ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Propuesta de un modelo de madurez de la cultura de Ciberseguridad para una IES

Integrantes:
Sahian Abadiano
Santiago Camacho

Tutor: Ing. Mario Ron

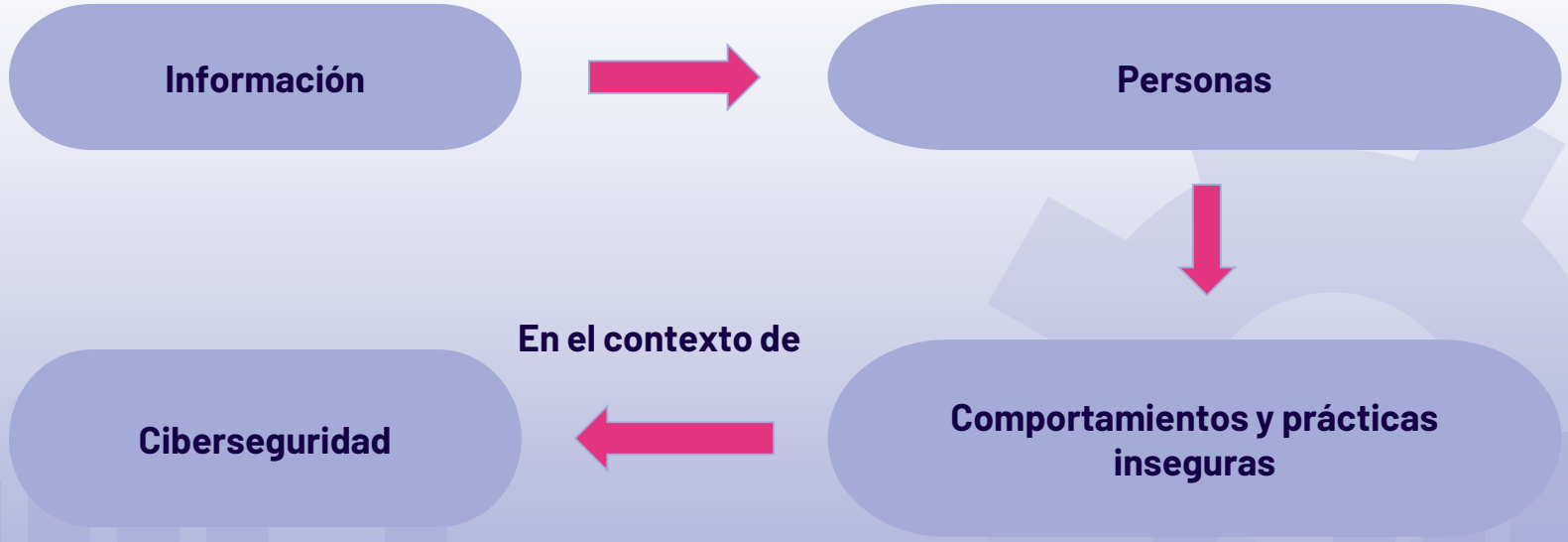
11 de marzo del 2024

Tabla de Contenido

01

Aspectos Generales

Planteamiento del problema



Objetivo General

Elaborar un Modelo de Madurez de la Cultura de Ciberseguridad para una Institución de Educación Superior, como caso de referencia la Universidad de las Fuerzas Armadas ESPE, considerando la familia de normas internacionales ISO/IEC/NTE 27000.

Objetivos Específicos

- Establecer el estado del arte mediante una revisión exhaustiva de la literatura existente acerca de Modelos de Madurez de la Cultura de Ciberseguridad.
- Determinar los componentes o elementos de la Cultura de Ciberseguridad en el contexto de una IES.
- Analizar modelos relacionados, para configurar los niveles y componentes del Modelo final de Madurez de la Cultura de Ciberseguridad.

