

## **El modelo de madurez de ciberseguridad C2M2**

Ramón Segarra Clara

BDM CCTV en VISIOTECH. Ing. de Telecomunicación y máster en Ciberseguridad, Director Seguridad. Miembro de la Junta Directiva de la Asocia. Valenciana de Ing. de Telecom (AVIT) y Vocal Presidente de ADISPO C. Valenciana

Fecha de publicación: 16 jun 2024

Fuente: <https://es.linkedin.com/pulse/el-modelo-de-madurez-ciberseguridad-c2m2-ram%C3%B3n-segarra-clara-ri2of>

El modelo de madurez de ciberseguridad C2M2 es un marco integral para evaluar y mejorar las capacidades de ciberseguridad en organizaciones que administran sistemas de infraestructura crítica. En este artículo, se detallará el origen, uso y cada uno de los niveles del modelo, así como los dominios, además, se proporcionará una guía paso a paso sobre cómo usar el C2M2 para realizar una auditoría de ciberseguridad de una infraestructura crítica.

### **Origen y uso del modelo de madurez de ciberseguridad C2M2**

El modelo C2M2 fue desarrollado a través de una colaboración esfuerzo entre organizaciones del sector público y privado, patrocinado por Estados Unidos Departamento de Energía (DOE), el Consejo Coordinador del Subsector Eléctrico (ESCC) y el Consejo Coordinador del Subsector Petróleo y Gas Natural (ONG SCC). Su objetivo es proporcionar un enfoque estructurado e integral para evaluar y mejorar las capacidades de ciberseguridad en organizaciones. El modelo consta de cinco niveles de madurez, cada uno de los cuales refleja un nivel creciente de madurez en ciberseguridad.

### **Niveles de madurez del modelo C2M2**

Los niveles de madurez del modelo C2M2 son:

1. Inicial: Las organizaciones en este nivel tienen un enfoque ad hoc de la ciberseguridad y carecen de procesos formalizados para gestionar los riesgos de la ciberseguridad.
2. Administrado: Las organizaciones en este nivel han establecido controles básicos de ciberseguridad, pero estos controles no están integrados en sus procesos comerciales generales.
3. Definido: Las organizaciones en este nivel tienen un programa de ciberseguridad formalizado y documentado que está integrado en sus procesos comerciales.
4. Medido: Las organizaciones en este nivel han establecido métricas y medidas para rastrear la efectividad de su programa de seguridad cibernética.
5. Optimizado: Las organizaciones en este nivel mejoran continuamente su programa de ciberseguridad al incorporar comentarios y refinar sus procesos.

## **Dominios del modelo C2M2**

El modelo C2M2 se divide en 10 grandes dominios que evalúan diferentes aspectos de la ciberseguridad:

1. Gestión de activos: Evalúa cómo las organizaciones gestionan y controlan sus activos IT y OT.
2. Gestión de amenazas: Evalúa cómo las organizaciones identifican y mitigan las amenazas cibernéticas.
3. Gestión de riesgos: Evalúa cómo las organizaciones identifican y gestionan los riesgos de seguridad cibernética.
4. Gestión de incidentes: Evalúa cómo las organizaciones manejan y resuelven incidentes de seguridad cibernética.
5. Gestión de vulnerabilidades: Evalúa cómo las organizaciones identifican y mitigan vulnerabilidades en sus sistemas.
6. Gestión de seguridad de la información: Evalúa cómo las organizaciones protegen y manejan la información confidencial.
7. Gestión de la cadena de custodia: Evalúa cómo las organizaciones manejan y controlan la cadena de custodia de la información.
8. Gestión de la configuración de seguridad: Evalúa cómo las organizaciones configuran y manejan sus sistemas para garantizar la seguridad.
9. Gestión de la concienciación y formación: Evalúa cómo las organizaciones conciencian y forman a su personal sobre la importancia de la seguridad cibernética.
10. Gestión de la supervisión y revisión: Evalúa cómo las organizaciones supervisan y revisan sus procesos y políticas de seguridad cibernética.

