1- Modelo C2M2 Gestión de Activos, Cambios y Configuraciones (ACCM)

Este dominio se enfoca en asegurar que una organización identifique, controle y gestione adecuadamente sus activos tecnológicos (hardware, software, datos, etc.), así como los cambios y configuraciones asociados. Esto garantiza que los activos críticos estén protegidos, se mantengan actualizados y se minimicen los riesgos operativos o de seguridad por configuraciones incorrectas o no autorizadas.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No hay una gestión definida de activos o configuraciones. No se lleva inventario ni se controlan los cambios.	Se manejan activos y cambios de forma reactiva, sin procedimientos formales	Hay procesos definidos para identificar, registrar y controlar activos y cambios	Los procesos están integrados y automatizados. Se monitorean cambios y configuraciones continuamente

Escenario: Caso de la empresa TECNOSOLUTIONS S.A.S.

TECNOSOLUTIONS es una empresa mediana en Colombia dedicada al desarrollo de software. Cuenta con 45 empleados, la mayoría ingenieros y diseñadores. Sus oficinas están en Medellín, y también tienen personal trabajando desde casa.

Estas son algunas de las prácticas actuales en cuanto a gestión de activos, cambios y configuraciones:

- No existe una herramienta formal para registrar los equipos, pero el área de TI lleva un Excel con la lista de computadores y licencias. A veces olvidan actualizarlo.
- Algunos empleados han instalado programas no autorizados en sus equipos, como editores de video y juegos.
- Cuando hay que hacer una actualización importante, el técnico de TI avisa por correo y cada empleado la hace cuando puede.
- No hay una política definida sobre cómo debe configurarse un equipo nuevo o cómo reportar cambios.
- Cuando se daña un equipo, el técnico lo reemplaza, pero no se guarda registro del cambio ni del contenido antiguo.
- Una vez se perdió un portátil con información importante de un cliente. No tenía cifrado ni contraseña segura.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra TECNOSOLUTIONS.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

2- Modelo C2M2 Gestión de Riesgos Cibernéticos (CRMG)

Este dominio se centra en **identificar, evaluar, priorizar y responder a los riesgos cibernéticos** que pueden afectar a la organización.
Una buena gestión de riesgos permite **tomar decisiones informadas**, proteger los activos críticos y **reducir la probabilidad e impacto** de incidentes de seguridad..

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No hay identificación ni gestión formal de riesgos cibernéticos	Se reconocen algunos riesgos, pero no se evalúan ni se documentan de forma estructurad	Se identifican y evalúan riesgos regularmente con métodos definidos.	La gestión de riesgos es continua y se integra en la toma de decisiones.

Escenario: Caso de la empresa GRUPO ALPHANET S.A.S

GRUPO ALPHANET es una empresa colombiana que ofrece servicios de conectividad y alojamiento web. Tiene presencia en varias ciudades y más de 80 empleados. Estas son algunas de sus prácticas actuales en gestión de riesgos cibernéticos:

- No cuentan con una política formal para evaluar riesgos tecnológicos.
- Solo actúan cuando ocurre un incidente grave (como caídas del servidor o hackeos).
- El área de seguridad hace recomendaciones, pero no hay una metodología clara para priorizar.
- El gerente de TI decide con base en su experiencia, sin análisis documentados.
- Han tenido fugas de datos y no han hecho análisis forense.
- No capacitan al personal en temas de riesgos digitales ni prevención de incidentes

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra GRUPO ALPHANET.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

3- Modelo C2M2 Gestión de Amenazas y Vulnerabilidades (TVM)

Este dominio se centra en identificar, evaluar, monitorear y mitigar **amenazas y vulnerabilidades** en los sistemas de información.
La gestión efectiva de vulnerabilidades permite prevenir ataques antes de que ocurran, manteniendo los sistemas seguros, actualizados y protegidos contra amenazas internas y externas. Una organización madura en este dominio tiene procesos automatizados para descubrir fallos, evaluarlos y solucionarlos a tiempo.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No se identifican ni se gestionan amenazas o vulnerabilidades.	Se gestionan vulnerabilidades solo cuando ocurre un incidente o tras una alerta crítica.	Se realizan análisis de vulnerabilidades periódicamente y se aplican parches según cronograma.	El monitoreo de vulnerabilidades es continuo y automatizado. Se correlacionan amenazas y riesgos para tomar decisiones estratégicas.

