

Política de Uso

CCSS

Colombian Clearing and Settlement System
CCSS 2.3
VERSION 1.0



CÁMARA DE RIESGO
CENTRAL DE CONTRAPARTE DE COLOMBIA

CONDICIONES DE USO

Los siguientes términos son parte de un acuerdo entre el participante directo, sus usuarios designados y la CRCC:

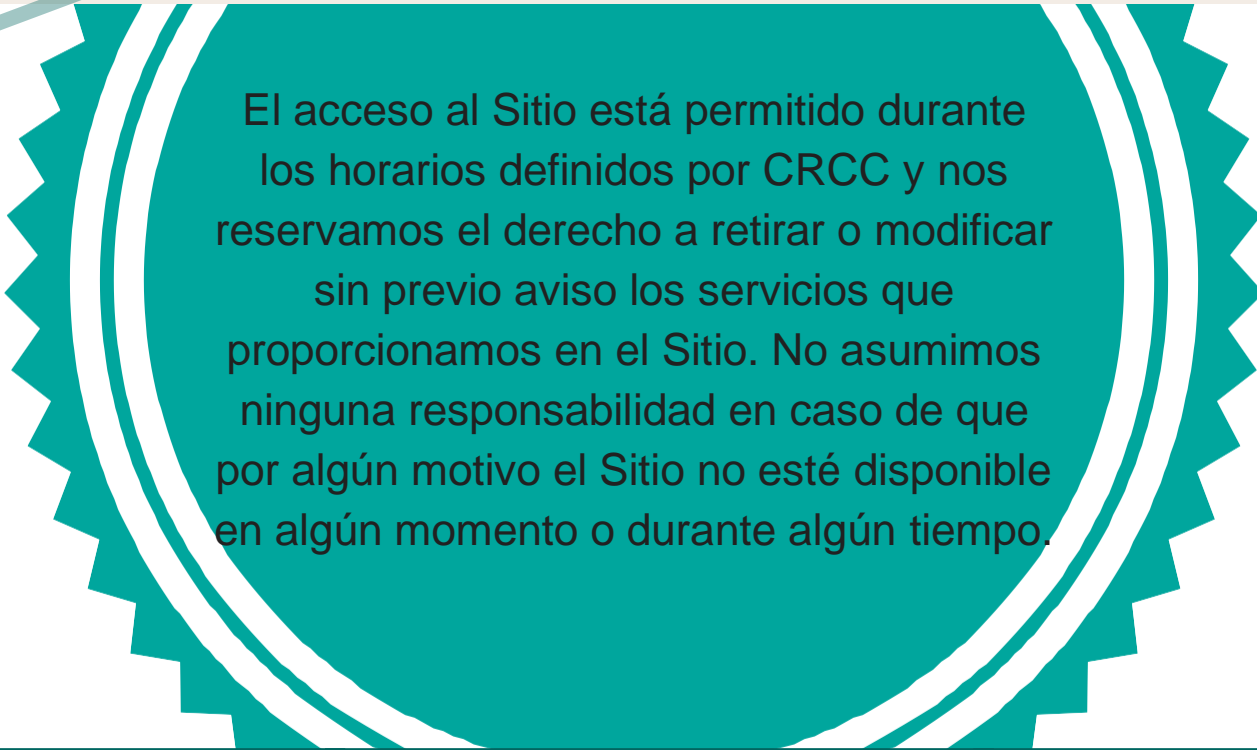
Al acceder o usar este sitio, reconoce que ha leído, entendido y acepta las disposiciones de estos términos y el cumplimiento de todas las leyes y reglamentaciones aplicables. Si no está de acuerdo con estos términos, no utilice este sitio

CRCC puede, sin previo aviso, en cualquier momento, modificar las presentes condiciones de uso y cualquier otra información contenida en este sitio.

CRCC también puede efectuar mejoras o cambios a los productos, servicios o programas descritos en este sitio en cualquier momento sin previo aviso.




Acceso al sitio




El acceso al Sitio está permitido durante los horarios definidos por CRCC y nos reservamos el derecho a retirar o modificar sin previo aviso los servicios que proporcionamos en el Sitio. No asumimos ninguna responsabilidad en caso de que por algún motivo el Sitio no esté disponible en algún momento o durante algún tiempo.