## **Propuesta de uso del modelo de madurez de ciberseguridad C2M2 para realizar una auditoría de ciberseguridad**

Para realizar una auditoría de ciberseguridad con el modelo C2M2, es recomendable seguir los siguientes pasos:

1. Planificación y Preparación: Definir el alcance de la auditoría. Reunir información relevante, como políticas de seguridad, diagramas de red y registros de configuración. Entrevistar a personal clave para entender los procedimientos y prácticas actuales. Establecer un equipo de auditoría compuesto por auditores internos o externos con experiencia en ciberseguridad.
2. Evaluación de Riesgos: Identificar activos críticos y evaluar su importancia y el impacto potencial de una brecha de seguridad. Identificar amenazas y vulnerabilidades utilizando herramientas de escaneo de vulnerabilidades y análisis de amenazas. Evaluar los programas de formación en ciberseguridad para el personal y verificar la efectividad de la concienciación sobre las amenazas de seguridad.
3. Evaluación del Modelo C2M2: Utilizar la herramienta de autoevaluación del modelo C2M2 para evaluar las capacidades de ciberseguridad de la organización. Identificar áreas de mejora y priorizar las acciones necesarias para mejorar la madurez en ciberseguridad.

4. Informe de Auditoría y Recomendaciones: Crear un informe detallado que describa las vulnerabilidades y debilidades encontradas. Proporcionar recomendaciones específicas para mitigar los riesgos identificados. Desarrollar un plan de acción para implementar las recomendaciones.
5. Seguimiento y Revisión Continua: Supervisar la implementación de las recomendaciones y asegurarse de que se completen correctamente. Programar auditorías de ciberseguridad periódicas para asegurar una mejora continua.

**Tabla de recursos del modelo de madurez de ciberseguridad C2M2**

Recurso	Descripción
<a href="#">Self-Evaluation Guide</a>	Guía para planificar y facilitar un taller de evaluación de ciberseguridad con participantes clave en la organización.
<a href="#">Self-Evaluation Workshop Kickoff Presentation</a>	Presentación para apoyar la planificación de un taller de evaluación de ciberseguridad.
<a href="#">HTML-based Tool User Guide</a>	Guía paso a paso para utilizar la herramienta de evaluación de ciberseguridad en formato HTML.
<a href="#">PDF-based Tool User Guide</a>	Guía paso a paso para utilizar la herramienta de evaluación de ciberseguridad en formato PDF.
<a href="#">C2M2 Model Practices (Excel file)</a>	Archivo de prácticas de ciberseguridad del C2M2 en formato de hoja de cálculo.
<a href="#">C2M2 Overview Presentation</a>	Presentación que introduce el modelo C2M2 a los decisores clave.
<a href="#">Self-Evaluation Cheat Sheet</a>	Guía de referencia en formato de placemat para participantes durante una evaluación de ciberseguridad.
<a href="#">C2M2 to CSF Mappings</a>	Mapeos bidireccionales entre el Marco de Seguridad de la Información de NIST (V1.1) y las prácticas del C2M2 (V2.1 y V2.0), que demuestran una fuerte alineación entre los marcos.
<a href="#">C2M2 Legacy Mapping: V1.1 to V2.1</a>	Mapeo de prácticas del modelo V1.1 a V2.1 para ayudar en la actualización de las evaluaciones.
<a href="#">C2M2 Legacy Mapping: V2.0 to V2.1</a>	Mapeo de prácticas del modelo V2.0 a V2.1 para ayudar en la actualización de las evaluaciones.
<a href="#">C2M2-CMMC Supplemental Guidance</a>	Orientación adicional para usuarios del C2M2 sujetos a la Certificación de Madurez de Seguridad de la Defensa (CMMC).
<b>Sample Threat Profile (No disponible actualmente)</b>	Ejemplo de perfil de amenazas de una organización, referenciado por varias prácticas del C2M2.