Banco Finandina

Centro de Soporte

Si tiene dudas comuníquese con la línea de servicio de lunes a viernes de 7:00 a.m a 7:00 p.m.

Línea fácil
Bogotá: **219 1919**
Resto del país
01 8000 912886

¡Interactúa con nosotros!

www.**bancofinandina**.com

Beneficios

Facilidad de uso.
Usted solo debe validar la clave dinámica generada en el dispositivo Token e ingresar los 6 dígitos que le aparece.

Autenticación fuerte.
El Banco combina 2 elementos: algo que poseo (dispositivo ó Token) y algo que conozco (Código empresarial Usuario y Clave actual de ingreso) para aumentar el nivel de seguridad.

Confianza.
Asegura el acceso de todos los usuarios porque cada uno tiene una clave exclusiva (clave actual más la clave Token) para cada nuevo acceso a realizar.

Prevención contra ataques de suplantación de página del Banco.
Esta eventualidad es conocida como Phishing y ocurre cuando se piden datos a través de enlaces en correos electrónicos que suplantan la página del Banco.

Mayor seguridad transaccional.
Al contar con un factor adicional de autenticación a través de dos claves únicas y aleatorias generada por el Token y que son válidas por un periodo de tiempo corto. Esto garantiza que, si por algún motivo la clave actual es comprometida, no se pueda ingresar por personal extraño al no tener la clave Token y la de sitio seguro.

Banco Finandina

www.**bancofinandina**.com

Instructivo de uso **Token** para la Banca empresarial Finandina

Para ingresar a la Banca Empresas de Finandina se debe autenticar a través del **TOKEN**, un dispositivo que le permitirá dicha autenticación con un **alto nivel de seguridad.**

¿Qué es? y ¿Cómo funciona?

Es un dispositivo físico asociado a su usuario, el cual genera una clave que cambia automáticamente **cada 60 segundos,** y que le será solicitada al momento de ingresar al Portal, además del Código empresarial, usuario y clave tradicional. Esta validación aplica tanto para el usuario primario como para los usuarios secundarios.

Premisas

- El servicio de **validación de Clave de Token** será activado comunicándose a nuestra línea de asistencia.
- El Banco asignará un token al **usuario primario de la empresa.** Es responsabilidad del usuario primario asignar los tokens a cada uno de los usuarios secundarios de su empresa.
- En caso de requerir token adicional por la empresa, debe **contactar a su ejecutivo de cuenta,** con el fin de tramitar la novedad.

Cuidados del Token

Manténgalo en un lugar seguro.

No lo exponga a temperaturas extremas.

No exponga el dispositivo a niveles anormales de esfuerzo físico (golpes fuertes, pisadas, caídas de altura elevada, objetos pesados sobre el dispositivo, etc.).

Duración de las Baterías: La batería del Token tienen una duración aproximada de 5 años; cuando esta llega a un nivel del 5% antes de generar la clave de ingreso en la pantalla, muestra el siguiente mensaje: **"batt 5%"**. Dicho mensaje aparecerá con anticipación, dándole tiempo para solicitar al Banco el reemplazo.

No intente abrir su Token para revisar la batería o placas de circuitos, esto ocasionará el daño irreparable del dispositivo ó el mal funcionamiento de este.

No se deberá sumergir en el agua, si bien es resistente al agua, no es sumergible. Si lo hace provocará el mal funcionamiento del mismo.

El Token es de carácter personal e intransferible, por lo tanto no puede ser compartido con otros usuarios.

Manejo de novedades

En caso de perdida, reasignación de tokens entre usuarios secundarios, robo o mal funcionamiento comuníquese con las líneas de atención, dónde recibirá la asesoría necesaria.

Si desea solicitar nuevos dispositivos, comuníquese con su ejecutivo de cuenta para tramitar la novedad.

Importante Recomendaciones de seguridad

Tenga presente que Banco Finandina nunca le enviara correos electrónicos con links predefinidos para ingresar al sitio web del Banco y nunca solicitará que sincronice sus tokens para poderlos utilizar. Si recibe este tipo de mensajes es posible que estén tratando de engañarlo para tener acceso a su información confidencial de autenticación. Si recibe un mensaje con estas características informe de inmediato al centro de contacto.

El uso del Token no requiere ninguna interacción con su computador, es decir, no se tiene que instalar o mantener ningún paquete de software adicional.

Es responsabilidad de los usuarios tanto primarios como secundarios que, una vez recibido su dispositivo, este debe ser custodiado personalmente por el usuario respectivo, debido a que tiene la misma importancia de la clave y usuario que actualmente posee para acceder al Portal Corporativo por ser una segunda clave de ingreso a sus transacciones.