



# Comercio electrónico



# BIEN VENI DO



El BN le da la bienvenida al mundo de Medios de Pago.

En las siguientes páginas usted encontrará información especialmente elaborada para obtener el mayor beneficio de su afiliación al sistema de pagos de Medios de Pago del Banco Nacional.

Es nuestro interés y sobre todo nuestra meta no escatimar esfuerzos para cumplir con la filosofía de trabajo de nuestra institución **"JUNTOS SOMOS PROGRESO"** por lo tanto, le reiteramos nuestra entera disposición para servirle como usted se merece.

Banco Nacional de Costa Rica, le recomienda este manual, debe de ser estudiado antes de comenzar a utilizar nuestros servicios, tanto para usted como propietario, como para el personal que usted tenga asignado a realizar transacciones con tarjetas, de igual forma si ya o está utilizando.

Según la experiencia la mayoría de las transacciones fraudulentas que se realizan en los comercios es por desconocimientos de las personas en los procedimientos de seguridad para realizar una venta con tarjetas.

Este manual le guiará de cómo utilizar de forma correcta nuestros dispositivos de pago y canales oficiales de comunicación y cuáles son los mecanismos de seguridad que se debe realizar para ayudar a evitar el fraude con tarjetas.

**GRACIAS POR SU PREFERENCIA.**



El Comercio Electrónico es un modelo de negocio basado en la compra, venta y comercialización de productos y servicios a través de un sitio web, con el resguardo seguro de la información y con la finalidad de tramitar el pago de compras mediante tarjeta de crédito o débito en la web del comercio.

## **BENEFICIOS**

- Protocolo 3D Secure, que protege contra fraudes y contracargos a los comercios afiliados, autenticando y autorizando las transacciones en tiempo real desde los servidores de Visa y MasterCard.
- Disponibilidad 24 horas, 7 días de la semana, 365 días al año.
- No requiere la compra de software o hardware.
- Procesa cualquier tarjeta Visa o MasterCard.
- Permite al comercio autoadministrar sus transacciones.
- El pago de las transacciones se acredita en 24 horas en su cuenta del Banco Nacional, por medio del cierre automático.
- Procesa transacciones en dólares y colones.
- Comisiones accesibles.
- Incrementa las ventas al aumentar la seguridad y credibilidad.

## **COSTO Y PARÁMETROS**

- Costo por certificación inicial de las marcas \$275, incluye apoyo técnico en la etapa de pruebas.
- Costo de anualidad \$225 se cobra año vencido de utilizar el servicio.
- Costo de cambios en el desarrollo del sitio web \$200.
- No cuenta con límites transaccionales para el comercio.
- Mantener el sitio Web en un Protocolo de Internet válido y seguro.
- Utilizar tecnologías de encriptación, como mínimo de 128 bits (criptografía simétrica o 1024 bits para criptografía asimétrica), tecnología tipo Secure Socket Layer (SSL) o futuras tecnologías de seguridad digital internacional de las marcas Visa y Master Card.





- Contar con los antivirus óptimos y reconocidos en el mercado, y el AFILIADO se compromete a actualizarlos en forma periódica.
- EL AFILIADO debe proteger la confidencialidad de los datos, archivos de respaldo, y claves de los usuarios o compradores bajo formatos cifrados.
- EL AFILIADO se compromete en mantener las seguridades antes descritas en lo relacionado a información encriptada, llaves privadas, y mantenimiento seguro del detalle de las transacciones, por lo anterior se releva al Banco de toda responsabilidad por el mal uso, controversia o fraude que se diera, en estos casos EL AFILIADO asume toda la responsabilidad.
- Suministrar la información sobre el contacto del sitio del comercio que sirve de Host para EL AFILIADO.
- Se debe colocar en la página Web el catálogo de productos, procedimientos y políticas de entrega, tiempos de ejecución, devolución, cancelación, reembolso, restricciones de exportación, impuestos, tipos de monedas a transar, servicio al cliente, privacidad y seguridad; así como los logos de Visa y MasterCard. El BANCO entregará los logos al AFILIADO en el proceso de certificación. A su vez, EL AFILIADO se compromete en notificar inmediatamente al Banco si existe algún cambio en sus procedimientos u ofertas de los productos.
- Deberá proporcionar al tarjetahabiente las prácticas, costos, manejo e impuestos por envío, así como los tiempos de respuesta para la entrega de la mercadería.
- Debe informar del recibido de la transacción al comprador, como de las instrucciones de entrega de los bienes y servicios adquiridos.
- Debe cumplir con los datos mínimos requeridos en el recibo de transacción, tales como:
- Localizador de recurso universal del comercio (operador logístico).
- Información del contacto de servicio al cliente incluyendo el código y área de teléfono del país. Si el comercio entrega bienes o servicios internacionales, el comercio tiene que listar los números de teléfono accesibles tanto local como internacionalmente.
- Fecha exacta en que termina el período gratis de prueba, si se ofrece.
- Términos y condiciones de la venta, si es restringida.
- Términos y condiciones deben de verse reflejados de forma automática en la página del check out, sin enlaces o redireccionamiento



