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

Abadiano Guamantica, Sahian Alejandra y Camacho Tene, Santiago Alexander

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de titulación previo a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Ron Egas Mario Bernabé

29 de febrero de 2024

Copyleaks

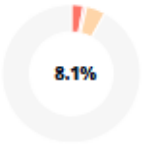
Plagiarism and AI Content Detection Report

TIF-Modelo de madurez de la cultura ...

Scan details

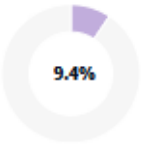
Scan time:	Total Pages:	Total Words:
March 17th, 2024 at 23:52 UTC	92	22862

Plagiarism Detection



Types of plagiarism		Words
Identical	2.9%	657
Minor Changes	0.7%	164
Paraphrased	4.5%	1039
Omitted Words	0%	0

AI Content Detection



Text coverage		Words
AI text	9.4%	2159
Human text	90.6%	20703

Learn more

Plagiarism Results: (94)

Lección 1 de 6: Ciberseguridad y Derecho. Aspectos generales. – derechoi... 0.3%

https://www.derechoinformatico.cl/leccion-1-ciberseguridad-y-derecho/

Skip to main content derechoinformatico.CL ...

OBTENCIÓN DE LA CERTIFICACIÓN CMMC PARA CONTRATISTAS DE DEFENS... 0.3%

https://cases-quality-insights.wp-magazines.com/magazine/qualityinsightsvol4-spanish/cmmc/

Search Editions ...

Matriz_requisitos_comunes.pdf 0.3%

https://www.alcaldiabogota.gov.co/docsig/documentos/acciones/matriz_requisitos_comunes.pdf

Ellien Yulieth Rodríguez Rincon

REQUISITOS COMUNES NORMA ISO 27001, MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL REQUISITO NORMA ISO 27001 MSPI ...

T-UIDE-0140.pdf 0.3%

https://repositorio.uide.edu.ec/bitstream/37000/4588/1/t-uide-0140.pdf

Carolina Almeida Morales

MAESTRÍA EN PSICOPEDAGOGÍA INFORME DE INVESTIGACIÓN TÍTULO: TÉCNICAS DE MINDFULNESS Y SU INFLUENCIA EN LOS PROFESIONALES EN ENFERMERÍA ...

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de titulación: "**Propuesta de un modelo de madurez de la cultura de Ciberseguridad para una IES**" fue realizado por los señores **Abadiano Guamantica Sahian Alejandra y Camacho Tene Santiago Alexander;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 29 de febrero de 2024

.....

Ron Egas Mario Bernabé

C. C. 1704229747

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Nosotros, **Abadiano Guamantica Sahian Alejandra y Camacho Tene Santiago Alexander**, con cédulas de ciudadanía N.° 1751991140 y N.° 1900788751, declaramos que el contenido, ideas y criterios del trabajo de titulación: **Propuesta de un modelo de madurez de la cultura de Ciberseguridad para una IES** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 29 de febrero de 2024

Firma:

Abadiano Guamantica Sahian Alejandra

C.C.: 1751991140

Camacho Tene Santiago Alexander

C.C.:1900788751

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Nosotros **Abadiano Guamantica Sahian Alejandra y Camacho Tene Santiago Alexander**, con cédulas de ciudadanía N.° 1751991140 y N.° 1900788751, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación **Propuesta de un modelo de madurez de la cultura de Ciberseguridad para una IES,** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 29 de febrero de 2024

Firma:

.....	.....
Abadiano Guamantica Sahian Alejandra	**Camacho Tene Santiago Alexander**
C.C.: 1751991140	C.C.:1900788751

Dedicatoria

A ti abuelito querido, que siempre esperaste este momento, y aunque ya no estés aquí sé que ves y compartes mi alegría.

Sahián Alejandra Abadiano Guamantica

Para ti mamá que siempre eres mi motor para salir adelante.

Santiago Alexander Camacho Tene

Agradecimientos

Agradezco a Dios, a mi madre que ha sido mi principal apoyo y motivación, a mi familia y seres queridos quienes estuvieron en cada tapa de mi vida hasta este momento en el que he cumplido una meta más en el ámbito profesional.

Sahián Alejandra Abadiano Guamantica

Agradezco primeramente a Dios, por permitirme culminar este objetivo de vida, a mi amada madre Guina que nunca perdió la fe en mí y me apoyó en cada obstáculo que se atravesó durante esta etapa, a mi querido padre Luis por forjar mi carácter, a mi querido hermano Adrián que supo apoyarme en este trayecto de mi vida y a mi amada hermana Daniela que siempre estuvo para mí.

Santiago Alexander Camacho Tene

Índice de contenido

Índice de Tablas

Índice de Figuras

Resumen

La Cultura de Ciberseguridad se ha convertido en un elemento clave para la gestión de riesgos informáticos a nivel organizacional. El siguiente resumen destaca los puntos críticos, las tácticas empleadas y los beneficios de la creación de este modelo, ofreciendo una perspectiva general del camino hacia una cultura de ciberseguridad sólida y adaptable. En este estudio se elaboró un modelo de la cultura de ciberseguridad aplicable a Instituciones de Educación Superior. La metodología consistió en una extensa revisión bibliográfica de nueve modelos de madurez de ciberseguridad, y a su vez se aplicó el método ecléctico, el cual consiste en la combinación de elementos de diversas fuentes. A partir de esto se definen siete componentes principales: 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. Estos componentes abarcan controles relacionados a los distintos grupos ocupacionales dentro de una Institución de Educación Superior. Para el modelo se definen también los niveles de madurez, que se obtienen mediante la misma metodología, entonces se tienen seis niveles, empezando con el nivel 0– Cultura inexistente, nivel 1–inicial, nivel 2–Planificado, nivel 3–Establecido, nivel 4–Certificado y nivel 5–Innovado, siendo el nivel 0 el más bajo y el indicativo de una cultura de ciberseguridad deficiente o casi inexistente; y el nivel 5, el nivel de madurez más alto, que representa una cultura bien cimentada, definida, y en proceso de mejora continua.

Palabras clave: Ciberseguridad, Modelo de Madurez, ISO 27001, Cultura de Ciberseguridad, Institución de Educación Superior.

Abstract

Cybersecurity Culture has become a key element in managing IT risk at the organizational level. The following summary highlights the critical points, tactics employed, and benefits of creating this model, providing an overview of the path to a robust and adaptive cybersecurity culture. This study developed a model of cybersecurity culture applicable to Higher Education Institutions (HEIs). The methodology consisted of an extensive literature review of nine models on the topic of cybersecurity maturity models, and in turn the eclectic method was applied, which consists of combining elements from various sources, from this seven main components are defined: Organizational governance and controls, Cybersecurity skills training and awareness, Legal and regulatory framework of the cybersecurity strategy, Technology asset management, User and access management, Risk and threat management strategies, Information protection and procedures. These components cover controls related to the different occupational groups within a Higher Education Institution. For the model, the maturity levels are also defined, which are obtained through the same methodology, so there are six levels, starting with Level 0 - non-existent culture, Level 1 - initial, Level 2 - planned, Level 3 - established, Level 4 - certified and Level 5 - innovated, with Level 0 being the lowest level of maturity and indicative of a deficient or almost non-existent cybersecurity culture; and Level 5, the highest maturity level, representing a culture that is well established, defined, and in the process of continuous improvement.

Keywords: Cybersecurity, Maturity Model, ISO 27001, Cybersecurity Culture, Higher Education Institution.

Capítulo I: Aspectos Generales

Antecedentes

En una Institución de Educación Superior (IES), la innovación, la tecnología y el aprendizaje son esenciales para mejorar la eficiencia y automatizar procesos en todas las áreas. La evolución tecnológica brinda oportunidades significativas para crear entornos de aprendizaje más avanzados, superando las barreras educativas actuales. Aunque la adopción de tecnología en la educación enfrenta desafíos al cuestionar las prácticas educativas tradicionales, cada vez más instituciones optan por estas herramientas para facilitar el aprendizaje dentro y fuera de las aulas. (Rico, 2022)

Las IES son organizaciones complejas y diversas que se esfuerzan por cumplir sus funciones educativas, de investigación y desarrollo dentro de un ambiente cambiante de innovación, preparando a los estudiantes para su futuro como profesionales. En este contexto como lo menciona Novelo et al. (2019), la innovación tecnológica se vuelve crucial para que estas instituciones integren nuevos proyectos de Tecnologías de la Información y Comunicación (TIC). Cada día surgen tecnologías, conceptos y estándares de manera acelerada en sectores como la industria, el gobierno y otros organismos. Esto incluye áreas como Inteligencia Artificial, Big Data, Minería de Datos, Ciberseguridad y Seguridad de la Información, entre otros. La ciberseguridad se destaca como un componente esencial en este panorama tecnológico en constante evolución, siendo crucial para proteger la integridad de la información y garantizar la seguridad en las operaciones de las IES.

A partir de aquí, la manera en la que las organizaciones manejan la capacidad de ciberseguridad es fundamental para establecer un sistema de seguridad cibernética efectivo, eficiente y sostenible. Con el fin de mejorar la seguridad, la industria y la comunidad técnica han desarrollado Modelos de Madurez de Ciberseguridad. Estos modelos evalúan las habilidades de seguridad cibernética y las clasifican en diferentes niveles, brindando una base para la mejora continua. Por lo tanto, es esencial identificar cuáles de ellos son los principales y están disponibles en el mercado. (Rea et al., 2017)

Debemos tomar en cuenta que, como menciona Rea et al. (2017), un Modelo de Madurez de Ciberseguridad se refiere a un conjunto de características que indican la capacidad y evolución de una IES en cuanto a seguridad cibernética. Incluye mejores prácticas y puede incorporar normas o códigos específicos de esta disciplina. Entonces, en el contexto de una institución, este modelo considera la ciberseguridad en distintas áreas interconectadas. Cada área proporciona factores e indicadores que permiten entender en qué etapa de madurez se encuentra la institución. Las etapas van desde un nivel inicial, donde se aborda la ciberseguridad, hasta un nivel dinámico, donde existe una mayor adaptación a los cambios, ya sea en términos de amenazas, vulnerabilidades, riesgos, estrategias económicas o necesidades organizacionales cambiantes.

En el contexto de nuestro país, Morales & Medina (2021), en su estudio referente a este tema, mencionan que en Ecuador aún no se ha formulado una estrategia nacional integral de ciberseguridad específicamente dirigida a las IES. Esta estrategia sería fundamental para definir las pautas, metas y acciones necesarias para resguardar los servicios, la información, las infraestructuras críticas y a los usuarios frente a las amenazas cibernéticas presentes en el espacio digital.

Por este motivo, la presente investigación pretende definir un Modelo de Madurez de la Cultura de Ciberseguridad en el contexto de una IES, basándose en Modelos de Madurez de Ciberseguridad antes definidos y aplicados a entornos similares, incluyendo la familia de normas internacionales ISO 27000:2022.

Formulación del problema

Se creía en un principio que solo la información era importante para cualquier organización dado que era el activo más importante, sin embargo, la infraestructura tecnológica y el personal, constituyen también el motor fundamental de una organización y deben ser protegidos ante posibles ciberataques.

Según Cornejo et al. (2019): “La ciberseguridad es el conjunto de políticas y acciones dirigidas a proteger los activos de información de una organización en general, y a la comunidad en el ciberespacio “.

Para comenzar a abordar la ciberseguridad, la organización debe analizar su situación actual implementando Modelos de Madurez de Ciberseguridad. En el nivel inicial de madurez, los modelos principales detallados en estudios científicos, identifican la gestión de riesgos de ciberseguridad como un componente fundamental y cada uno de ellos describe los componentes necesarios para la gestión de riesgos de manera diferente.

Teniendo en cuenta lo anterior, se considera que las organizaciones pueden disponer de un Modelo de Madurez que permita evaluar el estado actual de la cultura de ciberseguridad, identificar áreas de mejora y establecer objetivos específicos para fortalecer la protección de datos y sistemas en la institución.

Las IES no son la excepción, por tanto, se busca implementar un Modelo de Madurez de la Cultura de Ciberseguridad para garantizar la protección de la información sensible y la continuidad de sus operaciones.

Justificación

La Propuesta de un Modelo de Madurez de la Cultura de Ciberseguridad en una IES se justifica en el contexto actual, donde cualquier organización que maneje sistemas y tecnologías de la información, enfrenta riesgos y amenazas cibernéticas que pueden comprometer su funcionamiento. Así como lo menciona(Guerrero, 2023), la protección de la información implica la implementación de normas, reglamentos, leyes y políticas que contribuyan a gestionar la ciberseguridad, salvaguardando así los sistemas de información e infraestructuras cruciales para el crecimiento y desarrollo de la estrategia organizacional.

Se comprende que la protección de la información no solo requiere la implementación de normas y políticas, sino también una evaluación continua del nivel de seguridad. En este contexto, la evaluación de riesgos se presenta como una herramienta fundamental para determinar la efectividad de las medidas de seguridad implementadas.(Vallejo, 2023)

La propuesta de un modelo de madurez se fundamenta en estándares y principios reconocidos internacionalmente en la familia de normas ISO 27000:2022.

Este modelo de madurez no solo proporciona una estructura para evaluar el nivel de madurez de la cultura de seguridad, sino que también ofrece la facilidad de enfocarse en las acciones correctivas, contribuyendo al desarrollo de una estrategia organizacional en este entorno.

Objetivos

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 27000:2022.

Objetivos específicos

- Establecer el estado del arte mediante una revisión exhaustiva de la literatura existente acerca de modelos de madurez de cultura de ciberseguridad.
- Indagar y definir 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 de Madurez de la Cultura de Ciberseguridad final.

Alcance

El trabajo de investigación comprende la elaboración de un Modelo de Madurez de la Cultura de Ciberseguridad para una IES, como referencia, a la Universidad de las Fuerzas Armadas-ESPE, mismo que será definido de acuerdo a componentes / elementos propios de

la IES y varios niveles de madurez que servirán para establecer la condición de la cultura de ciberseguridad.

Capítulo II: Revisión Sistemática de Literatura

Marco Conceptual

Ciberseguridad

La ciberseguridad es la tarea de proteger computadoras, dispositivos y datos contra ataques maliciosos. Se divide en áreas como la seguridad de red, que brinda protección contra intrusos, y la seguridad de las aplicaciones, que mantiene el software seguro desde su diseño. La recuperación ante desastres y la continuidad del negocio son planes para responder a incidentes, así como también la capacitación del usuario final, que se enfoca en enseñar al personal, buenas prácticas de seguridad para evitar amenazas (Castillo & Polanco, 2016).

Según ISACA (2024), la ciberseguridad es: “La protección de los activos, abordando las amenazas a la información procesada, almacenada y transportada por sistemas interconectados.”

Existen tres tipos principales de ciber amenazas según Fortaleza Abogados (2023) :

- Delito Cibernético: Involucra a individuos o grupos que atacan sistemas para obtener ganancias financieras o causar interrupciones.
- Ciberataques: Intento malicioso de comprometer la integridad, confidencialidad o disponibilidad de sistemas informáticos, redes o datos digitales.
- Ciberterrorismo: Busca debilitar sistemas electrónicos para causar pánico o temor.

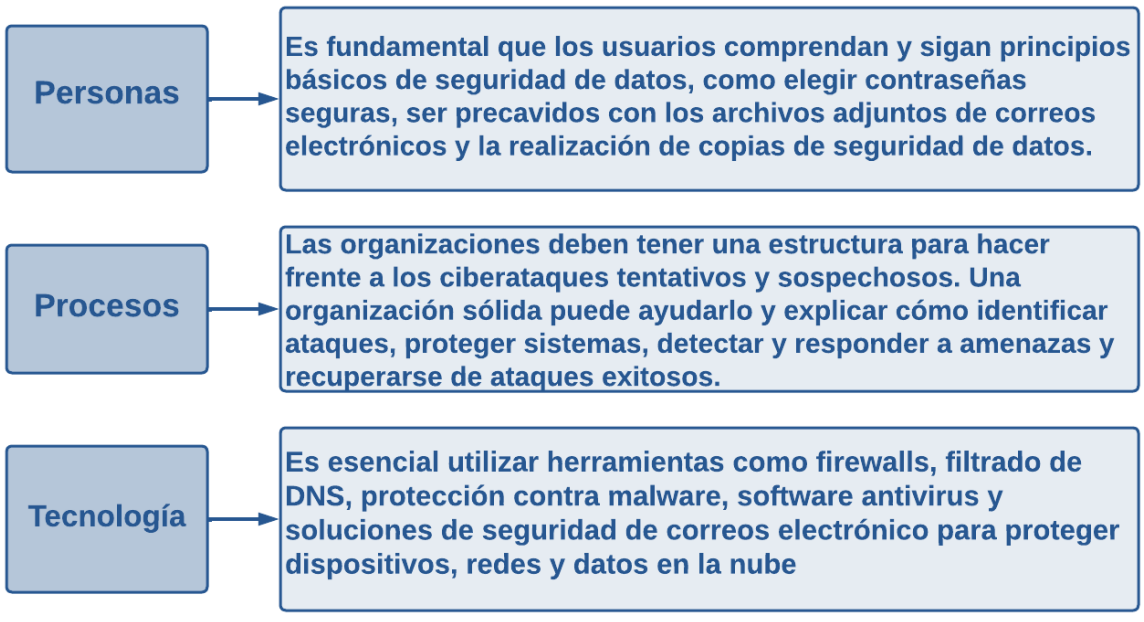
Los agentes malintencionados utilizan varios métodos para amenazar la ciberseguridad:

- Malware: Software malicioso, como virus, troyanos, spyware, ransomware, adware y botnets, que dañan o interrumpen los sistemas.

- Inyección de Código: Ataque para tomar control y robar datos de bases de datos explotando vulnerabilidades en aplicaciones basadas en datos.
- Phishing: Ataques con correos electrónicos que parecen legítimos para obtener información confidencial.
- Ataque Man-in-the-Middle: Intercepción de comunicaciones para robar datos, como en redes Wi-Fi no seguras.
- Ataque de Denegación de Servicio: Sobrecarga de redes y servidores para hacer que un sistema sea inutilizable, impidiendo funciones vitales.

