

Buenos Aires 22 de Junio de 2018

A quien corresponda

Ref. Comunicación "A" 4609 del 27 de diciembre 2006  
 Banco Central de la República Argentina  
 Circular RUNOR 1 – 805  
 "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información"

A continuación se evalúan cada uno de los puntos que en ella se detallan.

Estándares de acceso, de identificación y autenticación, y reglas de seguridad.  
 Se deben implementar métodos de identificación y autenticación para controlar el acceso lógico a los sistemas y servicios informáticos, los que dependerán de la criticidad y el valor de los datos a proteger, debiéndose considerar:

Requerimiento	Status Siopel XL
La modificación de las contraseñas maestras y de cuentas especiales "por defecto" de los sistemas operativos, de los subsistemas administradores de seguridad, de las bases de datos y de las herramientas para la administración y el control	No aplica (no utiliza perfiles ni herramientas como las descriptas)
El cambio obligatorio de las contraseñas de acceso en el primer inicio de sesión	Cumple
8 (ocho) caracteres de longitud para las claves provistas a todo sistema informático de la entidad	Cumple
El control de la composición de las contraseñas (por ejemplo: caracteres alfabéticos, numéricos, especiales, mayúsculas y minúsculas)	Cumple <ul style="list-style-type: none"> <li>• Es case sensitive</li> <li>• Acepta caracteres especiales</li> <li>• Exige al menos un número y una letra</li> </ul>
El registro histórico de las últimas 12 (doce) contraseñas utilizadas, evitando ser reutilizadas	Cumple
El intervalo de caducidad automática de las mismas a los 30 (treinta) días	Cumple
El bloqueo permanente de la cuenta del usuario ante 3 (tres) intentos de acceso Fallidos	Cumple
La desconexión automática de la sesión de usuario en la aplicación y en la red por tiempo de inactividad a los 15 (quince) minutos	No aplica (el usuario debe poder observar el mercado sin participar)
La eliminación de las cuentas de usuario inactivas por un período mayor a 90 (noventa) días	Cumple
La no utilización de denominaciones de usuario genérico para perfiles asignados a personas físicas	Cumple
Técnicas de encriptación, con algoritmos de robustez reconocida internacionalmente, para el archivo de las contraseñas	Cumple (DES)
Asignación de contraseñas para todas las cuentas	Cumple

Restricción de accesos concurrentes	Cumple
La identificación única (ID) de usuarios	Cumple
Definición de opciones y menús para acceder a las funciones de los sistemas de información	Cumple
La dinámica en la actualización de los derechos de acceso, revocando los usuarios que se desvincularan de la entidad y modificando los perfiles de aquellos que cambiaron de función	Cumple
La permanente actualización de los sistemas operativos y herramientas con respecto a nuevas vulnerabilidades, y " <i>patches</i> "	No aplica (es responsabilidad del usuario)