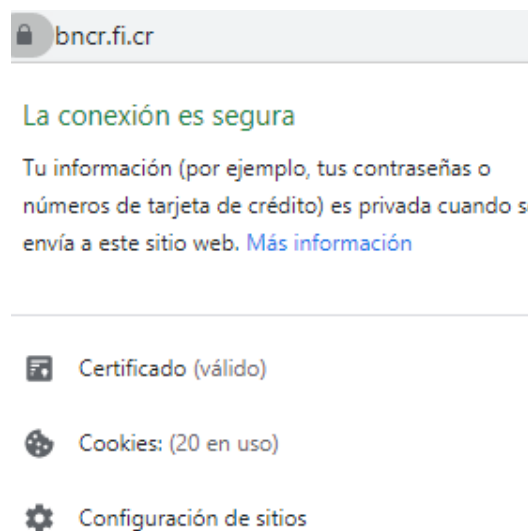
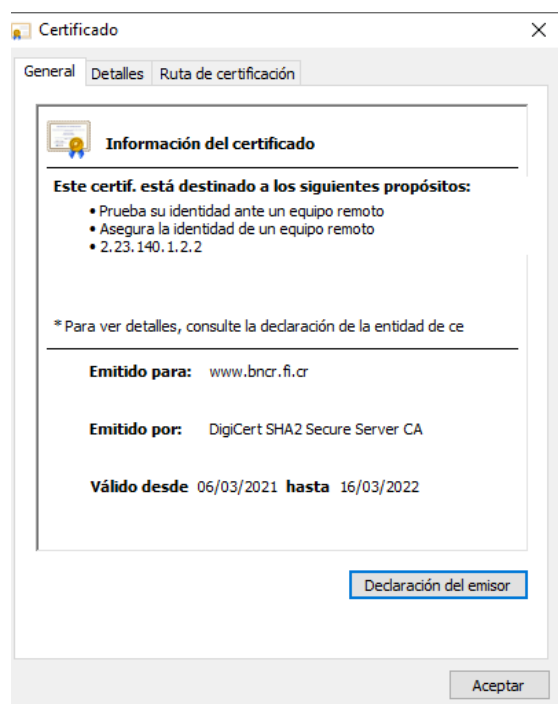
- Políticas de cancelación, devolución, términos y condiciones, las cuales deben ser aceptadas por el tarjetahabiente en el sitio WEB del afiliado mediante un check o clic antes de proceder a realizar el pago.
- Descripción de los bienes y servicios, con los precios e impuestos aplicables.
- La información contenida en las Políticas de cancelación, devolución, términos y condiciones válidas ante un contracargo, serán las que se establecieron y aprobaron por parte de EL BANCO al principio de la afiliación, en caso de que EL AFILIADO desee modificar o agregar deberá contar con la aprobación del BANCO.
- Fecha de la transacción.

