¿Qué tiene que ver el crecer con la seguridad?

¿Qué tiene que ver el crecer con la seguridad?

¿Qué tiene que ver crecer con la ciberseguridad?

Nivel de Madurez	Persona	Organización
1 Infantil (Caôtico)	 No cuida sus cosas, deja todo abierto.	No tiene reglas, ni protección, ni cotrol: todo es improvisado

¿Qué tiene que ver el crecer con la seguridad?

¿Qué tiene que ver crecer con la ciberseguridad?

Nivel de Madurez	Persona	Organización
1 Infantil (Caôtico)	 No cuida sus cosas, deja todo abierto.	No tiene reglas, ni protección, ni cotrol: todo es improvisado
2 Adolescente (Reactivo)	 Solo se protege cuãndo ya tuvo un problema	Solo actũan cuando ya hubo un ataque o pérdida de datos

¿Qué tiene que ver el crecer con la seguridad?

¿Qué tiene que ver crecer con la ciberseguridad?

Nivel de Madurez		Persona	Organización
1	Infantil (Caôtico)	 No cuida sus cosas, deja todo abierto.	No tiene reglas, ni protección, ni cotrol: todo es improvisado
2	Adolescente (Reactivo)	 Solo se protege cuãndo ya tuvo un problema	Solo actũan cuando ya hubo un ataque o pérdida de datos
3	Responsable (Definido)	 Usa contrase-ñas, piensa antes de compartir	Tiene politicas y procesos basicos para proteger iñormán

¿Qué tiene que ver el crecer con la seguridad?

¿Qué tiene que ver crecer con la ciberseguridad?

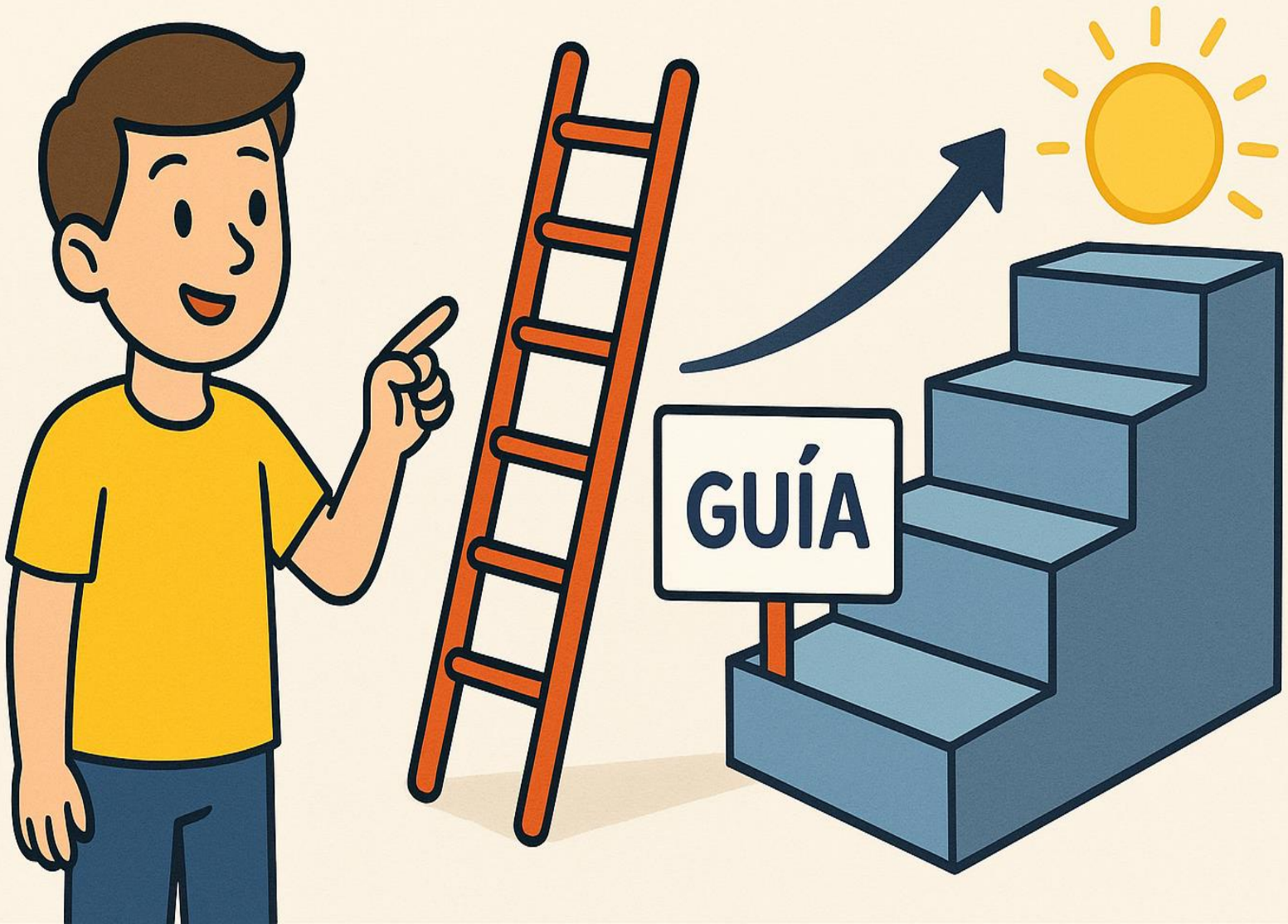
Nivel de Madurez		Persona	Organización
1	Infantil (Caôtico)	 No cuida sus cosas, deja todo abierto.	No tiene reglas, ni protección, ni cotrol: todo es improvisado
2	Adolescente (Reactivo)	 Solo se protege cuãndo ya tuvo un problema	Solo actũan cuando ya hubo un ataque o pérdida de datos
3	Responsable (Definido)	 Usa contrase-ñas, piensa antes de compartir	Tiene politicas y procesos basicos para proteger iñormán
4	Maduro (Gestionado)	 Enseña a otros, está un paso adelante	Monitorea, entrena al personal, sigue procedimientos
5	Sabio (Optimizado)	Mejora continua-mente.	Mejora continuamente, tiene cultura solida de seguridad

