

Modelos de Madurez en ciberseguridad

¡Agente Ciber!

El Consejo Internacional de Seguridad ha detectado brechas en organizaciones aliadas. Tu misión será evaluar el nivel de madurez cibernética de estas entidades, identificar debilidades y recomendar acciones estratégicas.

Debes demostrar conocimiento en Modelos de Madurez en Ciberseguridad y Dominios/Niveles del C2M2 (de Madurez de Capacidades de Ciberseguridad).

Tiempo límite: 40 minutos

Modalidad: Individual.



Fases de la Operación:

⭐ Fase 1: Reconocimiento de Modelos (3 preguntas)

- 1. ¿Qué modelo de madurez clasifica capacidades de seguridad desde nivel 0 (incompleto) hasta nivel 3 (optimizado)?**
 - a) C2M2 (Modelo de Madurez de Capacidades de Ciberseguridad)
 - b) NIST SP 800-53 (Guía de Controles de Seguridad del NIST)
 - c) CMMC (Certificación del Modelo de Madurez de Ciberseguridad)
 - d) COBIT (Control Objectives for Information and Related Technologies – Objetivos de Control para Información y Tecnologías Relacionadas)

- 2. ¿Qué modelo se enfoca especialmente en evaluar la madurez de contratistas de defensa en EE.UU.?**
 - a) C2M2
 - b) ISO 27001
 - c) CMMC
 - d) NIST CSF

- 3. En ISO 27001, el enfoque principal es:**
 - a) Lograr mejoras rápidas en la cultura organizacional.
 - b) Certificar la gestión de seguridad de la información.
 - c) Supervisar vulnerabilidades de terceros.
 - d) Automatizar respuestas ante incidentes.

⚠️ Fase 2: Diagnóstico de Situaciones (7 preguntas)

Caso breve: TECHSOLUTIONS S.A.S. no actualiza inventario de activos, no gestiona cambios formales y usuarios instalan software libremente.

4. ¿Dominio afectado principalmente?

- a) SA (Conciencia Situacional)
- b) ACCM (Gestión de Activos, Cambios y Configuraciones)
- c) ARCH (Arquitectura de ciberseguridad)
- d) IAM (Gestión de Identidades y Accesos)

5. Nivel de madurez actual:

- a) 0
- b) 1
- c) 2
- d) 3

6. Prioridad más urgente:

- a) Capacitar en manejo de incidentes.
 - b) Establecer un inventario formal de activos.
 - c) Implementar inteligencia de amenazas.
 - d) Crear una VPN.
-

Caso breve: GRUPO ALPHANET actúa solo tras incidentes, no gestiona riesgos formalmente.

7. Dominio involucrado:

- a) TVM (Gestión de Amenazas y Vulnerabilidades)
- b) CRMG (Gestión de Riesgos Cibernéticos y Gobernanza)
- c) IR (Respuesta ante Incidentes)
- d) WM (Gestión del Personal)

8. Nivel de madurez actual:

- a) 0
 - b) 1
 - c) 2
 - d) 3
-

Caso breve: SEGURITECH ejecuta análisis de vulnerabilidades diarios y correlaciona amenazas.

9. Dominio evaluado:

- a) TVM (Gestión de Amenazas y Vulnerabilidades)
- b) SA (Conciencia Situacional)
- c) SCED (Gestión de la Cadena de Suministro y Dependencias Externas)
- d) ARCH (Arquitectura de ciberseguridad)

10. Nivel de madurez actual:

- a) 0
- b) 1

- c) 2
 - d) 3
-

 **Fase 3: Dominio Maestro C2M2 (5 preguntas)**

11. El dominio que gestiona autenticaciones, roles y permisos es:

- a) SCED (Gestión de la cadena de suministros y dependencias externas)
- b) IAM (Gestión de identidad y accesos)
- c) ARCH (Arquitectura de ciberseguridad)
- d) IR (Respuesta a incidentes y continuidad de operaciones)

12. Si una empresa documenta su arquitectura tecnológica y la revisa antes de desplegar servicios, pero no la alinea aún con el negocio, ¿en qué nivel estaría en ARCH?

- a) 1
- b) 2
- c) 3
- d) 0

13. Un dominio que mide la capacidad de detectar amenazas en tiempo real sería:

- a) SA (Conciencia situacional)
- b) TVM (Gestión de amenazas y vulnerabilidades)
- c) RM (Gestión de riesgos)
- d) WM (Gestión del talento humano)

14. Si una organización establece programas de concientización y evalúa desempeño del personal, ¿qué dominio fortalece principalmente?

- a) ARCH (Arquitectura de ciberseguridad)
- b) SCED (Gestión de la cadena de suministros y dependencias externas)
- c) WM (Gestión del talento humano)
- d) SA (Conciencia situacional)

15. El dominio que implica formalizar la respuesta a incidentes y realizar simulacros es:

- a) IR (Respuesta a incidentes y continuidad de operaciones)
- b) CPM (Gestión del Programa de Ciberseguridad)
- c) SA (Conciencia situacional)
- d) SCED (Gestión de la cadena de suministros y dependencias externas)