

NO SE DEJE ENGAÑAR CON SITIOS FALSOS

NO SEA UNA VÍCTIMA DE ESTAFA

Tome en cuenta las siguientes recomendaciones:

- 1 El certificado de la página web debe de ser mayor a 3 meses.
- 2 La mayoría de los sitios web oficiales terminan en:
 - Gobierno .go.cr
 - Financiero .fi.cr
 - Salud .sa.cr
 - Organización .or.cr

✘ Si en una llamada telefónica indican que ingrese a una página "oficial de gobierno" que finalice con

.com


DESCONFÍE.



TENGA EN CUENTA!!

 <https://www.NombredeDominioCR.com>

Verifique que la dirección web a la que va a ingresar sea **https**

 Dar clic al candado que se encuentra a la izquierda, para asegurarse que el **certificado** tenga una validez de **1 año o más**.

Si el dominio tiene **CR** antes del punto de la extensión, **no se confíe**, no significa que sea un sitio oficial.

.go.cr	✓	.com	!
.fi.cr	✓	.net	!
.sa.cr	✓		
.or.cr	✓		

SITIOS .COM QUE SI SON OFICIALES ✓

- bancobcr.com
- baccredomatic.com
- bancobct.com
- bancocathay.com
- bnfondos.com
- grupoimprosa.com
- lafise.com
- becasmicitt.com
- ins-cr.com
- grupoice.com
- scotiabankcr.com
- coopeande1.com
- credilat.com
- prival.com
- crpreviene.com
- coopelecheros.com
- munigoicoechea.com
- procomer.com
- aldesa.com

NO SE DEJE ENGAÑAR



NO SE DEJE ENGAÑAR CON SITIOS FALSOS.

Recuerde que:



- La Firma Digital certificada sólo se puede obtener por medio de una cita en cualquiera de las Oficinas de Registro que se encuentran en la página oficial del Banco Central de Costa Rica, el cuál es la fuente oficial.
- Si desea obtener la Firma Digital certificada, el trámite es únicamente presencial y ninguna entidad financiera le estará contactando para ofrecérsela en línea.
- Verifique que se encuentre en el sitio oficial de la entidad, en caso de ver logos o enlaces a otros sitios, se recomienda consultar con la entidad correspondiente para asegurar la veracidad de ello.
- El retiro del FCL y el ROP **NO** se hace a través de ninguna plataforma, no ingrese ninguno de sus datos personales.



Algunos ciberdelincuentes le hacen ingresar primero a un sitio oficial verdadero de alguna entidad para ganarse su confianza, y luego le hacen ingresar a un segundo sitio. Ese es el **FALSO**.

¡Abra los ojos! Los ciberdelincuentes harán todo lo posible por engañarle.

Su seguridad está en **sus** manos.



**NO SE DEJE
ENGAÑAR**