1. **Define el proceso de autentificación. (0,25pts) Qué dos principios de seguridad debe cumplir. (0,5pts) ¿Qué son las credenciales? (0,25pts**)
   Para acceder a un ordenador, por ejemplo, necesitaremos las credenciales que es el nombre del usuario, y la contraseña de ese usuario. Podemos añadir una barrera de seguridad encriptando el disco, en el cual existiría otra contraseña.

2. **Por qué no se debe abrir sesión como administrador para realizar tareas que no son de administración. (0,5 pts) ¿Existe alguna excepción? (0,25 pts)**
   Porque le estás dando permisos excesivos a una tarea que no las necesita. Eso puede llevar a una brecha de seguridad. Puedes tener un programa con algún malware que solo se ejecuta cuando abres el programa en modo de administración.

   Una excepción puede ser el administrador de una red de ordenadores de una empresa. Que tenga que acceder al ordenador de un trabajador y realizar tareas con el modo administrador.

3. **Qué debemos considerar para definir una buena política de contraseñas para el acceso al sistema informático. (1,5 ptos)**
   Deben ser contraseñas largas, de 15 caracteres, caracteres Unicode como”·$&?!, números, minúsculas y mayúsculas.

4. **¿Qué son los grupos de usuarios? (0,5 pts) Qué son las listas de control de acceso (ACL) (0,5 pts)**

   En una empresa, las ACL o en español Listas de Control de Acceso, son listas donde se define quién tiene permiso para acceder a un sistema u software.

5. **¿Qué es el “Predominio de la denegación”? (0,25 pts) Pon un ejemplo. (0,25 pts)**
   Es el poder que tiene un administrador para denegar el acceso a ciertos niveles a los usuarios.

6. **Qué es la "Herencia de permisos" y qué dos ventajas tiene. (0,75 pts**)
   Son los permisos que hereda un usuario al estar en un grupo. Por ejemplo, en la empresa tienen un grupo de Operadores de Copia de Seguridad, solo los usuario que formen parte de ese grupo podrán realizar copias de seguridad.

7. **En qué consisten los sistemas biométricos. (0,25 pts). Cuáles son sus principales características. (0,75)**
   Los sistemas biométricos son aquellos sistemas de seguridad donde las credenciales son partes de una persona, es decir, para desbloquear el teléfono móvil podemos poner el típico patrón de números o también añadir nuestra huella, eso es un sistema biométrico. También he visto que existen sensores biométricos para los ojos, pero los costes se elevaran.

8. **En qué consiste el sistema de autentificación de dibujo sobre patrones. (0,25 pts) Y dibujo sobre imágenes (0,25 pts)**
   El sistema de autentificación de patrones funciona guardando un patrón para cuando se acceda, si ambos patrones son idénticos, el usuario puede acceder.

9. **Por qué motivos las actualizaciones de software merecen especial atención para los administradores (0,5 pts). ¿Está práctica conlleva algún tipo de riesgo? (0,5 pts)**

   EL software siempre se debe de actualizar porque como mencionó el profesor en una clase, muchos de nosotros instalamos un software para una tarea en concreta y lo dejamos, ya sea porque pesa poco o lo pensamos usar de nuevo en el futuro. Pero el problema está en, si ese software deja de obtener soporte por el creador, se convierte en una brecha de seguridad. Se podría utilizar para colar un virus por el programa.

10. **Qué es una auditoria de seguridad (0,25 pts). Cuál debería ser el contenido mínimo de un informe, una auditoría de seguridad, definido como "Directrices para la auditoria de Sistemas de Gestión" (1,75 pts).**
    La auditoria de seguridad es un informe en el cual se recopilan varias normas de seguridad que se van a llevar a cabo.

    En las directrices para el sistema de gestión se debe tener los grupos y/o usuarios que podrán gestionar el sistema. Contraseñas seguras.