02

Marco Conceptual

Ciberseguridad

Políticas y acciones → Activos de información → Organización

Ciberamenzas

- **Delito cibernético**
- **Ciberataques**
- **Ciberterrorismo**

Métodos

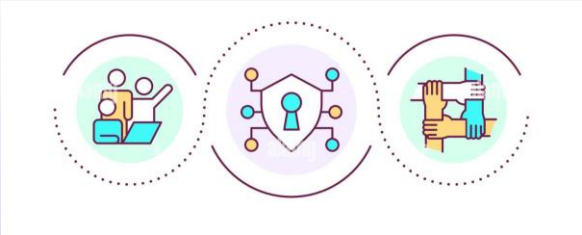
Phishing

Inyección de código

Malware

Ataque de denegación de servicios

Cultura de Ciberseguridad



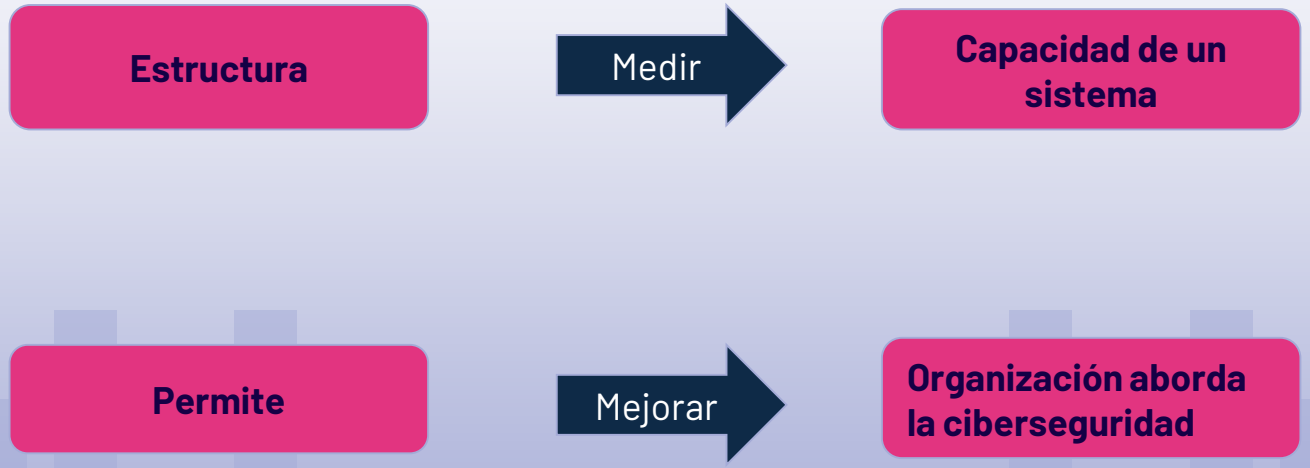
Aborda aspectos

- **Educación**
- **Formación**
- **Concientización**
- **Responsabilidad individual**

