Libro III, Título II

D. Requerimientos de seguridad

1. El Sistema deberá incorporar, al menos, el uso de certificados con llaves públicas y privadas, con el fin de contar con mecanismos que resguarden la confidencialidad, integridad, autenticación, no repudio y control de acceso en la transmisión de la información.

Se entenderá por

a) Confidencialidad: Si la información contenida en las transmisiones sólo puede ser conocida y recibida por el o los destinatarios del mensaje.

b) Integridad: Si la información no es alterada durante la transmisión.

c) Autenticación: Si el destinatario puede verificar la identidad del emisor.

d) No repudio: Si el emisor de la información no puede negar su autoría y contenido.

e) Control de acceso: Si sólo pueden tener acceso al Sistema aquellas personas que cuenten con la autorización necesaria y sólo respecto a las áreas que les compete o en las que se encuentren autorizados.

2. El Sistema deberá contar con medidas que resguarden las bases de datos que contengan la información recibida y procesada y que impidan que personas no autorizadas accedan a ella. Así también, se deberá llevar un adecuado registro de los eventos de seguridad, que permitan la identificación oportuna de sucesos que afecten al sistema, sin perjuicio de aplicar las mejores prácticas en materias de seguridad de la información.

Entre los controles que debe realizar el Sistema, al menos deberá considerar lo siguiente:

a) El acceso a la Base de Datos del Sistema, por parte de los partícipes, sólo será permitido para direcciones IP autorizadas, las que deberán estar debidamente inscritas en un Registro de Direcciones IP del Sistema, dejando el correspondiente "log" que refleje las nuevas inscripciones de direcciones IP y las direcciones IP que han sido desactivadas. El requerimiento de contar con IP autorizado no será exigido a los asesores previsionales. El uso de IP corporativas extranjeras deberá ser informado a ambos Supervisores.

Nota de actualización: Esta letra fue reemplazada por la Norma de Carácter General Nº 43, de fecha 7 de mayo de 2012.

b) El acceso para las direcciones IP autorizadas, señaladas en la letra a) anterior, estará restringido sólo a días hábiles chilenos y en horario hábil, para aquellos procesos que las Compañías y Administradoras establezcan como riesgosos. Sin perjuicio de lo anterior, los procesos masivos y la descarga de notificaciones podrán efectuarse fuera del horario hábil.

Los procesos que se establezcan como no riesgosos y que por lo tanto su acceso no estará restringido a los días y horario hábil, deberán ser autorizados por ambos Supervisores.

Nota de actualización: Esta letra fue reemplazada por la Norma de Carácter General Nº 43, de fecha 7 de mayo de 2012.

c) Definir tiempos máximos de conexión continua, para las direcciones IP autorizadas, con o sin actividad.

De lo anterior se podrán excepcionar los procesos masivos y las descargas de notificaciones. Para aquellos procesos en línea que se encuentren con actividad, el sistema deberá permitir terminar la transacción antes de finalizar la conexión.

Nota de actualización: Este párrafo fue incorporado por la Norma de Carácter General Nº 43, de fecha 7 de mayo de 2012.

d) Toda la comunicación entre el Sistema y los usuarios (AFP, Compañías de Seguro, Supervisores, etc.) deberá estar cifrada vía VPN u otra equivalente como HTTPS.

e) No se permitirán conexiones simultáneas, en el Sistema, para un mismo usuario.

Al respecto, se deberá cumplir con las buenas prácticas respecto a los usuarios, los cuales deben ser únicos, personales e intransferibles. No deberán existir claves genéricas, en especial para aquellos usuarios que son fiscalizados tanto por la Comisión para el Mercado Financiero como por la Superintendencia de Pensiones. Para ello deberá existir un procedimiento de claves por cada usuario, que contemple al menos una entrega de clave inicial junto a un tiempo de expiración.

Nota de actualización: Este párrafo fue incorporado por la Norma de Carácter General Nº 43, de fecha 7 de mayo de 2012.

Adicionalmente, será responsabilidad de los partícipes del Sistema un mantenimiento adecuado de los usuarios, esto es, al menos deberán mantener vigentes sólo usuarios dependientes de la Compañía o Administradora y cuyas funciones estén relacionadas con la operación del sistema, dando de baja aquellas cuentas de personas desvinculadas laboralmente de la Compañía o Administradora o que hayan cambiado de funciones, según corresponda. El Sistema deberá contar con una aplicación que permita a las Compañías y Administradoras dar de baja a usuarios dependientes de éstas.

