kutxabank

cajasur

ACEPTACIÓN DEL ACCESO REMOTO A SISTEMAS DE INFORMACION

Kutxabank S.A. ("Kutxabank") y Cajasur Banco, S.A ("Cajasur") (en adelante, conjuntamente las "Entidades" e individualmente, la "Entidad") han desarrollado una solución de acceso remoto a sus Sistemas de Información mediante la utilización de dispositivos y técnicas de identificación seguras. Podemos separar los elementos involucrados en este tipo de accesos en dos tipos:

- Dispositivos físicos corporativos o propios: ordenador portátil, tablet, teléfono móvil …
- Elementos de identificación : usuario-contraseña, PIN, token RSA, token SMS, certificados digitales …

Dependiendo de los requerimientos del acceso remoto solicitado y en caso de ser necesario, la Entidad proporcionará al solicitante uno o varios de los elementos anteriores que sean necesarios para el acceso solicitado. Asimismo, el solicitante indicará en el presente documento, el nº de teléfono móvil donde se le enviará el PIN temporal de autenticación.

La utilización por Vd. de este tipo de acceso y de los dispositivos relacionados, exige conocer y asumir la correcta utilización del mismo conforme a las reglas generales para el uso de los Sistemas de Información de la Entidad recogidas en el documento "Normativa para la Seguridad de la Información" publicado en la Intranet de la Entidad.

En concreto y entre otras medidas:

- Se informa expresamente que la Entidad se reserva la facultad de monitorización, investigación e inspección de los accesos realizados y de los contenidos accedidos, por medio de revisiones aleatorias, globales o individualizadas.
- Los elementos de identificación para el acceso remoto son personales e individuales, por lo que en ningún caso pueden comunicarse a terceros, siendo responsabilidad del usuario solicitante garantizar su confidencialidad.
- Los dispositivos de acceso deberán contar con medidas de protección propias y específicas, como el acceso mediante contraseña robusta, patrón personal o datos biométricos, actualizaciones de seguridad periódicas y un antivirus activo y permanentemente actualizado.
- La confidencialidad de los datos accedidos quedará bajo la responsabilidad del usuario solicitante que garantizará que no sean accesibles por terceros no autorizados.
- El solicitante se compromete a cumplir, en función de la información a la que acceda, con lo especificado en las diferentes normativas que puedan ser de aplicación en cada caso: Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), normativa en materia de protección de datos de carácter personal, y otras normativas legales vigentes en el momento.
- Se prohíbe la descarga y/o extracción de cualquier tipo de información sensible/confidencial al equipo a través del cual se realiza el acceso remoto, salvo que sea estrictamente necesario y esté debidamente autorizado.
- En caso de teléfonos propios, el número informado para la recepción del PIN es personal e intransferible. El usuario impedirá el acceso al mismo a terceras partes no autorizadas aplicando las medidas de seguridad oportunas.
- Deberá comunicar cualquier incidencia que se produzca en el propio acceso remoto o en cualquiera de los elementos involucrados en el mismo mediante llamada al CAU (Centro de Atención a Usuarios) a los siguientes teléfonos : Directo interno: 4004, desde el exterior : 946019969

***Conozco y acepto la Normativa para la Seguridad de la Información de la Entidad y las normas y condiciones de uso* específicas expresadas en el presente documento:**

Nombre: **Fecha:**

Nº Teléfono móvil:

Recibido y conforme (Firma):