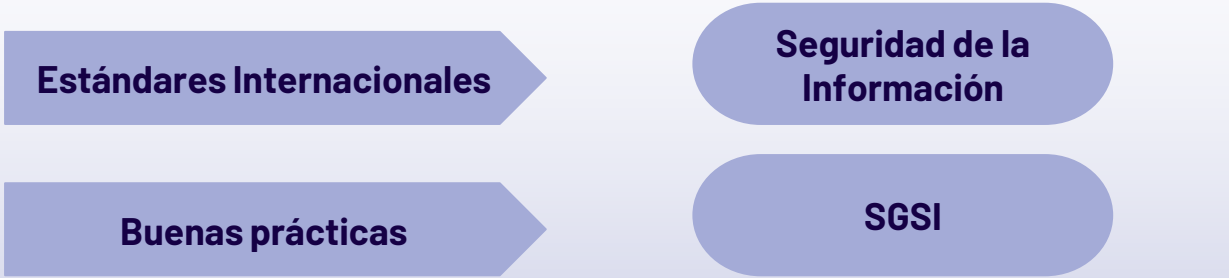
Proteger

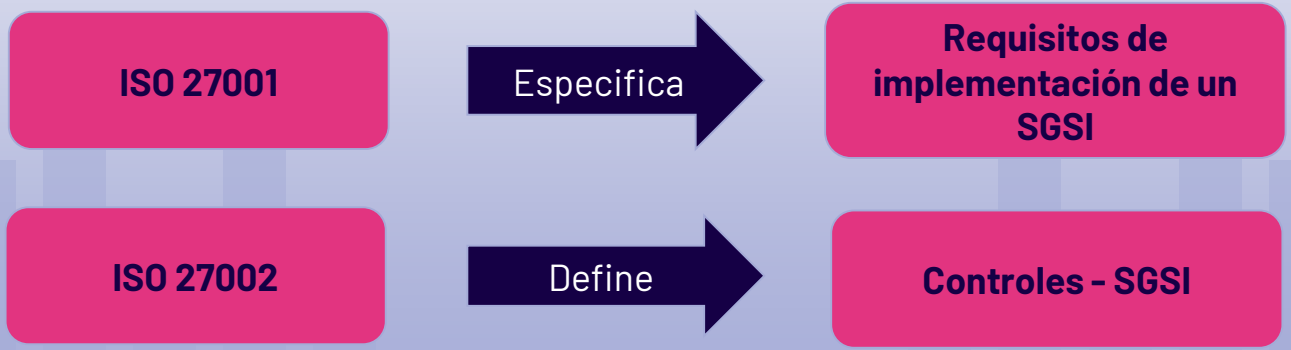
Confidencialidad
Integridad
Disponibilidad

Modelo de Madurez



Familia ISO 27000





03

Diseño del Modelo de Madurez

Análisis de Contexto

En materia de cultura de ciberseguridad, dentro de una institución de educación superior se toma en cuenta:

- La Estructura académica y administrativa
- Los activos de información crítica.

Grupos Ocupacionales

- Directivos
- Funcionarios técnicos en informática
- Funcionarios administrativos
- Docentes
- Trabajadores
- Estudiantes
- Proveedores de servicios

Definición de Componentes de ciberseguridad

Componentes ISO	Componentes INCIBE	Componentes OEA	Componentes ENISA	Componentes FINAL - MODELO PROPIO
Controles organizacionales	Gestión de riesgos	Política y Estrategia de Ciberseguridad	Gobernabilidad y normas de ciberseguridad	**Gobernabilidad y controles organizacionales**
Controles de personas	Gestión de activos	Cultura Cibernética y Sociedad	Creación de la capacidad y concienciación	**Capacitación y concienciación en habilidades de ciberseguridad**
Controles físicos	Gestión de accesos	Educación, Capacitación y Habilidades en Ciberseguridad	Jurídico y normativo	**Marco jurídico y normativo de la estrategia de ciberseguridad**

Componentes de ciberseguridad

Componentes ISO	Componentes INCIBE	Componentes OEA	Componentes ENISA	Componentes FINAL - MODELO PROPIO
Controles tecnológicos.	Gestión de amenazas	Marcos Legales y Regulatorios	Cooperación	**Gestión de activos tecnológicos**
	Gestión de ciberseguridad	Estándares, organizacionales y tecnologías		**Gestión de usuarios y accesos**
	Gestión de usuarios			**Estrategias de gestión de riesgos y amenazas**
				Protección de la información y procedimientos

Clasificación de los controles

Componentes FINAL - MODELO PROPIO	Controles ISO 27001
Gobernabilidad y controles organizacionales	• Segregación de deberes • Responsabilidades de la dirección • Contacto con las autoridades • Contacto con grupos de interés especial • Selección • Términos y condiciones de empleo
Capacitación y concienciación en habilidades de ciberseguridad	• Seguridad de la Información en la gestión de proyectos • Protección de registros • Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés) • Revisión independiente de la seguridad de la información • Conciencia de seguridad de la información, educación y formación

Clasificación de controles según componentes y grupos ocupacionales

								Grupos ocupacionales						
Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001	Componentes ISO	Componentes INCIBE	Componentes OEA	Componentes ENISA	Componentes FINAL - MODELO PROPIO	Directivos	Docentes	Funcionarios Técnicos en Inf.	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Políticas de la seguridad de la información	Deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización.	Controles organizacionales	Gestión de riesgos	Política y Estrategia de Ciberseguridad	Gobernabilidad y normas de ciberseguridad	Gobernabilidad y controles organizacionales	x		x	x			
	Roles y responsabilidades en la Seguridad de la Información	Se deben definir y asignar de acuerdo con las necesidades de la organización.	Controles de personas	Gestión de activos	Cultura Cibernética y Sociedad	Creación de la capacidad y concienciación	Capacitación y concienciación en habilidades de ciberseguridad	x	x	x	x	x	x	x
	Segregación de deberes	Los deberes y áreas de responsabilidad en conflicto deberían segregarse.	Controles físi	Gestión de accesos	Educación, Capacitación y Habilidades en Ciberseguridad	Jurídico y normativo	Marco jurídico y normativo de la estrategia de ciberseguridad	x	x	x	x	x	x	x
	Responsabilidades de la dirección	La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida	Controles tecnológicos.	Gestión de amenazas	Marcos Legales y Regulatorios	Cooperación	Gestión de activos tecnológicos	x						