Es posible que en algún momento restrinjamos el acceso a algunas partes del Sitio, o al Sitio en general, a los usuarios que se han registrado con nosotros.

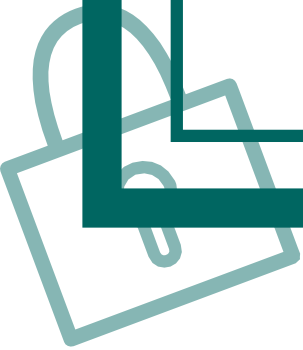
Si usted elige o recibe un código de identificación de usuario, contraseña o cualquier otra información como parte de nuestros procedimientos de seguridad, deberá tratar dicha información como confidencial y no revelársela a nadie.





Si consideráramos que usted no ha cumplido alguna de las estipulaciones de estas condiciones de uso, nos reservamos el derecho a inhabilitar en cualquier momento su código de identificación de usuario o contraseña, tanto si los ha elegido usted como si se los hemos asignado nosotros.

Es responsabilidad de la entidad Participante y los usuarios designados por ella, disponer todo lo necesario para tener acceso al Sitio. También es responsabilidad suya asegurarse de que todas las personas que accedan al Sitio a través de su conexión de internet conozcan y cumplan estas condiciones.



Servicio

La CRCC ha incluido en lo concerniente a Seguridad de la Información, Administración de Riesgos y mejores prácticas de seguridad; una serie de rutinas y políticas de manejo que cumplen con todo lo estipulado por la reglamentación aplicable, sin embargo, CRCC no garantiza el acceso permanente e ininterrumpido al sitio cs.camaraderiesgo.com, ni que este acceso sea libre de errores o que el servicio o el servidor disponibles, estén libres de virus u otros agentes nocivos

Cuando el usuario acceda al sitio, será responsabilidad del mismo, tomar las medidas pertinentes para evitar y/o corregir los efectos indeseados de dichos agentes.

Riesgos inherentes

Denial-of-service attack: es un incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un determinado servicio de red, la pérdida temporal de toda la conectividad y todos los servicios de red. Este tipo de vulnerabilidad se conoce en español con el nombre de DoS o ataque de denegación de servicio.

Para todos los efectos, la Entidad Participante y sus usuarios designados asumen los riesgos inherentes al uso de los Medios Autorizados para la Función de Control, enunciados algunos, sin que eso implique que algún otro riesgo diferente a estos se pueda materializar:

Cross-site scripting: es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar. Este tipo de vulnerabilidad se conoce en español con el nombre de Secuencias de órdenes en sitios cruzados.

SQL injection: es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos. Este tipo de vulnerabilidad se conoce en español con el nombre de Inyección SQL.

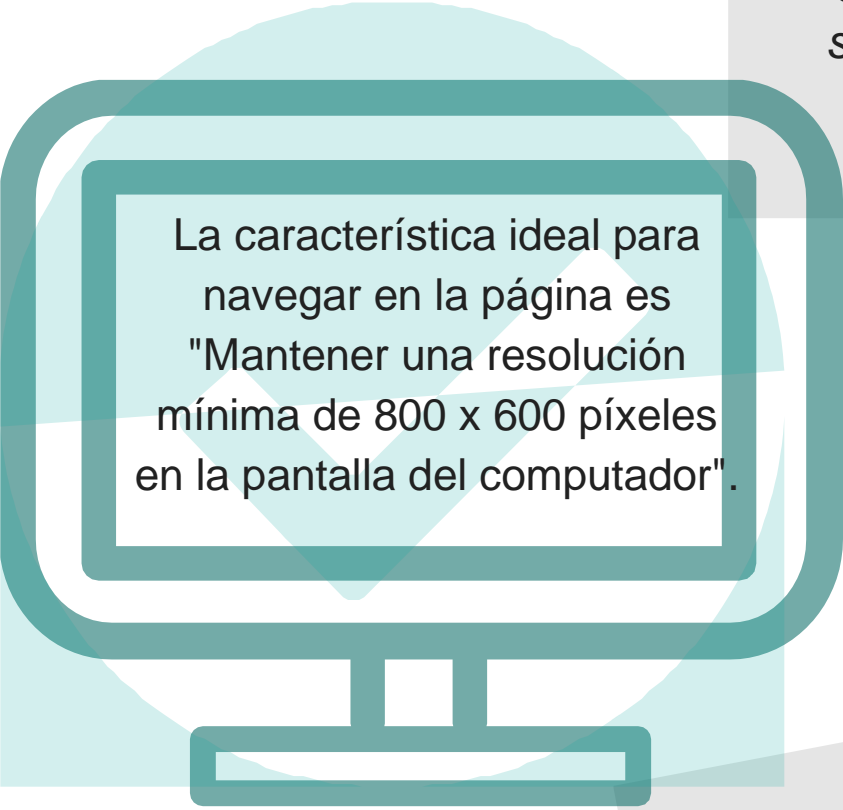
DNS Hijacking: se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Este tipo de vulnerabilidad se conoce en español con el nombre de Suplantación de identidad por nombre de dominio