En una organización los componentes principales que se deben supervisar para hacer frente a los ciberataques según Cisco (2024), son los detallados en la Figura 1:

Figura 1
Componentes clave de una organización en el ámbito de ciberseguridad.



Nota. La figura presenta los componentes principales de la ciberseguridad. Tomado de (Cisco, 2024)

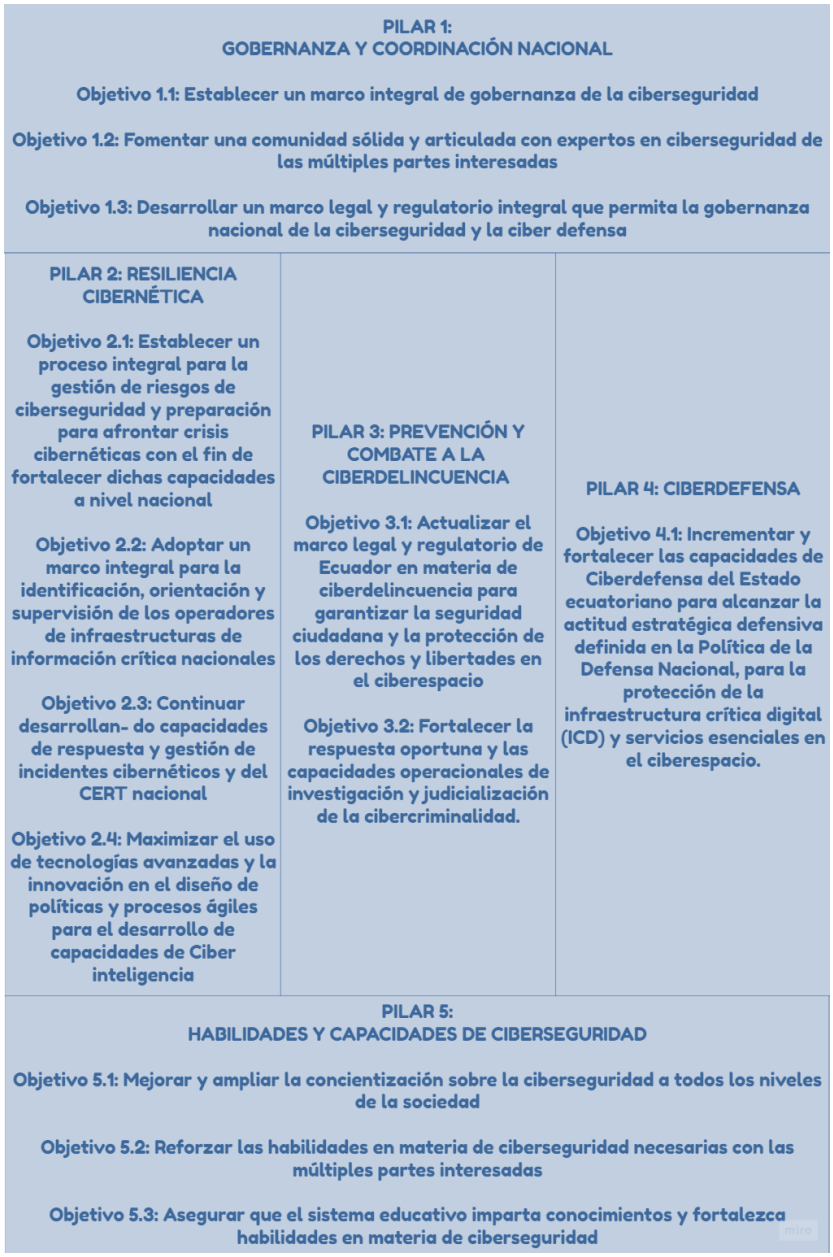
Ciberataques en Ecuador

Los ataques cibernéticos en la región han aumentado, principalmente dirigidos a las entidades financieras de América Latina. El aumento de la actividad digital en la región como resultado de la pandemia de COVID-19 ha puesto en evidencia las vulnerabilidades del espacio digital de América Latina y el Caribe (BID & OEA, 2020).

En los últimos años, Ecuador ha trabajado para mejorar y ampliar el acceso al Internet para la población, empresas y administración pública en todo el país, lo que ha acelerado el progreso económico y social en toda la nación. Por otro lado, las amenazas han incluido ciberataques a nuestras Infraestructuras Críticas Digitales (ICD), infraestructuras tecnológicas obsoletas, altos costos para la adquisición de tecnología y marcos legales y regulatorios desactualizados, lo que nos ha hecho vulnerables (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

El gobierno de Ecuador ha planteado seis pilares de la Estrategia Nacional de Ciberseguridad, y se detalla en la Figura 2, un resumen de la importancia de la ciberseguridad, la situación actual, los problemas y desafíos prioritarios que se deben abordar, con los objetivos estratégicos y líneas de acción que acompañan a las medidas que se deben cumplir en relación con cada pilar.

Figura 2
Pilares de la estrategia Nacional de Ciberseguridad



Nota. Pilares y objetivos de la Estrategia Nacional de Ciberseguridad del Ecuador. Tomado de (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022)

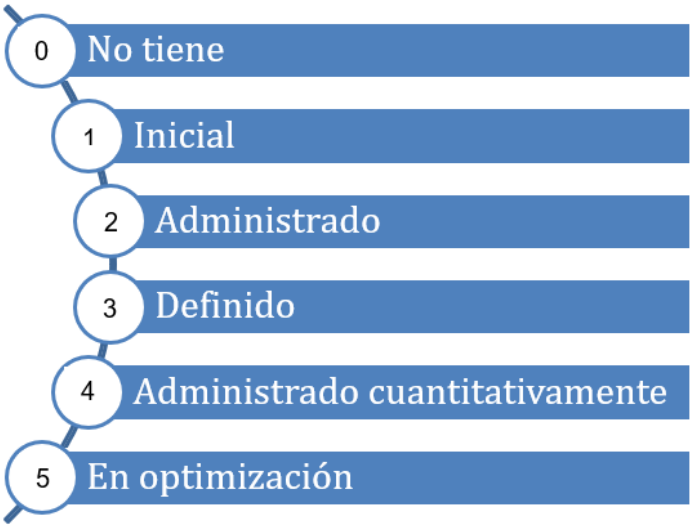
Modelo de Madurez de ciberseguridad

Rea (2020) describe al modelo de madurez como: “Un conjunto de características, atributos, indicadores o patrones que representan la capacidad y la progresión en una disciplina en particular.”

Por lo tanto, un modelo de madurez proporciona una estructura que permite a las organizaciones medir la eficacia de sus procesos en comparación con las mejores prácticas de la industria. Funciona como un estándar independiente que permite evaluar el nivel de madurez en diferentes áreas relacionadas, sirviendo como un punto de referencia para medir el desempeño de la organización.

El Modelo de Integración de la Madurez y la Capacidad (CMMI), es un estándar de calidad ampliamente adoptado a nivel mundial, especialmente en organizaciones de desarrollo de software. Ofrece dos enfoques para la mejora y evaluación de procesos, denominados representaciones: continua y escalonada. En la representación continua, las organizaciones eligen áreas específicas, mientras que la representación escalonada sigue un conjunto definido de áreas de proceso. El modelo utiliza niveles de capacidad y madurez para describir las rutas recomendadas y en sus dos enfoques, los niveles representan mejoras desde un estado inicial poco definido hasta un estado alineado con los objetivos del negocio. El CMMI ofrece flexibilidad, al permitir a las organizaciones elegir entre dos caminos para alcanzar un estado superior de mejora.(Pérez et al., 2014)

Figura 3
Niveles de madurez del modelo CMMI.



Nota. La figura muestra los niveles de madurez del modelo estándar CMMI. Tomado de (Pérez et al., 2014)

No hay un único modelo definido de madurez cuando hablamos de ciberseguridad, sino que existen varios marcos y modelos utilizados en la industria para evaluar y mejorar la madurez en ciberseguridad. Algunos de los modelos de madurez de ciberseguridad más conocidos según (Pérez et al., 2014), incluyen:

- Modelo de Madurez de Capacidades (CMM): Evalúa la capacidad de una organización para realizar procesos específicos. En el contexto de seguridad cibernética, proporciona una estructura para medir y mejorar las capacidades de seguridad.
- Marco de ciberseguridad del NIST: Emitido por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., ofrece pautas para ayudar a las organizaciones a gestionar y mejorar su postura de seguridad cibernética.
- ISO/IEC 27001: Esta norma internacional establece requisitos para un sistema de gestión de la seguridad de la información (SGSI). Aunque no es exclusivamente un modelo de madurez, su enfoque en la gestión de la seguridad informática puede contribuir a la madurez en este ámbito.
- Modelo de madurez de la Capacidad de Ciberseguridad (C2M2): Desarrollado por el Departamento de Energía de los EE. UU., se centra en la gestión de la ciberseguridad para organizaciones del sector energético.

Cultura de ciberseguridad

Según Hernández (2018) : “La Cultura de Ciberseguridad es entendida como el conjunto de principios, valores y acciones en materia de educación, formación y concientización.”

Dicho esto, la Cultura de Ciberseguridad se refiere a las actitudes, comportamientos y prácticas que una organización adopta en relación con la seguridad de la información y la tecnología. Los ataques cibernéticos son una de las principales amenazas a la seguridad nacional e internacional. No es posible una respuesta efectiva a las amenazas cibernéticas sin la participación de todos los sectores de la sociedad a través de una cultura de

ciberseguridad. No obstante, entendemos que esta no puede ser abordada por sí sola, sino como parte de una cultura de seguridad y defensa más amplia (De Tomás Morales, 2014).

En otro concepto, la cultura de ciberseguridad hace referencia a los procedimientos que una organización establece para que todos sus empleados sepan cómo actuar en situaciones relacionadas con la integridad de los datos, mientras cumplen con sus deberes. Los actores humanos y las políticas de ciberseguridad son las principales causas de las filtraciones de información dentro de las organizaciones (Ioannou et al., 2019).

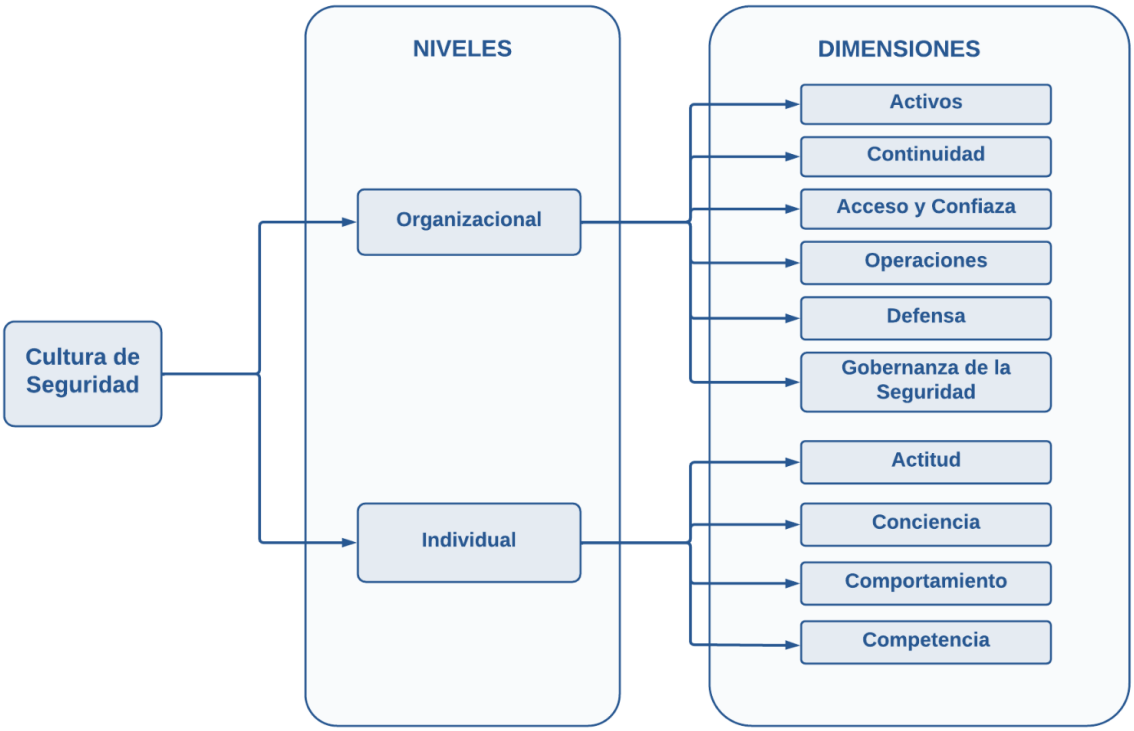
Elementos de la Cultura de ciberseguridad

La cultura de ciberseguridad se desarrolla mediante un proceso largo y progresivo en el que intervienen una variedad de factores que contribuyen al estado cultural de una organización a través de pruebas, exámenes y entrevistas. Esta interacción continua de evaluación ayuda a reducir las amenazas cibernéticas humanas o personales.

Los estudios y enfoques de expertos en seguridad de la información han logrado elaborar un modelo de cultura de seguridad detallado en la Figura 4, en el cual se han combinado elementos y rasgos humanos con parámetros organizativos internos y externos. Más concretamente, este modelo define claramente dos niveles: El nivel organizativo pretende abarcar todos los factores relacionados con la infraestructura tecnológica de seguridad de una organización, operaciones, políticas y procedimientos, mientras que el nivel individual se centra en los atributos y características de los empleados con un impacto inmediato en su actitud y comportamiento en materia de seguridad. (Georgiadou et al., 2022)

De esta manera, se integran las dos perspectivas antes mencionadas y el modelo sugerido logra integrar los elementos humanos externos e internos.

Figura 4
Modelo de cultura de ciberseguridad



Nota. La figura detalla los niveles y dimensiones del modelo de cultura de ciberseguridad. Tomado de Georgiadou et al. (2022).

Georgiadou et al. (2022) describió cada nivel en diferentes dimensiones.

El nivel organizativo se divide en dimensiones como el diseño, el desarrollo, la documentación y la aplicación de políticas y procedimientos de seguridad para diferentes áreas de la empresa. Más específicamente:

- Activos: Se refiere a los activos de la organización (incluidas las personas, edificios, máquinas, sistemas y activos de información) e incluye políticas que aplican varios niveles de confidencialidad, disponibilidad e integridad.
- Continuidad: Tiene por objeto garantizar la continuidad de las operaciones, los servicios y la producción de una organización a niveles predefinidos, salvaguardando al mismo tiempo la reputación y los intereses de las principales partes interesadas en caso de incidentes.

- Acceso y confianza: Se centra en el acceso adecuado a recursos en toda la organización, aclarando al mismo tiempo roles y permisos. Además, delimita las interacciones de la organización con factores de terceros, como proveedores, clientes, autoridades, entre otros.
- Operaciones: Se refiere a la administración de las prácticas empresariales para crear el mayor nivel de eficiencia posible dentro de una organización, teniendo en cuenta al mismo tiempo los aspectos de seguridad que salvaguardan sus resultados finales.
- Defensa: Se centra en la previsión de haber planificado, adquirido y configurado adecuadamente todos los activos técnicos necesarios para la mejora y el funcionamiento eficaz de su seguridad de la información.
- Gobernanza de la seguridad: Se refiere a las medidas adoptadas para planificar, gestionar y mejorar eficazmente la seguridad de la información.

Georgiadou et al. (2022) por otra parte también describió el nivel individual, mismo que se compone de las siguientes dimensiones:

- Actitud: Se refiere a los sentimientos y creencias de los empleados hacia los protocolos y temas de seguridad.
- Conciencia: Examina la comprensión, el conocimiento y la concienciación de los empleados sobre las cuestiones y actividades de seguridad.
- Comportamiento: Estudia el comportamiento consciente de la seguridad exhibido en el día a día en el lugar de trabajo de un individuo.
- Competencia: Evaluación de las habilidades, destrezas, conocimientos y experiencia de los empleados que les permiten desempeñar sus funciones y conocimientos para ajustarse a las políticas y procedimientos de seguridad de la organización.

Familia normas ISO 27000

Abarca desde la norma 27000 hasta la 27019 y de la 27030 a la 27044, tiene asignado a cada norma un número específico dentro de esta serie. Es crucial destacar que esta

estandarización no solo proporciona controles y procesos para gestionar riesgos relacionados con la seguridad de la información, sino que también incluye una norma inicial, la ISO 27000, que establece definiciones y términos clave para toda la serie. Esta norma juega un papel esencial al proporcionar un vocabulario claramente definido, evitando así malentendidos en la interpretación de conceptos técnicos y de gestión. (Alonso, 2023)

Es importante señalar que la norma ISO 27000, a diferencia de otras en la serie, está disponible de manera gratuita, facilitando su acceso y uso en comparación con las normas que conllevan costos de implementación.

En resumen, como lo detalla Alonso (2023), el conjunto de estándares de la familia ISO 27000, comprende los siguientes:

- ISO 27001: Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Es la norma más importante de la familia y es certificable.
- ISO 27002: En soporte del proceso de gestión de riesgos de la norma ISO/IEC-27001, define un conjunto de buenas prácticas para la implantación del SGSI, a través de 93 controles, estructurados en 4 grandes dominios.
- ISO 27003: Proporciona una guía para la implantación de forma correcta de un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.
- ISO 27004: Proporciona pautas orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI.
- ISO 27005: Define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información, orientado en cómo establecer la metodología a emplear.
- ISO 27006: Establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001.
- ISO 27007: Es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar implementaciones de la ISO/IEC-27001.

