ACUERDO DE USO DE LOS RECURSOS Y SERVICIOS INFORMÁTICOS DE LA EMPRESA DE ACUEDUCTO DE BOGOTÁ. Versión 1.0

ANEXO PRIMERO

CONDICIONES Y TÉRMINOS PARA EL MANEJO DE CUENTAS Y CONTRASEÑAS EN LOS SISTEMAS DE INFORMACIÓN DEL ACUEDUCTO DE BOGOTÁ

INTRODUCCIÓN

El presente anexo tiene por objetivo definir las condiciones y términos para el manejo de cuentas y contraseñas en los sistemas de información y recursos informáticos del Acueducto de Bogotá.

CAMPO DE APLICACIÓN

Las presentes condiciones son aplicables y extensivas al manejo de cuentas y contraseñas en los sistemas de información del Acueducto de Bogotá. Todo Usuario que tenga cuenta(s) de acceso a los sistemas de información o recursos informáticos del Acueducto de Bogotá deberá tener presentes las siguientes precauciones en su manejo para responder por sus obligaciones de buen uso, evitar suplantación, evitar pérdidas de información y evitar alteración no deseada de información o la manipulación ajena de los recursos a su cargo.

TÉRMINOS Y CONDICIONES.

- La(s) cuenta(s) de acceso asignadas al usuario son de propiedad del Acueducto de Bogotá y son de carácter personal e intransferible.
- La asignación, adición, modificación o eliminación de la(s) cuenta(s) de acceso deberá ser realizado por medio del procedimiento “Administración de Cuentas de Acceso y Autorizaciones – 2GT100575”.
- El usuario al que se le ha asignado una(s) cuenta(s) de acceso es el único responsable por la(s) misma(s). El usuario es responsable por toda la actividad que se genere a partir de la(s) cuenta(s) de acceso asignada(s). La responsabilidad de esta actividad es entendida ya sea por acción, omisión o extralimitación y debe(n) ser usada(s) observando, entre otros, lo dispuesto en los numerales 4, 5, 21,22 y 40 del artículo 34 y numerales 16 y 43 del artículo 48 de la Ley 734 de 2002 – Código Disciplinario Único, que tratan de los cuidados a que se está obligado con los bienes públicos confiados a su guarda.
- El usuario debe velar por la privacidad de su(s) clave(s) de acceso a la red y aplicaciones, evitando comunicarla(s) a terceros. En caso de que la palabra(s) clave(s) de acceso (contraseña) pudiera estar en conocimiento de terceras personas, el usuario deberá cambiar la(s) clave(s) de manera inmediata a la mayor brevedad posible.

- El usuario debe bloquear la sesión de trabajo al dejar su puesto de labor y es el único responsable por la actividad que se genere con la(s) cuenta(s) asignada(s). Para que otro usuario pueda utilizar un puesto de trabajo ajeno, debe hacerlo con sus propias cuentas, es decir, el usuario original de la estación debe cerrar su sesión de trabajo antes de permitir a otros el uso de su estación.
- El usuario debe usar contraseñas robustas para evitar que puedan ser descifradas automáticamente. Las contraseñas se deben construir a partir de los siguientes lineamientos:
  - Usar contraseñas con mínimo 8 caracteres de longitud.
  - Usar en las contraseñas caracteres alfabéticos, numéricos y caracteres especiales.
  - No usar como contraseña la identificación de la cuenta de acceso.
  - No usar palabras conocidas tomadas del diccionario o contraseñas simples como “acueducto”, “empresa”, “123456”.
  - Evitar el uso de información personal como números telefónicos, nombres de personas, números de identificación, fechas especiales, etc.
  - Evitar el uso de la misma contraseña con diferentes cuentas de acceso.
  - Cambiar regularmente las contraseñas.
  - Cambiar las contraseñas que le son entregadas como predeterminadas.
  - Evitar apuntes de contraseñas en lugares visibles o que puedan caer en manos ajenas.
- Los usuarios con subalternos deben solicitar el bloqueo de las cuentas de acceso cuando estos sean retirados, trasladados de su cargo o cuando se encuentren incapacitados, de vacaciones o de permiso o cuando no vayan a seguir usando el sistema.
- El usuario debe solicitar el bloqueo de las cuentas de acceso cuando vaya a suspender actividades por un periodo como vacaciones, permiso o licencia u otro.
- El funcionario interventor debe solicitar cancelación de las cuentas de acceso a los sistemas, asignadas a los contratistas y consultores, cuando finalicen los contratos correspondientes.

SUSPENSIÓN DE LAS CUENTAS DE ACCESO

El uso fuera de las condiciones antes establecidas de las cuentas de acceso a los sistemas de información puede ocasionar la suspensión temporal o permanente de la cuenta de acceso. El Acueducto de Bogotá podrá revocar temporal o definitivamente las diferentes cuentas de acceso a los sistemas de información, sin detrimento de las acciones contractuales, legales y/o disciplinarias que pueda conllevar los actos realizados.