Modelos de madurez

Modelo	Niveles	Componente /Dominios
El Modelo de Madurez de la Capacidad de Ciberseguridad	5 Niveles	5 Dimensiones
Línea de base de la ciberseguridad: An Exploration, que permite delinear la Ciberseguridad Nacional en Ecuador - OEA / ISACA	6 Niveles	23 Factores
Modelo de madurez de las capacidades de ingeniería de seguridad de sistemas (SSE - CMM)	5 Niveles	22 Áreas de proceso
Modelo comunitario de madurez de la ciberseguridad (CCSMM)	5 Niveles	4 Dimensiones

Modelos de madurez

Modelo	Niveles	Componente /Dominios
Certificación del Modelo de Madurez de Ciberseguridad (CMMC)	5 Niveles	17 Dominios
Modelo de madurez de las capacidades de ciberseguridad C2M2	4 Niveles	10 Dominios
Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero (MMCCSF)	4 Niveles	4 Dominios
Iniciativa Nacional para la Educación en Ciberseguridad (NICE)	3 Niveles	3 Áreas de aplicación

Niveles de madurez

Niveles	BID / OEA	OEA / ISACA	SSE - CMM	CCSMM	CMMC	C2M2	MMCCSF	NICE	Modelo final
0		Nivel: Incompleto Descripción: El proceso que no se ha llevado a cabo en su totalidad y no ha cumplido con su propósito.				Nivel: 0 Descripción: No se realizan prácticas.	Nivel: Inexistente Descripción: En este nivel no se habla de ciberseguridad, se asume que la tecnología ya cuenta con las características de seguridad necesarias.		Nivel Inexistente - Nivel Cero: Descripción: En esta etapa, la ciberseguridad carece de madurez o se encuentra en un etapa muy temprana. El proceso que no se ha iniciado formalmente y no se conoce su importancia ni propósito. No se realizan prácticas relacionadas en forma organizada. En este nivel no se habla de ciberseguridad, se asume que la tecnología ya cuenta con las características de seguridad necesarias.
1	Nivel: Inicial Descripción: En esta etapa, la ciberseguridad carece de madurez o se encuentra en un etapa muy temprana.	Nivel: Implementado Descripción: El proceso cumple su propósito.	Nivel: Realizado informalmente Descripción: Se concentra en si una organización o proyecto implementa un proceso que incorpora las prácticas fundamentales.	Nivel: Inicial Descripción: Las organizaciones, comunidades y estados de este nivel tienen poca o ninguna conciencia de las evaluaciones, el análisis y la seguridad cibernética.	Nivel: Realizados Descripción: No hay procesos de madurez evaluados. Salvaguardar la información del contrato federal.	Nivel: 1 Descripción: Las prácticas iniciales se realizan.	Nivel: Limitada Descripción: en este nivel se considera la seguridad como un criterio únicamente del área de tecnología y seguridad de la organización.	Nivel: Limitado Descripción: Es el más básico representado por una organización con establecimiento limitado de procesos y que carece de una orientación clara.	Nivel Inicial - Nivel Uno: Descripción: Las prácticas de ciberseguridad se realizan. Existe conciencia de la ciberseguridad en un nivel básico Se han aplicado controles de manera intuitiva.
2	Nivel: Formativa Descripción: Algunos aspectos han comenzado a desarrollarse y formularse, pero pueden ser improvisados, desorganizados, mal definidos o simplemente nuevos. Sin embargo, hay pruebas evidente de este aspecto.	Nivel: Gestionado Descripción: El proceso se planifica, supervisa y mantiene, al igual que sus productos.	Nivel: Planificado y seguido Descripción: Se centra en la definición, planificación y problemas de rendimiento a nivel de proyecto.	Nivel: Establecido Descripción: Los líderes de las organizaciones, comunidades y estados a este nivel están conscientes de los problemas, las amenazas y la necesidad de adoptar la ciberseguridad.	Nivel: Documentados Descripción: Servir como paso de transición en la progresión de madurez de ciberseguridad para proteger la información no clasificada controlada (CUI) .	Descripción: Se documentan las prácticas. Se proporcionan los recursos adecuados para apoyar los procesos. El personal que realiza las prácticas tiene las habilidades y conocimientos necesarios Se asigna la autoridad y responsabilidad para realizar las	Nivel: Proactiva Descripción: En esta etapa los directivos son consientes de la importancia de la ciberseguridad y la promueven en toda la organización.	Nivel: Progresivo Descripción: describe un área de actividad clave, y es representada por una organización que establece una infraestructura para apoyar los esfuerzos de planificación de la fuerza de trabajo.	Nivel Planificado: Nivel Dos Descripción: Los directivos son consientes de la importancia de la ciberseguridad y apoyan la planificación. Se elabora y aprueba el proyecto de ciberseguridad. Se establece una línea base. Algunos aspectos han comenzado a desarrollarse y formularse, pero pueden ser improvisados, desorganizados, mal definidos o simplemente nuevos. Sin embargo, hay pruebas evidente de este aspecto.