Madurez en el Desarrollo de Software

Modelos de Madurez para la Seguridad de la Información

Andrés Julián Valencia Osorio
ajvalenciao@sena.edu.co

Qué es un modelo de madurez para la seguridad de la información?



Los **modelos de madurez de ciberseguridad** son herramientas que permiten a las organizaciones evaluar su nivel de preparación y madurez en seguridad informática. Estos modelos proporcionan un marco estructurado para identificar áreas de mejora y establecer metas para avanzar hacia una mayor resiliencia ante amenazas

Estándares, Marcos de referencia y Modelos

Estándar internacional que define requisitos para establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI)

Marco de referencia que guía a las organizaciones en la gestión del riesgo cibernético

Modelo que evalúa la madurez de las capacidades de ciberseguridad en organizaciones del sector energético y otros sectores críticos

Modelo colombiano que proporciona lineamientos para gestionar la seguridad y privacidad en el sector público

Modelo del Departamento de Defensa de EE. UU. que establece niveles de madurez para asegurar la cadena de suministro en contratistas y proveedores

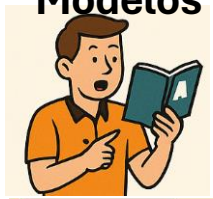
Estándares, Marcos de Referencia y Modelos

Estándar 	• Define reglas claras y específicas sobre **cómo se debe jugar** No tiene fuerza de ley por sí solo, **pero se adopta globalmente** para garantizar que todos jueguen bajo las mismas condiciones. • Las ligas, torneos y federaciones que **quieren estar alineadas con la FIFA** deben seguir ese estándar		• Define **cómo una organización debe proteger su información**: roles, procesos, controles, políticas, etc. • No es obligatorio por ley, **pero es adoptado globalmente** como mejor práctica y exigido por muchas empresas. • Las organizaciones que desean certificarse o alinearse con **buenas prácticas de seguridad deben cumplir con ISO/IEC 27001**

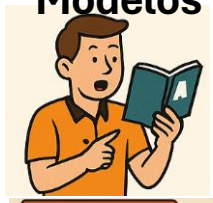
Estándares, Marcos de Referencia y Modelos

Estándar 	• Define reglas claras y específicas sobre **cómo se debe jugar** No tiene fuerza de ley por sí solo, **pero se adopta globalmente** para garantizar que todos jueguen bajo las mismas condiciones. • Las ligas, torneos y federaciones que **quieren estar alineadas con la FIFA** deben seguir ese estándar		• Define **cómo una organización debe proteger su información**: roles, procesos, controles, políticas, etc. • No es obligatorio por ley, **pero es adoptado globalmente** como mejor práctica y exigido por muchas empresas. • Las organizaciones que desean certificarse o alinearse con **buenas prácticas de seguridad deben cumplir con ISO/IEC 27001**
Marco 	• Ayuda a formar **buenos equipos** • Permite **adaptar** ejercicios, tácticas y planes según el nivel • **Mejora** habilidades, estrategias y coordinación del equipo • **No reemplaza el reglamento FIFA**, pero lo complementa		• Ayuda a manejar la seguridad de forma **efectiva en la organización** • Se **adapta** al tamaño, riesgos y capacidades de cada organización • **Mejora** la capacidad de prevenir, detectar y responder a incidentes • **No reemplaza a ISO 27001**, pero lo complementa como guía práctica