- ISO 27008: Define cómo se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos.
- ISO 27009: Complementa la norma ISO/IEC-27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivo de hacer más eficaz su implantación.
- ISO 27010: Indica cómo debe ser tratada la información cuando es compartida entre varias organizaciones, qué riesgos pueden aparecer y los controles que se deben emplear para mitigarlos, especialmente cuando están relacionados con la gestión de la seguridad en infraestructuras críticas.
- ISO 27011: Establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando cómo implantar los controles de manera eficiente.
- ISO 27013: Establece una guía para la integración de las normas ISO/IEC-27001 (SGSI) y ISO/IEC-20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.
- ISO 27014: Establece principios para el gobierno de la seguridad de la información.
- ISO 27015: Facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros y de seguros.
- ISO 27016: Proporciona una guía para la toma de decisiones económicas vinculadas a la gestión de la seguridad de la información, como apoyo a la dirección de las organizaciones.
- ISO 27017: Proporciona una guía para los servicios Cloud, con controles basados en la norma ISO/IEC-27002.
- ISO 27018: Complementa a las normas ISO/IEC-27001 y ISO/IEC-27002 en la implantación de procedimientos y controles para proteger datos personales en aquellas organizaciones que proporcionan servicios en Cloud para terceros.

- ISO 27019: Facilita una guía basada en la norma ISO/IEC-27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI.
- ISO 27021: Establece los requisitos de competencia para los profesionales del SGSI que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del SGSI.
- ISO 27022: Proporciona un modelo de referencia de procesos para el SGSI.
- ISO 27023: facilita una guía de correspondencias entre las normas ISO/IEC-27001 y ISO/IEC-27002.
- ISO 27031: Proporciona apoyo para la adecuación de las tecnologías de la información y comunicación.
- ISO 27032: Facilita la identificación de las líneas generales para fortalecer el estado de la ciberseguridad en una compañía.
- ISO 27033: Establece las pautas de seguridad de la administración, operación y uso de las redes.
- ISO 27034: Proporciona orientación en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación.
- ISO 27035: Define un conjunto de mejores prácticas relacionadas con la gestión de incidentes de seguridad haciendo hincapié en la detección, reporte y evaluación de incidentes de seguridad.
- ISO 27036: Referida a la Seguridad de la información para las relaciones con proveedores, ofrece orientación sobre la evaluación y el tratamiento de los riesgos de información involucrados en la adquisición de bienes y servicios de proveedores.
- ISO 27037: Ofrece directrices para la identificación, recolección, adquisición y preservación de evidencias digitales.
- ISO 27038: Especifica las características de las técnicas para la redacción digital.
- ISO 27039: Proporciona una guía para ayudar a las compañías con la selección, despliegue y operación de sistemas de detección y prevención de intrusión.

- ISO 27040: Facilita unas pautas para proteger la seguridad de los sistemas de almacenamiento, así como para la protección de los datos contenidos en los mismos.
- ISO 27041: Ofrece una guía y directrices para garantizar la idoneidad y adecuación de los métodos de investigación de incidentes.
- ISO 27042: Define las directrices para un correcto análisis e interpretación de evidencias digitales.
- ISO 27043: Proporciona una guía de principios y procesos para la recopilación de evidencias digitales e investigación de incidentes.
- ISO 27050: Se trata de una norma desarrollada en cuatro partes que trata sobre la información almacenada en dispositivos electrónicos.
- ISO 27070: Define requisitos de seguridad que tienen como objetivo establecer raíces de confianza para la provisión de entornos informáticos confiables.
- ISO 27099: Ofrece requisitos para gestionar la seguridad de la información para los proveedores de servicios de confianza de infraestructura de clave pública (PKI).
- ISO 27100: Facilita una visión general de la ciberseguridad y define conceptos relevantes que estén relacionados.
- ISO 27102: Describe pautas de gestión para cuando se considere la adquisición de seguros cibernéticos como una opción de tratamiento de riesgos.
- ISO 27103: Ofrece una guía sobre el aprovechamiento de los estándares y normas existentes en un marco de ciberseguridad.
- ISO 27110: Basada en los principios de flexibilidad, compatibilidad e interoperabilidad, esta norma proporciona directrices para estandarizar medidas de seguridad.
- ISO 27400: Proporciona una guía basada en directrices sobre riesgos, principios y controles para la seguridad y privacidad de las soluciones de Internet de las cosas (IoT).
- ISO 27550: Ofrece pautas de ingeniería de privacidad orientadas a ayudar a las organizaciones a integrar en sus procesos del sistema los avances en la ingeniería de privacidad.

- ISO 27555: Facilita directrices para el desarrollo e implantación de políticas y procedimientos para la eliminación de la información de identificación personal (PII) en las organizaciones.
- ISO 27570: Proporciona orientación sobre la protección de la privacidad en el desarrollo de los ecosistemas de las ciudades inteligentes.
- ISO 27701: Desarrollada como una guía de extensión a los requerimientos y controles de la ISO 27001, aporta a las organizaciones los requisitos para administrar, gestionar los datos y proteger la privacidad de la información de identificación personal (PII).
- ISO 27799: Define directrices para la implementación de la ISO/IEC-27002 en la industria de la salud.

Figura 5
Clasificación de la familia de normas ISO 27000

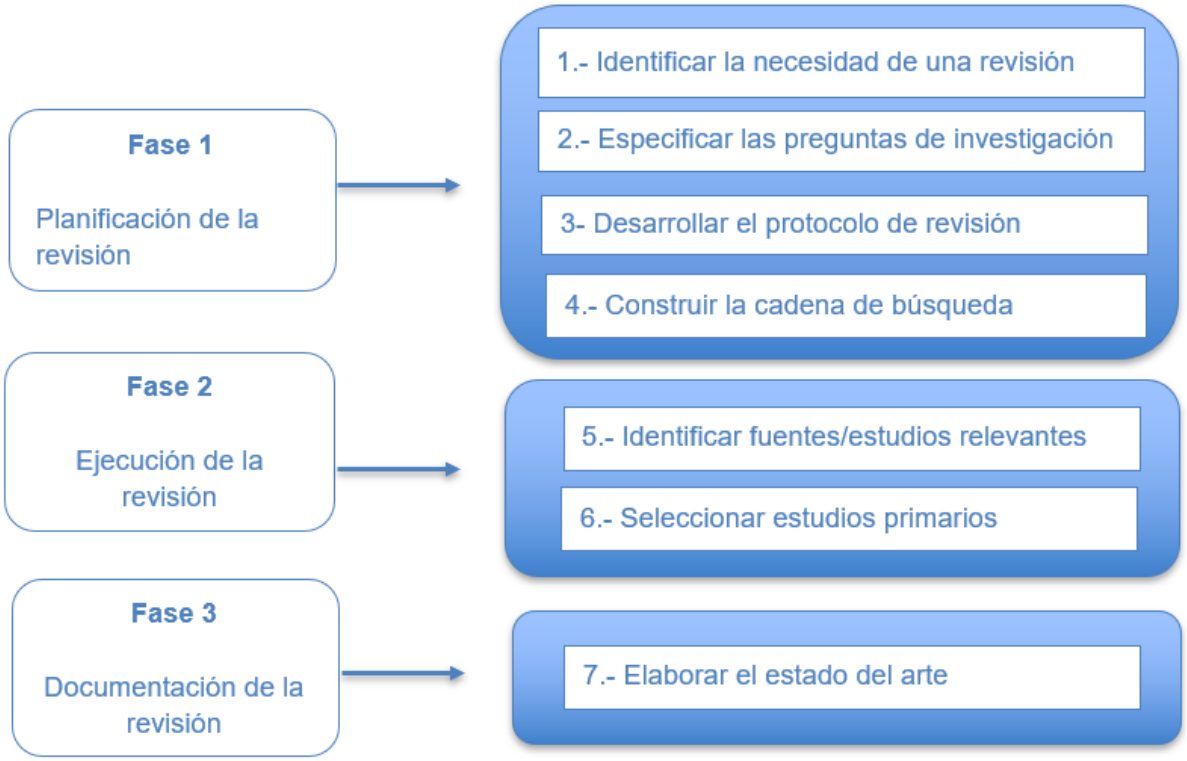
Nota. La figura muestra la clasificación de la familia de normas ISO 27000. Tomado de (Alonso, 2023)

Estado del arte

Realizar una revisión sistemática de la literatura nos permitirá obtener los mejores conocimientos acerca de los distintos modelos de madurez de ciberseguridad como base para desarrollar una buena cultura organizacional en el contexto de la ciberseguridad, para

ello se ha tomado como referencia el método propuesto por Bárbara Kitchenham cuyas fases se muestran a continuación:

Figura 6
Esquema de revisión de literatura



Nota. La figura detalla los pasos del esquema de revisión de literatura tomado de la metodología de Bárbara Kitchenham

Planificación de la Revisión

Identificar la Necesidad de una Revisión

Al plantear el problema central de esta investigación, nace la necesidad de ampliar el conocimiento sobre esta temática, apoyándonos en trabajos de investigación relacionados, que sean relevantes, aporten herramientas y fundamentos válidos y actualizados para el desarrollo de los objetivos planteados.

Especificar las Preguntas de Investigación

RQ1. ¿Cuáles son los modelos de madurez existentes para evaluar la cultura de ciberseguridad en contextos similares a instituciones de educación superior?

RQ2. ¿Cuáles son los criterios de evaluación y métricas más relevantes para medir la madurez de la cultura de ciberseguridad en una IES, según la literatura actual?

RQ3. ¿Cuáles son los desafíos que enfrentan las IES en términos de ciberseguridad y cómo pueden abordarse a través de un modelo de madurez de la cultura de ciberseguridad?

RQ4. ¿Cómo influye la madurez de la cultura de ciberseguridad en las IES en la protección de datos sensibles y la prevención de amenazas cibernéticas?

Desarrollar el protocolo de revisión

Criterios de inclusión

Los artículos de investigación que se seleccionó para que formen parte de la revisión cumplen los siguientes criterios:

- Aquellos trabajos que estén directamente relacionados con el tema planteado.
- Aquellos trabajos que contengan como palabras claves, los temas usados para formular las cadenas de búsqueda.
- Aquellos trabajos que se incluyen en fuentes reconocidas, como revistas científicas, portales de difusión o bibliotecas electrónicas.

Criterios de exclusión

Se excluyen aquellos trabajos relacionados, publicados fuera de un rango de tiempo entre 2018 - 2023, cuyas fuentes no fueron confiables y su contenido no estaba completamente disponible.

Construir la cadena de búsqueda.

Repositorios Digitales

Los repositorios digitales que se utilizarán en este proceso son: IEEE (https://www.ieee.org/)
Google Académico (https://scholar.google.es/schhp?hl=es), Dialnet (https://dialnet.unirioja.es/) y Scielo (https://scielo.org/es/), ENISA (https://www.enisa.europa.eu/) e INCIBE (https://www.incibe.es/)

Cadenas de Búsqueda

[All: cybersecurity maturity model] AND [All: ISO 27000] AND [All: higher education institution]

[All: cybersecurity culture] AND [All: cybersecurity maturity model] AND [All: higher education institution]

[All: cybersecurity maturity model] AND [All: higher education institution] AND [cybersecurity culture] AND [Ecuador]

[modelo de madurez de ciberseguridad] AND [institución de educación superior]

[madurez de ciberseguridad] AND [ISO 27000] AND [institución de educación superior] AND [Ecuador]

[madurez de ciberseguridad] AND [IES] AND [Ecuador]

Ejecución de la Revisión

Identificar Fuentes/Estudios Relevantes

Al aplicar las cadenas de búsqueda en las diferentes bases digitales, repositorios digitales se obtuvo alrededor de 28 artículos relacionados con el tema, siendo un número de artículos bastante considerable.

Seleccionar Estudios Primarios

Tabla 1
Estudios Primarios

Código	Título	Cita
EP1	Línea Base de Ciberseguridad: Una Exploración, que permite delinear la Estrategia Nacional de Ciberseguridad en el Ecuador	(Ron et al., 2019)
EP2	Modelo De Gestión De Ciberseguridad Para Resolver Incidentes En Instituciones De Educación Superior	(Guerrero, 2023)
EP3	Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad	(Rea, 2020)

EP4	Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas	(González et al., 2023)
EP5	Desarrollar Cultura en Seguridad (INCIBE)	(INCIBE, 2023)
EP6	Informe del estado de cultura de ciberseguridad en el entorno empresarial.	(PwC, 2020)
EP7	Modelo de madurez para determinar el nivel de cultura de ciberseguridad en organizaciones industriales	(Bazalar et al., 2022)
EP8	Guía de ciberseguridad para pymes	(ENISA, 2023)

Nota. La tabla contiene los estudios primarios seleccionados a partir de la revisión de documentación.

Documentación de la Revisión

Elaborar el Estado del Arte

EP1 Línea Base de Ciberseguridad: Una Exploración, que permite delinear la Estrategia Nacional de Ciberseguridad en el Ecuador

Este estudio busca conocer el estado actual de la ciberseguridad en Ecuador, siguiendo un proceso sistemático y organizado considerando el nivel de madurez como uno de los criterios más importantes en una Estrategia Nacional de Ciberseguridad.

Contribuye con un modelo de nivel de madurez basándose en modelos ya existentes, como, el Modelo de Madurez publicado por la OEA, el Modelo de Capacidad de Proceso definido por ISACA y el modelo proporcionado en ISO/IEC 15504-2. Cada modelo consta de cinco y seis niveles respectivamente. A partir de lo mencionado, se definen seis niveles para el nuevo modelo que son: incompleto, implementado, gestionado, formalizado, consistente e innovador, siendo este último el nivel más óptimo, donde existiría la capacidad de innovar, y reaccionar rápidamente ante cambios en el entorno. Este modelo permite definir el estado actual del país y el nivel que el país podría alcanzar después de la aplicación de ciertas políticas. (Ron et al., 2019)

EP2 Modelo De Gestión De Ciberseguridad Para Resolver Incidentes En Instituciones De Educación Superior

La implementación de un modelo de gestión de incidentes sugiere establecer medidas respaldadas por estándares y normas para asegurar la integridad de la red, servidores, voz, datos y sistemas de información afectados, así como los recursos técnicos necesarios. La creciente amenaza de ciberataques ha impulsado la necesidad de desarrollar un proyecto enfocado en identificar y abordar las vulnerabilidades a las que las instituciones de educación superior podrían estar expuestas, con el objetivo de garantizar su correcto funcionamiento y proteger los datos frente a posibles amenazas. (Guerrero, 2023)

EP3 Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad

Se detallan varios modelos de madurez en Ciberseguridad al igual que se realiza una revisión y análisis de dichos modelos para realizar una comparación haciendo énfasis en la gestión de riesgos de ciberseguridad tales como: activos, amenazas y vulnerabilidades de ciberseguridad. Los elementos que participan en la identificación y evaluación de riesgos en ciberseguridad también son estudiados para la propuesta de un marco de trabajo que responda a los objetivos estratégicos institucionales de las organizaciones. (Rea, 2020)

EP4 Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas

Aborda los desafíos que enfrenta el sector financiero en cuanto a la ciberseguridad, destacando la necesidad de no solo proteger tecnologías, sino también a las personas en el entorno informático. Propone el diseño de un Modelo de Madurez de Cultura de Ciberseguridad para este sector, basado en buenas prácticas de instituciones y expertos en seguridad. La metodología empleada considera factores que influyen en la cultura de ciberseguridad, los mide mediante una valoración de atributos e indica un nivel de madurez. Este nivel proporciona a la organización conciencia sobre su estado actual, identifica brechas y retos, y sugiere acciones de control para la mejora continua. (González et al., 2023)

EP5 Desarrollar Cultura en Seguridad (INCIBE)

Se centra en el usuario como el eslabón más débil de una cadena por lo que hace énfasis en dar a comprender que la tecnología nunca es suficiente para garantizar la seguridad de la información.

Para establecer una cultura de seguridad en una empresa se deben realizar en primera instancia acciones de formación en seguridad para los empleados que están conformados por el personal técnico del Departamento de Informática y los usuarios de la empresa que tienen acceso a los sistemas de información corporativos. Como segunda instancia se deben establecer políticas, normas y procedimientos de seguridad que recogen las intenciones y objetivos que marca la organización en cuanto a la seguridad de la información y cuyo objetivo es declarar oficialmente que la seguridad es una parte importante de la cultura de nuestra empresa. La tercera instancia se trata de supervisar que se cumplan las buenas prácticas en seguridad por lo que debe existir un encargado responsable de seguridad para velar por la vigencia y actualización de las normas y procedimientos definidos anteriormente, la implantación de los mismos y el cumplimiento por parte de todos los empleados.

Por último y no menos importante se deben realizar acciones de sensibilización y concienciación en seguridad para empleados dado que el fracaso está garantizado si los empleados no se consideran parte importante de este proceso, porque son los principales protagonistas. (INCIBE, 2023)

EP6 Informe del estado de cultura de ciberseguridad en el entorno empresarial

Menciona que la cultura de ciberseguridad se centra en que las personas inviertan en cortafuegos humanos para protegerse contra los ciberataques y otras amenazas y riesgos de seguridad del día a día. Describe un framework de cultura en ciberseguridad, que permite ubicar a las organizaciones en cinco niveles de cultura y ayuda a establecer objetivos clave y

concretos para avanzar de nivel con iniciativas y acciones que involucren tanto el conocimiento como el comportamiento y la estrategia.

Recomienda que, para construir una cultura de ciberseguridad sólida, se necesitan capacitación, conciencia, promoción y medición constantes. El compromiso con los empleados garantizará que participen en la construcción de defensas sólidas contra el delito cibernético. (PwC, 2020)

EP7 Modelo de madurez para determinar el nivel de cultura de ciberseguridad en organizaciones industriales.

Este estudio se enfoca en cómo el comportamiento de las personas representa la mayor amenaza para la ciberseguridad. Considerando la realidad del entorno de estudio, los autores proponen un modelo para evaluar qué tan fuerte es la cultura de ciberseguridad en organizaciones industriales. Este modelo permite seguir de cerca la cultura mediante métricas específicas, presentando resultados fáciles de entender que respaldan proyectos para mejorar la conciencia de seguridad. El estudio se aplica a una empresa minera, mostrando su nivel de cultura de ciberseguridad actualmente y qué cambios se necesitan para alcanzar un nivel más seguro. El objetivo final es que los empleados cambien su comportamiento para hacer que la ciberseguridad sea una prioridad más sólida. (Bazalar et al., 2022)

EP8 Guía de ciberseguridad para pymes.

