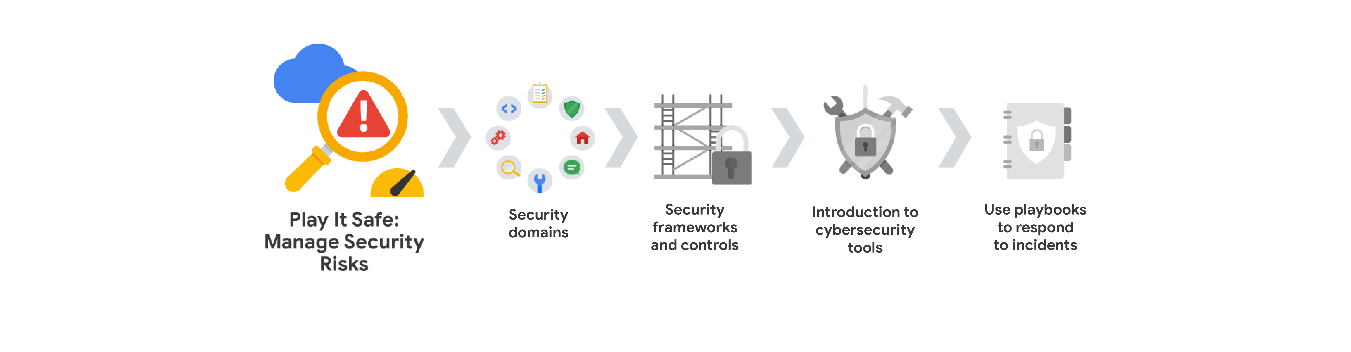
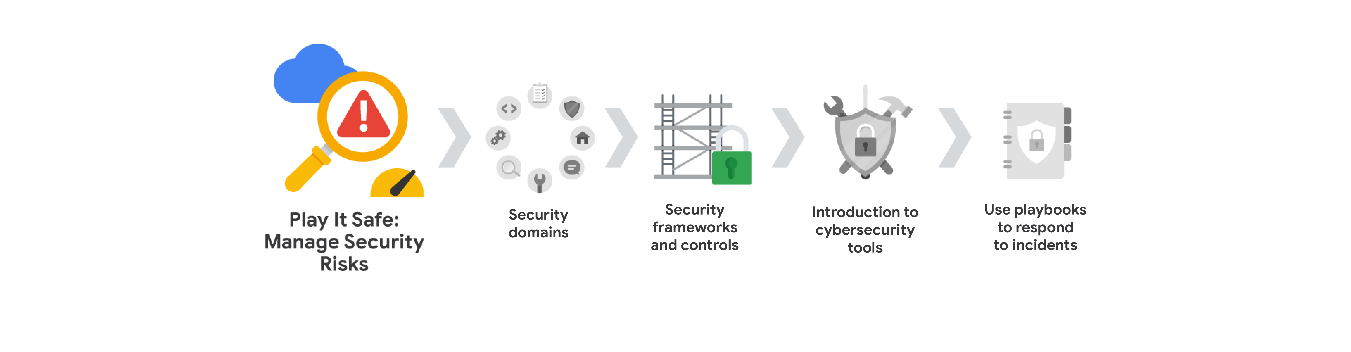
1. **Módulo 1: Dominios de Seguridad**



