BANCO CREDIFINANCIERA S.A. tiene definida una política de seguridad de la información, cuyo objetivo es asegurar que los recursos tecnológicos y la información sean utilizados de manera correcta y efectiva, que las modificaciones sólo dependan de las personas que se asignaron para hacerlo y que todos nuestros clientes, manejen la información de forma segura.

RECOMENDACIONES GENERALES

• Su información financiera es confidencial, evite compartirla con otras personas, manéjela con reserva.

• No de información personal para reclamar supuestos premios de sorteos en los cuales no participó.

• Reclame los documentos que entregó a la entidad financiera para el estudio de créditos, cuando se haya cancelado el crédito se debe solicitar el pagaré

• Infórmese de las recomendaciones y mecanismos de seguridad que le ofrece BANCO CREDIFINANCIERA S.A.

• Revise periódicamente el estado de sus cuentas en las centrales de riesgos para validar posibles reportes negativos del comportamiento crediticio.

• En caso de pérdida o hurto de sus documentos de identificación formule la correspondiente denuncia y repórtela a BANCO CREDIFINANCIERA.

• Denuncie ante las autoridades cualquier fraude del cual haya sido víctima.

RECOMENDACIONES PARA EL USO DE OFICINAS

• Consulte a los empleados sólo en sus puestos de trabajo y confirme que porten el carné que los identifica como funcionarios de BANCO CREDIFINANCIERA S.A.

• No use equipos de comunicación dentro de la oficina. Si advierte que alguien lo hace, informe a los funcionarios de BANCO CREDIFINANCIERA S.A.

• Si observa situaciones sospechosas, informe a los funcionarios identificados de la oficina.

• Una persona puede ser sospechosa si cede varias veces el turno, entra y sale continuamente de la oficina o utiliza distintas áreas de la entidad sin realizar ninguna operación.

SEGURIDAD EN INTERNET

• No utilice links dentro de un correo electrónico para ingresar a los portales de BANCO CREDIFINANCIERA S.A, para ingresar escriba la URL www.credifinanciera.com.co en el navegador.

• Para evitar que sea víctima de fraude bajo la modalidad de phishing, nunca responda a mensajes de correo electrónico que requieran información personal o financiera, y nunca haga clic en una

cadena en ese tipo de correos. Si tiene dudas respecto a la legitimidad del correo, o si cree que ha sido víctima de un engaño por phishing por favor enviar correo a seguridadti@credifinanciera.com.co

• Nunca diligencie formatos de texto en mensajes de correo que le soliciten información personal o confidencial.

• Si usted recibe un correo de parte de nosotros notificándole que ha realizado una operación que usted no reconoce, no dude en comunicarse a la línea de Servicio al Cliente a los teléfonos:

Ciudad	Teléfono
Bogotá	(1) 4823382
Cali	(2) 4850018
Medellín	(4) 6040162
Barranquilla	(5) 3091723
Cartagena	(5) 6930194
Bucaramanga	(7) 6972262
Villavicencio	(8) 6784090
El resto del país	18000423814

También puede escribirnos a nuestro buzón electrónico servicioalcliente@credifinanciera.com.co

• Asegure que su computador tiene instalado software antivirus y software para protección de instalación de programas espías y que tanto el equipo como el navegador de Internet se encuentran al día con las últimas actualizaciones de seguridad. No instale programas de procedencias dudosas o aquellos enviados mediante correos electrónicos.

• Para crear contraseñas, utilice palabras fáciles de recordar, pero difíciles de adivinar, no utilice secuencias como “enero" "febrero" "marzo”, “12345”, "54321", “abcdef”.

• Utilice contraseñas diferentes para cada uno de los accesos que tenga.

• Nunca revele ni comparta sus contraseñas. Tenga en cuenta que la contraseña es personal e intransferible. • No incluya contraseñas en mensajes electrónicos.

• No escriba su contraseña en papeles como post-it, ni la deje en sitios como debajo del teclado, encima de su escritorio, debajo del monitor o la CPU.

• Cambie sus contraseñas periódicamente.

LÍNEAS DE SERVICIO AL CLIENTE

• Siempre que realice su llamada desde un teléfono con pantalla, verifique que al marcar la tecla redial no quede almacenada la información digitada (Número de identificación y Clave). De lo contrario marque un número diferente y así borrará su información.

- Si recibe llamadas a nombre de BANCO CREDIFINANCIERA S.A. para actualizar sus datos u ofrecerle algún producto y/o servicio, procure que el asesor sea quien los confirme, en ningún caso responda con su información personal o financiera.

- Memorice el nombre del asesor que lo está contactando. Preferiblemente tome nota en caso de que lo requiera de nuevo.

- Evite o tenga cuidado al utilizar este servicio desde cabinas telefónicas públicas

- Desista de las consultas telefónicas si detecta ruidos extraños en la línea. Puede estar siendo víctima de fraude y es recomendable cambiar las claves.

- Evite utilizar teléfonos celulares de personas desconocidas para realizar operaciones

MODALIDADES DE FRAUDE EN LA RED

Pesca (Phishing)

Consiste en el envío de correos electrónicos muy convincentes que, aparentando provenir de fuentes fiables intentan obtener datos confidenciales del usuario a través de links a supuestas páginas de entidades o empresa de servicios.

¿Qué hacer para prevenirlo?

No utilice links dentro de un correo electrónico para ingresar a los portales de BANCO CREDIFINANCIERA S.A o de cualquier entidad o empresa de servicios, para ingresar siempre escriba la URL directamente en el navegador.

Suplantación de Sitios Web o Email (Spoofing)

Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación, la identidad puede ser capturada a través de sitios Web falsos o mediante mensajes de correo en los cuales se solicita información financiera o datos de usuario y contraseña.

¿Qué hacer para prevenirlo?

- Asegúrese que el sitio Web al que ingrese es seguro, verifique que aparece el candado cerrado en el navegador.

- Desconfié de páginas extrañas o que no parezcan de la entidad, validé con la compañía si se ha realizado algún cambio

Software Espía (Spyware)

Son programas que funcionan dentro de la categoría malware, que se instalan furtivamente en un computador para recopilar información sobre las actividades realizadas en éste, puede ser utilizado

para detectar tendencias de navegación o para capturar información de las personas como usuarios, contraseñas, números de tarjetas de crédito, números de identidad, etc.

¿Qué hacer para prevenirlo?

- Instale software antivirus y software para protección de instalación de programas espías en el computador y verifique que se encuentren al día con las últimas actualizaciones.
- No utilizar computadores públicos.
- Tenga precaución en el uso de redes públicas de Internet.

Pharming.

Es un programa utilizado por delincuentes que busca la captura de información como números de tarjetas de crédito e identidad.

¿Qué hacer para prevenirlo?

- Mantén actualizado el antivirus y activado el cortafuegos (firewall) de tu PC.
- No abras mensajes de correos electrónicos sospechosos o de los cuales desconozcas su procedencia.
- Siempre revisa con tu antivirus los dispositivos de almacenamientos (CD, memorias USB) antes de abrir su contenido.
- No instales programas desde páginas desconocidas, ni visites sitios de dudosa reputación