CONTENIDO

1. OBJETIVO

El objetivo del presente documento es establecer reglas para garantizar la gestión y utilización seguras de las claves de acceso de los usuarios del Hospital Departamental San Antonio de Pitalito.

2. ALCANCE

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los puestos de trabajo y sistemas ubicados dentro del alcance del SGSI.

3. USUARIOS

Los usuarios de este documento son todos los empleados del Hospital Departamental San Antonio de Pitalito.

4. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
- Política de seguridad de la información
- Declaración de aceptación de los documentos del SGSI (acuerdo de confidencialidad).

5. DESCRIPCION DEL PROCEDIMIENTO

- **Obligaciones de los usuarios**

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- ✓ No se deben revelar las claves a otras personas, incluyendo la gerencia y los administradores del sistema.

- ✓ No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por área de Sistemas de información del Hospital Departamental San Antonio.

- ✓ Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).

- ✓ Se deben escoger claves seguras de la siguiente forma:
  - utilizando al menos ocho caracteres.
  - utilizando al menos un carácter numérico.
  - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula.
  - utilizando al menos un carácter especial.
  - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás.
  - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.).
  - no se deben usar nuevamente las últimas tres claves.

- ✓ Se deben cambiar las claves cada 3 meses.

- ✓ Se deben cambiar las claves en el primer ingreso al sistema.

- ✓ Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).

- ✓ No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.

- **Gestión de la clave del usuario**

Cuando se asignan y utilizan claves de usuarios, se deben respetar las siguientes reglas:

- ✓ Al firmar la Declaración de aceptación de los documentos del SGSI(acuerdo de confidencialidad), los usuarios también aceptan la obligación de mantener sus claves en forma confidencial, como se establece en este documento.

- ✓ Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.

- ✓ Cada usuario debe tener la posibilidad de escoger su propia clave.

- ✓ Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo establecido Anteriormente.

- ✓ Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.

- ✓ El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez.

- ✓ El sistema de gestión de claves debe requerir que el usuario escoja contraseñas seguras.

- ✓ El sistema de gestión de claves debe requerir que los usuarios cambien sus claves cada tres meses.

- ✓ Si el usuario solicita una nueva clave, el sistema de gestión de claves debe determinar la identidad del usuario.

- ✓ El usuario debe confirmar la recepción de la clave.

- ✓ La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
- ✓ Si un usuario ingresa una clave incorrecta tres veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión.

- ✓ Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.

- ✓ Los archivos que contienen claves deben ser guardados en forma separada de los datos de sistema de la aplicación.

6. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta el31 de diciembre de 2017.

El propietario de este documento es el Hospital Departamental San Antonio de Pitalitoque debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes relacionados con el uso indebido de claves por personas no autorizadas.
- Cantidad de incidentes relacionados con el manejo inadecuado de claves.

7. NORMATIVIDAD APLICABLE AL PROCEDIMIENTO.

No.	Descripción	Interna	Externa
1	Decreto 943 de 2014 – MECI 2014		**X**
2	Ley 1273 de 2009		**X**
3	Resolución 527 de 1999		**X**
4	Decreto 1011 del 2006		**X**

8. CONTROL DE CUMPLIMIENTO Y SANCIONES

En caso de existir incumplimiento de las Políticas de Seguridad de la Información de la E.S.E. y de los Procedimientos descritos en el presente Manual, por parte de un trabajador de la Institución, se comunicará al líder del proceso de Gestión de Talento Humano para que tomen las medidas de sanción respectivas por la inobservancia de la normatividad vigente (interna y externa), además de las responsabilidades civiles y penales a que hubiere lugar.