Estándares, Marcos de Referencia y Modelos

Estándar 	• Define reglas claras y específicas sobre **cómo se debe jugar** No tiene fuerza de ley por sí solo, **pero se adopta globalmente** para garantizar que todos jueguen bajo las mismas condiciones. • Las ligas, torneos y federaciones que **quieren estar alineadas con la FIFA** deben seguir ese estándar		• Define **cómo una organización debe proteger su información**: roles, procesos, controles, políticas, etc. • No es obligatorio por ley, **pero es adoptado globalmente** como mejor práctica y exigido por muchas empresas. • Las organizaciones que desean certificarse o alinearse con **buenas prácticas de seguridad deben cumplir con ISO/IEC 27001**
Marco 	• Ayuda a formar **buenos equipos** • Permite **adaptar** ejercicios, tácticas y planes según el nivel • **Mejora** habilidades, estrategias y coordinación del equipo • **No reemplaza el reglamento FIFA**, pero lo complementa		• Ayuda a manejar la seguridad de forma **efectiva en la organización** • Se **adapta** al tamaño, riesgos y capacidades de cada organización • **Mejora** la capacidad de prevenir, detectar y responder a incidentes • **No reemplaza a ISO 27001**, pero lo complementa como guía práctica
Modelos  	• **Evalúa qué tan avanzado está un equipo**, cómo se encuentra en la tabla de posiciones • Ayuda a identificar **en qué debe mejorar el equipo** • Puede **clasificar equipos en divisiones** o categorías		• **Evalúa qué tan madura está una organización** en su gestión de ciberseguridad • Ayuda a la organización a trazar **un plan de mejora en ciberseguridad** • **Clasifica la organización en niveles** de madurez en ciberseguridad

Estándares, Marcos de Referencia y Modelos

Estándar 	• Define reglas claras y específicas sobre **cómo se debe jugar** No tiene fuerza de ley por sí solo, **pero se adopta globalmente** para garantizar que todos jueguen bajo las mismas condiciones. • Las ligas, torneos y federaciones que **quieren estar alineadas con la FIFA** deben seguir ese estándar		• Define **cómo una organización debe proteger su información**: roles, procesos, controles, políticas, etc. • No es obligatorio por ley, **pero es adoptado globalmente** como mejor práctica y exigido por muchas empresas. • Las organizaciones que desean certificarse o alinearse con **buenas prácticas de seguridad deben cumplir con ISO/IEC 27001**
Marco 	• Ayuda a formar **buenos equipos** • Permite **adaptar** ejercicios, tácticas y planes según el nivel • **Mejora** habilidades, estrategias y coordinación del equipo • **No reemplaza el reglamento FIFA**, pero lo complementa		• Ayuda a manejar la seguridad de forma **efectiva en la organización** • Se **adapta** al tamaño, riesgos y capacidades de cada organización • **Mejora** la capacidad de prevenir, detectar y responder a incidentes • **No reemplaza a ISO 27001**, pero lo complementa como guía práctica
Modelos  	• **Evalúa qué tan avanzado está un equipo**, cómo se encuentra en la tabla de posiciones • Ayuda a identificar **en qué debe mejorar el equipo** • Puede **clasificar equipos en divisiones** o categorías		• **Evalúa qué tan madura está una organización** en su gestión de ciberseguridad • Ayuda a la organización a trazar **un plan de mejora en ciberseguridad** • **Clasifica la organización en niveles** de madurez en ciberseguridad
	• Los equipos que quieren **participar en torneos importantes** deben tener licencias válidas • Hay que **cumplir con requisitos** (infraestructura, finanzas, reglamentos, etc.) para obtener la licencia		• Empresas que **quieren contratar con el Departamento de Defensa de EE.UU.** deben cumplir con CMMC • Hay que **pasar una auditoría formal** para obtener la certificación CMMC