Este artículo proporciona doce medidas de alta calidad, diseñadas para ayudar a las pymes a proteger de manera efectiva los sistemas y negocios en este contexto. Esto debido a la pandemia de la COVID-19 que resaltó la importancia crucial de Internet y las computadoras para las pequeñas y medianas empresas (pymes) y en respuesta a la necesidad de adaptarse, muchas pymes implementaron acciones como el uso de servicios en la nube, la mejora de sus servicios en línea, la actualización de sus sitios web y la implementación del trabajo remoto para asegurar la continuidad de sus operaciones.(ENISA, 2023)

Resumen del estado del arte

Con la información recopilada tenemos que, estos artículos abordan diversas facetas de la ciberseguridad y la gestión de riesgos en diferentes contextos. Guerrero (2023) propone un modelo de gestión de incidentes para instituciones de educación superior, enfatizando medidas respaldadas por estándares. Rea (2020) se centra en la madurez en la identificación y evaluación de riesgos en ciberseguridad, proponiendo un marco de trabajo alineado con objetivos estratégicos. González et al. (2023) destacan la importancia de la cultura organizacional en el sector financiero, proponiendo un modelo de madurez basado en buenas prácticas.

INCIBE (2023), resalta la importancia de enfocarse en el factor humano, proponiendo formación, políticas y supervisión para fortalecer la seguridad. PwC España (2020), se centra en la cultura de ciberseguridad, proponiendo un marco de evaluación y destacando la necesidad de invertir en la capacitación continua de los empleados (Bazalar et al., 2022), presenta un modelo de madurez para evaluar la cultura de ciberseguridad en organizaciones industriales, haciendo hincapié en cambiar el comportamiento de los empleados. El informe de ENISA (2023) ofrece una guía para pymes, enfocándose en doce medidas para proteger sus sistemas y negocios, especialmente relevante en el contexto de la pandemia de la COVID-19 y la creciente dependencia tecnológica. Y por último (Ron et al., 2019) define un modelo de madurez basado en modelos establecidos por la OEA, ISACA e ISO /IEC 15504-2, que servirá como punto de partida para el análisis del estado actual de un país en el contexto de ciberseguridad, y permitirá destacar las políticas que se necesitarían para alcanzar un mayor nivel de madurez.

Respuestas

RQ1. ¿Cuáles son los modelos de madurez existentes para evaluar la cultura de ciberseguridad en contextos similares a instituciones de educación superior?

Según la revisión sistemática de literatura se encontraron algunos modelos de madurez de ciberseguridad enfocados a otros contextos que guardan relación con contexto de instituciones de educación superior, como el sector financiero y empresarial, entre estos modelos tenemos:

- Modelo de Madurez de Capacidades (CMM).
- Marco de ciberseguridad del NIST.
- ISO/IEC 27001.
- Modelo de madurez de la Capacidad de Ciberseguridad (C2M2).

RQ2. ¿Cuáles son los criterios de evaluación y métricas más relevantes para medir la madurez de la cultura de ciberseguridad en una IES, según la literatura actual?

Los diferentes modelos presentan diferentes criterios de evaluación. El modelo C2M2 presenta diez criterios muy detallados:

- Gestión de riesgos (RIESGO).
- Gestión de amenazas y vulnerabilidades (AMENAZA).
- Activos, cambios y gestión de la configuración (ACTIVO).
- Gestión de accesos e identidades (ACCESO).
- Conocimiento de la situación (SITUACIÓN).
- Respuesta a eventos e incidentes (RESPUESTA).
- Cadena de suministros y gestión de dependencias externas (DEPENDENCIAS).
- Gestión del personal (PERSONAL).
- Arquitectura de Ciberseguridad (ARQUITECTURA)
- Gestión del programa de ciberseguridad (PROGRAMA).Rea, 2020)

RQ3. ¿Cuáles son los desafíos que enfrentan las IES en términos de ciberseguridad y cómo pueden abordarse a través de un modelo de madurez de la cultura de ciberseguridad?

Según Guerrero (2023) algunos de los desafíos que enfrentan las IES son:

- Exceso de trabajo y escasez de personal en los departamentos de Tecnologías de la Información y Comunicación (TIC).
- Aumento en la cantidad de ciberataques contra las IES en los últimos años.
- Vulnerabilidad de la información procesada, almacenada y transmitida por los sistemas de información interconectados en las instituciones educativas.
- Riesgos inherentes en las IES debido a la gestión de sistemas y tecnologías de la información.
- Brechas de seguridad de datos y filtraciones de información confidencial.

Estos desafíos en ciberseguridad que enfrentan las IES pueden abordarse a través de la implementación de un modelo de madurez de la cultura de ciberseguridad que establezca lineamientos, características y medidas de seguridad informática basadas en estándares y normas reconocidas. Este enfoque puede contribuir significativamente a la protección de la información y la mitigación de los riesgos cibernéticos.

RQ4. ¿Cómo influye la madurez de la cultura de ciberseguridad en las IES en la protección de datos sensibles y la prevención de amenazas cibernéticas?

La madurez en ciberseguridad según Guerrero (2023) tiene impactos positivos clave, ya que se basa en:

- Conciencia y capacitación: Fomenta la conciencia y capacitación en seguridad cibernética, previniendo ataques de ingeniería social y mejorando la identificación de amenazas.
- Cumplimiento de estándares: Involucra la adopción de estándares y buenas prácticas, reduciendo vulnerabilidades y evitando brechas de seguridad.

- Gestión eficaz de incidentes: Facilita la implementación de un modelo de gestión de incidentes eficaz, permitiendo respuestas rápidas y coordinadas ante amenazas cibernéticas para proteger la integridad de los datos.
- Evaluación y mejora continua: Incluye evaluaciones periódicas de riesgos, implementando medidas correctivas basadas en la mejora continua para fortalecer la protección de datos y prevenir amenazas cibernéticas.

Capítulo III: Diseño del Modelo de Madurez

Análisis de Contexto

En cuanto al contexto de una IES, se deben tomar en cuenta diferentes aspectos para definirla como tal en materia de cultura de ciberseguridad. Empezando por entender la estructura académica y administrativa, lo que incluye la misión y visión de la institución. Es importante también analizar los activos de información crítica, por ejemplo, los registros estudiantiles, documentos de investigación y procurar resguardar estos activos.

Se debe tomar en cuenta dentro del contexto de la IES, el trabajo conjunto de los líderes académicos en favor de las estrategias para la ciberseguridad, tomando en cuenta las prioridades institucionales, las políticas y la normativa de seguridad.

Definición de los Grupos Ocupacionales.

Directivos

El nivel directivo de la Universidad de las Fuerzas Armadas ESPE está compuesto por el Honorable Consejo Universitario y Rectorado, que es el órgano colegiado de cogobierno superior y autoridad máxima de la universidad, está integrado por el Rector quien lo presidirá, cuatro Vicerrectores (Académico General, Docencia, Investigación, Innovación y Transferencia de Tecnología, Vicerrector Administrativo), Directores de Sede, cuatro representantes del personal académico, un representante de estudiantes, un representante de empleados y trabajadores, que se integrará cuando se traten asuntos administrativos.

Contará con el asesoramiento legal del Coordinador Jurídico o quien ejerza sus funciones en la institución (Universidad de las Fuerzas Armadas Espe, 2019).

En base a la información brindada en el Manual de Descripción, Valoración y Clasificación de Puestos, y en el documento del Reglamento Orgánico de gestión Organizacional por Procesos de la Universidad de las Fuerzas Armadas ESPE, se reconocen también los siguientes grupos ocupacionales que forman parte de la institución:

Funcionarios Públicos

Los funcionarios Públicos de la universidad están compuestos por todo el personal que presta sus servicios dentro del campus:

- Personal Administrativo: Se encarga de la gestión y administración, especialmente en las áreas de recursos humanos, organización administrativa, asuntos económicos, informática, archivos, bibliotecas, información y servicios generales.
- Funcionarios Técnicos en Informática: Es el encargado de brindar el soporte tecnológico dentro y fuera del campus. Brindan apoyo, asistencia y asesoramiento a las autoridades académicas y a los estudiantes, así como a la gestión y administración de los recursos tecnológicos de la universidad.

Docentes

Son profesionales que tienen la responsabilidad de impartir conocimientos, guiar el aprendizaje y facilitar el desarrollo académico de los estudiantes. También pueden estar involucrados en la investigación y en actividades de extensión.

Trabajadores

Son todas las personas que pertenecen al Personal de Seguridad, de Limpieza y de Mantenimiento que realizan sus actividades correspondientes dentro del campus en sus respectivos horarios.

Estudiantes

Los estudiantes universitarios civiles y militares son aquellos que buscan adquirir conocimientos y habilidades en un campo específico de estudio, ya sea en ciencias, artes, ingeniería, humanidades, negocios u otras disciplinas.

Proveedores de servicios

Son entidades externas que ofrecen servicios específicos para respaldar el funcionamiento de la institución académica. Estos proveedores pueden abarcar diversas áreas para satisfacer las necesidades y requisitos de la universidad.

Definición de Componentes de la Cultura de Ciberseguridad.

Considerando que existen varios modelos revisados en los estudios primarios es necesario contemplar aquellos cuya aplicación ha tenido un gran aporte, por lo que a continuación se detallan algunos de ellos:

El Modelo de Madurez de la Capacidad de Ciberseguridad-OEA

El Centro Global de Capacidad en Seguridad Cibernética (GCSCC) desarrolló el modelo C2M2 para las Naciones, mismo que busca proporcionar una evaluación de madurez de las capacidades de seguridad cibernética de un país, asignándole un nivel específico que corresponde a su grado de logro en seguridad cibernética. El modelo consta de cinco niveles:

- Inicial: La ciberseguridad no tiene madurez o se encuentra en una etapa muy temprana.
- Formativo: Algunos elementos han comenzado a desarrollarse y formularse, pero pueden ser improvisados, desorganizados, mal definidos o simplemente completamente nuevos.
- Consolidado: Los indicadores se han instalado y han comenzado a funcionar. La asignación de recursos no se toma en cuenta.
- Estratégico: En esta etapa, se han tomado decisiones sobre qué indicadores son más significativos y cuáles son menos significativos para la organización.
- Dinámico: Existen mecanismos claros para adaptar la estrategia en función de las circunstancias prevalentes.

Línea Base de Ciberseguridad: Una Exploración, que permite delinear la Estrategia Nacional de Ciberseguridad en Ecuador

Según Ron et al. (2019): “Se plantea un modelo basado en otros ya existentes como el Modelo de Madurez publicado por la OEA, el Modelo de Capacidad de Proceso definido por ISACA y el Modelo proporcionado en ISO/IEC 15504-2”. Este modelo cuenta con seis niveles los mismos que se detallan a continuación:

- Nivel 0-Incompleto: El proceso no está completo y no ha cumplido con su propósito.
- Nivel 1-Implantado: Aquí el proceso cumple su propósito.
- Nivel 2-Gestionado: En este nivel el proceso es planificado, supervisado y mantenido, así como sus productos.
- Nivel 3-Formalizado: El proceso emplea un conjunto de acciones registradas y estandarizadas.
- Nivel 4-Consistente: En este nivel el proceso es medido y llevado a cabo con precisión.
- Nivel 5-Innovado: El proceso es capaz de innovar, resistir y reaccionar rápidamente a los cambios ambientales.

Ron et al. (2019) menciona, que el estudio se basa en criterios y aspectos declarados por algunos países de Sudamérica, sin embargo, también se toman en cuenta los definidos por la OEA. Mediante un diagrama de afinidad se agrupan estos elementos propuestos para determinar el criterio.

Información de contexto:

- Industria y tecnología
- Infraestructura de la información
- Impacto económico
- Estrategia nacional
- Planificación
- Institucionalidad y organización
- Coordinación y colaboración

- Cooperación y asistencia

Cultura y formación:

- Cultura y sensibilización:
- Prácticas de los operadores
- Formación y educación
- Desarrollo de capacidades
- Investigación e innovación

Legislación:

- Marco jurídico y reglamentario
- Normas y criterios técnicos
- Lucha contra la ciberdelincuencia
- Promoción de los derechos

Procesos técnicos:

- Gobernanza
- Gestión de riesgos
- Continuidad operativa
- Infraestructuras críticas
- Respuesta a incidentes
- Supervisión y evaluación

Modelo de Madurez de las Capacidades de Ingeniería de Seguridad de Sistemas (SSE-CMM)

Este modelo describe los elementos clave del proceso de ingeniería de seguridad de una organización que deben existir para garantizar la calidad de seguridad. Desarrolladores de productos, proveedores de servicios, administradores de sistemas e incluso especialistas en seguridad son solo algunas de las muchas organizaciones que emplean ingeniería de seguridad (SSE-CMM Project, 1999). A continuación, se detalla la aplicabilidad:

- La definición de conceptos, el análisis de requisitos, el diseño, el desarrollo, la integración, la instalación, la operación, el mantenimiento y el retiro son todas las actividades de ingeniería de seguridad del sistema para un producto seguro o un sistema confiable que aborde el ciclo de vida completo.
- Los requisitos de los desarrolladores de productos, los desarrolladores e integradores de sistemas seguros, las empresas que ofrecen servicios de seguridad informática y la ingeniería de seguridad informática.
- Todos los tipos y tamaños de organizaciones de ingeniería de seguridad, desde comerciales hasta gubernamentales y académicas.

La arquitectura SSE-CMM permite la evaluación de la madurez del proceso de una organización de ingeniería de seguridad.

El SSE-CMM tiene dos dimensiones que son el dominio y la capacidad. De las dos, el dominio es la más fácil de comprender. Esta área abarca únicamente todas las prácticas que conforman la definición colectiva de ingeniería de seguridad. Y la segunda, muestra las prácticas que indican la capacidad de gestión institucional y de procesos. (SSE-CMM Project, 1999).

El SSE-CMM tiene 129 prácticas básicas divididas en 22 áreas de proceso. De estas 61 prácticas, todas abarcan todas las áreas de la ingeniería de seguridad y están organizadas en 11 áreas de proceso. Las 68 prácticas básicas que quedan son sobre temas de organización y proyecto (Rea, 2020).

Así mismo SSE-CMM Project (1999) detalla las áreas de proceso de ingeniería de seguridad de sistemas:

- PA01 Administrar los controles de seguridad.
- PA02 Evaluar el impacto.
- PA03 Evaluar los riesgos de seguridad.
- PA04 Evaluar la amenaza.
- PA05 Evaluar la vulnerabilidad.

- PA06 Construir argumento de aseguramiento.
- PA07 Coordinar la seguridad.
- PA08 Controlar la postura de seguridad.
- PA09 Proporcionar información de seguridad.
- PA10 Especificar las necesidades de seguridad.
- PA11 Verificar y validar la seguridad.

También incluye once áreas de proceso relacionadas con las prácticas de los proyectos y la organización.

- PA12 Asegurar la calidad.
- PA13 Gestionar la configuración
- PA14 Gestión de los riesgos del proyecto.
- PA15 Supervisar y controlar el esfuerzo técnico.
- PA16 Planificar el esfuerzo técnico.
- PA17 Definir el proceso de ingeniería de sistemas de la organización.
- PA18 Mejorar el proceso de ingeniería de sistemas de la organización.
- PA19 Gestionar la evolución de la línea de productos.
- PA20 Gestionar el entorno de soporte de ingeniería de sistemas.
- PA21 Proporcionar habilidades y conocimientos continuos.
- PA22 Coordinar con los proveedores.

SSE-CMM Project (1999) también describe los niveles de capacidad:

- Nivel 1-Realizado informalmente: Se enfoca en si una organización o proyecto realiza un proceso que incorpora las prácticas base.
- Nivel 2-Planificado y seguido: Se centra en la definición, planificación y problemas de rendimiento a nivel de proyecto.
- Nivel 3-Bien definido: Se centra en adaptación disciplinada de procesos definidos a nivel de organización.

- Nivel 4-Controlado cuantitativamente: Se enfoca en las mediciones que están vinculadas a los objetos comerciales de la organización.
- Nivel 5-Mejora Continua: Aprovecha las ventajas de todas las mejoras en la práctica administrativa, observadas en los niveles anteriores, y luego enfatiza los cambios culturales que sostendrán los logros obtenidos.

Modelo de Madurez de la Ciberseguridad Comunitaria (CCSMM)

El modelo está diseñado para satisfacer las necesidades de los estados y las comunidades al desarrollar un programa de ciberseguridad que sea sostenible y viable. El CCSMM proporciona un criterio para determinar la postura actual sobre la ciberseguridad, una hoja de ruta para ayudar a mejorar esa postura y un punto de referencia común para compartir experiencias y lecciones aprendidas (Rea, 2020).

El modelo incorpora elementos como la comprensión de la seguridad cibernética, las normas y procedimientos de seguridad, el intercambio de información dentro de las organizaciones y, entre otros, la capacitación y educación en seguridad.

El modelo responde a las conexiones que existen entre el estado, la comunidad y las organizaciones, ya que los estados se componen de comunidades.

Rea (2020) describe los cinco niveles que presenta este modelo:

- Nivel 1-Inicial: Las organizaciones, las comunidades y los estados de este nivel tienen poca o ninguna conciencia de seguridad cibernética, análisis y evaluaciones.
- Nivel 2-Establecido: Las organizaciones, comunidades y estados en este nivel son conscientes de las amenazas cibernéticas, los problemas y el imperativo de adoptar la ciberseguridad. También, reconocen la necesidad de capacitación y educación cooperativa en seguridad cibernética.
- Nivel 3-Autoevaluado: En este nivel, los líderes dentro de las organizaciones, las comunidades y lo estados promueven activamente la conciencia de seguridad cibernética y cooperan con otros en el establecimiento de programas de capacitación y educación.

- Nivel 4-Integrado: Cuando la seguridad cibernética está integrada, se incorpora en cada proceso que tiene una organización, comunidad o estado.
- Nivel 5-Vanguardia: Para las organizaciones, comunidades y estados en este nivel, la seguridad cibernética es un imperativo empresarial. Las entidades en este nivel son capaces de enseñar a otros.

Actualmente, CCSMM es uno de los modelos creado para abordar los problemas de seguridad cibernética nacional a nivel estatal y local, brindando mejores oportunidades para que un país desarrolle un enfoque de seguridad.

