POLÍTICA DE CONTRASEÑAS

1 Objetivo:

Proteger la información y los recursos de tecnologias de información de la Universidad Laica Eloy Alfaro de Manabí de riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información.

2 Base Legal:

- Esquema Gubernamental de Seguridad de la Información.
- Política de Seguridad de Información.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

3 Responsables:

Unidad Central de Cordinación Informática:

- Elaboración y actualización de la presente Política.
- Evaluación del cumplimiento de la presente Política.
- Establecer mecanismos de control y auditoria.

Todos los funcionarios:

a) Cumplir con las normas y procedimientos establecidos en esta política.

b) Es responsabilidad de cada usuario realizar cambios periódicos de sus contraseñas.

4 Descripción de la Política:

- Toda contraseña correspondiente a cuentas de usuario final es personal e intransferible, por lo tanto, no debe compartirse por ningún motivo.

- Las contraseñas establecida por cada uno de los funcionarios para las diferentes sistemas informáticos serán administradas y gestionadas bajo su única responsabilidad.

- La UCCI configurará los sistemas informáticos para que el límite de intentos fallidos al ingresar una contraseña, sea de 5 intentos, luego de lo cual se bloqueará la cuenta de usuario.

- La UCCI configurará el sistema operativo, de forma que éste se bloquee indefinidamente hasta que por pedido del usuario, solicite el desbloqueo.

- Para generar contraseñas seguras para las cuentas de usuario final, éstas deberán cumplir los siguientes parámetros:

    - Tener una longitud mínima de 8 caracteres.
    - Contener Mayúsculas y Minúsculas.
    - Contener números y caracteres especiales (ej: “#*?)

- Los sistemas se configurarán de manera que los usuarios finales, al cambiar de contraseña, no puedan utilizar ninguna de las 3 contraseñas anteriores ingresadas.
- Se prohíbe solicitar y/o entregar contraseñas vía telefónica o por escrito en medios como correo electrónico o papeles.

- Las contraseñas correspondientes a cuentas especiales de administración de infraestructura serán de uso y responsabilidad del área.

- En el caso de que se requiera obtener información del computador de escritorio o portátil, de un funcionario que se encuentre ausente de forma temporal o definitiva, únicamente podrá ser solicitado por el jefe inmediato a la UCCI, a través del formulario de obtención de información.

- El área de Soporte a Usuarios, es responsable de obtener la información solicitada en el literal anterior mediante la cuenta de Administrador Local del equipo.

- Todos los equipos de la institución deben tener un usuario de administrador local cuya contraseña sera gestionada unicamente por personal de la UCCI.

- Siempre que un funcionario sospeche que la confidencialidad de su contraseña este comprometida, deberá cambiarla inmediatamente o deberá forzar el cambio de clave.

La inobservancia de la presente Política podrá conducir a la aplicación de sanciones Administrativas correspondientes, sin perjuicio de las responsabilidades civiles o penales que sean aplicables, según el caso.