- 
-

# NORMATIVA DE REVISIÓN DE SEGURIDAD DE SU SITIO

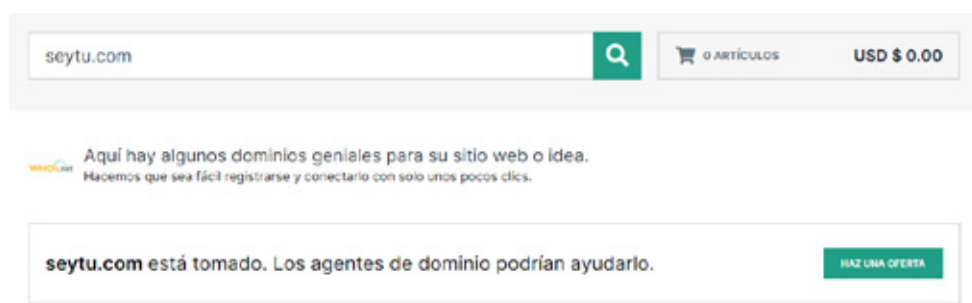
## EXTRACCIÓN DE CERTIFICADOS SSL Y CERTIFICADO DE DOMINIO

**SSL:** Ingresa directamente en la página del comercio

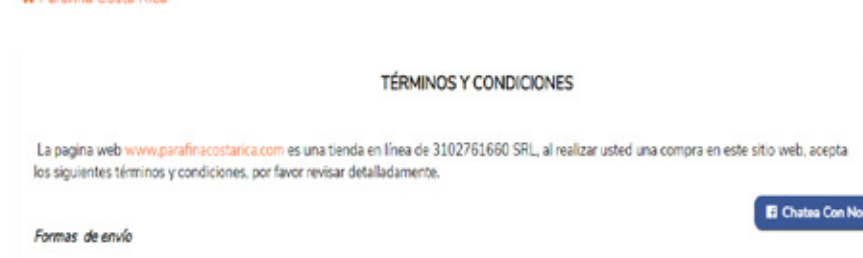


**Certificado dominio:** Ingresa a los siguientes sitios para que pueda validar la disponibilidad de tu dominio en la red:

<https://www.nic.cr/> (todos los terminados en cr) y/ o [www.whois.net](http://www.whois.net) (.com)



### Términos y Condiciones



**Nota:** El Banco no maneja plantillas de términos de condiciones, ya que los mismos son específicos para la actividad de los comercios.





# NORMATIVA DE REVISION DE SEGURIDAD DE SU SITIO

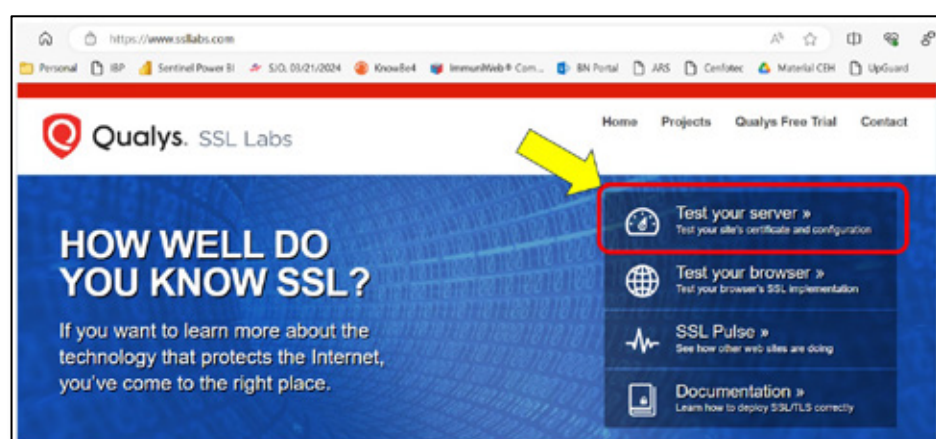
## COMO EVALUAR LA SEGURIDAD DE LA COMUNICACIÓN

**SSL labs:** Es una herramienta de revisión de sitios que permite obtener la postura de seguridad de los elementos involucrados en la comunicación.

