1. ¿Qué es seguridad?
    i. la ausencia de riesgos o peligros. Se trata de un concepto muy vinculado a la confianza y a la prevención, cuyo sentido estricto puede variar dependiendo del campo de los saberes humanos desde el cual se lo aborde.
2. ¿Qué es seguridad informática?
    i. La seguridad informática es una rama de la seguridad que se dedica a proteger los sistemas informáticos de amenazas externas e internas. Las amenazas externas son aquellas que provienen del entorno exterior en el que se encuentra el sistema como, por ejemplo: ataques informáticos, virus, robos de información, etc. Las amenazas internas son aquellas que provienen del propio sistema, como: errores humanos, exposición pública de credenciales, fallos o desactualizaciones en el software y fallos en el hardware, entre otros.
        a) Disponibilidad. Los sistemas deben permitir el acceso a la información cuando el usuario lo requiera, sin perder de vista la privacidad.
        b) Confidencialidad. La información solo debe ser accesible para las personas autorizadas.
        c) Integridad. Los sistemas deben garantizar la integridad de la información, sin errores ni modificaciones.
        d) Autenticación. La información que procede de un usuario debe verificarse para garantizar que es quien dice ser.
3. ¿Qué es la WEB?
    i. La web es una colección de páginas web interconectadas que contienen contenido como texto, imágenes, videos, enlaces y otros elementos multimedia. La accesibilidad y la facilidad de compartir información en la web han tenido un impacto significativo en la forma en que las personas obtienen conocimiento, se comunican y realizan actividades en línea.
4. ¿Qué es una app?
    i. Herramientas de Software, escritas en distintos lenguajes para teléfonos inteligentes o tablets, se caracterizan por ser útiles, dinámicas, fáciles de instalar y de manejar.
5. ¿Qué es una amenaza?
    i. Una amenaza es un fenómeno o proceso natural o causado por el ser humano que puede poner en peligro a un grupo de personas, sus cosas y su ambiente, cuando no son precavidos.
6. ¿Qué es un ataque?
    i. Se refiere a un acto deliberado de agresión, daño o intento de perjudicar a algo o alguien. Puede aplicarse en diversos contextos, como la seguridad cibernética, la seguridad personal, el ámbito militar y más. En cada caso, implica la intención de causar daño o afectar negativamente a un objetivo específico.
7. ¿Qué es un mecanismo?
    i. Es un conjunto organizado de componentes interrelacionados y en funcionamiento que trabaja de manera conjunta para lograr un propósito o efecto específico. Los mecanismos se encuentran en una amplia variedad de campos y disciplinas, desde la ingeniería y la física hasta la biología y la sociología. Estos sistemas organizados

pueden ser simples o complejos, pero todos tienen en común la idea de que sus partes interactúan de manera predecible para realizar una tarea o producir un resultado deseado.

8. ¿Qué es un servicio de seguridad?
    i. Se refiere a una serie de medidas, herramientas y técnicas diseñadas para proteger los sistemas, sitios web y aplicaciones contra amenazas cibernéticas y ataques maliciosos. Estos servicios se implementan para asegurar que la información confidencial, los datos de los usuarios y el funcionamiento general de las plataformas en línea estén resguardados de posibles vulnerabilidades y explotaciones.