3.1 Preguntas sobre seguridad lógica

1. ¿Qué diferencia hay entre seguridad física y seguridad lógica? ¿ de qué se encarga cada una de ellas?

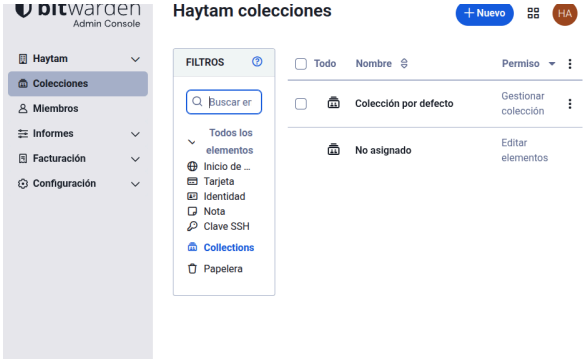
- La seguridad física protege el hardware.
- La seguridad lógica protege la información y el software.

2. Visualiza el siguiente vídeo sobre gestores de contraseñas e indica qué ventajas se mencionan en el mismo sobre el uso de gestores de contraseñas.

- Permite crear contraseñas seguras y únicas para cada cuenta.
- Evita tener que recordar muchas contraseñas.
- Autocompleta los inicios de sesión de forma segura.
- Sincroniza contraseñas entre varios dispositivos.
- Ayuda a detectar contraseñas débiles o duplicadas.
- Almacena de forma cifrada la información.

3. Investiga sobre una herramienta de gestión de contraseñas y describe de forma textual y gráfica cómo se utiliza. Para ello, instálala y realiza alguna prueba. Realiza capturas de pantalla que faciliten la comprensión del uso y utilidad de la herramienta.

- **Guardar contraseñas:** Te pregunta si deseas guardar tu contraseña.
- **Autocompletar:** Completa automáticamente el usuario y contraseña.
- **Generador de contraseñas seguras:** Te deja crear contraseñas aleatorias con letras, números y símbolos.



4. Define un diccionario de contraseñas acerca de un perfil de persona que te inventes. Define el nombre y apellidos de la persona, edad, año de nacimiento, idioma en el que habla, si tiene mascotas, o cualquier información que sería relevante para crear un diccionario de contraseñas para este perfil. A continuación, escribe al menos 10 contraseñas que formarían parte del diccionario de contraseñas de esta persona y justifica por qué.

Perfil:

- Nombre: José Nikolas Gutiérrez
- Edad: 18 años
- Año de nacimiento: 2006
- Idioma: Español
- Mascota: Su gato Lia
- Equipo favorito: FC Barcelona

- Color favorito: azul
- Ciudad: Málaga

Posibles contraseñas del diccionario:

- jose1997
- nikolas123
- barcelona97
- josegutierrez
- malaga2025
- azullia
- joseFCB
- miGatoLia
- jng1997
- viscaBarca

Justificación: Las contraseñas que he puesto tienen información personal y por eso son fáciles de adivinar y por eso no son tan seguras.

5. Indica cuáles son las normas básicas que deben seguirse en las políticas de creación de contraseñas. Invéntate una contraseña que tenga una fortaleza de seguridad elevada y explica por qué. Así mismo, invéntate una contraseña con seguridad débil e indica por qué lo es.

- Longitud mínima de 12 caracteres.
- Incluir mayúsculas, minúsculas, números y símbolos.
- No usar datos personales.
- No reutilizar contraseñas.
- Cambiarlas periódicamente o si hay sospecha de robo.
- Usar un gestor de contraseñas para almacenarlas.

Contraseñas seguras.

Ni2@ko-1561#

Es segura porque tiene como mínimo 12 caracteres e incluye números, mayúsculas, minúsculas, signos, etc, y eso lo hace difícil de adivinar.

Contraseña no segura.

Niko123456

No es segura porque contiene su información personal y números seguidos así se hace fácil de adivinar.