud deberá contener la siguiente información:

- Cuenta de usuario (asignada por la SUPEN al funcionario de la entidad supervisada)
- Nombre completo (nombre y dos apellidos)
- Número de identificación (cédula de identidad)

Artículo 5. Plazos de las gestiones normadas.

Una vez recibida la información requerida, la SUPEN dispondrá de un plazo máximo de 3 días hábiles, contados a partir del ingreso del oficio, para realizar la gestión correspondiente.

Una vez transcurrido ese plazo, el funcionario de la entidad supervisada para quien se solicitó una nueva cuenta de usuario o un cambio de contraseña, deberá presentarse ante la Superintendencia de Pensiones donde firmará, ante dos testigos, la *Carta de Compromiso y aceptación de contraseña* (Anexo 2) o la *Carta de Compromiso y aceptación de del TOKEN* (Anexo 3), según corresponda.

Artículo 6. Retiro de documentos del usuario.

El tiempo límite para retirar los documentos del usuario de la entidad supervisada será de 15 días hábiles, contados a partir de la fecha de recepción de los documentos en la Superintendencia. Si transcurrido este tiempo el funcionario no se hace presente a retirar los documentos, la entidad supervisada deberá iniciar el trámite nuevamente.

Artículo 7. Cambio de clave.

Las contraseñas que emita la SUPEN serán temporales. Las mismas serán válidas, únicamente, para el primer ingreso que el usuario de la entidad supervisada haga al sistema. Este último

deberá cambiar su clave personal inmediatamente después de que ingrese utilizando para esto la opción "*Cambiar Clave"*.

Artículo 8. Derogaciones

Se dejan sin efecto el *Oficio SP- 1770 de fecha 22 de setiembre de 2005.*

Artículo 9. Vigencia

Estas disposiciones rigen a partir de su comunicación.

ANEXO 1
(Llenar un formulario por empleado)

	SUPERINTENDENCIA DE PENSIONES		
	Departamento de Tecnologías de la Información		
	Formulario de información de usuarios externos con acceso a los sistemas institucionales		
INFORMACIÓN PERSONAL DEL USUARIO EXTERNO			
Nombre de la Entidad			
Dependencia			
Nombre del funcionario			
Cédula de identidad			
Teléfono	**Habitación:**	**Trabajo:**	
Profesión			
Domicilio	**Dirección exacta:**		
	Provincia:	**Cantón:**	**Distrito:**
Estado Civil	☐ **Soltero**	☐ **Casado**	
	☐ **Viudo**	☐ **Divorciado**	
	☐ **Unión Libre**		
INFORMACIÓN TECNICA			
Acceso solicitado (puede seleccionar más de una opción)	☐ **Valoración de Inversiones**		
	☐ **Saldos Contables**		
	☐ **Afiliados**		
	☐ **Información Cualitativa**		
	☐ **Operaciones únicas o Múltiples**		
	☐ **Modificación de datos personales**		

ANEXO 2

CARTA DE COMPROMISO Y ACEPTACIÓN DEL USUARIO PARA EL USO DE LA CLAVE DE ACCESO A LA VENTANILLA ELECTRÓNICA DE SERVICIOS (SUPEN)

El suscrito **(nombre completo)**, cédula **de identidad (número)**, **(estado civil)**, **(Profesión u oficio)**, con domicilio en **(Domicilio exacto)**, en adelante denominado *Usuario*, funcionario de **(entidad supervisada),** en adelante denominada la *Entidad Supervisada*, manifiesto:

PRIMERO: Que el **Usuario** ha sido designado expresamente por el (**Gerente de la Operadora o Presidente del Órgano de Dirección**), mediante el oficio (**Número de oficio y fecha**), con el fin de utilizar la clave de acceso que en este acto le suministrará la Superintendencia. El usuario corresponde al **(número de clave de acceso)**.

SEGUNDO: Que la Superintendencia de Pensiones, en este acto, hace entrega al **Usuario,** de la clave de acceso a la **VENTANILLA ELECTRÓNICA DE SERVICIOS.**

TERCERO: Que el Usuario es responsable ante la SUPEN, sin perjuicio de la responsabilidad que pueda caberle a la entidad, por la remisión de la información mediante el uso de la **VENTANILLA ELECTRÓNICA DE SERVICIOS** de la **SUPEN**, en los términos indicados en las normas emitidas por la Superintendencia.

CUARTO: Que el **Usuario** se compromete en forma prioritaria (inmediatamente que ingrese por primera vez al mismo) a cambiar la clave de acceso que se le entrega en este momento, por su clave personal respetando los parámetros establecidos en el apartado siguiente.

QUINTO: Que el **Usuario** se compromete a:

a) No revelar su clave de acceso ni su clave personal a ninguna persona, incluyendo sus superiores, teniendo en cuenta que la misma es de su uso exclusivo y personal y, únicamente, para los fines establecidos en las normas emitidas por la SUPEN.
b) Cerrar el módulo utilizado de la **VENTANILLA ELECTRÓNICA DE SERVICIOS** de la SUPEN cuando no lo esté utilizando.
c) Cambiar su clave periódicamente (el plazo máximo para el cambio de contraseñas será de 60 días) respetando los siguientes aspectos:
   - ✓ Deberá ser de al menos ocho caracteres.
   - ✓ Deberá tener un máximo de 20 caracteres.
   - ✓ Deberá estar compuesta por letras, números y símbolos.
   - ✓ El primer carácter debe ser una letra.
   - ✓ No debe ser igual a las tres últimas claves de acceso utilizadas.
d) No utilizar una clave ajena para acceder a la **VENTANILLA ELECTRÓNICA DE SERVICIOS** de la SUPEN.