Niveles de madurez

Niveles	BID / OEA	OEA / ISACA	SSE - CMM	CCSMM	CMMC	C2M2	MMCCSF	NICE	Modelo final
3	Nivel: Consolidada Descripción: Los indicadores se han instalado y han comenzado a funcionar. La asignación de recursos, por otro lado, ha sido ignorada.	Nivel: Formalizado Descripción: El proceso utiliza un conjunto de actividades documentadas y normalizadas.	Nivel: Bien definido Descripción: Se enfoca en la adaptación disciplinada de procedimientos establecidos a nivel organizacional.	Nivel: Autoevaluado Descripción: En este nivel, los líderes de las organizaciones, las comunidades y los estados trabajan juntos para desarrollar programas de capacitación y educación en seguridad cibernética.	Nivel: Administrada Descripción: Proteger la información no información no clasificada (CUI, Controlled Unclassified Information).	Nivel: 3 Descripción: Las actividades se guían por políticas o directivas organizacionales. Se establecen objetivos de desempeño para las actividades de dominio, y se monitorean para rastrear los logros. Las prácticas documentadas de las actividades de dominio se estandarizan y se mejoran en toda la empresa.	Nivel: Integrada Descripción: En esta etapa la ciberseguridad se integra en todos los procesos de la organización y todos se sienten responsables de la ciberseguridad.	Nivel: Madurez en optimización Descripción: Representa un área de actividad clave o un segmento de capacidad de planificación de la fuerza laboral de ciberseguridad desarrollado plenamente, integrado con otros procesos de negocio y soporta diferentes niveles de trabajo y análisis de carga de trabajo.	Nivel Establecido: Nivel Tres Descripción: Se pone en marcha el proyecto de ciberseguridad incluyendo los recursos. Se establecen objetivos de desempeño y se documenta el progreso de las actividades. Los líderes y la comunidad trabajan juntos en programas de educación en seguridad cibernética. Se incluye en la responsabilidad de la ciberseguridad a todos los procesos de la organización.
4	Nivel: Estratégica Descripción: En esta etapa, se han tomado decisiones sobre qué indicadores de este aspecto son más significativos y cuáles son menos significativos para la organización o el Estado en particular.	Nivel: Consistente Descripción: El proceso se mide y se lleva a cabo de forma predecible.	Nivel: Controlado cuantitativamente Descripción: Se concentra en las mediciones relacionadas con los objetivos comerciales de la organización.	Nivel: Integrado Descripción: Cuando la seguridad cibernética está integrada, se incorpora en cada proceso que tiene una organización, comunidad o estado.	Nivel: Revisados Descripción: Proteger la CUI y reducir el riesgo de ciberseguridad de amenazas (APT, Advanced Persistent Threat)				Nivel Certificado-Consistente: Nivel Cuatro Descripción: Se evalúan los controles y se implementan medidas de protección avanzadas. El proceso se mide y se pone en práctica de manera continua. Las mediciones se relacionan con los objetivos organizacionales más significativos. Las actividades están más organizadas y regidas por políticas o directivas organizacionales. Se establece una cultura de seguridad sostenible a largo plazo.
5	Nivel: Dinámica Descripción: En esta etapa, existen mecanismos claros para adaptar la estrategia a las circunstancias actuales, como el aumento de la sofisticación tecnológica del entorno de amenazas, el conflicto global o un cambio significativo en un tema de preocupación (como el delito informático o la privacidad).	Nivel: Innovado Descripción: El proceso es innovador, resistente y puede reaccionar con rapidez a los cambios ambientales.	Nivel: Mejora continua Descripción: Enfatiza los cambios culturales que sostendrán los logros obtenidos y aprovecha las ventajas de todas las mejoras en la práctica administrativa observadas en los niveles anteriores.	Nivel: Vanguardia Descripción: La seguridad cibernética es un imperativo empresarial para estas organizaciones, comunidades y estados. A este nivel, las organizaciones tienen la capacidad de enseñar a otros.	Nivel: Optimizando Descripción: Reducción del riesgo de Amenzas Persistentes Avanzadas (APT)				Nivel Innovado-Mejora Continua: Nivel Cinco Descripción: Se tiene un marco de trabajo bien definido y robusto Se establecen mecanismos claros para adaptar las estrategias ante circunstancias actuales y reaccionar con rapidez ante cualquier cambio a futuro. Se toma como ventaja las mejoras obtenidas de las prácticas de niveles anteriores, para la mejora continua. La organización tiene una cultura fuerte de ciberseguridad