Arbitrary code execution: se trata de la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación a su antojo, generalmente aprovechando alguna vulnerabilidad. Este tipo de vulnerabilidad se conoce en español con el nombre de ejecución arbitraria de código.

Características del equipo para la óptima navegación



Las páginas pueden ser cargadas desde cualquier navegador o browser, pero es posible que algunas páginas no funcionen o no se vean bien porque requieren de una configuración especial de la pantalla y del browser.



La característica ideal para navegar en la página es "Mantener una resolución mínima de 800 x 600 píxeles en la pantalla del computador".



Se recomienda utilizar navegadores recientes, que soporten los últimos protocolos de seguridad en el transporte de información, por ejemplo, Microsoft Edge, o navegadores como Firefox, Chrome y Safari en sus últimas versiones.



Restricciones aplicables al uso del sitio web

Además de aceptar las demás restricciones enumeradas en estas Condiciones de Uso, el participante directo, sus usuarios designados se obliga:

A no disfrazar el origen de la información transmitida vía el Sitio Web.

A no colocar información falsa o engañosa en el Sitio Web.

A no utilizar ni acceder a ningún servicio, información, aplicación o software disponible vía el Sitio Web de formas prohibidas por CRCC.

A no introducir ni cargar en el Sitio Web información:

- Que contenga virus, caballos de Troya, gusanos, bombas lógicas u otras rutinas informáticas cuyo fin sea dañar, interceptar, expropiar o interferir con algún sistema, el Sitio Web o la Información o
- Que infrinja los derechos de Propiedad Intelectual de terceros.

A no utilizar ni acceder al Sitio Web, a los Sistemas o Servicios de CRCC de maneras que afecten adversamente la función, el funcionamiento de los mismos, o que impidan a terceros autorizados acceder a los mismos.

Exención de la responsabilidad

Además de los supuestos de exención de responsabilidad previstos en otras cláusulas de estas condiciones generales y en otras secciones de esta página web, la CRCC no garantiza ni se responsabiliza por los daños directos e indirectos (incluyendo, pero sin limitar, a aquellos que se traduzcan en pérdidas de utilidades, costos para contratar servicios o pérdidas de oportunidades) que surjan o se relacionen con:

El uso de la información suministrada por un usuario, por parte de terceras personas distintas a la CRCC, que hubieren decodificado dicha información mediante el uso de sistemas informáticos.

Daños ocasionados a los equipos y/o programas de los usuarios por la posible contaminación de virus informáticos.

Retrasos, deficiencias o imposibilidad en cuanto al acceso a la página, debido a circunstancias que estén fuera del control del banco.

La interrupción o suspensión de los servicios disponibles en la página web o acceso a esta, por mantenimiento, fallas en el sistema, servicio eléctrico, telefónico, por razones de orden técnico o de cualquier otra índole.

DUDAS E INQUIETUDES

(57) (1) 327 7000

mesadeayuda@camaraderiesgo.com.co



CÁMARA DE RIESGO
CENTRAL DE CONTRAPARTE DE COLOMBIA