SEGURIDAD DE LA INFORMACION
INTERMEDIARIOS DE SEGUROS

REPONSABILIDAD DE SEGURIDAD DE LA INFORMACIÓN

Los Intermediarios de Seguros y sus canales de comercialización tienen responsabilidades que deben cumplir:

a. Salvaguardar la confidencialidad, integridad, disponibilidad de la información que administre y/o maneje de Previsora durante la vigencia del contrato.

b. Devolver la información digital y/o física que le fue entregada al momento de iniciar el contrato con Previsora y durante la vigencia de este hasta su finalización. Así mismo deberá destruir de manera segura la información que repose en sus sistemas una vez terminada la relación con la compañía.

c. Revisar mínimo mensualmente los usuarios a su cargo que tienen acceso a los sistemas de información de Previsora y notificar inmediatamente los ingresos o retiros para su activación/desactivación en las plataformas tecnológicas.

d. Todos los usuarios del Intermediario que tienen acceso a los recursos tecnológicos e información de Previsora deben poseer un identificador único.

e. Todos los usuarios del Intermediario deberán cambiar su contraseña inmediatamente después de su primer ingreso a los sistemas de información de Previsora.

f. El usuario y contraseña de acceso asignados son personales, confidenciales e intransferibles. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas.

g. Cada funcionario del Intermediario es responsable por los posibles daños o perjuicios que se ocasionen por las actividades realizadas en los sistemas de información de Previsora con su usuario.

h. Toda contraseña deberá ser cambiada por el usuario de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

i. Los usuarios no deben dejar el computador desatendido. Deben cerrar o bloquear la sesión iniciada cada vez que se retiren del puesto de trabajo.

j. Los Intermediarios deben ser conscientes de los riesgos de seguridad cuando se conectan a internet, por tanto, deben tener en cuenta las prácticas seguras para navegación.

k. Evitar conexiones desde redes Wi Fi públicas.

l. Los Intermediarios deben implementar los controles necesarios para evitar que terceros no autorizados ingresen a los sistemas de información de la Previsora.

m. Reportar al Oficial de Seguridad los incidentes de seguridad que involucren la información o los sistemas de información de Previsora, a través del correo **novedades.riesgo@previsora.gov.co**

REQUISITOS DE SEGURIDAD INFORMÁTICA

A continuación, se detallan los requerimientos mínimos de los computadores que utilicen los Intermediarios para acceder a los sistemas de información de Previsora:

a. Sistemas operativos (Windows, MAC) y aplicaciones (MS Office, Adobe, etc.) licenciados y actualizados.

b. Software antivirus y antispam debidamente licenciado y actualizado, no se acepta antivirus gratuito.

c. Firewall del sistema operativo habilitado.

d. Deshabilitar los permisos de administrador, para evitar el cambio de configuraciones por parte de personas no autorizadas.

e. Bloquear acceso a páginas que representen riesgo para la seguridad de la información como por ejemplo aquellas con contenido para adultos, ocio, páginas de descarga de software, videos, etc.

f. Implementar mecanismos de revisión (antivirus) para cualquier medio extraíble (memorias USB, CDs, DVDs, teléfonos móviles, etc.), que sea conectado al computador.

g. Todas las estaciones de trabajo de los usuarios deben tener activado el protector de pantalla protegida por contraseña.

Es preciso aclarar que el Intermediario podrá implementar controles de seguridad adicionales a los anteriormente expuestos, para proteger la confidencialidad, integridad y disponibilidad de la información.