Definición de Niveles de madurez

Niveles de madurez	Descripción
Nivel Cero: Cultura inexistente	● La ciberseguridad carece de madurez o se encuentra en una etapa muy temprana. ● El proceso no se ha iniciado formalmente y no se conoce su importancia ni propósito. ● No se realizan prácticas relacionadas en forma organizada. ● En este nivel no se habla de ciberseguridad, se asume que la tecnología ya cuenta con las características de seguridad necesarias.
Nivel Uno: Inicial	● Las prácticas de ciberseguridad se realizan. ● Existe conciencia de la ciberseguridad en un nivel básico. ● Se han aplicado controles de manera intuitiva.
Nivel Dos: Planificado	● Existe conciencia de la importancia de la ciberseguridad y apoyan la planificación. ● Se elabora y aprueba el proyecto de ciberseguridad. ● Se establece una línea base. Algunos aspectos han comenzado a desarrollarse y formularse, pero pueden ser improvisados, desorganizados, mal definidos o simplemente nuevos. Sin embargo, hay pruebas evidentes de este aspecto.

Definición de Niveles de madurez

Niveles de madurez	Descripción
Nivel Tres: Establecido	• Se pone en marcha el proyecto de ciberseguridad incluyendo los recursos. • Se establecen objetivos de desempeño y se documenta el progreso de las actividades. • Los líderes y la comunidad trabajan juntos en programas de educación en seguridad cibernética. • Se incluye en la responsabilidad de la ciberseguridad a todos los procesos de la organización.
Nivel Cuatro: Certificado – Consistente	• Se evalúan los controles y se implementan medidas de protección avanzada. • El proceso se mide y se pone en práctica de manera continua. • Las mediciones se relacionan con los objetivos organizacionales más significativos. • Las actividades están más organizadas y regidas por políticas o directivas organizacionales. • Se establece una cultura de seguridad sostenible a largo plazo.
Nivel Cinco: Innovado - Mejora continua	• Se tiene un marco de trabajo bien definido y robusto. • Se establecen mecanismos claros para adaptar las estrategias ante circunstancias actuales y reaccionar con rapidez ante cualquier cambio futuro. • Se toma como ventaja las mejoras obtenidas de las prácticas de niveles anteriores, para la mejora continua. • La organización tiene una cultura fuerte de ciberseguridad.

