4 de enero de 2012
CI-0009-2012

Señores (as)
Administradores de Recursos Informáticos Desconcentrados (RIDs)
Universidad de Costa Rica
S.O.

Estimados (as) señores (as):

Un aspecto vital de la seguridad informática de la Universidad de Costa Rica, es el manejo de las claves de acceso utilizadas para administrar los recursos relacionados con las Tecnologías de la Información y la Comunicación (TICs). A fin de regular y estandarizar la administración de estas claves, me permito hacer de su conocimiento las siguientes disposiciones básicas para la administración de claves de acceso en los equipos de cómputo y Sistemas de Información en la Universidad de Costa Rica.

DISPOSICIONES BÁSICAS PARA LA ADMINISTRACIÓN DE CLAVES DE ACCESO DE RECURSOS RELACIONADOS CON LAS TICS

1. Acerca de la elección de Claves de acceso.

Es necesario tomar en cuenta los siguientes factores para definir las claves de acceso a los recursos relacionados con TICs:

1.1. La clave de acceso para ingresar o administrar un recurso relacionado con TICs, debe estar formada por, al menos, ocho caracteres, y estará compuesta por una combinación de cada uno de los siguientes elementos: letras minúsculas, letras mayúsculas, números y caracteres especiales. No debe contener vocales ni caracteres repetidos en forma consecutiva.

1.2. No se deben crear claves de acceso que estén formadas por nombres propios, palabras comunes del diccionario, nombres de los usuarios combinados con números, fechas, número

UNIVERSIDAD DE COSTA RICA
CENTRO DE INFORMÁTICA

secuenciales, o bien, palabras de paso en blanco o iguales que el nombre del usuario.

1.3. No deben crearse claves de acceso que sean totalmente numéricas, y que tengan algún significado (Ej. Cédula, fecha de cumpleaños, número de teléfono, placa del automóvil, etc.).

1.4. Para facilitar la administración de claves de acceso para grupos de equipos o de recursos, se sugiere utilizar una clave de acceso base y algunas variantes de esta para cada grupo.

2. Acerca de la protección de las Claves de Acceso.

2.1. La definición y protección de las claves de acceso son responsabilidad del administrador RID de cada Unidad. Es importante agregar que si se compromete la seguridad de una cuenta se puede estar comprometiendo la seguridad de toda la red.

2.2. Las claves de acceso creadas automáticamente por el sistema. (Root, System, Demo, Guest, etc.), deben ser utilizadas únicamente durante los procesos de instalación y configuración, y posteriormente deberán ser deshabilitadas.

2.3. No se debe permitir la existencia de cuentas de usuario sin clave.

2.4. La clave de acceso no debe ser enviada por correo electrónico ni ser mencionada verbalmente.

2.5. La clave de acceso no debe utilizarse en forma indefinida, sino que debe ser cambiada regularmente. Se recomienda cambiarlas en forma trimestral. Debe crearse una lista de claves que puedan utilizarse en forma cíclica, a fin de no repetirlas en cada cambio.

UNIVERSIDAD DE COSTA RICA
CENTRO DE INFORMÁTICA

3. Acerca de la administración de las Claves de Acceso.

3.1. Es responsabilidad del Administrador RID de cada Unidad, mantener un control digital e impreso, tanto de las claves de ingreso a los equipos de cómputo, como a los Sistemas de Información y demás recursos relacionados con TICs, que estén a su cargo.

3.2. Las claves de acceso deberán estar debidamente documentadas y solamente serán conocidas por el administrador RID principal quien deberá entregar una copia al Director de la Unidad.

En caso de consultas técnicas relacionadas con la definición y administración de las claves de acceso, puede dirigirse al número telefónico 5000 o a través del correo ci5000@ucr.ac.cr, o bien comunicarse con el Lic. Edgardo Baltodano X., coordinador del área de Gestión de Usuarios, al teléfono 2511-1840, o al correo electrónico edgardo.baltodano@ucr.ac.cr

Atentamente,

UNIVERSIDAD DE COSTA RICA
CENTRO DE INFORMATICA

M.Sc. Abel Brenes
Director

AB/cb*
Cc: Archivo