Se accede a través del siguiente URL:

<https://www.ssllabs.com/>

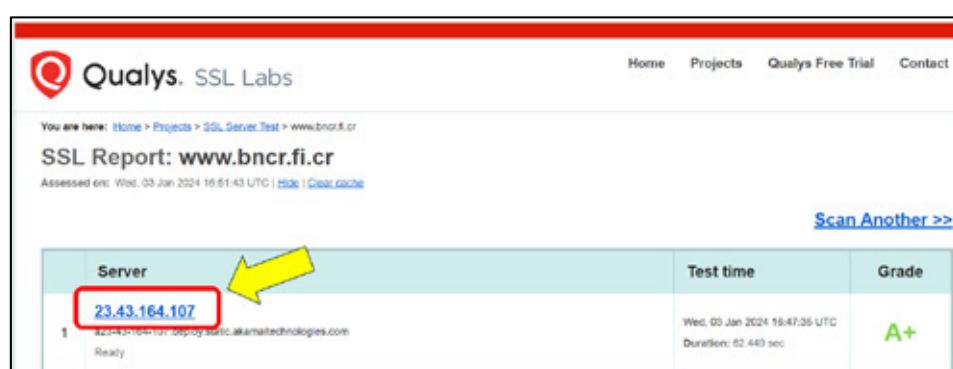
Para revisión de sitios se debe acceder a la opción "Test your server"



Se debe indicar la dirección del sitio:



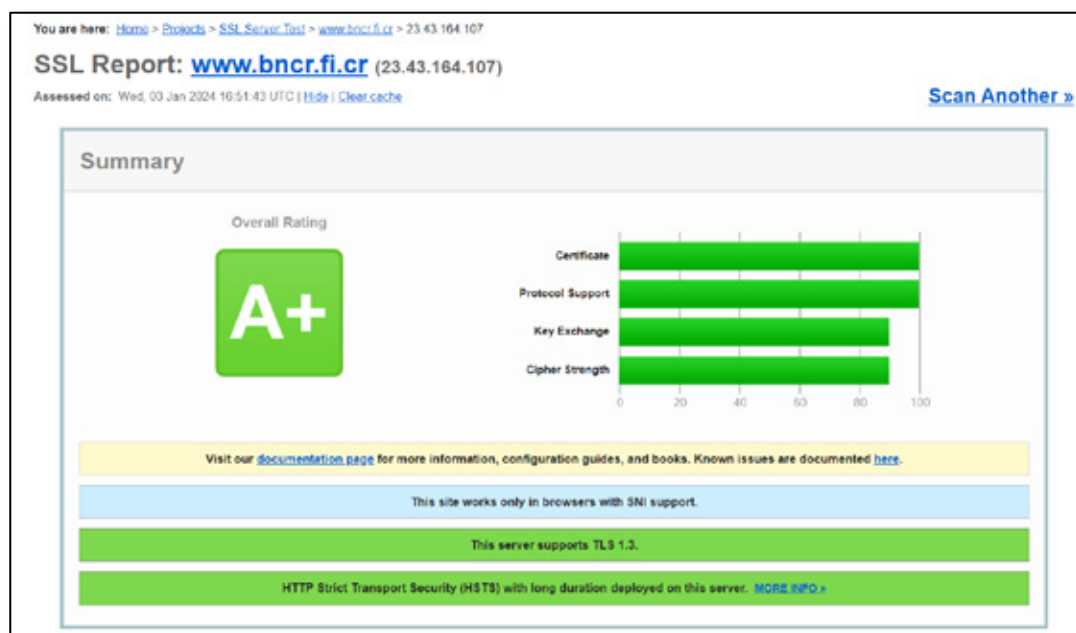
Si el sitio cuenta con varias direcciones, se debe seleccionar la más conocida:



# NORMATIVA DE REVISION DE SEGURIDAD DE SU SITIO

## Qué resultados se esperan:

1. Que los principales aspectos de la comunicación estén configurados en forma tal que muestren una calificación adecuada.



## 2. Que los certificados del sitio presenten como mínimo las siguientes características:

1. Estar dentro del periodo de validez
2. Llave de 256 o superior.
3. Haber sido emitido por una Entidad Certificadora (CA) reconocida
4. Algoritmo seguro para firma digital y de al menos 256 bits.
5. Que no haya sido revocado.

