Por este motivo nos permitimos realizar las siguientes recomendaciones en el uso seguro de los servicios de internet y transmisión de datos.

Privacidad:

La elección y uso de un conjunto usuario:contraseña, es fundamental en el ambito de la seguridad informática y en la protección de la privacidad, una contraseña mal escogida o sin una buena protección puede ser fácilmente vulnerada y provocar serios problemas de seguridad tanto a nivel personal como corporativo. Por esta razón es fundamental que el cliente tome todos los correctivos necasarios para evitar ser víctima de ataques y/o fraudes electrónicos. El usuario es responsable de velar por la seguridad de las contraseñas asignadas, para el uso en los distintos servicios ofrecidos por Puntonet.

- Su nombre de usuario y contraseña son personales, ninguna otra persona debe tener acceso a ellos.
- No utilice contraseñas obvias o que se deriven de información personal o preferencias del usuario como el mismo nombre de usuario, el nombre de la mascota, nombres de personas, artistas preferidos, estilo de musica, numero de identificación, teléfono, fechas de nacimiento, etc.
- Cambie en forma periódica su contraseña, con una periodicidad de por lo menos 6 meses, si sospecha que su contraseña fue comprometida, cambiarla de forma inmediata.
- Tener una longitud de 6 o más caracteres, mientras más larga es la cadena, más complicado es vulnerar la seguridad de la clave.
- En los casos donde se soporte la contraseña debería ser una mezcla de caracteres alfabéticos (A..Z, a..z), numéricos (0..9) y especiales (!#$%&/...), en el caso de las letras se puede utilizar una mezcla de mayúsculas y minúsculas.

Suplantación de identidad (*Phishing*)

Phishing, con este término en ingles que significa pescar, se denomina a la práctica fraudulenta de suplantación de sitios web, principalmente de instituciones financieras, realizada por estafadores que envían mensajes de correo electrónico o mensajes de aparición automática en sitios web (pop-up ads) para atraer con engaños a los consumidores y sustraer su información personal o financiera sin que se den cuenta. Para evitar que lo "pesquen" con este anzuelo:

- No responda a los mensajes electrónicos o de aparición automática (pop-up ads) mediante los que le soliciten información personal o financiera ni haga clic sobre los vínculos o enlaces incluidos en estos mensajes.
- No utilice la función copiar y pegar (copy and paste) para colocar el enlace en el navegador de internet — los "pescadores de información" o *phishers* pueden lograr que los vínculos aparenten llevarlo a un sitio Web pero en realidad lo conectan a uno diferente.
- Algunos estafadores envían un email que parece provenir de un negocio legítimo en el que le informan que su acceso a los sevicios en línea ha sido bloqueado y en el texto del mensaje le indican que acceda a un sitio web para actualizar sus datos y/o desbloquear su acceso.
- Un banco jamás le pedirá su número secreto por correo electrónico. Los números secretos deben ser utilizados sólo en la página del servicio (Bancos, Servicio de Pagos, Tarjetas de crédito, etc.)

- Verifique que la dirección del sitio web inicie con la determinación del protocolo **https://** en lugar de **http://** que es el que se encuentra normalmente en las páginas web.
- No envíe información personal ni financiera por correo electrónico.
- Revise los estados de cuenta de su tarjeta de crédito y cuenta bancaria tan pronto como los reciba para verificar si se le han imputado cargos que usted no ha autorizado.
- Tenga cuidado al abrir archivos electrónicos adjuntados o al descargar archivos de mensajes electrónicos recibidos, independientemente de la identidad del remitente.
- Reenvíe estos mensajes de "phising" a la compañía, banco u organización cuyo nombre fue falsamente invocado como remitente del mensaje de correo electrónico.
- No deje desantendida su computadora mientras se encuentra en los sitios web de sus servicios financieros.
- Siempre utilice la opción **Salir** que se encuentra en el sitio de su banco, para cerrar la sesión en línea, no basta con cerrar la ventana o pestaña del sitio, acostúmbrese a eliminar la información temporal de estos sitios en su navegador.
- En caso de extraviar sus tarjetas de acceso a sus servicios financieros en línea, comuniquese de inmediato con su institución financiera para realizar el bloqueo de la misma.
- Si usted fue afectado por este tipo de ataque, puede aceder a los servicios de la Fiscalía General de la Nación o Defensoría del Pueblo.

Protección Infantil

En la actualidad el uso de las tecnologías de la información por parte de los niños se realiza desde edades más tempranas, internet se ha convertido en una herramienta sumamente importante para el aprendizaje de los niños, pero también se debe tener en cuenta que la libertad que existe en el medio la hace sumamente peligrosa, es deber de los padres el control de uso de las tecnologías de la información y el acceso a los sevicios de internet, se recomienda la supervisión de los padres o apoderados de los niños o adolecentes en la administración del uso que le den a esta herramienta, los adultos deben involucrarse proactivamente en las actividades de sus hijos en internet y controlar el contenido, existen varias alternativas desde gratuitas hasta de pago, que permiten el control de contenido, el usuario deberà verificar cual es la que mejor se adecua a sus preferencias.