Nota de actualización: Este párrafo fue incorporado por la Norma de Carácter General Nº 43, de fecha 7 de mayo de 2012.

f) El Sistema fijará un límite máximo de transacciones por minuto para la conexión y un límite para la cantidad de transacciones diarias por dirección IP y cuenta usuario.

g) El o los servidores del Sistema deben tener su fecha y hora sincronizada con al menos dos servidores ntp públicos disponibles en redes de Internet nacionales, de forma que las horas registradas en los logs de actividades de todos los servidores involucrados sean consistentes, utilizando para ello la hora de Chile Continental.

h) El Sistema debe proporcionar un registro de "log" continuo en el que se identifique, a lo menos, la dirección IP desde la cual se realiza el acceso, el perfil del usuario, la identificación del usuario, tiempo de conexión, tipo de operación (consulta, ingreso, modificación, etc.) y la operación al estilo de transaction log.

i) El registro de "log" continuo debe ser guardado de manera permanente por el Sistema, proveyéndose todas las medidas de seguridad necesarias para garantizar su resguardo e integridad. Para tal efecto, el "log" debe ser guardado por el Sistema con Firma Electrónica Avanzada, todas las semanas, de acuerdo a un cronograma fijo.

j) Los registros del "log" guardados por el Sistema, deben estar disponibles para el uso y consulta, por parte de los Supervisores, cuando éstos así lo requieran.

k) Ante eventos de caídas o fallas operativas del Sistema que impidan continuar con el registro normal del "log", el Sistema se detendrá y no permitirá ningún tipo de transacción, incluidas las consultas, hasta que se disponga de un nuevo "log". De igual forma, el "log" existente al momento de presentarse la falla, deberá ser guardado y firmado de inmediato con Firma Electrónica Avanzada. Paralelamente, se hará llegar un informe, por escrito, del Gerente de Operaciones del Sistema a los Supervisores, indicando detalladamente las causas que ocasionaron la falla del Sistema, las acciones que se adoptaron para corregir la falla y las acciones correctivas destinadas a evitar que dicha falla se produzca en el futuro. Dicho informe deberá ser remitido a los respectivos Supervisores en un plazo máximo de dos (2) días, desde el momento en que se originó la falla.

l) El Sistema mantendrá, en línea, un registro (bitácora o "log") actualizado de los usuarios activos, los que han sido dados de baja y los que han sido modificados, el cual deberá estar disponible para el uso y consulta, por parte de los Supervisores, cuando éstos así lo requieran.

m) El Sistema deberá proveer, a los Supervisores, de réplicas representativas (no operativas) de cada tipo de perfil para fines de fiscalización y control.

n) Los respaldos del Sistema deben ser resguardados adecuadamente para garantizar su integridad, tomándose todas las medidas necesarias para que sólo personal autorizado pueda acceder

a ellos, dejando registro escrito y electrónico, del funcionario, día, hora y motivo por el cual se recurre al respaldo de datos del Sistema.

o) El registro electrónico de acceso a respaldos debe estar disponible para el uso y consulta, por parte de los Supervisores, cuando éstos así lo estimen pertinente.

El Sistema deberá comunicar y describir a los Supervisores los perfiles que requiere para su operación, dentro del plazo de dos días hábiles contados desde la entrada en vigencia de la presente norma. Además, cada vez que se cree, modifique o elimine un determinado perfil y/o su asignación, se deberá remitir a ambos Supervisores, su descripción y funcionalidades asociadas, a más tardar el día hábil siguiente de ocurrido el hecho.

Para efectos de la asignación de perfiles, se deberán establecer de acuerdo a las necesidades y atribuciones de los involucrados en el sistema. No obstante, los Supervisores, podrán objetar y requerir la anulación de tales privilegios.

Por otra parte, junto con el informe de auditoría descrito en el número 7 siguiente, se deberá informar a ambos Supervisores la nómina de personas registradas en cada uno de estos perfiles al último día del mes de febrero de cada año. Dicha nómina contendrá al menos RUT, nombres completos, perfil asignado, fecha y hora de último ingreso realizado, empresa o entidad a la que pertenece la persona que se está informando y cargo.

Asimismo, el Sistema deberá contemplar una funcionalidad para los perfiles fiscalizadores que permita en cualquier momento, visualizar la nómina actualizada y el historial de modificaciones que ésta ha experimentado.