Niveles de Aplicación de Componentes

Nivel de aplicación	Valor numérico	Descripción
Nivel Nulo	**0**	Representa que no existe ninguna aplicación de estos controles.
Nivel Bajo	**1**	Representa que, si existe al menos el conocimiento sobre el tema de ciberseguridad.
Nivel Medio	**2**	Representa la aplicación de estos controles.
Nivel Alto	**3**	Representa el desarrollo consistente de la ciberseguridad en la organización.

Modelo Final de Madurez de la Cultura de Ciberseguridad

Componente / Nivel	Gobernabilidad y controles organizacionales	Capacitación y concienciación en habilidades de ciberseguridad	Marco jurídico y normativo de la estrategia de ciberseguridad	Gestión de activos tecnológicos	Gestión de usuarios y accesos	Estrategias de gestión de riesgos y amenazas	Protección de la información y procedimientos
Nivel Cero: Cultura inexistente	Nulo	Nulo	Nulo	Bajo	Bajo	Nulo	Bajo
Nivel Uno: Inicial	Bajo	Bajo	Nulo	Bajo	Bajo	Bajo	Bajo
Nivel Dos: Planificado	Medio	Medio	Bajo	Medio	Medio	Medio	Medio
Nivel Tres: Establecido	Alto	Alto	Medio	Alto	Medio	Medio	Medio
Nivel Cuatro: certificado	Alto	Alto	Alto	Alto	Medio	Medio	Medio
Nivel Cinco: Innovado, de mejora continua:	Alto	Alto	Alto	Alto	Alto	Alto	Alto

4

Resultados, Conclusiones y Recomendaciones

Simulación de puntuación de componentes

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
	Directivos	Protección de los sistemas de información durante las pruebas de auditoría	¿Las pruebas de auditoría y otras actividades de aseguramiento que implican la evaluación de los sistemas operativos se planifican y acuerdan entre el probador y la dirección?	0 = Nunca se planifican y acuerdan conjuntamente. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre se planifican y acuerdan conjuntamente.	2
		Uso de la criptografía	¿Se han establecido e implementado estándares para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas?	0 = No existen estándares. 1 = No, no se han definido ni implementado estándares. 2 = Sí, hay estándares pero no implementación completa. 3 = Sí, se han definido e implementado estándares.	2
		Ciclo de vida de desarrollo seguro	¿Existen estándares para el desarrollo seguro de software y sistemas que se implementan en la universidad?	0 = No existen estándares. 1 = No, no se han definido ni implementado estándares. 2 = Sí, hay estándares pero no implementación completa. 3 = Sí, se han definido e implementado estándares.	2

Simulación de puntuación de componentes

Protección de la información y procedimientos	Funcionarios Técnicos en Inf.	Arquitectura de sistemas seguros y principios de ingeniería	¿Se aplican formalmente los principios de ingeniería de sistemas seguros en todas las actividades de desarrollo de sistemas de información?	0 = Nunca se aplican. 1 = No, rara vez se aplican. 2 = Sí, en su mayoría. 3 = Sí, siempre se siguen.	3
		Codificación segura	¿Se implementan activamente los principios de codificación segura al desarrollar programas informáticos?	0 = Nunca se implementan. 1 = No, rara vez se implementan 2 = Sí, en su mayoría. 3 = Sí, siempre se implementan.	3
		Pruebas de seguridad en el desarrollo y aceptación	¿Considera que se han establecido e implementado procedimientos de prueba de seguridad en todas las fases del ciclo de vida del desarrollo de la sistemas o aplicaciones?	0 = Nunca se implementan. 1 = No, rara vez se implementan 2 = Sí, en la mayoría de las fases. 3 = Sí, en todas las fases del desarrollo.	3
		Gestión del cambio	¿Existen procedimientos formales de gestión de cambios para modificar las instalaciones y sistemas de procesamiento de información?	0 = Nunca están sujetos a gestión de cambios. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre están sujetos a gestión de cambios.	2