Certificación del Modelo de Madurez en Ciberseguridad (CMMC)

El modelo fue creado por el Departamento de Defensa de los Estados Unidos cuyo principal objetivo es proteger la información del sector de la Base Industrial de Defensa (BID). Esta se clasifica como Información de Contratos Federales (FCI), proporcionada o generada por el Gobierno en virtud de contratos que no están destinados a ser divulgados al público, o Información no Clasificada Controlada (CUI), la cual necesita ser protegida de acuerdo con las leyes, reglamentos y políticas generales del Gobierno (Sarri et al., 2020) .

El CMMC tiene en cuenta diecisiete dominios, cada uno representando diferentes procesos y capacidades de ciberseguridad.

Sarri et al. (2020) detalla los dominios a continuación:

- Control de accesos (CA).
- Gestión de activos (GA).
- Auditoría y responsabilidad (AU).
- Concienciación y formación (CF).
- Gestión de la configuración (GC).
- Identificación y autenticación (IA).
- Respuesta a incidentes (RI).
- Mantenimiento (MA).

- Protección de los medios de comunicación (PM).
- Seguridad del personal (SP).
- Protección física (PF).
- Recuperación (RE).
- Gestión de riesgos (GR).
- Evaluación de seguridad (ES).
- Consciencia situacional (CS).
- Protección de los sistemas y las comunicaciones (PS).
- Integridad de los sistemas y la información (IS).

El CMMC define cinco niveles de madurez basados en procesos y prácticas. Una organización debe cumplir con los requisitos previos del mismo nivel e inferiores, para alcanzar uno más alto.

Sarri et al. (2020) presenta los niveles detallando los procesos y las prácticas:

- Nivel 1:
    - Procesos–realizados: Dado que posiblemente la organización sólo pueda realizar estas prácticas con carácter ad hoc y podría basarse o no en la documentación. La madurez de los procesos no se evalúa para el nivel 1.
    - Prácticas–ciber higiene básica: Se centra en la protección de la FCI, que consiste únicamente en prácticas que se corresponden con los requisitos básicos de salvaguardia.
- Nivel 2:
    - Procesos–documentados: Requiere que una organización establezca y documente prácticas y políticas que guíen la implementación de sus esfuerzos de CMMC. La documentación de las prácticas permite a los individuos realizarlas de modo repetible. Las organizaciones desarrollan capacidades maduras al documentar sus procesos y luego practicarlos tal como están documentados.

    - Práctica–ciber higiene intermedia: Sirve como una transición del nivel 1 al nivel 3 y consiste en un subconjunto de los requisitos de seguridad, así como las prácticas de otras normas y referencias.

- Nivel 3:
    - Procesos–gestionados: Requiere que una organización establezca, mantenga y dote de recursos un plan que demuestre la gestión de las actividades para que implemente la práctica. El plan puede incluir información sobre las misiones, los objetivos, los planes de proyecto, los recursos, la formación necesaria y la participación de los interesados relevantes.
    - Prácticas–correcta ciber higiene: Se centra en la protección de CUI y abarca todos los requisitos de seguridad, así como las prácticas añadidas de otras normas y referencias que mitiguen las amenazas
- Nivel 4:
    - Procesos–revisados: Requiere que una organización examine y mida las prácticas de eficacia. Además, pueden adoptar medidas correctivas cuando sea necesario e informar a los directivos de nivel superior sobre la situación o los problemas de manera recurrente.
    - Prácticas–proactivas: Se centra en la protección de la CUI y abarca un subconjunto de los requisitos de seguridad reforzada. Estas prácticas mejoran las capacidades de detección y respuesta de una organización para que aborde y se adapte a las tácticas, técnicas y procedimientos que cambian.
- Nivel 5:
    - Procesos–optimización: Requiere que una organización estandarice y optimice la implementación de procesos.
    - Prácticas–avanzadas/ proactivas: Se centra en la protección del CUI. Las prácticas añadidas aumentan la profundidad y la sofisticación de las capacidades de ciberseguridad.

El CMMC es un modelo bastante joven, terminado recientemente en el primer trimestre de 2020, por lo que se espera que se implemente para fomentar las buenas prácticas de ciberseguridad.

Modelo de Madurez de la Capacidad de Ciberseguridad (C2M2)

Fue creado a partir del Modelo de Madurez de Capacidad de Ciberseguridad del subsector de Electricidad del departamento de energía de los EE.UU. Se enfoca en la implementación y gestión de prácticas de ciberseguridad referentes a los activos de información y tecnología de operaciones.

Entre los principales objetivos de este modelo, según Rea (2020) están:

- Fortalecer las capacidades de seguridad cibernética de las organizaciones.
- Permitir la evaluación y comparación efectivas y consistentes de las capacidades en ciberseguridad.
- Compartir conocimiento, mejores prácticas y referencias relevantes entre organizaciones como un medio de mejora de las capacidades de ciberseguridades.
- Permitir a las organizaciones priorizar acciones e inversiones para la mejora de la ciberseguridad.

Rea (2020) menciona que este modelo se compone de diez dominios que representan a las áreas principales que son riesgo, activo, acceso, amenaza, situación, respuesta, dependencias, personal, arquitectura y programa:

- Gestión de riesgo
- Activos, cambios y gestión de la configuración
- Gestión de accesos e identidades
- Gestión de amenazas y vulnerabilidades.
- Conocimiento de la situación.
- Respuesta a eventos e incidentes.
- Cadena de suministro y gestión de dependencias externas.

- Gestión del personal
- Arquitectura de Ciberseguridad.
- Gestión del programa de ciberseguridad.

Y detalla cuatro niveles de madurez del cero a tres:

- Nivel 0: No se realizan prácticas.
- Nivel 1: Se realizan prácticas iniciales.
- Nivel 2: Las prácticas se documentan, se proporcionan recursos para apoyar los procesos, el personal cuenta con habilidades y conocimientos adecuados, se asignan responsabilidades
- Nivel 3: Las actividades se guían por políticas, se establecen objetivos de desempeño y se monitorean para obtener el nivel de logro, se estandariza y se mejora la documentación de las actividades.

Este modelo permitiría evaluar las capacidades de seguridad cibernética de manera significativa con el fin de priorizar la inversión de áreas de ciberseguridad e implementar planes para abordar los incidentes de seguridad.

El C2M2 está diseñado para que una organización lo utilice con una metodología de autoevaluación y herramientas que midan y mejoran su programa de ciberseguridad. Las herramientas pueden completar una autoevaluación en un día, pero pueden adaptarse a un esfuerzo de evaluación más riguroso (Sarri et al., 2020).

Modelo de Madurez de Cultura Organizacional de Ciberseguridad para el Sector Financiero (MMCCSF)

Este modelo está adaptado al sector financiero, basado en las actividades diseñadas, empezando por el establecimiento de objetivos, el diseño de la arquitectura, la construcción del instrumento de medición y la validación del modelo.

Permite a la organización diagnosticar la situación de la cultura de ciberseguridad en la que se encuentran con el fin de proponer opciones de mejora para alcanzar un mayor nivel de madurez.

González et al. (2023), describe cuatro niveles de madurez:

- Nivel 0-Inexistente: Se considera que la tecnología cuenta con las características necesarias de seguridad, no existe conciencia en el personal.
- Nivel 1-Limitado: Se considera la seguridad como un aspecto únicamente del personal de TI, no existen buenas prácticas de seguridad como cultura.
- Nivel 2-Proactivo: Se consideran los riesgos de seguridad para la toma de decisiones, y se fomenta la cultura de ciberseguridad desde los directivos a toda la organización.
- Nivel 3-Integrado: Se integra la ciberseguridad en todos los procesos de la organización y existe un nivel evolucionado de cultura de ciberseguridad.

Iniciativa Nacional para la Educación en Seguridad Cibernética (NICE)

Desarrolla un CMM que segmenta las actividades en tres áreas principales según Rea (2020):

- Proceso y análisis: El proceso representa las actividades reales de una organización que permiten realizar la planificación de la fuerza de trabajo y se integran con el resto de procesos de toda la organización.
- Gobernanza integrada: Representa actividades que permiten el establecimiento de estructuras de gobierno y la toma de decisiones, es la base de la estrategia de planificación de la fuerza de trabajo.
- Profesionales capacitados y tecnología habilitadora: Representan las actividades que permiten el establecimiento de profesionales planificadores de la fuerza de trabajo y la tecnología habilitadora representa actividades acordes a la accesibilidad y uso datos.

Este modelo también cuenta con tres niveles de madurez que según Rea (2020) son:

- Nivel limitado: Es el nivel más básico, que se encuentra en inicio de desarrollo y se representa por una organización con un establecimiento limitado de procesos y con poca orientación.

- Nivel progresivo: Se representa por una organización que ya ha empezado a establecer una infraestructura para apoyar la planificación de la fuerza de trabajo.
- Nivel final: Representa un pleno desarrollo, en cuanto a integración de procesos, nivel de trabajo y análisis de carga de trabajo, favoreciendo la toma de decisiones.

Para aplicar este modelo la organización debe tener conocimiento de las capacidades actuales de planificación de la fuerza laboral sobre el cual se va a construir un mayor nivel de madurez, mediante la recopilación de datos sobre los principales puntos que defina el modelo, el análisis de datos y la determinación de niveles de madurez por área y finalmente desarrollar planes de acción.

Tabla 2
Modelos de madurez de ciberseguridad

Modelo	Niveles	Componentes / Dominios
El Modelo de madurez de la Capacidad de la Ciberseguridad OEA	5 Niveles	5 Dimensiones
Línea Base de Ciberseguridad: Una Exploración, que permite delinear la Estrategia Nacional de Ciberseguridad en Ecuador	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 de Madurez de la Ciberseguridad Comunitaria (CCSMM)	5 Niveles	4 Dimensiones
Certificación del Modelo de Madurez en Ciberseguridad (CMMC)	5 Niveles	17 Dominios
Modelo de Madurez de la Capacidad 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 Seguridad Cibernética (NICE)	3 Niveles	3 Áreas de aplicación

Nota. El cuadro describe los modelos de madurez de ciberseguridad estudiados, definiendo sus niveles y dimensiones.

Los modelos revisados anteriormente presentan componentes bastantes similares, algunos categorizan los controles en dimensiones, áreas y componentes. Sin embargo, para no desviarse del objetivo que es el elaborar un modelo de la cultura de ciberseguridad para una IES, se ha tomado en cuenta los componentes de: ISO 27001:2022 Anexo “A”, controles definidos en el tratamiento de riesgos del Esquema Gubernamental de Seguridad de la Información (EGSI-ESPE V2), políticas disponibles de INCIBE, componentes de la Organización de Estados Americanos (OEA) y los componentes de ENISA.

Selección de los componentes de la cultura de ciberseguridad.

La elaboración del modelo de madurez de la cultura de ciberseguridad se consigue mediante el método ecléctico, el cual se basa en la combinación y selección de elementos de distintos enfoques o modelos, para desarrollar una solución que se adapte a nuestro contexto de investigación.

Partimos de la información recopilada en el estado del arte, en la Tabla 2**,** que contiene el resumen de los diferentes modelos compatibles con el contexto de una IES. Para este fin se analizan los componentes y niveles de cada modelo seleccionado y se consideran además los controles de la norma ISO 27001:2022 Anexo A, donde se detallan los requisitos para la adopción de un buen sistema de gestión de seguridad. La norma ISO 27001:2022 es aplicable en nuestro contexto de investigación porque según Alonso (2023), el objetivo de esta norma

es, “evaluar la capacidad de la organización para cumplir los requisitos de seguridad de la información”. Además, detalla los requisitos de evaluación y tratamiento de riesgos de seguridad, que al ser genéricos se pueden aplicar en todo tipo de organización independientemente su tamaño o tipo. Entonces se toman en cuenta los controles detallados en el Anexo A de la norma ISO 27001:2022, como los procedimientos o medidas base a aplicar en la IES, ante riesgos y amenazas de ciberseguridad, estos controles se clasificarán de acuerdo a los componentes del modelo de madurez obtenidos mediante el análisis de otros modelos, en conjunto con el contexto de la investigación.

Tabla 3
Controles de seguridad ISO 27001

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
Organizacionales	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.
	Roles y responsabilidades en la Seguridad de la Información	Se deben definir y asignar de acuerdo con las necesidades de la organización.
	Segregación de deberes	Los deberes y áreas de responsabilidad en conflicto deberían segregarse.
	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
	Contacto con las autoridades	La organización debe establecer y mantener contacto con las autoridades pertinentes.
	Contacto con grupos de interés especial	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Inteligencia de amenazas	La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.
	Seguridad de la Información en la gestión de proyectos	La seguridad de la información se debe integrar en la gestión de proyectos.
	Inventario de información y otros activos asociados	Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios.
	Uso aceptable de la información y otros activos asociados	Se deben identificar, documentar e implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.
	Devolución de activos	El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.
	Clasificación de la información	La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.
	Etiquetado de la información	Se debe elaborar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptada por la organización.
	Transferencia de información	Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
	Control de acceso	Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
		empresarial y de la información.
	Gestión de identidades	Se debe gestionar el ciclo de vida completo de las identidades.
	Información de autenticación	La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.
	Seguridad de la información en las relaciones con proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.
	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor.
	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.
	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios
	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información.
	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.
	Aprender de los incidentes de seguridad de la información	
	Recopilación de evidencias	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
	Seguridad de la información durante una interrupción	La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.
	Preparación de las TIC para la continuidad de negocio	La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
	Requisitos legales, reglamentarios y contractuales	Los requisitos lega les, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.
	Protección de registros	Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados.
	Privacidad y protección de la información de identificación personal (Pll, por sus siglas en inglés)	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la Pll de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
	Revisión independiente de la seguridad de la información	El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.
	Cumplimiento de políticas, reglas y estándares de seguridad de la información	El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.
	Procedimientos operativos documentados	Los procedimientos operativos de las instalaciones de procesamiento de la información se deben documentar y poner a disposición del personal que los necesite.
Personas	Selección	Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos
	Términos y condiciones de empleo	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Conciencia de seguridad de la información, educación y formación	El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral.
	Proceso disciplinario	Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.
	Responsabilidades después de la terminación o cambio de empleo	Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.
	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.
	Trabajo remoto	Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.
	Informes de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.
Físicos	Perímetros de seguridad física	Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Entrada física	Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.
	Asegurar oficinas, habitaciones e instalaciones	Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.
	Monitoreo de la seguridad física	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.
	Protección contra amenazas físicas y ambientales	Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.
	Trabajar en áreas seguras	Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras.
	Escritorio y pantalla limpios	Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.
	Emplazamiento y protección de equipos	El equipo debe estar situado de forma segura y protegida
	Seguridad de los activos fuera de las instalaciones	Los activos externos deben estar protegidos.
	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Servicios públicos de apoyo	Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.
	Seguridad del cableado	Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.
	Mantenimiento de equipos	El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.
	Disposición o reutilización segura de los equipos	Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.
Tecnológicos	Dispositivos de punto final de usuario	Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.
	Derechos de acceso privilegiado	La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.
	Restricción de acceso a la información	El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.
	Acceso al código fuente	El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente
	Autenticación segura	Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Gestión de la capacidad	El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.
	Protección contra malware	La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.
	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.
	Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.
	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario
	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
	Prevención de fugas de datos	Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos
	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Registro	Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.
	Actividad de seguimiento	Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.
	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.
	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación; debe restringirse y controlarse estrictamente.
	Instalación de software en sistemas operativos	Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos.
	Seguridad de redes	Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.
	Seguridad de los servicios de red	Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
	Segregación de redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.
	Filtrado web	El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.
	Uso de la criptografía	Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

Categorías - Anexo A 27001	Objetivos de control- Anexo A 27001	Descripción de control- Anexo A 27001
	Ciclo de vida de desarrollo seguro	Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.
	Requisitos de seguridad de las aplicaciones	Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.
	Arquitectura de sistemas seguros y principios de ingeniería	Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener e implementar a cualquier actividad de desarrollo de sistemas de información.
	Codificación segura	Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.
	Pruebas de seguridad en el desarrollo y aceptación	Los procesos de ensayo de seguridad se deben definir e implementar en el ciclo de vida del desarrollo.
	Desarrollo externalizado	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
	Separación de entornos de desarrollo, evidencia y producción	Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos.
	Gestión del cambio	Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
	Información de las pruebas	La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente.
	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección

Nota. Controles detallados en el anexo A, de la norma ISO 27001

Los componentes seleccionados abarcan cada uno de los controles categorizados en sus distintas áreas. Para el nuevo modelo de madurez, se analizan otros modelos como los publicados por la OEA, INCIBE, ENISA y la ISO, de cada uno de ellos tomamos los componentes que tienen asociados, y los comparamos. A partir de esto se definen siete componentes de ciberseguridad que se pueden aplicar a nuestro entorno. Entonces los componentes para el nuevo modelo de madurez se detallan en la Tabla 4**.**

Tabla 4
Componentes del nuevo modelo de madurez

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 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;

Una vez obtenidos los componentes de nuestro modelo, se clasifica cada uno de los controles de la familia ISO 27001:2022 Anexo A, dentro del componente al que pertenezcan según su área de aplicación, obteniendo la Tabla 5.

