RNPS 2487 • ISSN 2708-3411
Vol. 5 • Nro. 4 • oct-dic 2024 • e272

ARTÍCULO ORIGINAL

Índice sintético de ciberseguridad, de la Facultad de Turismo, Universidad de La Habana

Synthetic index of cybersecurity of the Tourism Faculty, Havana University

Emilio Enrique Guerra Castellón
emilito042@gmail.com • *https://orcid.org/0009-0005-2436-7186*

Edgar Núñez Torres
enunez8609@gmail.com

Yasser Vázquez Alfonso
yalfos1@gmail.com.com • *https://orcid.org/0000-0002-4074-0711*

UNIVERSIDAD DE LA HABANA

Recibido: 2024-10-08 • Aceptado: 2024-12-23

RESUMEN

La ciberseguridad se encarga de la protección de la estructura computacional y la información almacenada en los equipos de cómputo, de las organizaciones pertenecientes a diferentes sectores de la sociedad. El propósito de esta investigación es evaluar, mediante un índice sintético, la madurez de ciberseguridad en la Facultad de Turismo, de la Universidad de La Habana. Este índice está basado en dimensiones e indicadores clave, como compromiso de la alta dirección, educación y conciencia sobre ciberseguridad, así como la implementación de tecnologías y sistemas de gestión, lo que permite identificar fortalezas y debilidades en el contexto del enfrentamiento de los riesgos de ciberseguridad que se han intensificado últimamente en las universidades cubanas. Se aplicaron los métodos: análisis-síntesis, para integrar los resultados de diferentes fuentes; inductivo-deductivo, para emitir conclusiones generales basadas en observaciones específicas; estadístico, que facilitó la validación de los datos obtenidos, mientras que herramientas como Excel, SPPS y RStudio apoyaron el análisis cuantitativo. El trabajo de campo y el grupo focal proporcionaron información cualitativa valiosa, y el esquema lógico del índice sintético sirvió para estructurar el cálculo de los indicadores de madurez de ciberseguridad. La investigación refleja resultados positivos para la facultad y el índice general, las dimensiones y los indicadores revelan una alta madurez. Se demuestra la importancia de superar los puntos débiles existentes, como la asignación de responsabilidades claras y el entendimiento de las obligaciones y riesgos para prevenir amenazas que atentan contra la seguridad de la información.

Palabras clave: ciberseguridad, dimensiones, indicadores, índice sintético, universidad.

ABSTRACT

Cybersecurity is responsible for the protection of the computer structure and the information stored in the computer equipment of organizations in different sectors of society. The purpose of this research is to evaluate the maturity of cybersecurity in the Faculty of Tourism of the University of Havana by means of a synthetic index. This index, based on key dimensions and indicators such as top management commitment, cybersecurity education and awareness, as well as the implementation of technologies and management systems, allows identifying strengths and weaknesses in the context of facing the cybersecurity risks that have intensified in recent years in Cuban universities. Methods such as analysis-synthesis were applied to integrate the results from different sources; inductive-deductive methods were used to draw general conclusions based on specific observations; the statistical method facilitated the validation of the data obtained, while tools such as Excel, SPPS and RStudio supported the quantitative analysis. On the other hand, the fieldwork and the focus group provided valuable qualitative information, and the logical scheme of the synthetic index served to structure the calculation of the cybersecurity maturity indicators. The research reflects positive results for the faculty, the overall index, dimensions and indicators show a high maturity. It demonstrates the importance of overcoming existing weaknesses such as the allocation of clear responsibilities and understanding of obligations and risks to prevent threats to information security.

Keywords: cibersecurity, dimensions, indicators, synthetic index, university.

INTRODUCCIÓN

En esta era del conocimiento donde se mueve la sociedad y más aún, en el mundo globalizado actual, la información se ha vuelto un recurso de gran valor. Eventos, como: fuga de información, ataques informáticos, protocolos y sistemas de seguridad doblegados y demás fallas de seguridad que involucran tanto al sector privado como al público, hacen pensar en los riesgos de los sistemas que albergan la información (Venter et al., 2019).

En este sentido, la ciberseguridad o seguridad informática, términos que son sinónimo en la literatura, cobran una vital importancia. El concepto aparece como un mecanismo para la defensa nacional digital, una vez que se comprenden los peligros de la manipulación de la información y de los sistemas en los que se alberga, lo que puede provocar desestabilidad de los sectores sociales (Valencia et al., 2020).