El Sistema deberá proveer a ambos Supervisores de estadísticas en línea que indiquen, a lo menos, la cantidad de accesos, tiempo de conexión, identificación de perfil e identificación de usuarios que hayan o no efectuado transacciones (incluyendo las consultas) o movimientos en el Sistema, las que deberán estar disponibles en el Sistema.

3. El Sistema deberá contar con medidas de contingencia, a utilizar en caso que no se pueda establecer comunicación entre los partícipes. Una vez producida la contingencia, ésta deberá ser comunicada en forma inmediata, tanto a los partícipes como a ambos Supervisores, señalando el tiempo estimado que demandará su solución, como asimismo cuando las comunicaciones se hayan reestablecido. Igualmente, con una anticipación de al menos 48 horas, deberá informar cuando, por razones de mantención del Sistema u otras actividades planificadas, se vaya a interrumpir la comunicación.

4. El Sistema deberá resguardar la privacidad de la información que maneje de acuerdo a lo dispuesto en la Ley Nº 19.628, sobre protección de datos de carácter personal.

5. Los partícipes serán responsables de adoptar todas las medidas necesarias para garantizar la máxima seguridad en el acceso al Sistema, debiendo cuidar y resguardar debidamente los medios a través de los cuales se accede a éste.

6. El Sistema deberá utilizar firma electrónica avanzada al menos en los siguientes procesos:

a) Envío del Certificado Electrónico de Saldo desde la Administradora de origen al Sistema.

b) Envío de las ofertas de renta vitalicia desde las Compañías al Sistema.

c) Envío electrónico del Certificado de Ofertas desde el Sistema al consultante.

7. Las Compañías y Administradoras deberán presentar anualmente a ambos Supervisores, a más tardar el primer día hábil del mes de marzo, un informe de auditoría externa al 31 de diciembre del año anterior, que evalúe la operación y condiciones de seguridad del Sistema y que se ajuste a lo establecido en el 2º párrafo del Capítulo I de la Letra C del presente Título.

8. El sistema deberá contar con adecuados controles que permitan identificar eventos inusuales que afecten la seguridad de la información, dejando registro operacional de tal situación. Aquellos casos de mayor impacto y que puedan tener efecto sobre los consultantes y/o partícipes, deberán ser comunicados a los Supervisores, en el momento en que se tome conocimiento del hecho. Para lo anterior, se tendrá en cuenta lo establecido en la Norma Chilena de Seguridad de la Información o algún otro estándar equivalente.

9. Las Administradoras y Compañías deberán informar a ambos Supervisores cualquier cambio tecnológico que efectúen en el Sistema y/o plataforma que lo soporta, que pueda impactar en la operación y continuidad del Sistema. Dichos cambios deberán ser informados en el momento en que se decida implementarlos, presentando un informe que contendrá a lo menos los motivos del cambio, la evaluación de impacto sobre los sistemas y los datos y la programación de las actividades.

Tratándose de cambios de emergencia, no será necesario el envío de la programación de actividades, debiendo informarse si la solución implementada será permanente o en caso contrario, entregar el plan de vuelta a la operación normal.

Tratándose de cambios originados por emisión de legislación y /o normativa que genere un alto impacto en el Sistema, se deberá enviar un informe a más tardar 30 días luego de emitida la normativa, el que contendrá la evaluación de impacto sobre los sistemas y los datos y la programación de las actividades.

Los Supervisores podrán solicitar documentación técnica de la implementación de los cambios, tales como pruebas, casos de prueba, aprobaciones de cambios de ambiente (desarrollo, prueba, producción), entre otros.

Nota de actualización: Este número fue incorporado por la Norma de Carácter General Nº 89, de fecha 3 de julio de 2013.

10. Las Administradoras y Compañías deberán enviar a ambos Supervisores, en carácter de reservado, el contrato de prestación de servicios celebrado con su operador tecnológico, a más tardar 5 días hábiles de haberse suscrito.

Asimismo, deberán informar cuando el contrato finalice anticipadamente y las gestiones que efectuarán para contratar los servicios de un proveedor tecnológico. En el primer caso, se informará en el plazo de 5 días hábiles contado desde que se tome conocimiento del término del contrato y, en el segundo caso, a más tardar 5 días hábiles de iniciadas las referidas gestiones.

Nota de actualización: Este número fue incorporado por la Norma de Carácter General Nº 89, de fecha 3 de julio de 2013.