Tabla 5
Clasificación de controles de seguridad ISO 27001:2022

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 (Pll, por sus siglas en inglés) - Revisión independiente de la seguridad de la - Información - Conciencia de seguridad de la información, educación y formación
Marco jurídico y normativo de la estrategia de ciberseguridad	- Políticas de la seguridad de la información - Abordar la seguridad de la información dentro de los acuerdos con proveedores - Seguridad de la información para el uso de servicios en la nube - Requisitos legales, reglamentarios y contractuales - Derechos de propiedad intelectual - Cumplimiento de políticas, reglas y estándares de seguridad de la información - Procedimientos operativos documentados - Proceso disciplinario - Acuerdos de confidencialidad o no divulgación - Enmascaramiento de datos

Componentes FINAL - MODELO PROPIO	Controles ISO 27001
Gestión de activos tecnológicos	- Inventario de información y otros activos asociados - Uso aceptable de la información y otros activos asociados - Devolución de activos - Preparación de las TIC para la continuidad de negocio - Responsabilidades después de la terminación o cambio de empleo - Trabajo remoto - Perímetros de seguridad física - Entrada física - Asegurar oficinas, habitaciones e instalaciones - Monitoreo de la seguridad física - Escritorio y pantalla limpios - Emplazamiento y protección de equipos - Seguridad de los activos fuera de las instalaciones - Medios de almacenamiento - Servicios públicos de apoyo - Seguridad del cableado - Mantenimiento de equipos - Disposición o reutilización segura de los equipos - Dispositivos de punto final de usuario - Gestión de la capacidad - Gestión de la configuración - Copia de seguridad de la información - Redundancia de las instalaciones de procesamiento de información - Registro - Sincronización de reloj - Instalación de software en sistemas operativos - Seguridad de redes - Seguridad de los servicios de red - Segregación de redes - Requisitos de seguridad de las aplicaciones - Desarrollo externalizado - Separación de entornos de desarrollo, evidencia y producción

Componentes FINAL - MODELO PROPIO	Controles ISO 27001
Gestión de usuarios y accesos	- Roles y responsabilidades en la Seguridad de la Información - Clasificación de la información - Etiquetado de la información - Transferencia de información - Control de acceso - Gestión de identidades - Información de autenticación - Derechos de acceso - Derechos de acceso privilegiado - Restricción de acceso a la información - Acceso al código fuente - Autenticación segura
Estrategias de gestión de riesgos y amenazas	- Inteligencia de amenazas - Seguridad de la información en las relaciones con proveedores - Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC) - Seguimiento, revisión y gestión del cambio de los servicios de los proveedores - Planificación y preparación de la gestión de incidentes de seguridad de la información - Evaluación y decisión sobre eventos de seguridad de la información - Respuesta a incidentes de seguridad de la información - Aprender de los incidentes de seguridad de la información - Recopilación de evidencias - Seguridad de la información durante una interrupción - Informes de eventos de seguridad de la información - Protección contra amenazas físicas y ambientales - Trabajar en áreas seguras - Protección contra malware - Gestión de vulnerabilidades técnicas - Prevención de fugas de datos - Actividad de seguimiento - Uso de programas de utilidad privilegiados - Filtrado web

Componentes FINAL - MODELO PROPIO	Controles ISO 27001
Protección de la información y procedimientos;	- Uso de la criptografía - Ciclo de vida de desarrollo seguro - Arquitectura de sistemas seguros y principios de ingeniería - Codificación segura - Pruebas de seguridad en el desarrollo y aceptación - Gestión del cambio - Información de las pruebas - Protección de los sistemas de información durante las pruebas de auditoría

Nota. En la tabla se clasifican los controles de seguridad según cada componente según el área de aplicación.

Una vez definidos los componentes y controles asociados del modelo, se toma en cuenta los grupos ocupacionales que forman parte de la IES; que dentro de nuestro contexto investigativo se dividen en directivos, docentes, funcionarios técnicos en informática, funcionarios administrativos, estudiantes, trabajadores y proveedores de servicios; para determinar qué grupo se relacionan con cada control.

Figura 7
Componentes y controles del modelo de la cultura de ciberseguridad

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 Informática	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			

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	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						
	Contacto con las autoridades	La organización debe establecer y mantener contacto con las autoridades pertinentes.		Gestión de ciberseguridad	Estándares, organizaciones y tecnologías		Gestión de usuarios y accesos	x	x	x	x	x	x	x
	Contacto con grupos de interés especial	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad		Gestión de usuarios			Estrategias de gestión de riesgos y amenazas	x		x	x			x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Contacto con grupos de interés especial	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad		Gestión de usuarios			Estrategias de gestión de riesgos y amenazas	x		x	x			x
	Inteligencia de amenazas	La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.					Protección de la información y procedimientos			x				
	Seguridad de la Información en la gestión de proyectos	La seguridad de la información se debe integrar en la gestión de proyectos.						x		x	x			
	Inventario de información y otros activos asociados	Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios.						x	x	x	x		x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Uso aceptable de la información y otros activos asociados	Se deben identificar, documentar e implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.						x	x	x	x	x	x	x
	Devolución de activos	El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.						x	x	x	x	x	x	
	Clasificación de la información	La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.						x		x	x			

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Etiquetado de la información	Se debe elaborar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.								x	x			
	Transferencia de información	Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.						x	x	x	x	x	x	x
	Control de acceso	Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la infromación						x	x	x	x	x	x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
Organizacionales	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.						x	x	x	x	x	x	x
	Seguridad de la información en las relaciones con proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.						x		x	x			x
	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor.						x		x	x			x
	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.								x	x			x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios						x		x	x			x
	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización						x		x	x			x
	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.						x		x	x			

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información.						x		x				
	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.						x	x	x	x	x	x	x
	Aprender de los incidentes de seguridad de la información	Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.								x				

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Recopilación de evidencias	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.								x				
	Seguridad de la información durante una interrupción	La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.						x		x	x			
	Preparación de las TIC para la continuidad de negocio	La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.						x		x	x			

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Requisitos legales, reglamentarios y contractuales	Los requisitos lega les, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.						x		x	x			
	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.						x	x	x	x	x	x	x
	Protección de registros	Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados.						x	x	x	x	x	x	x
	Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.						x	x	x	x	x	x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Revisión independiente de la seguridad de la información	El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.						x	x	x	x	x	x	x
	Cumplimiento de políticas, reglas y estándares de seguridad de la información	El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.						x	x	x	x	x	x	x
	Procedimientos operativos documentados	Los procedimientos operativos de las instalaciones de procesamiento de la información se deben documentar y poner a disposición del personal que los necesite.								x	x			

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Selección	Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos						x			x			
	Términos y condiciones de empleo	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de información						x			x			
	Conciencia de seguridad de la información, educación y formación	El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral.						x	x	x	x	x	x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
Personas	Proceso disciplinario	Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información						x	x	x	x	x	x	x
	Responsabilidades después de la terminación o cambio de empleo	Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.						x	x	x	x		x	
	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.						x	x	x	x	x	x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Trabajo remoto	Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.						x	x	x	x	x	x	x
	Informes de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.						x	x	x	x	x	x	x
	Perímetros de seguridad física	Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.								x	x		x	

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Entrada física	Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.						x		x			x	
	Asegurar oficinas, habitaciones e instalaciones	Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.						x	x	x	x	x	x	x
	Monitoreo de la seguridad física	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.								x			x	
	Protección contra amenazas físicas y ambientales	Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.						x		x				

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
Físicos	Trabajar en áreas seguras	Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras.						x	x	x	x	x	x	x
	Escritorio y pantalla limpios	Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.						x	x	x	x	x	x	x
	Emplazamiento y protección de equipos	El equipo debe estar situado de forma segura y protegida						x	x	x	x		x	x
	Seguridad de los activos fuera de las instalaciones	Los activos externos deben estar protegidos.						x	x	x	x		x	x
	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.						x	x	x	x		x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Servicios públicos de apoyo	Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.								x			x	x
	Seguridad del cableado	Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.								x			x	x
	Mantenimiento de equipos	El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.						x	x	x	x	x	x	x
	Disposición o reutilización segura de los equipos	Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.						x	x	x	x	x	x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Dispositivos de punto final de usuario	Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.						x	x	x	x	x	x	x
	Derechos de acceso privilegiado	La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.						x		x	x		x	x
	Restricción de acceso a la información	El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.						x	x	x	x	x	x	x
	Acceso al código fuente	El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente								x				

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Autenticación segura	Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.						x	x	x	x	x	x	x
	Gestión de la capacidad	El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.						x	x	x	x	x	x	x
	Protección contra malware	La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.						x	x	x	x	x	x	x
	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.								x	x			

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.								x	x			
	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario						x	x	x	x	x	x	x
	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.								x				
	Prevención de fugas de datos	Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.						x	x	x	x	x	x	x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
Tecnológicos	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos.						x	x	x	x	x	x	x
	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad.								x				
	Registro	Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.						x		x	x		x	x
	Actividad de seguimiento	Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.								x			x	

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.								x				
	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación; debe restringirse y controlarse estrictamente.								x				
	Instalación de software en sistemas operativos	Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos.								x				
	Seguridad de redes	Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.								x				
	Seguridad de los servicios de red	Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.								x				

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Segregación de redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.						x	x	x	x	x	x	x
	Filtrado web	El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.						x	x	x	x	x	x	x
	Uso de la criptografía	Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.						x	x	x	x	x	x	x
	Ciclo de vida de desarrollo seguro	Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.						x		x				
	Requisitos de seguridad de las aplicaciones	Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.						x		x	x			x
	Arquitectura de sistemas seguros y principios de ingeniería	Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener e implementar a cualquier actividad de desarrollo de sistemas de información.						x		x	x			x
	Codificación segura	Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.								x				x

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 Informática	Funcionarios Administrativos	Estudiantes	Trabajadores	Proveedores de servicios
	Pruebas de seguridad en el desarrollo y aceptación	Los procesos de ensayo de seguridad se deben definir e implementar en el ciclo de vida del desarrollo.								x				x
	Desarrollo externalizado	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.						x		x	x			x
	Separación de entornos de desarrollo, evidencia y producción	Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos.								x				x
	Gestión del cambio	Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.						x		x	x			x
	Información de las pruebas	La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente.								x	x			x
	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección						x		x	x			x

Nota. Clasificación de los controles ISO 27001 según los componentes y los grupos ocupacionales a los que pertenecen

Selección de los niveles de madurez del modelo.

Como un componente más del Modelo de Madurez de la Cultura de Ciberseguridad, es necesario definir los niveles, que representan las etapas de desarrollo de las prácticas de seguridad dentro de la institución. Esto permite evaluar la capacidad que tiene la organización en cuanto al manejo de ciberseguridad, partiendo de un nivel inicial o bajo, hasta un nivel avanzado o robusto, que representaría una alta capacidad de identificación, control y recuperación de riesgos y amenazas de ciberseguridad, incluyendo también el papel que juegan los miembros de la organización en cuanto a actitudes, valores y comportamientos en favor de la ciberseguridad.

De la misma manera, se hace una recopilación de los distintos niveles que manejan otros modelos de madurez de ciberseguridad como SSE-CMM, CCSMM, CMMC, C2M2, MMCCSF, NICE, entre otros.

Figura 8
Comparación de niveles de madurez

Niveles de madurez	BID / OEA	OEA / ISACA	SSE - CMM	CCSMM	CMMC	C2M2	MMCCSF	Modelo de madurez para determinar el nivel de cultura de ciberseguridad en organizaciones industriales	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: Sin programa de sensibilización sobre seguridad. Descripción: No hay intentos de capacitar y educar a la organización en temas de ciberseguridad.	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) .	Nivel: 2 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 prácticas.	Nivel: Proactiva Descripción: En esta etapa los directivos son consientes de la importancia de la ciberseguridad y la promueven en toda la organización.	Nivel: Enfocado en el cumplimiento normativo. Descripción: se cumple los requisitos específicos de cumplimiento normativo y auditoría, cumpliendo regulaciones y estándares establecidos.	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.
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: Promoviendo el ambio de comportamiento y sensibilización. Descripción: En esta eatapa se realiza una planificación previa para iniciar el cambio de comportamiento.	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: Cambio de cultura sostenible a largo plazo. Descripción: En esta eatapa existe un programa que promueve la conciencia y el cambio.		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: Métrias estructuradas. Descripción: Se mide el cambio de comportamientos con indicadores establecidos.		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

Nota. La figura detalla los niveles de madurez de otros modelos de madurez de ciberseguridad y los niveles del modelo final.

Se tiene los siguientes seis niveles y su descripción, detallados en la Tabla 6, para el nuevo Modelo de Madurez de la Cultura de ciberseguridad.

Tabla 6
Niveles de madurez modelo final

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.

Niveles de madurez	Descripción
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 de la ciberseguridad. - 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.
Nivel Tres: Establecido	- Se pone en marcha el proyecto 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 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.
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.

Nota. La tabla detalla los niveles de madurez del modelo final y su descripción.

Una vez seleccionados los componentes con sus controles y los niveles de madurez, es necesario definir los niveles de aplicación, que permitan calificar de manera cualitativa el

grado de aplicación de los controles dentro de la institución. Entonces tenemos los niveles de aplicación descritos en la Tabla 7:

Tabla 7
Niveles de aplicación

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

Nota. La tabla detalla los niveles de aplicación tanto de los controles como de los componentes.

El Modelo final de Madurez de la Cultura de Ciberseguridad se muestra en la Tabla 8**,** con el detalle del nivel de aplicación requerido en cada componente, para poder determinar el nivel de madurez.

Tabla 8
Modelo 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

Nota. Modelo final, con el nivel de aplicación requerido para cada nivel de madurez.

A su vez, para obtener el nivel de aplicación de cada componente, va a ser necesario evaluar cada uno de los controles que forman parte de los mismos, para lo cual, se utiliza como métricas, los mismos niveles de aplicación, asignándoles un valor numérico, siendo:

Tabla 9
Métricas de evaluación

Nivel de aplicación	Valor
Nivel Nulo	0
Nivel Bajo	1
Nivel Medio	2
Nivel Alto	3

Nota. La tabla define los valores numéricos asignados a cada nivel de aplicación.

Capítulo IV: Resultados

Resultados de la simulación del modelo final de madurez.

Con el Modelo final de Madurez de la Cultura de Ciberseguridad, se realiza una simulación de su aplicación, para determinar el resultado en un escenario posible dentro de una IES.

Para este motivo se elabora una encuesta en base a cada control y los grupos ocupacionales que involucran:

Tabla 10
Preguntas de evaluación de controles de seguridad

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Políticas de la seguridad de la información	¿Se han implementado las reglas, directrices, procedimientos y prácticas para proteger la información que maneja la universidad?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Roles y responsabilidades en la Seguridad de la Información	¿Cuál es el nivel de definición de los roles y responsabilidades en la seguridad de la información de acuerdo a las necesidades de la universidad?	0 No definido 1 En proceso de definición 2 Parcialmente definido 3 Bien definido
Segregación de deberes	¿Qué nivel de distribución y separación de las tareas y responsabilidades relacionadas con los procesos críticos de la universidad entre diferentes personas o grupos existe?	0 No definido 1 En proceso de definición 2 Parcialmente definido 3 Bien definido
Responsabilidades de la dirección	¿Las autoridades dentro de la universidad, exigen al personal , la aplicación de la seguridad de la información de acuerdo a las políticas de seguridad de información establecidas?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre
Contacto con las autoridades	¿La universidad cuenta con procedimientos y canales de comunicación con las autoridades pertinentes en caso de incidentes o delitos cibernéticos?	0 No existen procedimientos 1 En proceso de desarrollo 2 Parcialmente 3 Procedimientos completamente establecidos
Contacto con grupos de interés especial	¿La universidad establece y mantiene contacto con grupos de interés especial y asociaciones profesionales especializados en Seguridad?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Inteligencia de amenazas	¿Dentro de la universidad se lleva a cabo la recopilación, análisis y utilización de información sobre amenazas cibernéticas para proteger los activos digitales y mejorar las respuestas ante amenazas?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre
Seguridad de la Información en la gestión de proyectos	¿Dentro de la universidad se considera la seguridad de la información como un componente clave en la planificación, ejecución y entrega de proyectos?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre
Inventario de información y otros activos asociados	¿Se ha implementado práctica de identificar, catalogar y mantener un registro actualizado de todos los activos de información y recursos relacionados dentro de la universidad?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Uso aceptable de la información y otros activos asociados	¿Se han identificado y establecido políticas y procedimientos que definan cómo deben ser utilizados los activos de información y recursos relacionados dentro de la universidad, incluyendo tanto los datos digitales como el hardware, software y otros activos relacionados con la tecnología de la información?	0 No establecido 1 En proceso de establecimiento 2 Parcialmente establecido 3 Totalmente establecido
Devolución de activos	¿Se establecen procedimientos para garantizar que los activos digitales, como dispositivos informáticos, cuentas de usuario, credenciales de acceso y otros recursos relacionados, sean recuperados de manera segura cuando un miembro de la comunidad universitaria deja de estar asociado con la institución?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Clasificación de la información	¿Se establece una clasificación de los datos según su nivel de sensibilidad y el grado de protección que requieren, para garantizar que se apliquen medidas de seguridad adecuadas para proteger la información de manera proporcional a su importancia y riesgo asociado?	0 No establecido 1 En proceso de establecimiento 2 Parcialmente establecido 3 Totalmente establecido
Etiquetado de la información	¿Se han implementado sistemas y herramientas dentro de la universidad, que permitan el etiquetado automático o manual de la información para indicar su nivel de sensibilidad, su propósito y otras características relevantes, para garantizar que los datos se manejen de manera segura?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Transferencia de información	Dentro de la universidad se manejan reglas, procedimientos o acuerdos vigentes de transferencia de información, entre la institución y otras partes, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Control de acceso	¿Existen normas establecidas para la gestión y regulación de quién tiene permiso para acceder a los recursos de información y sistemas dentro de una organización, así como a qué recursos específicos pueden acceder y en qué capacidad?	0 No establecidas 1 En proceso de establecimiento 2 Parcialmente establecidas 3 Totalmente establecidas
Gestión de identidades	¿Dentro de la universidad se gestiona la administración y control de las identidades de usuarios, lo que incluye la creación, modificación, eliminación y gestión de privilegios de acceso de los usuarios a recursos digitales?	0 = No existe gestión. 1 = No gestionados adecuadamente. 2 = Sí, con restricciones limitadas. 3 = Gestionados adecuadamente.
Información de autenticación	¿Existe control en la asignación y gestión de información de autenticación, incluyendo nombres de usuario, contraseñas, códigos de acceso, tokens de seguridad y cualquier otra información requerida para autenticar la identidad de un usuario en la universidad?	0 No existe un control definido 1 Parcialmente, algunos aspectos están controlados. 2 Sí, pero es insuficiente. 3 Existe un control bien establecido.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Derechos de acceso	¿Se establecen políticas y reglas, para la gestión y regulación de los privilegios de acceso que tienen los usuarios dentro de los sistemas de información de la universidad?	0 No establecidas 1 En proceso de establecimiento 2 Parcialmente establecidas 3 Totalmente establecidas
Seguridad de la información en las relaciones con proveedores	¿Se implementa medidas de seguridad para proteger la información compartida con proveedores externos de la universidad?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Abordar la seguridad de la información dentro de los acuerdos con proveedores	¿Se establecen cláusulas y disposiciones específicas en los contratos y acuerdos de la universidad con proveedores externos, para garantizar la protección adecuada de la información compartida con ellos incluyendo requisitos y responsabilidades claras en caso de incidentes de seguridad?	0 No establecidas 1 En proceso de establer 2 Parcialmente establecidas 3 Totalmente establecidas
Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	¿Existen medidas de seguridad implementadas para proteger la información y los activos digitales a lo largo de toda la cadena de suministro de tecnología de la información y las telecomunicaciones, desde la adquisición de productos y servicios hasta su despliegue y mantenimiento?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	Se realiza un monitoreo y evaluación de los servicios proporcionados por los proveedores externos de la universidad de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Seguridad de la información para el uso de servicios en la nube	¿Se han implementado medidas de seguridad para proteger los datos y sistemas de la universidad cuando se utilizan servicios en la nube, como almacenamiento de datos, plataformas de colaboración, aplicaciones web y servicios de infraestructura?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Planificación y preparación de la gestión de incidentes de seguridad de la información	¿Se definen planes y procedimientos para la gestión de incidentes de seguridad dentro de una universidad, mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes?	0 No definido 1 En proceso de definición 2 Parcialmente definido 3 Bien definido
Evaluación y decisión sobre eventos de seguridad de la información	Dentro de la universidad se analiza y se toma medidas adecuadas en respuesta a eventos relacionados con la seguridad de la información de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Respuesta a incidentes de seguridad de la información	El nivel de identificación, manejo y mitigación de eventos o incidentes de seguridad cibernética que podrían afectar la confidencialidad, integridad o disponibilidad de los datos y sistemas dentro de la universidad, se considera:	0 Nulo 1 Bajo 2 Medio 3 Alto
Aprender de los incidentes de seguridad de la información	En la universidad se lleva a cabo el análisis y revisión de los incidentes de seguridad, con el objetivo de identificar lecciones aprendidas, mejorar las prácticas de seguridad y prevenir futuros incidentes similares, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Recopilación de evidencias	¿Se establecen procedimientos para recopilar y preservar pruebas relevantes en caso de incidentes de seguridad cibernética o auditorías de seguridad dentro de la universidad?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos
Seguridad de la información durante una interrupción	¿Se establecen medidas y procedimientos para proteger la seguridad de la información y los sistemas de una universidad durante situaciones de interrupción, como desastres naturales, cortes de energía, fallos de infraestructura o cualquier otro evento que afecte la disponibilidad o funcionalidad de los sistemas?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos
Preparación de las TIC para la continuidad de negocio	¿Se implementan medidas y procedimientos para garantizar que los sistemas de tecnología de la	0 No implementado 1 En proceso de implementación

