
# MEDIDAS DE SEGURIDAD

## TÓMELAS EN CUENTA

• Para ingresar a nuestra pagina web digite en la barra de direcciones del navegador www.vidaplena.fi.cr

• Verifique que la página donde navega comience con https. La "s" es un indicador de seguridad

• Nunca de clic en correos electrónicos que anuncien o contengan enlaces a esta página

• Recuerde que sus claves y datos personales son confidenciales. No los comparta con cualquier persona ni a través de medios como internet, correos electrónicos, teléfono, encuestas, entre otros

• Recuerde que Vida Plena OPC nunca solicitará información de sus claves por ningún medio. Absténgase de responder correos que soliciten sus claves de ingreso a la Oficina Virtual, así estos parezcan provenir de Vida Plena OPC

• Cambie sus claves periódicamente, es una buena práctica y evita que éstas sean vulneradas

• Elija una contraseña segura que no sea fácil de deducir por otras personas para el ingreso a la Oficina Virtual, recuerde que la contraseña tiene que tener como mínimo 8 caracteres y contener mayúsculas, minúsculas, caracteres especiales y números. No use su fecha de nacimiento, número de cédula, teléfono o apellidos

• Recuerde siempre presionar el botón "salir" cuando termine de navegar en la Oficina Virtual ya sea a través de la plataforma web o de la plataforma móvil

• No descargue archivos provenientes de páginas web que no conozca

• No se conecte a redes públicas WIFI

# MAYOR SEGURIDAD

Recuerde que Vida Plena OPC nunca le pedirá por teléfono o correo electrónico información confidencial como:

- Usuario y contraseña de la Oficina Virtual
- Clave o PIN de tarjetas
- Numeración completa de sus tarjetas, ni fecha de vencimiento y mucho menos los tres últimos dígitos de seguridad

Cualquier tipo de situación extraña o fuera de lo común que involucre el otorgamiento de premios o regalos indicando sus datos personales o confidenciales debe ser consultado o reportado al 800 VIVAMOS (800- 8482667) o al correo electrónico afiliado@vidaplena.fi.cr

# ROBO DE INFORMACIÓN

El robo o fraude de identidad se produce cuando alguien roba información que define la identidad de otra persona, por ejemplo, su nombre, número de cédula, número de pasaporte, números de cuentas bancarias y número de tarjetas de crédito, con el fin de obtener los beneficios que le corresponden a dicha perosna. Estos beneficios pueden ser financieros, tales como el acceso a sus cuentas y tarjetas de crédito, o pueden estar relacionados con la reputación, ya que los delincuentes o estafadores pueden utilizar su identidad para conseguir el acceso a sus cuentas o cometer un delito.

¿Cómo pueden los delicuentes robar su información personal o confidencial?

## Ingenieria Social

La ingeniería social consiste en engañar a la gente para que cedan su información personal como contraseñas o datos bancarios o para que permitan el acceso a un equipo con el fin de instalar software malicioso de forma inadvertida. Los delincuentes y estafadores utilizan la ingeniería social porque es más fácil engañar a alguien para que revele su contraseña que vulnerar su seguridad.

## ¿Cómo prevenir la ingeniería social?

- Nunca de por cierto nada de lo que no esté absolutamente seguro
- No acepte ninguna oferta que no haya solicitado
- No haga clic en ningún enlace que provenga de fuentes desconocidas
- No revele su contraseña o sus datos personales

## Phishing:

El phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

## ¿Cómo evitar el phishing?

• Mantenga buenos hábitos y no responda a enlaces en correos electrónicos no solicitados o en redes sociales.
• No abra adjuntos de correos electrónicos no solicitados.
• Proteja sus contraseñas y no las revele a nadie.
• No proporcione información confidencial a nadie por teléfono, en persona o a través del correo electrónico.
• Compruebe la URL del sitio (dirección web). En muchos casos de phishing, la dirección web puede parecer legítima, pero la URL puede estar mal escrita o el dominio puede ser diferente (.com cuando debería ser .fi.cr).
• Mantenga actualizado su navegador y aplique los parches de seguridad.

## Spam

El spam es un mensaje no solicitado que hace publicidad de un servicio o producto; la versión electrónica del "correo basura". Los mensajes pueden incluir spyware, registradores de pulsaciones, malware y vínculos a sitios de phishing.

## ¿Cómo evitar el spam?

• Cuando se registre en cuentas o servicios en línea, asegúrese de anular la selección de las opciones que suelen estar activadas de forma predeterminada.
• Al seguir los enlaces o responder a los mensajes de spam está confirmando que su dirección de correo electrónico es válida y recibirá aún más correo basura, por lo que debe evitar la tentación de hacer clic.
• Regístrese en un servicio de desafío/respuesta contra el spam.
• Abra una segunda dirección de correo electrónico específica para sus visitas a paginas web, salas de chat, registro en servicios, etc. para reducir la probabilidad de que el spam atasque su bandeja de entrada principal.