SEXTO: Que el suscrito Usuario conoce la legislación penal existente sobre la materia, concretamente, los artículos 196 bis, 217 bis y 229 bis del Código Penal que literalmente dicen:

- ✓ Artículo 196 bis. Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

- ✓ Artículo 217 bis. Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

- ✓ Artículo 229 bis. Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

SÉTIMO: Que si por dolo o culpa del Usuario se altere, borre, dañe o destruya la **VENTANILLA ELECTRÓNICA DE SERVICIOS** de la SUPEN, alguno de sus módulos, la información que este contiene, o se compruebe el acceso ilegal al mismo, el Usuario será responsable civil y penalmente de conformidad con la legislación vigente.

En fe y aceptación de lo anterior, firmamos a las (**hora**) el (**día**) de (**mes**) del (**año**).

_____

(Nombre)
(Cédula de identidad)
USUARIO

_____	_____
(Nombre) (Cédula de identidad) Testigo 1	(Nombre) (Cédula de identidad) Testigo 2

ANEXO 3

CARTA DE COMPROMISO Y ENTREGA DE UN DISPOSITIVO ELECTRÓNICO (TOKEN) Y ACEPTACIÓN DEL GERENTE PARA EL USO DEL PIN DE ACCESO A LA RED PRIVADA VIRTUAL (VPN) DE LA SUPERINTENDENCIA DE PENSIONES (SUPEN)

El suscrito **(nombre completo)**, cédula **de identidad (número)**, **(estado civil)**, **(Profesión u oficio)**, con domicilio en **(Domicilio exacto)**, en su condición de *Gerente General*, de **(entidad supervisada)** en adelante denominada la *Entidad Supervisada*, manifiesto:

PRIMERO: Que la Superintendencia de Pensiones (SUPEN) en este acto hace entrega al **Gerente,** de un Dispositivo Electrónico (Token) y el pin para el acceso a la **RED PRIVADA VIRTUAL (VPN)** de la SUPEN.

SEGUNDO: Que el dispositivo electrónico (Token) que se entrega en este acto, es un SafeWord Token, Cisco Compatible, que le permitirá a la entidad supervisada tener acceso a la **RED PRIVADA VIRTUAL** de la SUPEN

TERCERO: Que el pin entregado en este acto es de uso institucional y no podrá ser cambiado por la entidad supervisada.

CUARTO: Que el suscrito Gerente es responsable ante la SUPEN por el uso y manipulación del Dispositivo Electrónico y de la remisión de la información mediante el uso de la **RED PRIVADA VIRTUAL (VPN)** de la **SUPEN**, en los términos indicados en las normas emitidas por la Superintendencia.

QUINTO: Que el **Gerente** se compromete a:

e) No revelar su pin de acceso a ninguna persona, teniendo en cuenta que el mismo es de uso exclusivo de la entidad supervisada al igual que el dispositivo electrónico (Token) y sólo puede ser utilizado para los fines establecidos en las normas emitidas por la SUPEN.
f) Cerrar la **RED PRIVADA VIRTUAL (VPN)** de la SUPEN cuando no lo esté utilizando.
g) No utilizar un pin ajeno o no autorizado para acceder a la **RED PRIVADA VIRTUAL (VPN)** de la SUPEN.
h) Garantizar un ancho de banda mínimo de 2 Mbps (Megabits por segundo) de acceso a Internet en la entidad para que la comunicación entre ambas instituciones sea adecuada con la finalidad de que la **RED PRIVADA VIRTUAL (VPN)** tenga un comportamiento apropiado.

SEXTO: Que la entidad supervisada **(nombre de la entidad)** se compromete a:

a) Dar un buen uso y manipulación al dispositivo electrónico (Token) que se le está entregando en este mismo acto.

b) Comunicar de inmediato a la Superintendencia de Pensiones en caso de deterioro o pérdida del dispositivo electrónico (Token).
c) En caso de pérdida del dispositivo electrónico (Token) debe reponerse de forma inmediata. El costo del mismo correrá por cuenta de la entidad supervisada.

SÉTIMO: El uso y manipulación de este dispositivo electrónico (Token) que se entrega en este acto es responsabilidad única y exclusivamente de la entidad supervisada.

OCTAVO: Que en caso de que la *Entidad Supervisada* desee disponer de más de un dispositivo electrónico (Token) deberá adquirirlo por su cuenta en el mercado y entregar el numero de serie que en el producto adquirido se identifica como *SafeWord software Serial Number* y el identificador grupal de los dispositivos etiquetado como *Token Group ID Number* a la Superintendencia de Pensiones para la autorización de su uso. El uso y manipulación que se le den a los dispositivos electrónicos adicionales al que se entrega en este acto, serán responsabilidad única y exclusivamente del Gerente de la entidad

NOVENO: Que el suscrito Gerente conoce la legislación penal existente sobre la materia, concretamente los artículos 196 bis, 217 bis y 229 bis del Código Penal que literalmente dicen:

- ✓ Artículo 196 bis. Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

- ✓ Artículo 217 bis. Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

- ✓ Artículo 229 bis. Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

DÉCIMO: Que si por dolo, imprudencia o negligencia del Gerente se procesa, altera, borra, dañe o destruya la **RED PRIVADA VIRTUAL (VPN)** de la SUPEN, alguno de sus módulos, la

información que este contiene o se compruebe el acceso ilegal al mismo, el Usuario será responsable civil y penalmente de conformidad con la legislación vigente.

En fe y aceptación de lo anterior, firmamos a las (**hora**) el (**día**) de (**mes**) del (**año**).

_____

(Nombre)
(Cédula de identidad)
USUARIO

_____	_____
(Nombre) (Cédula de identidad) Testigo 1	(Nombre) (Cédula de identidad) Testigo 2