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
	información y comunicación (TIC) de la universidad estén listos para continuar operando de manera efectiva durante situaciones de emergencia o interrupción, garantizando así la continuidad de las operaciones críticas?	2 Parcialmente implementado 3 Totalmente implementado
Requisitos legales, reglamentarios y contractuales	En la universidad se cumple con las leyes, regulaciones y acuerdos contractuales relevantes en materia de seguridad de la información, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Derechos de propiedad intelectual	¿Se implementan procedimientos para la protección de los activos intangibles de la universidad, como la propiedad intelectual, la propiedad de software, los derechos de autor y las patentes, frente a posibles amenazas cibernéticas?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Protección de registros	Los registros y datos sensibles de la universidad están protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)	¿Se implementan medidas para proteger la privacidad y la seguridad de la información que pueda identificar a individuos dentro de la universidad, lo que incluye datos como nombres, direcciones, números de seguridad social, números de teléfono, direcciones de correo electrónico, entre otros?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Revisión independiente de la seguridad de la información	Se implementan auditorías por parte de terceros independientes para evaluar la efectividad de los controles de seguridad de la información dentro de la universidad, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Cumplimiento de políticas, reglas y estándares de seguridad de la información	Las políticas, reglas y estándares establecidos para la seguridad de la información dentro de una universidad se cumplen entro de la universidad, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Procedimientos operativos documentados	Los procedimientos operativos de las instalaciones de procesamiento de la información se documentan y se ponen a disposición del personal que los necesite, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Selección	¿En la universidad se verifican los antecedentes de los candidatos a personal, teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre
Términos y condiciones de empleo	¿En los acuerdos contractuales, se establecen las políticas y directrices que regulan el uso apropiado de los recursos de tecnología de la información (TI) por parte de los empleados de la universidad?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos
Conciencia de seguridad de la información, educación y formación	Se destinan actividades para aumentar el conocimiento y la comprensión del personal sobre la importancia de la seguridad de la información y las mejores prácticas para proteger los activos de la universidad contra amenazas cibernéticas, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente
Proceso disciplinario	¿Se establecen los procedimientos para abordar violaciones de la política de seguridad de la información, que implica la aplicación de medidas disciplinarias apropiadas contra los empleados que incumplen las políticas y procedimientos de seguridad de la información de la institución?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Responsabilidades después de la terminación o cambio de empleo	¿Se establecen medidas y procedimientos para garantizar la protección de los activos de información de la universidad cuando un empleado termina su relación laboral o cambia de puesto dentro de la institución?	0 No establecidos 1 En proceso de establecer 2 Parcialmente establecidos 3 Totalmente establecidos
Acuerdos de confidencialidad o no divulgación	¿Se establecen contratos o acuerdos entre la universidad y sus empleados, contratistas o terceros, que reflejen las obligaciones de mantener la confidencialidad de la información sensible de la institución?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos
Trabajo remoto	¿Se implementan medidas de seguridad para proteger la información y los sistemas de la universidad cuando los empleados trabajan fuera de las instalaciones físicas de la institución, ya sea desde sus hogares u otro lugar remoto?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado
Informes de eventos de seguridad de la información	¿En la universidad, existe un mecanismo establecido para que el personal informe de manera oportuna sobre eventos de seguridad de la información observados o sospechosos? (Ejemplos: incidentes de ciberseguridad, comportamientos inusuales, etc.)	0 = No existe 1 = No hay un mecanismo formal establecido. 2 = Si, mecanismo no muy efectivo. 3 = Sí, mecanismo bien establecido y eficaz.
Perímetros de seguridad física	En la universidad, ¿se han definido y están siendo utilizados de manera efectiva los perímetros de seguridad para proteger las zonas que contienen información y otros activos asociados?	0 = No existen 1 = No, perímetros de seguridad no definidos. 2 = Sí, efectividad limitada. 3 = Sí, bien definidos y se utilizan de manera efectiva.
Entrada física	¿Las zonas seguras (instalaciones que necesitan un nivel adicional de seguridad) en la universidad están adecuadamente protegidas mediante controles de entrada y puntos de acceso?	0 = No existe protección. 1 = No, no cuentan con controles de entrada ni puntos de acceso adecuados. 2 = Sí, sus controles son limitados. 3 = Sí, controles de entrada y puntos de acceso eficaces.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Asegurar oficinas, habitaciones e instalaciones	¿En la universidad se ha diseñado e implementado adecuadamente la seguridad física de las oficinas, salas e instalaciones?	0 = No existe seguridad. 1 = No, no está adecuadamente diseñada o implementada. 2 = Sí, su implementación es limitada. 3 = Sí, está bien diseñada e implementada.
Monitoreo de la seguridad física	¿Las instalaciones son monitoreadas continuamente para detectar accesos físicos no autorizados?	0 = No existe monitoreo. 1 = No, no son monitoreadas continuamente. 2 = Sí, su efectividad es limitada. 3 = Sí, son monitoreadas continuamente y se detectan accesos no autorizados de manera efectiva.
Protección contra amenazas físicas y ambientales	¿Se ha diseñado e implementado adecuadamente la protección contra amenazas físicas y medioambientales, incluyendo catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas, a las infraestructuras?	0 = No existe. 1 = No, no está adecuadamente diseñada o implementada. 2 = Sí, su implementación es limitada. 3 = Sí, está bien diseñada e implementada.
Trabajar en áreas seguras	¿En la universidad se han diseñado e implementado medidas de seguridad para trabajar en zonas seguras (instalaciones que necesitan un nivel adicional de seguridad)?	0 = No existen medidas. 1 = No, no está adecuadamente diseñada o implementada. 2 = Sí, su implementación es limitada. 3 = Sí, medidas de seguridad efectivas para trabajar en zonas seguras.
Escritorio y pantalla limpios	¿Se han definido e implementado adecuadamente normas claras para los roles, los soportes de almacenamiento extraíbles y las pantallas en las instalaciones de tratamiento de la información?	0 = No existen normas. 1 = No, no se han definido normas claras. 2 = Sí, su implementación es limitada. 3 = Sí, se han establecido normas claras y están efectivamente implementadas.
Emplazamiento y protección de equipos	¿En la universidad, los equipos están situados de forma segura y protegida?	0 = Nunca. 1 = No, no están situado de forma segura. 2 = Sí, con medidas de

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
		protección limitada. 3 = Sí, y cuentan con medidas de protección adecuadas.
Seguridad de los activos fuera de las instalaciones	¿Los activos externos, como instalaciones, equipos y recursos, están adecuadamente protegidos?	0 = Nunca están protegidos. 1 = No, no cuentan con protección adecuada. 2 = Sí, su adecuación es limitada. 3 = Sí, están protegidos con medidas de seguridad efectivas.
Medios de almacenamiento	¿Los medios de almacenamiento se gestionan adecuadamente a lo largo de su ciclo de vida, incluyendo adquisición, uso, transporte y disposición, de acuerdo con el esquema de clasificación y los requisitos de manipulación establecidos por la universidad?	0 = No existe gestión. 1 = No, no se gestionan de manera adecuada a lo largo de su ciclo de vida. 2 = Sí, su gestión es limitada. 3 = Sí, se gestionan de acuerdo con los requisitos establecidos.
Servicios públicos de apoyo	¿En cuanto a las instalaciones de procesamiento de la información, están adecuadamente protegidas contra cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo?	0 = No existe adecuación. 1 = No, no están protegidas adecuadamente. 2 = Sí, medidas de protección limitada. 3 = Sí, adecuadamente protegidas.
Seguridad del cableado	¿Los cables que transportan energía, datos o servicios de información de apoyo están adecuadamente protegidos contra la interceptación, interferencias o daños?	0 = No existe protección. 1 = No, no están protegidos adecuadamente. 2 = Sí, medidas de protección limitada. 3 = Sí, medidas efectivas.
Mantenimiento de equipos	¿Se realizan los mantenimientos de los equipos correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información?	0 = No existen. 1 = No, no se mantiene de manera adecuada. 2 = Sí, medidas de mantenimiento limitada. 3 = Sí, mantenimiento adecuado.
Disposición o reutilización segura de los equipos	¿Para la disposición o reutilización de equipos, se verifica de manera adecuada que los elementos de los equipos que contienen medios de almacenamiento han eliminado de forma segura los datos sensibles y el software con licencia?	0 = No se verifica. 1 = No, no se realiza de manera adecuada. 2 = Sí, medidas de verificación limitada. 3 = Sí, se verifica adecuadamente.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Dispositivos de punto final de usuario	¿La información en los dispositivos de punto final del usuario está adecuadamente protegida en la universidad?	0 = No existe protección. 1 = No, no se realiza de manera adecuada. 2 = Sí, medidas limitadas. 3 = Sí, protegida adecuadamente.
Derechos de acceso privilegiado	¿En la universidad, la asignación y el uso de derechos de acceso privilegiado están adecuadamente restringidos y gestionados?	0 = No existe gestión. 1 = No, no gestionados adecuadamente. 2 = Sí, con restricciones limitadas. 3 = Sí, gestionados adecuadamente.
Restricción de acceso a la información	¿El acceso a la información y otros activos asociados se encuentra restringido de acuerdo con la política específica establecida sobre el control de acceso?	0 = No existe control. 1 = No, no restringido adecuadamente. 2 = Sí, con restricciones limitadas. 3 = Sí, restringido según la política.
Acceso al código fuente	¿En el área de desarrollo, el acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo y las librerías de software se gestiona apropiadamente?	0 = No existe gestión. 1 = No, no gestionado adecuadamente. 2 = Sí, con restricciones limitadas. 3 = Sí, gestionado adecuadamente.
Autenticación segura	¿En la universidad, se han implementado tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica sobre control de acceso?	0 = No existe gestión. 1 = No, no implementados adecuadamente. 2 = Sí, con implementaciones limitadas. 3 = Sí, implementados adecuadamente.
Gestión de la capacidad	¿Se monitorea y ajusta el uso de los recursos en función de las necesidades de capacidad actuales y previstas dentro de la universidad?	0 = No existe gestión. 1 = No, no monitoreado y ajustado adecuadamente. 2 = Sí, con monitoreo y ajustes limitados. 3 = Sí, monitoreado y ajustado adecuadamente.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Protección contra malware	¿En temas de seguridad, la protección contra el malware se implementa y respalda mediante la conciencia adecuada del usuario?	0 = No existe protección. 1 = No, no implementada y respaldada adecuadamente. 2 = Sí, con implementación y respaldo limitados. 3 = Sí, implementada y respaldada adecuadamente.
Gestión de vulnerabilidades técnicas	¿En la universidad, se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se evalúa la exposición a dichas vulnerabilidades y se toman medidas apropiadas?	0 = No existe gestión. 1 = No, no se obtiene información y no se adoptan medidas adecuadas. 2 = Sí, con información y medidas limitadas. 3 = Sí, se obtiene información y se adoptan medidas adecuadas.
Gestión de la configuración	¿Considera que las configuraciones de seguridad, de hardware, software, servicios y redes se establecen, documentan, implementan, monitorean y revisan adecuadamente?	0 = No existe gestión. 1 = No, no se establecen y documentan adecuadamente. 2 = Sí, con establecimiento y documentación limitados. 3 = Sí, se establecen y documentan adecuadamente.
Eliminación de información	¿Se elimina la información almacenada en dispositivos, sistemas de información o cualquier otro medio de almacenamiento cuando ya no se usa?	0 = Nunca se elimina. 1 = No, no se elimina adecuadamente. 2 = Sí, con eliminación limitada. 3 = Sí, se elimina adecuadamente.
Enmascaramiento de datos	¿Se utiliza el enmascaramiento de datos en la universidad de acuerdo con la política de control de acceso específica y otras políticas relacionadas, así como con las leyes y reglamentos comerciales pertinentes?	0 = Nunca se utiliza. 1 = No, no se utiliza adecuadamente. 2 = Sí, con limitaciones en el uso. 3 = Sí, se elimina adecuadamente.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Prevención de fugas de datos	¿Se han tomado medidas para evitar fugas de datos y dispositivos que procesan, almacenan o transmiten datos confidenciales?	0 = Nunca se toman medidas. 1 = No, no se implementan adecuadamente. 2 = Sí, con implementación limitada. 3 = Sí, se implementan adecuadamente.
Copia de seguridad de la información	¿Las copias de seguridad de la información, el software y los sistemas de la universidad se mantienen y prueban periódicamente de acuerdo con políticas específicas?	0 = Nunca se mantienen. 1 = No, no se mantienen y prueban adecuadamente. 2 = Sí, con mantenimiento y pruebas limitadas. 3 = Sí, se mantienen y prueban adecuadamente.
Redundancia de las instalaciones de procesamiento de información	¿Las instalaciones de procesamiento de información están instaladas con redundancia suficiente para cumplir con los requisitos de disponibilidad?	0 = No existe redundancia. 1 = No, sin redundancia suficiente. 2 = Sí, pero con limitaciones en la redundancia. 3 = Sí, con redundancia suficiente.
Registro	¿Se producen, almacenan, protegen y analizan adecuadamente los registros que contienen actividades, excepciones, fallas y otros eventos relevantes?	0 = No existen esos procesos. 1 = No, no se producen o almacenan adecuadamente. 2 = Sí, pero con limitaciones en la producción o análisis. 3 = Sí, se producen, almacenan y analizan adecuadamente.
Actividad de seguimiento	¿Se monitorean los comportamientos inusuales de las redes, sistemas y aplicaciones y se toman medidas adecuadas para evaluar posibles incidentes de seguridad de la información?	0 = No existen medidas. 1 = No, no se monitorea o evalúa adecuadamente. 2 = Sí, pero con limitaciones en el monitoreo o evaluación. 3 = Sí, se monitorea y adoptan medidas adecuadas.
Sincronización de reloj	¿Se sincronizan regularmente los relojes de los sistemas de procesamiento de información con fuentes de tiempo aprobadas?	0 = No existen sincronización. 1 = No, no se sincronizan regularmente. 2 = Sí, pero de manera irregular. 3 = Sí, se sincronizan regularmente.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Uso de programas de utilidad privilegiados	¿Es estrictamente limitado y controlado el uso de programas de utilidad que puedan anular los controles del sistema y las aplicaciones?	0 = No existen controles. 1 = No, no está restringido y controlado. 2 = Sí, pero con limitaciones. 3 = Sí, está estrictamente restringido y controlado.
Instalación de software en sistemas operativos	¿Existen protocolos y estrategias para administrar de manera segura la instalación de programas informáticos en los sistemas operativos?	0 = No existen protocoles. 1 = No, no se implementan procedimientos y medidas. 2 = Sí, pero con limitaciones. 3 = Sí, se implementan procedimientos y medidas.
Seguridad de redes	¿Se aseguran, gestionan y controlan las redes y los dispositivos de red para proteger la información de los sistemas y las aplicaciones?	0 = No existen protección. 1 = No, las redes y dispositivos de red no están asegurados. 2 = Sí, pero con limitaciones. 3 = Sí, las redes y dispositivos de red están asegurados.
Seguridad de los servicios de red	¿Se identifican, se implementan y se monitorean los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red?	0 = No existen monitoreo. 1 = No, no se identifican, implementan y monitorean los mecanismos de seguridad. 2 = Sí, monitero con limitaciones. 3 = Sí, se identifican, implementan y monitorean los mecanismos de seguridad.
Segregación de redes	¿Los sistemas de información, los usuarios y grupos de servicios de información están ubicados en diferentes redes?	0 = No existe segregación. 1 = No, no están segregados en las redes. 2 = Sí, hay segregación limitada. 3 = Sí, están segregados en las redes.
Filtrado web	¿Se controla el acceso a sitios web externos en su empresa para reducir la exposición a contenido malicioso?	0 = No existe gestión. 1 = No, el acceso no está controlado. 2 = Sí, hay control pero no suficiente. 3 = Sí, se gestiona el acceso con eficacia.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
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.
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.
Requisitos de seguridad de las aplicaciones	Al desarrollar o adquirir aplicaciones, ¿se identifican, especifican y aprueban los requisitos de seguridad de la información?	0 = No existen estándares. 1 = No, no se identifican, especifican ni aprueban los requisitos. 2 = Sí, pero limitadamente. 3 = Sí, se identifican, especifican y aprueban los requisitos.
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.
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.
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.