Escenario: SEGURITECH S.A.S. es una empresa especializada en soluciones de ciberseguridad para entidades gubernamentales y bancarias. Tiene un equipo dedicado a ciberinteligencia y prevención de amenazas.

Prácticas actuales en el dominio TVM:

- Ejecutan análisis de vulnerabilidades en todos sus sistemas diariamente mediante herramientas automáticas.
- Utilizan plataformas SIEM y threat intelligence para correlacionar vulnerabilidades con amenazas emergentes.
- Tienen alertas automáticas y flujos de trabajo predefinidos para priorizar y aplicar parches.
- El equipo de seguridad analiza tendencias y comparte boletines internos con recomendaciones preventivas
- Se realiza ciberinteligencia proactiva para identificar amenazas antes de que afecten a la organización o sus clientes.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra SEGURITECH S.A.S.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

4- Modelo C2M2 Arquitectura de Seguridad Cibernética (ARCH)

Este dominio se enfoca en **diseñar, desarrollar y mantener una arquitectura de seguridad** que proteja los sistemas, redes y datos de una organización.
Incluye la definición de principios, patrones, componentes y controles técnicos que permiten construir entornos tecnológicos seguros y resilientes. Una arquitectura bien definida ayuda a reducir vulnerabilidades desde el diseño, integrar controles de seguridad y asegurar el crecimiento ordenado de la infraestructura.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No existe una arquitectura de seguridad definida ni documentación técnica sobre protección estructural.	Existen controles técnicos básicos, pero sin una arquitectura formal o estandarizada.	Hay una arquitectura definida y documentada, alineada con requisitos de seguridad.	La arquitectura de seguridad es robusta, dinámica, alineada con los objetivos del negocio y con una mejora continua.

Escenario: NETWARE SYSTEMS S.A.S. Es una empresa de desarrollo de soluciones web para empresas de logística. En los últimos años ha mejorado su enfoque hacia la seguridad, especialmente en su arquitectura tecnológica.

Prácticas actuales en el dominio ARCH:

• Tiene una arquitectura de seguridad documentada, con componentes claramente definidos para aplicaciones, redes y bases de datos.

- Aplica patrones de diseño seguro recomendados por el OWASP y otras buenas prácticas.
- Los arquitectos de sistemas revisan las configuraciones antes de desplegar cualquier nuevo servicio.
- Aún no han integrado completamente sus decisiones de arquitectura con los objetivos del negocio.
- La documentación se actualiza solo cuando hay cambios importantes, no de forma continua.
- Existe colaboración entre los equipos de infraestructura y desarrollo, pero no siempre se alinea con una estrategia global.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra NETWARE SYSTEMS S.A.S.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

5- Modelo C2M2 Gestión de Identidades y Accesos (IAM)

Este dominio se enfoca en **asegurar que solo las personas correctas accedan a los recursos adecuados, en el momento correcto y con los permisos necesarios**. Gestionar identidades y accesos incluye autenticar usuarios, definir roles, controlar privilegios y registrar accesos.
Una buena gestión IAM protege los sistemas contra accesos no autorizados y reduce el riesgo de abuso de privilegios.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No se controlan los accesos ni se identifican los usuarios de forma adecuada.	Existen controles básicos, como contraseñas o permisos manuales, pero no hay procesos estandarizados.	Se definen políticas de acceso, se gestionan cuentas y privilegios con procedimientos formales.	IAM está integrado con autenticación multifactor, gestión de sesiones, revisiones periódicas y eliminación automática de accesos no vigentes.

Escenario: CONSULTINGAPP LTDA. Es una empresa emergente dedicada al desarrollo de software para gestión documental en pequeñas y medianas empresas.

Estas son sus prácticas actuales relacionadas con IAM:

• Cada empleado tiene una cuenta de usuario personal con contraseña, pero no usan autenticación multifactor.