Simulación de puntuación de componentes

		Protección de los sistemas de información durante las pruebas de auditoría	¿Las pruebas de auditoría y otras actividades de aseguramiento que implican la evaluación de los sistemas operativos se planifican y acuerdan entre el probador y la dirección?	0 = Nunca se planifican y acuerdan conjuntamente. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre se planifican y acuerdan conjuntamente.	3	
	Funcionarios Administrativos	Gestión del cambio	¿Existen procedimientos formales de gestión de cambios para modificar las instalaciones y sistemas de procesamiento de información?	0 = Nunca están sujetos a gestión de cambios. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre están sujetos a gestión de cambios.	2	
		Protección de los sistemas de información durante las pruebas de auditoría	¿Las pruebas de auditoría y otras actividades de aseguramiento que implican la evaluación de los sistemas operativos se planifican y acuerdan entre el probador y la dirección?	0 = Nunca se planifican y acuerdan conjuntamente. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre se planifican y acuerdan conjuntamente.	2	
					2,363636364	Nivel Medio

Comparación del nivel de madurez requerido y simulado

Componente / Nivel	Gobernabilidad y controles organizacionales	Capacitación y concienciación en habilidades de ciberseguridad	Marco jurídico y normativo de la estrategia de ciberseguridad	Gestión de activos tecnológicos	Gestión de usuarios y accesos	Estrategias de gestión de riesgos y amenazas	Protección de la información y procedimientos
Nivel Cero: Cultura inexistente	Nulo	Nulo	Nulo	Bajo	Bajo	Nulo	Bajo
Nivel Uno: Inicial	Bajo	Bajo	Nulo	Bajo	Bajo	Bajo	Bajo
Nivel Dos: Planificado	Medio	Medio	Bajo	Medio	Medio	Medio	Medio
Nivel Tres: Establecido	Alto	Alto	Medio	Alto	Medio	Medio	Medio
Nivel Cuatro: certificado	Alto	Alto	Alto	Alto	Medio	Medio	Medio
Nivel Cinco: Innovado, de mejora continua:	Alto	Alto	Alto	Alto	Alto	Alto	Alto

Componente / Nivel	Gobernabilidad y controles organizacionales	Capacitación y concienciación en habilidades de ciberseguridad	Marco jurídico y normativo de la estrategia de ciberseguridad	Gestión de activos tecnológicos	Gestión de usuarios y accesos	Estrategias de gestión de riesgos y amenazas	Protección de la información y procedimientos
Nivel Cero: Cultura inexistente	Nulo	Nulo	Nulo	Bajo	Bajo	Nulo	Bajo
Nivel Uno: Inicial	Bajo	Bajo	Nulo	Bajo	Bajo	Bajo	Bajo
Nivel Dos: Planificado	Medio	Medio	Bajo	Medio	Medio	Medio	Medio
Nivel Tres: Establecido			Medio		Medio	Medio	Medio
Nivel Cuatro: certificado					Medio	Medio	Medio
Nivel Cinco: Innovado, de mejora continua:							

Conclusiones

- **Se ha construido una propuesta de Modelo de Madurez en el contexto de las IES de manera particular, en base de varios modelos de madurez relacionados, realizando una síntesis integrativa y completando conceptos no comunes en los modelos de referencia.**

- **El establecer una cultura de ciberseguridad exitosa en una IES implica la integración de diversos componentes que aborden tanto los aspectos técnicos como los comportamientos y procesos organizativos. Al comprender y definir estos componentes, la IES estará mejor preparada para construir una cultura resistente a las amenazas cibernéticas.**

- **Con el análisis de los modelos relacionados se ha revelado que cada uno tiene sus propias ventajas. La combinación estratégica de elementos de estos modelos permite la creación de un Modelo de Madurez de la Cultura de Ciberseguridad adaptado a las necesidades específicas y al contexto de la organización.**

Recomendaciones

- **Se recomienda validar el modelo en forma comparativa con la simulación realizada, para probar el grado de aplicabilidad y la consistencia del modelo.**

- **Es importante elaborar y ejecutar un Plan de Mejora de la Cultura de la Ciberseguridad de la Información, en base de la aplicación del modelo, para fomentar una cultura de responsabilidad compartida, en la que cada miembro de la organización se vea como un defensor activo, esto implica la comprensión de que la ciberseguridad es responsabilidad de todos.**

- **Para la aplicación sistemática del modelo, se recomienda lograr un nivel mínimo de participación de los diferentes grupos ocupacionales, de esta manera los resultados serán más confiables y objetivos.**