

## Recomendaciones de seguridad deceval

El portal web de deceval cuenta con los más altos estándares de seguridad.

Sin embargo, la organización recomienda implementar las siguientes prácticas para que su información siempre esté segura.

- Cuando digite su clave verifique que nadie lo observe.
- Nunca comparta su clave. Si tiene dudas sobre la misma solicite el cambio a través de su depositante directo.
- Deceval S.A. nunca lo contactará para solicitarle o confirmarle información sobre su clave.
- Siempre ingrese a la página digitando la dirección <https://bvc.com.co> en la barra del explorador. Evite el acceso desde vínculos adjuntos en correos electrónicos y otras páginas.
- Ingrese a la consulta de su portafolio desde una terminal segura de uso frecuente. Evite el acceso desde sitios públicos.
- Verifique que una vez ingrese a la pantalla de consulta de su portafolio, la dirección del explorador contenga el protocolo <https://> y no sólo <http://>
- Si advierte alguna anomalía durante el proceso de consulta por favor notifíquese a [servicioalcliente@deceval.com.co](mailto:servicioalcliente@deceval.com.co).
- **CREE CONTRASEÑAS SEGURAS EN TODAS SUS PLATAFORMAS, TENGA EN CUENTA ESTAS RECOMENDACIONES.**
  - No use nombres propios, de mascotas, familiares, nombre de entidades o áreas a la que pertenece.
  - No use nombres de marcas, sistemas, avisos.
  - No use nombres de establecimientos cercanos a su lugar de residencia o trabajo
  - No use palabras de diccionarios como clave (en ningún idioma),
  - Alterne letras mayúsculas y minúsculas, números
  - Incluya caracteres especiales (#, @, \*, -, +, %, & entre otros).
  - Recuerde que la contraseña debe contener cuando menos ocho (8) caracteres.
  - Cambie con regularidad la contraseña de acceso a los diferentes sistemas y plataformas digitales.
  - Al digitar su usuario y contraseña asegúrese de no hacerlo a la vista de alguien.

- No utiliza contraseñas que utilice en otros sitios como redes sociales
- Evite usar la opción de "recordar contraseña" de los navegadores web

### **Recomendaciones de seguridad bvc**

El portal web de bvc cuenta con los más altos estándares de seguridad.

Sin embargo, la organización recomienda implementar las siguientes prácticas para que su información siempre esté segura.

- No facilite contraseñas de acceso a los sistemas, información clasificada como sensible o confidencial de la Cámara de forma telefónica o personas externas sin verificar sus datos.
- No use la misma contraseña para todos los registros, ni su misma cuenta de correo electrónico.
- No use sus redes sociales como método de Login en las diferentes plataformas, pueden ser usadas para ingeniería social
- Instale en sus dispositivos únicamente software legal.
- Verifique que sus dispositivos cuenten con un software antimalware eficiente que proteja la navegación web, firewall.
- Evitar conectarse a servicios corporativos, bancos desde redes públicas (cafés, centros comerciales, aeropuertos, hoteles, entre otros)