Objetivos de control- Anexo A 27001	Pregunta	Opciones de Respuesta
Desarrollo externalizado	¿Se dirigen, monitorean y revisan activamente las actividades relacionadas con el desarrollo de sistemas subcontratados?	0 = Nunca. 1 = No, rara vez se dirigen, monitorean y revisan. 2 = Sí, en su mayoría. 3 = Sí, siempre se dirigen, monitorean y revisan.
Separación de entornos de desarrollo, evidencia y producción	¿Los entornos de desarrollo, ensayo y producción están separados y protegidos adecuadamente?	0 = Nunca. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, están totalmente separados y protegidos.
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.
Información de las pruebas	¿Se seleccionan, protegen y gestionan adecuadamente la información de pruebas durante los procesos de prueba?	0 = Nunca se selecciona, protege y gestiona adecuadamente. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre se selecciona, protege y gestiona adecuadamente.
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.

Nota. La tabla define una pregunta con cuatro opciones para cada uno de los controles de seguridad.

Mediante una simulación con el Modelo final de Madurez de la Cultura de Ciberseguridad, se toman los siguientes valores que se obtendrían como resultado de la aplicación de las preguntas elaboradas según cada control, en relación al componente y grupo ocupacional al que pertenece, para determinar en qué nivel de madurez se encontraría

la institución, se toma como resultado la siguiente puntuación por cada componente que se detalla en las siguientes figuras:

Figura 9
Gobernabilidad y controles organizacionales

Componente	Grupo Ocupacional	Control			
	Directivos	Segregación de deberes	¿Qué nivel de distribución y separación de las tareas y responsabilidades relacionadas con los procesos críticos de la universidad entre diferentes personas o grupos existe?	0 No definido 1 En proceso de definición 2 Parcialmente definido 3 Bien definido	2
		Responsabilidades de la dirección	¿Las autoridades dentro de la universidad, exigen al personal , la aplicación de la seguridad de la información de acuerdo a las políticas de seguridad de información establecidas?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre	2
		Contacto con las autoridades	¿La universidad cuenta con procedimientos y canales de comunicación con las autoridades pertinentes en caso de incidentes o delitos cibernéticos?	1 En proceso de desarrollo 2 Parcialmente 3 Procedimientos completamente establecidos	3
		Contacto con grupos de interés especial	¿La universidad establece y mantiene contacto con grupos de interés especial y asociaciones profesionales especializados en Seguridad?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre	2
	Docentes	Contacto con las autoridades	¿La universidad cuenta con procedimientos y canales de comunicación con las autoridades pertinentes en caso de incidentes o delitos cibernéticos?	0 No existen procedimientos 1 En proceso de desarrollo 2 Parcialmente 3 Procedimientos completamente establecidos	1
		Contacto con grupos de interés especial	¿La universidad establece y mantiene contacto con grupos de interés especial y asociaciones profesionales especializados en Seguridad?	0 Nunca 1 Ocasionalmente 2 Frecuentemente 3 Siempre	1

Figura 10
Capacitación y concienciación en habilidades de ciberseguridad

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
	Directivos	Protección de registros	Los registros y datos sensibles de la universidad están protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	1
		Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés	¿Se implementan medidas para proteger la privacidad y la seguridad de la información que pueda identificar a individuos dentro de la universidad, lo que incluye datos como nombres, direcciones, números de seguridad social, números de teléfono, direcciones de correo electrónico, entre otros?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado	2
		Revisión independiente de la seguridad de la información	Se implementan auditorías por parte de terceros independientes para evaluar la efectividad de los controles de seguridad de la información dentro de la universidad, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	1
		Conciencia de seguridad de la información, educación y formación	Se destinan actividades para aumentar el conocimiento y la comprensión del personal sobre la importancia de la seguridad de la información y las mejores prácticas para proteger los activos de la universidad contra amenazas cibernéticas, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	1

Figura 11
Marco jurídico y normativo de la estrategia de ciberseguridad

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
	Directivos	Políticas de la seguridad de la información	¿Se han implementado las reglas, directrices, procedimientos y prácticas para proteger la información que maneja la universidad?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado	2
		Requisitos legales, reglamentarios y contractuales	En la universidad se cumple con las leyes, regulaciones y acuerdos contractuales relevantes en materia de seguridad de la información , de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	3
		Derechos de propiedad intelectual	¿Se implementan procedimientos para la protección de los activos intangibles de la universidad, como la propiedad intelectual, la propiedad de software, los derechos de autor y las patentes, frente a posibles amenazas cibernéticas?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado	2
		Cumplimiento de políticas, reglas y estándares de seguridad de la información	Las políticas, reglas y estándares establecidos para la seguridad de la información dentro de una universidad se cumplen entro de la universidad, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	2
		Proceso disciplinario	¿Se establecen los procedimientos para abordar violaciones de la política de seguridad de la información, que implica la aplicación de medidas disciplinarias apropiadas contra los empleados que incumplen las políticas y procedimientos de seguridad de la información de la institución?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos	2

Figura 12
Gestión de activos tecnológicos

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
	Directivos	Devolución de activos	¿Se establecen procedimientos para garantizar que los activos digitales, como dispositivos informáticos, cuentas de usuario, credenciales de acceso y otros recursos relacionados, sean recuperados de manera segura cuando un miembro de la comunidad universitaria deja de estar asociado con la institución?	0 No establecidos 1 En proceso de establecimiento 2 Parcialmente establecidos 3 Totalmente establecidos	3
		Preparación de las TIC para la continuidad de negocio	¿Se implementan medidas y procedimientos para garantizar que los sistemas de tecnología de la información y comunicación (TIC) de la universidad estén listos para continuar operando de manera efectiva durante situaciones de emergencia o interrupción, garantizando así la continuidad de las operaciones críticas?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado	2
		Trabajo remoto	¿Se implementan medidas de seguridad para proteger la información y los sistemas de la universidad cuando los empleados trabajan fuera de las instalaciones físicas de la institución, ya sea desde sus hogares u otro lugar remoto?	0 No implementado 1 En proceso de implementación 2 Parcialmente implementado 3 Totalmente implementado	3
		Emplazamiento y protección de equipos	¿En la universidad, los equipos están situados de forma segura y protegida?	2 = Sí, con medidas de protección limitada. 3 = Sí, y cuentan con medidas de protección adecuadas.	2

Figura 13
Gestión de usuarios y accesos

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
	Directivos	Roles y responsabilidades en la Seguridad de la Información	¿Cuál es el nivel de definición de los roles y responsabilidades en la seguridad de la información de acuerdo a las necesidades de la universidad?	0 No definido 1 En proceso de definición 2 Parcialmente definido 3 Bien definido	2
		Transferencia de información	¿Existen normas establecidas para la gestión y regulación de quién tiene permiso para acceder a los recursos de información y sistemas dentro de una organización, así como a qué recursos específicos pueden acceder y en qué capacidad?	0 No establecidas 1 En proceso de establecimiento 2 Parcialmente establecidas 3 Totalmente establecidas	2
		Control de acceso	¿Existen normas establecidas para la gestión y regulación de quién tiene permiso para acceder a los recursos de información y sistemas dentro de una organización, así como a qué recursos específicos pueden acceder y en qué capacidad?	0 No establecidas 1 En proceso de establecimiento 2 Parcialmente establecidas 3 Totalmente establecidas	2
	Docentes	Transferencia de información	Dentro de la universidad se manejan reglas, procedimientos o acuerdos vigentes de transferencia de información, entre la institución y otras partes, de manera:	2 Casi continua 3 Permanente	3
		Control de acceso	¿Existen normas establecidas para la gestión y regulación de quién tiene permiso para acceder a los recursos de información y sistemas dentro de una organización, así como a qué recursos específicos pueden acceder y en qué capacidad?	0 No establecidas 1 En proceso de establecimiento 2 Parcialmente establecidas 3 Totalmente establecidas	3

Figura 14
Estrategias de gestión de riesgos y amenazas

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
	Directivos	Planificación y preparación de la gestión de incidentes de seguridad de la información	¿Se definen planes y procedimientos para la gestión de incidentes de seguridad dentro de una universidad, mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes?	0 No definido 1 En proceso de definición 2 Parcialmente definido 3 Bien definido	2
		Evaluación y decisión sobre eventos de seguridad de la información	Dentro de la universidad se analiza y se toma medidas adecuadas en respuesta a eventos relacionados con la seguridad de la información de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	3
		Aprender de los incidentes de seguridad de la información	En la universidad se lleva a cabo el análisis y revisión de los incidentes de seguridad, con el objetivo de identificar lecciones aprendidas, mejorar las prácticas de seguridad y prevenir futuros incidentes similares, de manera:	0 Nula 1 Ocasional 2 Casi continua 3 Permanente	3
		Protección contra amenazas físicas y ambientales	¿Se ha diseñado e implementado adecuadamente la protección contra amenazas físicas y medioambientales, incluyendo catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas, a las infraestructuras?	diseñada o implementada. 2 = Sí, su implementación es limitada. 3 = Sí, está bien diseñada e implementada.	2
		Trabajar en áreas seguras	¿En la universidad se han diseñado e implementado medidas de seguridad para trabajar en zonas seguras (instalaciones que necesitan un nivel adicional de seguridad)?	diseñada o implementada. 2 = Sí, su implementación es limitada. 3 = Sí, medidas de seguridad efectivas para trabajar en zonas seguras.	3
		Prevención de fugas de datos	¿Se han tomado medidas para evitar fugas de datos y dispositivos que procesan, almacenan o transmiten datos confidenciales?	adecuadamente. 2 = Sí, con implementación limitada. 3 = Sí, se implementan adecuadamente.	3

Figura 15
Protección de la información y procedimientos

Componente	Grupo Ocupacional	Control	Preguntas	Opciones	Respuestas
Protección de la información y procedimientos	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?	conjuntamente. 1 = No, rara vez. 2 = Sí, en su mayoría. 3 = Sí, siempre se planifican y acuerdan conjuntamente.	2
	Funcionarios Técnicos en Inf.	Uso de la criptografía	¿Se han establecido e implementado estándares para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas?	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?	2 = Sí, hay estándares pero no implementación completa. 3 = Sí, se han definido e implementado estándares.	2
		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

Como un resumen de la simulación tenemos que el componente de Gobernabilidad y controles organizacionales, con 2.22, cae en un nivel medio de aplicación; Capacitación y concienciación en habilidades de ciberseguridad, con 1.54, cae en un nivel medio de aplicación; Marco jurídico y normativo de la estrategia de ciberseguridad, con 2.33 cae en el nivel medio de aplicación; Gestión de activos tecnológicos, con 2.33, cae en un nivel medio de aplicación; Gestión de usuarios y acceso, con 2.32, cae en un nivel medio de aplicación; Estrategias de gestión de riesgos y amenazas, con 2.48, cae en un nivel medio de aplicación y el componente; Protección de la información y procedimientos, con un 2.36, cae dentro de

un nivel medio de aplicación. Esto da como resultado la siguiente distribución de los niveles de aplicación de cada nivel de madurez, en comparación con los niveles requeridos, detallados en la Tabla 8.

Tabla 11
Nivel actual de la simulación del Modelo de Madurez

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:							

Nota. Resultado del nivel de madurez actual mediante la simulación de la aplicación del modelo de madurez.

Con los resultados obtenidos y en comparación con la tabla de niveles de aplicación requeridos para cada nivel de madurez, una institución determinada se ubica dentro del nivel dos de madurez, que se denomina nivel planificado, el cual representa que existe conciencia de la importancia de la ciberseguridad y apoyan la planificación de la ciberseguridad, se elabora y aprueba el proyecto de ciberseguridad, se establece una línea base de ciberseguridad, y en el que algunos aspectos han comenzado a desarrollarse y formularse, pero pueden ser aún improvisados, desorganizados, o simplemente nuevos.

Capítulo V: Conclusiones y Recomendaciones

Conclusiones

- Se ha construido una propuesta de modelo de madurez en el contexto de las Instituciones de Educación Superior 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 Institución de Educación Superior (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 de ellos tiene sus propias ventajas. La combinación estratégica de elementos de estos modelos permite la creación de un modelo de madurez de 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 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.

Referencias

Alonso, C. (2023). *¿Qué es ISO 27000 - Seguridad de la Información?* | *GSS*. https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Amplio, C., Antonio, L., Rodríguez, V., Pablo, M., & Recalde Varela, M. (2023). *Título del proyecto: Modelo de evaluación del nivel de madurez de la seguridad de la información Línea de Investigación: SEGURIDAD INFORMÁTICA*.

Bazalar, G. A., Ricse, C., & Rodriguez, J. (2022). *Modelo de madurez para determinar el nivel de cultura de ciberseguridad en organizaciones industriales*. http://hdl.handle.net/10757/669347

BID, & OEA. (2020). *Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe (2)*.

Castillo, U., & Polanco, M. (2016). *QUÉ ES LA CIBERSEGURIDAD?*

Cisco. (2024). *¿Qué es la ciberseguridad?* https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~tipos-de-amenazas

Cornejo, Y., Verdezoto, V., & Villacis, A. (2019). Ciberdefensa, Ciberseguridad Y Sus Efectos En La Sociedad. *International Multilingual Journal of Science and Technology (IMJST)*, *4*, 2528–9810. www.imjst.org

ENISA. (2023). *Guía de ciberseguridad para pymes*.

Fernando, D., & Sumalave, G. (2021). *UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA Documento FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO Código RESUMEN-TRABAJO DE GRADO AUTORES DIRECTOR TITULO EN INGLES*.

Fortaleza Abogados. (2023). *La Importancia de la Ciberseguridad* | *LinkedIn*. https://www.linkedin.com/pulse/la-importancia-de-ciberseguridad-fortaleza-abogados/?originalSubdomain=es

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

González, D. A., Soto, D. E., Peláez, L. E., Villamizar, A. E., Delgado, I. A., & Vidal, F. A. (2023). *Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas*.

Guerrero, D. (2023). *Modelo De Gestión De Ciberseguridad Para Resolver Incidentes En Instituciones De Educación Superior*.

Hernández, J. C. (2018). *Estrategias Nacionales de Ciberseguridad en América Latina*. https://www.researchgate.net/publication/325397629_Estrategias_Nacionales_de_Ciberseguridad_en_America_Latina

Herrera, B., Adolfo, G., Ricse, E., Danny, C., Neyra, R., & Pepe, J. (2022). *Modelo de madurez para determinar el nivel de cultura de ciberseguridad en organizaciones industriales Item Type info:eu-repo/semantics/masterThesis*. http://hdl.handle.net/10757/669347

INCIBE. (2023). *DESARROLLAR CULTURA EN SEGURIDAD*.

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*. https://doi.org/10.1109/CYBERSECPODS.2019.8885240

ISACA. (2024). *ISACA Interactive Glossary | ISACA*. https://www.isaca.org/resources/glossary

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR*.

Morales, S. D. T. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un “proyecto compartido”. Especial referencia al ámbito universitario. *ICADE. Revista de La Facultad de Derecho*, *0*(92), 13–47. https://doi.org/10.14422/ICADE.I92.Y2014.001

Morales-Paredes, P. I., & Medina-Chicaiza, P. (2021). Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua - Ecuador. *3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, *10*(2), 49–75. https://doi.org/10.17993/3ctic.2021.102.49-75

Novelo, C. D., Sebastián Martínez, Y., Pillado, X. D., Quintero-Martinez, M. I., Anduin, S., Balderas, T., Jesús, F., Pedraza, L., Consuelo, M., González, M., & Sandoval García, E. R. (2019). *La Inteligencia Artificial en la transformación de procesos universitarios Principales elementos para el diseño de la Gobernanza Institucional/ Organizacional de Seguridad de la Información*. https://www.ties.unam.mx/

Pérez-Mergarejo, E. I., Pérez-Vergara, I. I., & Rodríguez-Ruíz III, Y. (2014). *Maturity models and the suitability of its application in small and medium enterprises*.

PwC. (2020). *Informe del estado de cultura de ciberseguridad en el entorno empresarial*.

Rea, Á. M. (2020). *Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad*.

Rea-Guaman, A. M., Sánchez-García, I. D., San Feliu, T., & Calvo-Manzano, J. A. (2017). *Modelos de Madurez en Ciberseguridad: una revisión sistemática*.

Ron, M., Rivera, O., Fuertes, W., Toulkeridis, T., & Díaz, J. (2019). *Cybersecurity Baseline: An Exploration, which permits to delineate National Cybersecurity Strategy in Ecuador*.

Sarri, A., Kyranoudi, P., Thirriot, A., Charelli, F., & Dominique, Y. (2020). *MARCO DE EVALUACIÓN DE LAS CAPACIDADES NACIONALES SOBRE LA ENISA AUTORES*. https://doi.org/10.2824/895115

Systems Security Engineering Capability Maturity Model (SSE-CMM) Project. (1999). *Systems Security Engineering Capability maturity Model SSECMM Model Description Document*.

Universidad de las Fuerzas Armadas Espe. (2019). *Honorable Consejo Universitario*. https://hcu.espe.edu.ec/descripcion/

Willmer Rico Bautista, D., Darío Guerrero Santander, C., Alberto Collazos Ordóñez, C., & Paola Maestre Góngora, G. (2022). *Tesis para optar al título de Doctor en Ingeniería*.