Certificate #1: EC 256 bits (SHA256withRSA)	
Server Key and Certificate #1	
Subject	www.bncr.fi.cr
Common names	www.bncr.fi.cr
Alternative names	www.bncr.fi.cr
Serial Number	007876b0b0a000000000000000000000
Valid from	Wed, 18 Nov 2020 00:00:00 UTC
Valid until	Sat, 15 Nov 2024 23:59:59 UTC (expires in 18 months and 13 days)
Key	EC 256 bits
Weak key (Default)	No
Issuer	DigiCert TLS RSA SHA256 2020 CA1
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificates)
OCSP Must Staple	No
Revocation Information	CRL, OCSP
Revocation status	Good (not expired)
One CAA	No (0/0/0/0/0)
Trusted	Yes



# NORMATIVA DE REVISION DE SEGURIDAD DE SU SITIO

3. Que el soporte de protocolos del sitio presente las siguientes características:

- 1. Los protocolos TLS1.2 y superiores deben estás activos (Yes)
- 2. Los protocolos débiles o inseguros como SSL2, SSL3, TLS1.0 y TLS1.1 deben estar deshabilitados (No).

Configuration		
<div>Protocols</div>		
<div>TLS 1.3</div>	1	Yes
<div>TLS 1.2</div>		Yes
<div>TLS 1.1</div>		No
<div>TLS 1.0</div>	2	No
<div>SSL 3</div>		No
<div>SSL 2</div>		No

4. Que los conjuntos de cifrado (cipher suites) posean las siguientes características:

- 1. El sitio no debe contener conjuntos de cifrado de nivel “Inseguro” que utilicen algoritmos que hayan sido superados como DES, 3DES, RC2, RC4, Null

Cipher Suites		
# TLS 1.3 (suites in server-preferred order)		
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_8_SHA256 (0x1305)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304)	ECDH x25519 (eq. 3072 bits RSA) FS	128
# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a9)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128

El sitio debe presentar los conjuntos de cifrado en orden tal que se brinde prioridad a los de mayor seguridad y dejando aquellos que se consideren débiles (WEAK) con la menor prioridad. Para tal efecto, se recomienda que los sitios posean solamente los conjunto de cifrado de acuerdo a lo estipulado por NIST en su documento NIST.SP.800-52-r2, y además, en acatamiento a las mejores prácticas dictadas por

# NORMATIVA DE REVISION DE SEGURIDAD DE SU SITIO

OWASP, IETF y PCI, que posean la característica "Perfect Forward Secrecy".

**Los principales conjuntos de cifrado que cumplen esta característica son:**

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

## ACEPTACIÓN POR PARTE DEL AFILIADO

El AFILIADO se compromete a mantener en buen estado y mínimo por cinco años la documentación e información que respalde los cargos y compras de bienes o servicios, realizadas por los tarjetahabientes, y entregar al Banco la documentación que este último solicite en un término de cinco días hábiles posteriores a la solicitud.

EL AFILIADO no podrá ofrecer en su página WEB bienes o servicios o realizar transacciones utilizando los medios de pago de una tarjeta Visa o MasterCard, para actividades tales como juegos de azar, juegos de casino, loterías (con excepción de la lotería de gobierno), bingos, apuestas, venta de medicinas, cigarros, alcohol, citas, armas de fuego.

EL AFILIADO no podrá ofrecer en su página WEB bienes o servicios o realizar transacciones utilizando los medios de pago de una tarjeta Visa o MasterCard, para actividades tales como juegos de azar, juegos de casino, loterías (con excepción de la lotería de gobierno), bingos, apuestas, venta de medicinas, cigarros, alcohol, citas, armas de fuego.

# NORMATIVA DE REVISION DE SEGURIDAD DE SU SITIO

## SOPORTE

Soporte o atención de consultas relacionadas a la transaccionalidad con nuestro Comercio Electrónico, puede contactarnos en las opciones:

**Llamando a Canales Digitales a los teléfonos:**

2207-8618 o 2207-8633

**Cuenta de correo electrónico:**

[gestionescomercioelectronico2@bncr.fi.cr](mailto:gestionescomercioelectronico2@bncr.fi.cr)