- La asignación de permisos se realiza manualmente por el equipo de TI, sin un proceso definido por roles.
- Cuando un empleado cambia de área o se retira, el acceso se revoca de manera manual, aunque a veces con retraso.
- No se llevan registros centralizados ni auditorías periódicas sobre los accesos.
- Los permisos suelen ser los mismos para todos los desarrolladores, sin diferenciación por funciones específicas.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra CONSULTINGAPP LTDA.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

6- Modelo C2M2 Conciencia Situacional (SA)

Este dominio se encarga de **observar, identificar y entender eventos relevantes para la ciberseguridad**, como actividades sospechosas, amenazas o incidentes, en tiempo real o casi real. La conciencia situacional permite a la organización reaccionar rápidamente ante posibles riesgos y mantener un entorno seguro. Tener buena conciencia situacional significa monitorear los sistemas, correlacionar datos de eventos, y aprender de ellos para prevenir futuros ataques.

.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No se monitorean los sistemas ni se detectan eventos de seguridad de forma sistemática.	Se monitorean algunos sistemas de forma básica. Se revisan registros solo si ocurre un incidente.	Hay monitoreo continuo con herramientas definidas. Se recopilan datos de múltiples fuentes y se revisan regularmente.	Se cuenta con conciencia situacional avanzada y automatizada. Se analiza el comportamiento de los sistemas y se anticipan riesgos.

Escenario: INNOVALINK S.A.S. Es una pequeña empresa que presta servicios de mantenimiento tecnológico y redes a instituciones educativas.

Estado actual del dominio SA:

- No tienen herramientas de monitoreo ni registros centralizados de actividades.
- Solo se dan cuenta de fallos o ciberataques cuando los sistemas ya están caídos o los usuarios se quejan.
- No hay responsables de ciberseguridad, ni se realiza seguimiento de accesos, configuraciones o eventos.
- En un reciente ataque de ransomware, la empresa no supo en qué momento ni cómo se originó el problema.
- Los técnicos revisan los equipos manualmente, sin soporte de alertas ni de datos en tiempo real.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra INNOVALINK S.A.S.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

7- Modelo C2M2 Respuesta ante Incidentes (IR)

Este dominio se enfoca en **preparar, detectar, responder y recuperarse de los incidentes de ciberseguridad** que afectan la organización. Contar con un proceso de respuesta ante incidentes bien definido ayuda a minimizar el impacto de los ataques, recuperar operaciones rápidamente y aprender de lo sucedido para evitar que se repita.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No hay procedimientos para manejar incidentes. Se actúa de manera improvisada.	Se reconoce la necesidad de responder a incidentes, pero solo existen respuestas reactivas básicas.	Existe un plan documentado de respuesta a incidentes, con roles definidos y pasos a seguir.	Se mejora continuamente el proceso de respuesta. Se realizan simulacros, análisis post-incidente y coordinación con terceros.

Escenario: DATAINNOVO S.A.S. Es una empresa mediana que gestiona información de usuarios para servicios en la nube. Ha estado fortaleciendo sus procesos de ciberseguridad en los últimos años.

Esto es lo que actualmente realiza respecto al dominio IR:

- Cuenta con un plan formal de respuesta ante incidentes, aprobado por la gerencia.
- Tiene un equipo de respuesta conformado por personal de TI con roles definidos.
- El equipo sigue un procedimiento paso a paso para **identificar, contener, erradicar y reportar incidentes**.
- La empresa no realiza **simulacros periódicos** ni pruebas del plan.
- El aprendizaje de incidentes anteriores no siempre se documenta ni se incorpora como mejora del plan.
- No existe una coordinación activa con otras entidades o autoridades en caso de incidentes graves.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra DATAINNOVO S.A.S.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

8- Modelo C2M2 Gestión de la Cadena de Suministro y Dependencias Externas (SCED)

Este dominio se enfoca en **gestionar los riesgos de ciberseguridad relacionados con proveedores, socios, contratistas y otras dependencias externas**. Esto incluye asegurar que los terceros cumplan con requisitos de seguridad y que su relación con la empresa no introduzca vulnerabilidades.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No se consideran riesgos de ciberseguridad en la cadena de suministro.	Se reconocen algunos riesgos, pero no hay procesos definidos ni contratos formales con requisitos de seguridad.	Se evalúan riesgos de seguridad antes de contratar y se incluyen requisitos en contratos con terceros.	Se monitorean continuamente los proveedores y se revisan los contratos con regularidad. Hay gestión activa de dependencias.

