1. Explica el concepto de ciberriesgo y su relación con otros conceptos como el de amenaza, vulnerabilidad, incidente de seguridad o pérdida económica.
2. ¿En qué consiste el apetito por el riesgo? ¿Y la tolerancia al riesgo? Pon un ejemplo en que se entiendan ambos conceptos.
3. ¿A qué nos referimos con el concepto de ciberriesgo inherente? ¿Y con el de residual? Pon un ejemplo en que se entiendan ambos conceptos.
4. Explica qué es la resiliencia, qué aspectos comprende y por qué es tan importante en la actualidad.
5. ¿Qué diferencias existen entre los riesgos operativos y los riesgos estratégicos? Pon un ejemplo que te sirva para explicarlas.
6. ¿Qué es el riesgo corporativo? ¿Cómo se gestiona? ¿Qué relación tiene con el ciberriesgo? Pon un ejemplo.
7. ¿Cuándo se considera que un riesgo lo es para la Seguridad Nacional? Menciona y explica tres ejemplos de ciberriesgos que afectan a la seguridad nacional en este momento.
8. ¿Qué diferencia hay entre una metodología para la gestión del riesgo, un estándar y un marco de trabajo (framework)? ¿En qué te basarías para escoger el más adecuado en cada caso o contexto?
9. ¿A qué nos referimos con el concepto de nivel de madurez de una organización, en relación con la ciberseguridad? ¿Qué relación tiene este nivel de madurez con un proceso de análisis y gestión del ciberriesgo?
10. ¿Qué es el NIST Cybersecurity Framework? Explica brevemente para qué y cómo se usa. ¿Qué ventajas tiene trabajar con niveles de madurez de este tipo?
11. ¿Qué semejanzas y similitudes encuentras entre los métodos cualitativos y cuantitativos para el análisis de ciberriesgo?
12. ¿Qué ventajas e inconvenientes tienen los métodos cualitativos y cuantitativos para el análisis del ciberriesgo? ¿En qué casos o contextos te parece más adecuado cada uno de ellos?
13. Menciona y explica brevemente los métodos y herramientas que suelen emplearse cuando se realiza análisis del ciberriesgo de manera cualitativa.
14. Menciona y explica brevemente los métodos y herramientas que suelen emplearse cuando se realiza análisis del ciberriesgo de manera cuantitativa.
15. Explica los pasos más importantes que se siguen para analizar el riesgo de manera cualitativa (sin centrarte en ninguna metodología en concreto) y cuáles son las entradas para el proceso y las salidas o resultados esperados. ¿Qué metodologías conoces de este tipo?
16. Explica los pasos más importantes que se siguen para analizar el riesgo de manera cuantitativa (sin centrarte en ninguna metodología en concreto) y cuáles son las entradas para el proceso y las salidas o resultados esperados. ¿Qué metodologías conoces de este tipo?
17. ¿Qué es FAIR? Explica brevemente para qué y cómo se usa. ¿Qué ventajas tiene trabajar con metodologías de este tipo “Value-at-risk” frente a las tradicionales, más cualitativas?
18. ¿Qué relación existe entre la simulación de Montecarlo y los procesos de análisis de riesgo? ¿Para qué se usa? Explícalo con un ejemplo sencillo.
19. ¿Por qué la distribución triangular y la lognormal suelen ser las más utilizadas en procesos de análisis de riesgos? ¿Cómo se usan?
20. Menciona y explica las diferentes fuentes de datos o información que se suelen utilizar en procesos de análisis de riesgos. ¿Cómo se pueden clasificar? Pon al menos un ejemplo de cada tipo de fuente de datos o información que menciones.

21. ¿Qué tres métodos se suelen emplear para la calibración de la probabilidad en procesos de análisis de riesgos? Explícalos brevemente mencionando sus ventajas e inconvenientes.
22. ¿Qué relación existe entre el teorema de Bayes y los procesos de análisis de riesgo? ¿Para qué se usa? Explícalo con un ejemplo sencillo.
23. ¿Qué relación existe entre la distribución Beta y los procesos de análisis de riesgo? ¿Para qué se usa? Explícalo con un ejemplo sencillo.
24. Explica qué es un IoC, un IoA y un KRI. Pon un ejemplo de cada uno de ellos si lo que nos preocupa es el riesgo de una infección por ransomware. ¿Y si nos preocupa una denegación de servicio?
25. ¿Qué relación existe entre el método de Root Cause Analysis y los procesos de análisis de riesgo? ¿Para qué se usa? Explícalo con un ejemplo sencillo.
26. ¿Qué relación existe entre el proceso de modelado de amenazas y los procesos de análisis de riesgo? ¿Para qué se usa? Explícalo con un ejemplo sencillo.
27. ¿Qué relación existe entre los procesos de ciberinteligencia (o inteligencia de amenazas) y los procesos de análisis de riesgo? ¿Para qué se usa? Explícalo con un ejemplo sencillo.
28. ¿Por qué los procesos de análisis de riesgos para la ciberseguridad no se pueden aplicar directamente a los riesgos para la privacidad o la protección de datos? ¿Qué limitaciones tienen?
29. ¿Qué es una evaluación de impacto para la protección de datos? Explica los pasos que se siguen para realizar una y qué resultados se deberían conseguir. ¿Por qué son necesarias?
30. ¿Los procesos de análisis de riesgos para la ciberseguridad se pueden realizar con las metodologías tradicionales cuando se utilizan paradigmas como cloud, IoT, blockchain, etc.? ¿Por qué? ¿Qué pasos hay que seguir para poder hacerlo?
31. ¿Qué estrategias conoces para la gestión del ciberriesgo? Explícalas y pon un ejemplo de cómo se aplicarían en un escenario de brecha de datos.
32. ¿Qué es un Programa de Ciberseguridad y cuál es su objetivo? ¿Qué información hay que tener en cuenta para proponer uno? ¿Qué estructura/información debería contener?
33. ¿Qué es un Plan Director de Seguridad y cuál es su objetivo? ¿cuál es su relación con el Programa de Ciberseguridad?
34. ¿Qué maneras de priorizar mitigaciones conoces? Explícalas y pon un ejemplo de cómo se aplicarían en una empresa en la que preocupan las infecciones por ransomware, las brechas de datos, las suplantaciones de identidad y las denegaciones de servicio.
35. ¿Qué es el ROI de una inversión en ciberseguridad? ¿Cómo se pueden tener en cuenta aspectos económicos como estos en la gestión del ciberriesgo? Pon un ejemplo concreto.
36. ¿Qué es el TDR ó Technical Debt Ratio en relación con la ciberseguridad? ¿Cómo se pueden tener en cuenta en la gestión del ciberriesgo? Pon un ejemplo concreto.
37. ¿A qué nos referimos en ciberseguridad con el concepto de “cisne negro”? ¿Qué estrategia suele seguirse para gestionar este tipo de riesgos y por qué? Pon un ejemplo.
38. ¿Qué relación hay entre las SLAs y la gestión del ciberriesgo? ¿Qué aspectos son importantes para definir, negociar y firmar una SLA adecuada?
39. ¿Qué relación hay entre las ciberpólizas y la gestión del ciberriesgo? ¿Qué aspectos son importantes para contratar una ciberpóliza adecuada para cada caso o contexto?
40. ¿Qué tipo de tareas suele realizar hoy en día un director de seguridad? ¿Qué aspectos son más importantes para que realice estas tareas con calidad suficiente?