BPR BANK

CÁPSULAS DE SEGURIDAD

Consejos de Conectividad:

- Verifique la autenticidad del sitio web del banco, el mismo debe mostrarse como https://www.bprbank.com el cual indicará que es seguro.
- Verifique que la barra de direcciones sea de color verde. Esto le indica que es un sitio legítimo y seguro. Si es de color rojo, es un sitio no seguro, salga de inmediato y repórtelo a: **negocios.bpr@bprbank.com**
- Haga click en la imagen del candado () que se encuentra al lado izquierdo del navegador donde se coloca la dirección del sitio web, para verificar que el Certificado de Seguridad esté a nombre de https://www.bprbank.com
- Procure no realizar operaciones en la página del banco desde lugares públicos poco seguros como cyber café, centros comerciales, aeropuertos o similares.
- Conéctese desde un lugar seguro como su casa u oficina.
- No ingrese a nuestra página web a través de enlaces ubicados en otras páginas o vínculos que reciba por correo electrónico.
- Acceda a contenido o enlaces directamente del sitio web del banco y no por medio de correos electrónicos, mensajes de texto o publicad de dudosa procedencia.

Consejos de Prevención y Monitoreo:

- Asegúrese de validar la identidad de cualquier persona que se comunique en nombre del banco.
- El banco solo usará canales de comunicación aprobados para solicitar o actualizar su información.
- El banco jamás enviará enlaces donde te solicite información de claves de acceso a banca en línea, cuentas bancarias o datos de tu tarjeta de crédito/débito.
- Revise periódicamente los movimientos de su cuenta y reporte cualquier dato sospechoso.
- Almacene o destruya de forma segura los documentos relacionados a su cuenta.
- Instale y mantenga actualizados el antivirus, firewall o cortafuegos y otros programas que utilice como mecanismo de protección, para minimizar la posibilidad de instalación de aplicaciones no deseadas.
- Verifique que el antivirus este actualizado y que se realicen escaneos periódicos a todos los archivos almacenados en la computadora.

Consejos de Control de Accesos:

- Actualice regularmente su contraseña de acceso.
- Defina contraseñas complejas; compuestas por letras mayúsculas y minúsculas, números y caracteres especiales.
- Defina sus contraseñas con una longitud mínima de 8 a 12 caracteres.
- No comparta su contraseña. Recuerde que ésta es personal e intransferible.
- No permita la opcion de autocomempletar contraseñas o no almacene las mismas en el navegador
- Evite el uso de la misma contraseña para múltiples cuentas.
- Procura no instalar en tu computadora ningún software pirata, pues estos pueden contener virus o programas para obtener tus claves.
- Asegúrese de cerrar la sesión antes de alejarse o cerrar la página web del banco.
- Asegúrese de cerrar la sesión en el App del banco cuando no la utilice.

El uso adecuado de los medios electrónicos y el seguimiento a las cápsulas de seguridad disminuirán la posibilidad de ser víctimas de fraude.

Conceptos:

- Fraude de identidad: El fraude de identidad y el robo de identidad son términos que se utilizan para referirse a todos los tipos de delitos en los que alguien obtiene y utiliza indebidamente los datos personales de otra persona de alguna manera que implica fraude o engaño, generalmente con fines económicos. (NIST)

- Phishing: Es un delito cibernético en el que un objetivo u objetivos son contactados por correo electrónico, teléfono, mensaje de texto y sitios web fraudulentos que se parecen mucho a las fuentes legítimas con la intención de cometer fraude financiero. (NIST)

- Ransomware: Es un malware que emplea cifrado para retener la información de la víctima a cambio de un rescate. Los datos críticos de un usuario u organización están encriptados para que no puedan acceder a archivos, bases de datos o aplicaciones. Luego se exige un rescate para proporcionar acceso. (Mcafee)

- Virus: Es un programa informático que puede copiarse a sí mismo e infectar una computadora sin permiso o conocimiento del usuario. Un virus puede dañar o borrar datos en una computadora, usar programas de correo electrónico para propagarse a otras computadoras o incluso borrar todo lo que hay en un disco duro. (NIST)