Escenario: INNOVARED S.A.S. Es una empresa de telecomunicaciones con 10 años de experiencia en el mercado.

Esto es lo que realiza actualmente en el dominio SCED:

• Evalúa exhaustivamente a sus proveedores antes de contratarlos (aspectos técnicos y legales de ciberseguridad).

- Los contratos con terceros incluyen **requisitos específicos de ciberseguridad**, auditorías y planes de respuesta ante incidentes.
- Revisa periódicamente las relaciones con terceros para evaluar cumplimiento y realizar mejoras.
- Monitorea de forma continua las integraciones externas, como servicios en la nube o software de terceros.
- Cuenta con un plan para **gestionar interrupciones o riesgos provenientes de terceros**.
- Realiza talleres de sensibilización conjunta con proveedores clave.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra INNOVARED S.A.S.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

9- Modelo C2M2 Gestión de Personal (WM – Workforce Management)

Este dominio se centra en asegurar que la organización cuente con el **personal adecuado, competente y capacitado** para operar, gestionar y mejorar sus capacidades de ciberseguridad. Incluye actividades como la formación continua, evaluación de habilidades y retención de talento.

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No hay políticas ni programas de gestión de personal enfocados en ciberseguridad.	Se identifica la necesidad de contar con talento, pero la selección y formación es reactiva o limitada.	Existen políticas básicas para contratación, formación y evaluación del personal en temas de ciberseguridad.	Hay un programa formal de desarrollo del talento, planes de carrera, retención y mejora continua.

Escenario: DATASERVICES ANDINA. Es una empresa que brinda soluciones de análisis de datos y almacenamiento en la nube con 3 años de experiencia en el mercado.

.

Esto es lo que hacen en el dominio WM:

- Cuentan con perfiles definidos para roles técnicos y de ciberseguridad.
- Realizan **capacitaciones básicas** en seguridad informática al personal técnico dos veces al año.
- Evalúan el desempeño del personal, incluyendo criterios relacionados con prácticas seguras.
- Implementaron una herramienta interna para pruebas de conocimientos básicos en ciberseguridad.
- Los nuevos empleados reciben una **inducción con aspectos clave de seguridad digital**.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra DATASERVICES ANDINA.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.

10- Modelo C2M2 Gestión del Programa de Ciberseguridad (CPM)

Este dominio se enfoca en **establecer y mantener un programa de ciberseguridad** que esté alineado con los objetivos estratégicos de la organización. Incluye políticas, gobernanza, liderazgo, planificación y mejora continua del programa de seguridad..

🔴 Nivel 0	🟡 Nivel 1	🟠 Nivel 2	🟢 Nivel 3
No existe un programa de ciberseguridad formal. Las acciones de seguridad son reactivas y aisladas.	Se reconoce la necesidad de seguridad, pero no hay una estructura organizada ni liderazgo definido.	Hay un programa formal, con responsables designados y planes de acción periódicos.	El programa está alineado con los objetivos del negocio, tiene mejora continua y seguimiento estratégico.

Escenario: NOVABANK DIGITAL es una entidad financiera 100% digital con operación en Latinoamérica.

Esto es lo que hacen en el dominio CPM:

- El programa de ciberseguridad está alineado con la visión estratégica del negocio y forma parte del plan corporativo.
- Cuenta con un CISO (Chief Information Security Officer) que reporta directamente al comité ejecutivo.
- Se aplican indicadores clave de rendimiento (KPIs) para evaluar la efectividad del programa.
- Se realiza **mejora continua**, con auditorías internas, retroalimentación y adaptación constante.
- La seguridad es parte de la cultura organizacional: todos los departamentos están involucrados.
- Se aplican simulaciones de incidentes y pruebas de resiliencia cibernética al menos dos veces al año.

Analiza el caso presentado e identifica en qué nivel de madurez (0 al 3) crees que se encuentra NOVABANK DIGITAL.

1. **Justifica tu diagnóstico** con argumentos claros.
2. **Propón mínimo 3 acciones concretas** que la empresa debería emprender para subir de nivel o mejorar si ya se encuentra en el nivel 3.