**PRÁCTICA N°2**

**TEMA: “GESTIÓN DE POLÍTICAS Y PROTECCIÓN DE DATOS”**

**1. OBJETIVOS**

1.1 Configurar políticas de seguridad en Windows orientadas en permisos de usuario y longitud, complejidad, caducidad de contraseñas.

1.2 Implementar el cifrado de información en Windows utilizando herramientas nativas.

**5. INFORME**

***5.1 Explique en sus propias palabras la importancia de las políticas de seguridad y el cifrado de los datos.***

Las políticas de seguridad son importantes para centralizar y mantener una sola normativa dentro de la organización basándose en los estándares y marcos de seguridad. Estos estándares ayudan a mantener controles de accesos adecuados y seguros evitando dejar brechas de seguridad.

El cifrado de los datos permite cifrar la información contenida en el disco duro y sistema operativo de un dispositivo en el caso de robo o perdida del dispositivo no se filtre dicha información ya que esta puede ser información confidencial.

***5.2 Analizar las configuraciones realizadas en el Editor de Políticas y cifrado de datos.***

#### **Resultados de la configuración de las políticas de seguridad**

Después de configurar una política de seguridad en el sistema operativo Windows, en consecuencia, exige que las contraseñas deben tener un mínimo de 12 caracteres. Dicha política se implementó a través de las directivas de seguridad local (Local Security Policy), para garantizar que todas las nuevas contraseñas cumplan con los requisitos establecidos para fortalecer la seguridad en el ingreso a los sistemas.

Una vez implementada la política de seguridad, se intentó crear un nuevo usuario de nombre TIC y se introdujeron contraseñas que no cumplen los requisitos de longitud mínima como lo muestra la Figura 1.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figura 1: Contraseña que no cumplen los requisitos de longitud media

#### **Resultados de la Configuración del Cifrado de datos.**

Luego de la activación del cifrado BitLocker en la unidad del sistema operativo (Unidad C:).

Verificar que el cifrado este correctamente habilitado y cumpla con las políticas de seguridad configuradas, como se muestra en la Figura 2.

Las opciones presentes de administración como Suspender protección, Copia de seguridad de la clave de recuperación y Desactivar BitLocker, están disponibles, indicando que el cifrado se encuentra configurado correctamente.

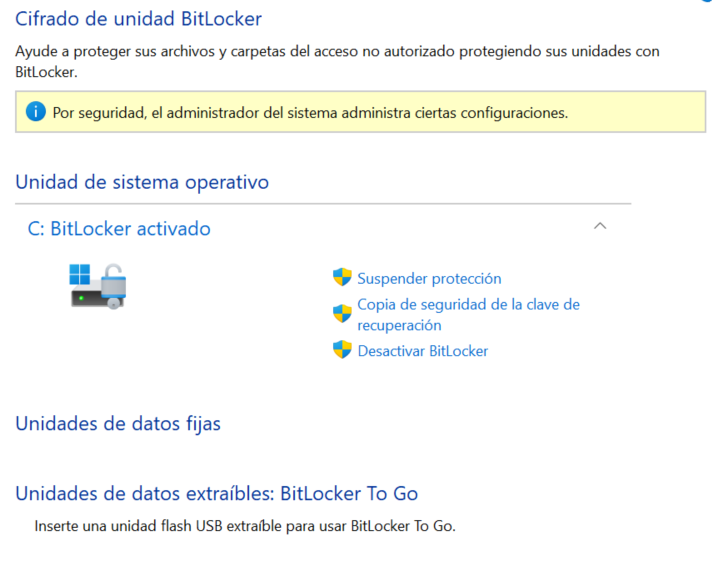


Figura 2: Estado de BitLocker

Comprobar el método de cifrado: Seleccionar una carpeta a proteger:

**Datos Personales**

**Clic Derecho** > **Propiedades** > **Opciones Avanzadas** > **Opción de Cifrar** **contenido para proteger datos** > **Aceptar** (Figura 3).

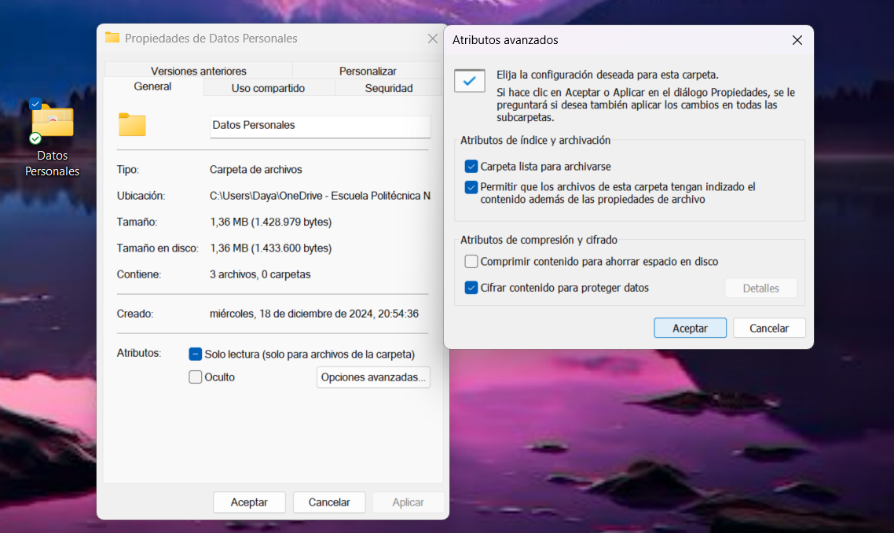


Figura 3.Cifrado de Carpeta

***5.3 Cual es el impacto de las políticas implementadas y el cifrado en la seguridad del sistema.***

Las políticas de seguridad tienen impacto en la seguridad de acceso como el control de la longitud de la contraseña, siendo esta más compleja para que sea descifrada por los hackers.

De esta manera se mantiene segura la información manteniendo un control de acceso al sistema por parte de lo usuarios y se puede identificar los accesos por fuera de la organización.