Políticas para la generación segura de Password individual

En el inicio se les generará un password genérico y por sistema se pedirá que ese password se intercambie por uno que sea personal, para lo cual les presentará un mensaje en su equipo que menciona que el password está vencido y que deben de cambiarlo.

Las reglas de seguridad condicionan a que el password debe de contener al menos 8 dígitos, los cuales se conforman por letras en mayúscula y minúscula, caracteres especiales y números. Además que no deben de ser iguales a los nombres de la cuenta, que no debe de ser números que sean fácilmente relacionados al dueño tales como fechas de cumpleaños, etc.

También por sistema se cotejará que los passwords no sean iguales ya que guardará un historial de 24 passwords de tal manera que al compararlos no deben de ser similares.

Todos los equipos que se interconecten a la red utilizarán la pantalla de escritorio común que será la institucional de UIENL.

El Tiempo máximo para activar el protector de pantalla será de 10 minutos y esto servirá para que nadie más pueda utilizar el equipo sino es el responsable del mismo, ya que solicitará el password para volver a ingresar al escritorio.

Por sistema se negará el acceso a cambios en la configuración de conexiones. Se les solicitará que intercambien el password frecuentemente para seguir con los lineamientos que nos rigen en la Norma Internacional del ISO 9001.