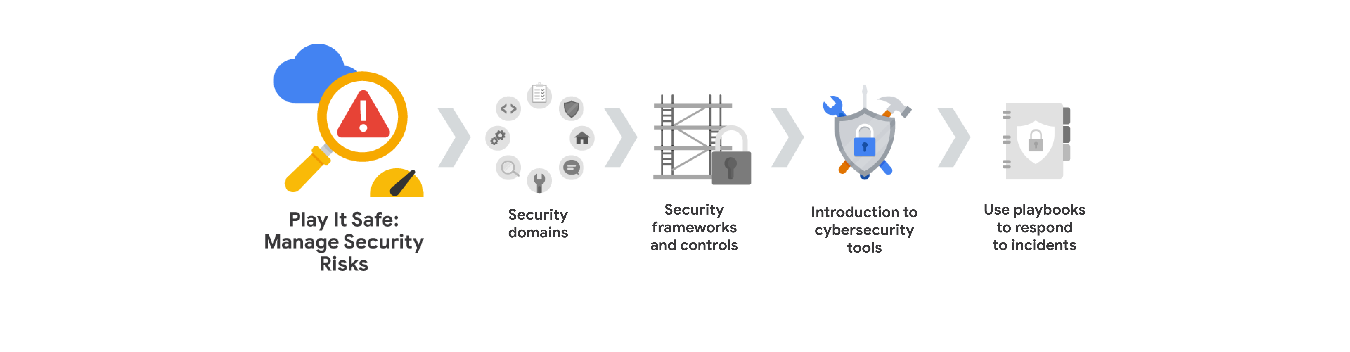
Conocerá los ocho dominios de Seguridad del CISSP. A continuación, conocerá las principales amenazas, riesgos y vulnerabilidades de las operaciones empresariales. Además, explorará el Framework de Gestión de Riesgos del Instituto Nacional de Estándares y Tecnología (NIST) y los pasos de la gestión de riesgos.

1. **Módulo 2: Marcos de seguridad y Controles**



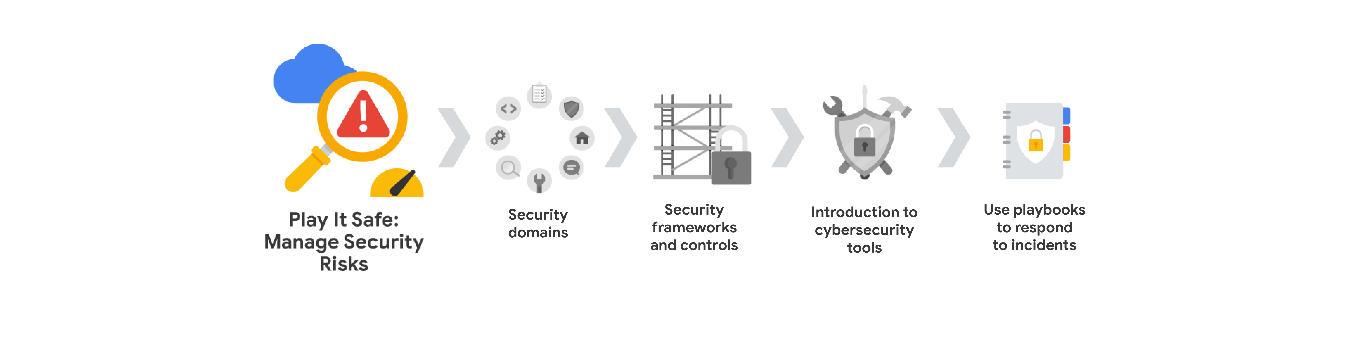
Se centrará en los marcos y controles de Seguridad, junto con los componentes básicos de la tríada Confidencialidad, integridad y disponibilidad (CID). Aprenderá sobre los principios de seguridad y las auditorías de seguridad del Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP).

1. **Módulo 3: Introducción a las herramientas de ciberseguridad**



Explorará las herramientas de gestión de información y eventos de seguridad (SIEM) líderes del sector que utilizan los profesionales de la seguridad para proteger las operaciones empresariales. Aprenderá cómo los analistas de seguridad de nivel básico utilizan los cuadros de mando SIEM como parte de su trabajo diario.

1. **Módulo 4: Utilizar manuales de estrategias para responder a incidentes**



Aprenderá sobre los propósitos y usos comunes de los manuales de estrategias. También explorará cómo los profesionales de la ciberseguridad utilizan los libros de jugadas para responder a las amenazas, riesgos y vulnerabilidades identificados.