Estándares, Marcos de Referencia y Modelos

Estándar 	• Define reglas claras y específicas sobre **cómo se debe jugar** No tiene fuerza de ley por sí solo, **pero se adopta globalmente** para garantizar que todos jueguen bajo las mismas condiciones. • Las ligas, torneos y federaciones que **quieren estar alineadas con la FIFA** deben seguir ese estándar		• Define **cómo una organización debe proteger su información**: roles, procesos, controles, políticas, etc. • No es obligatorio por ley, **pero es adoptado globalmente** como mejor práctica y exigido por muchas empresas. • Las organizaciones que desean certificarse o alinearse con **buenas prácticas de seguridad deben cumplir con ISO/IEC 27001**
Marco 	• Ayuda a formar **buenos equipos** • Permite **adaptar** ejercicios, tácticas y planes según el nivel • **Mejora** habilidades, estrategias y coordinación del equipo • **No reemplaza el reglamento FIFA**, pero lo complementa		• Ayuda a manejar la seguridad de forma **efectiva en la organización** • Se **adapta** al tamaño, riesgos y capacidades de cada organización • **Mejora** la capacidad de prevenir, detectar y responder a incidentes • **No reemplaza a ISO 27001**, pero lo complementa como guía práctica
Modelos 	• **Evalúa qué tan avanzado está un equipo**, cómo se encuentra en la tabla de posiciones • Ayuda a identificar **en qué debe mejorar el equipo** • Puede **clasificar equipos en divisiones** o categorías		• **Evalúa qué tan madura está una organización** en su gestión de ciberseguridad • Ayuda a la organización a trazar **un plan de mejora en ciberseguridad** • **Clasifica la organización en niveles** de madurez en ciberseguridad
	• Los equipos que **quieren participar en torneos importantes** deben tener licencias válidas • Hay **que cumplir con requisitos** (infraestructura, finanzas, reglamentos, etc.) para obtener la licencia		• Empresas que **quieren contratar con el Departamento de Defensa de EE.UU.** deben cumplir con CMMC • Hay que **pasar una auditoría formal** para obtener la certificación CMMC
	• **Solo los equipos de cierta liga o país deben cumplirlo** • **Incluye categorías, divisiones,** requisitos mínimos según el nivel del equipo		• **Solo aplica de forma obligatoria a entidades públicas del Estado colombiano** • **El MSPI incluye niveles de madurez** y una estructura para mejorar la gestión de seguridad


C2M2 Cybersecurity
Capability Maturity Model

Dominios C2M2

C2M2 Dominios

🖥️ **Gestión de Activos, Cambios y Configuraciones (ACCM)**	Controla los activos tecnológicos, los cambios y sus configuraciones para mantener la integridad y seguridad del entorno.
🐞 **Gestión de Amenazas y Vulnerabilidades (TVM)**	Identifica y corrige debilidades que pueden ser explotadas por amenazas internas o externas.
⚖️ **Gestión de Riesgos (RM)**	Evalúa los riesgos de ciberseguridad y define cómo tratarlos para proteger la organización.
🏛️ **Arquitectura de Ciberseguridad (ARCH)**	Diseña estructuras seguras para proteger la infraestructura tecnológica y la información.
🧑‍💻 **Gestión de Identidad y Accesos (IAM)**	Administra quién puede acceder a qué recursos, asegurando autenticación y autorización adecuadas.
👁️ **Conciencia Situacional (SA)**	Monitorea continuamente el entorno para detectar y responder a incidentes de ciberseguridad.
🚨 **Respuesta a Incidentes y Continuidad de Operaciones (IR)**	Responde eficazmente a incidentes y garantiza que las operaciones continúen incluso durante una crisis.
📦 **Gestión de la Cadena de Suministro y Dependencias Externas (SCED)**	Supervisa a proveedores y terceros para mitigar riesgos de seguridad que puedan venir del exterior.
👷 **Gestión del Talento Humano (WM)**	Desarrolla personal capacitado en ciberseguridad, definiendo roles y responsabilidades claras.
📋 **Gestión del Programa de Ciberseguridad (CPM)**	Supervisa y mejora continuamente el programa de ciberseguridad, alineándolo con los objetivos estratégicos.

C2M2 Niveles de Madurez

Nivel 0		**Incompleto**: No se realiza la práctica o no hay evidencia de que se haga regularmente.

C2M2 Niveles de Madurez

Nivel 0 🟥		**Incompleto**: No se realiza la práctica o no hay evidencia de que se haga regularmente.
Nivel 1 🟡		**Inicial**: Se realiza la práctica de forma improvisada y reactiva, sin planificación formal.

C2M2 Niveles de Madurez

Nivel 0 🟥		**Incompleto**: No se realiza la práctica o no hay evidencia de que se haga regularmente.
Nivel 1 🟡		**Inicial**: Se realiza la práctica de forma improvisada y reactiva, sin planificación formal.
Nivel 2 🟠		**Estructurado**: Ya existe una planificación, roles definidos y recursos asignados.

C2M2 Niveles de Madurez

Nivel 0 🟥		**Incompleto**: No se realiza la práctica o no hay evidencia de que se haga regularmente.
Nivel 1 🟡		**Inicial**: Se realiza la práctica de forma improvisada y reactiva, sin planificación formal.
Nivel 2 🟠		**Estructurado**: Ya existe una planificación, roles definidos y recursos asignados.
Nivel 3 🟢		**Gestionado**: La práctica está integrada, monitoreada y se mejora continuamente.

Vamos a Hackear tus conocimientos

https://dashboard.blooket.com/my-sets

Casos de Estudio Prácticos

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.