La ciberseguridad, según Von Solms y Van Niekerk (2013), hace referencia a las áreas de la ciencia de la computación que se encargan de la protección tanto de la estructura computacional y de la información que es soportada en esta, que es uno de los recursos más importantes para proteger. Involucra el estudio y análisis de las redes computacionales, a través de una serie de estándares, protocolos, métodos y demás herramientas que se tienen para poder minimizar los posibles riesgos a la infraestructura y a la información circundante, por lo que se involucran el software, el hardware y las redes (Jaiyen y Sornsuwit, 2019).

De esta manera, la ciberseguridad busca garantizar el mantenimiento de las propiedades de seguridad de los activos de la organización, así como a los usuarios y su información, contra riesgos propios del ciber entorno (Ganesan et al., 2016).

En el contexto cubano, el término «ciberseguridad» es reconocido en el decreto N° 360, de 2019, publicado en la Gaceta Oficial de la República de Cuba. En el artículo 5 del Capítulo I se plantea: «La ciberseguridad es el estado que se alcanza, mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio».

Según el periódico Granma (2024), Cuba reafirma la voluntad de proteger la seguridad de las instituciones y personas en el ámbito digital. Distintas legislaciones propician un marco regulatorio con las medidas que deben implementar las instituciones, en caso de un ataque cibernético o una contaminación por algún programa maligno, afirmó el director general de la Oficina de Seguridad para las Redes Informáticas (OSRI).

La evaluación de la ciberseguridad en las universidades es un aspecto crucial en la era digital actual. Varias instituciones académicas están ofreciendo programas y títulos especializados en ciberseguridad, para abordar la creciente demanda de profesionales capacitados en este campo, por ejemplo, el Banco Interamericano de Desarrollo (BID) y el Laboratorio de Seguridad Informática (COSEC), de la Universidad Carlos III, de Madrid (U3CM), han colaborado para desarrollar un programa de Maestría en Ciberseguridad, específicamente diseñado para universidades de América Latina y el Caribe (Nowersztern, 2021), cuyo objetivo es cerrar la brecha entre educación y profesionales en ciberseguridad, de la región, al proporcionar conocimiento y recursos expertos. Además de los programas de maestría, las universidades también ofrecen títulos especializados, como Licenciatura en Ciberseguridad, que equipa a los estudiantes con las habilidades necesarias para analizar, auditar y asesorar en asuntos de ciberseguridad (Universidad Rey Juan Carlos, 2024). También existen programas de maestría en línea, que se centran en auditorías de seguridad, ciencia forense digital y aplicación de las matemáticas en ciberseguridad (Universidad de León, 2024). Estos programas resaltan la importancia de incorporar habilidades prácticas y conocimientos teóricos en la educación en ciberseguridad.

Las universidades también están estableciendo alianzas con expertos de la industria para mejorar la educación en ciberseguridad. El Gobierno cubano ha puesto en marcha cátedras universidad-industria, en áreas como la ciberseguridad, para mejorar la colaboración entre entidades públicas y privadas (Ministerio de Ciencia, Innovación y Universidades, 2024). Esta colaboración tiene como objetivo fortalecer las prácticas de ciberseguridad y abordar las amenazas emergentes en el panorama digital. En Cuba existe la Ingeniería en Ciberseguridad y el técnico superior en Administración de Redes y Seguridad Informática, con la Universidad de Ciencias Informáticas (UCI) como centro rector de ambas carreras, donde se desarrollan competencias avanzadas en gestión de riesgos y protección de sistemas. Estos programas han demostrado su impacto, al preparar profesionales que lideran iniciativas de seguridad digital en instituciones y empresas.

Se han realizado estudios de investigación para evaluar las prácticas de ciberseguridad entre los estudiantes universitarios. Un estudio en la Universidad Politécnica Salesiana de Guayaquil evaluó las buenas prácticas de ciberseguridad entre los estudiantes, enfatizando la importancia de promover una cultura de concienciación sobre la ciberseguridad (Torres et al., 2024). Esta investigación subraya la importancia de evaluar y promover las mejores prácticas de ciberseguridad entre los estudiantes universitarios, para mejorar las medidas de seguridad generales.

La evaluación de la ciberseguridad en las universidades es un esfuerzo multifacético, que involucra programas académicos, asociaciones con la industria e iniciativas de investigación. Al evaluar y mejorar continuamente las

prácticas de ciberseguridad en los entornos educativos, las universidades pueden preparar mejor a los estudiantes para carreras en ciberseguridad y contribuir a un entorno digital más seguro. La revisión de la literatura sobre la evaluación de la ciberseguridad en las universidades cubanas es limitada. Si bien hay un enfoque en varios aspectos de la gestión y la educación universitaria en Cuba, hay una falta de investigación específica sobre ciberseguridad en este contexto.

La constante evolución de las tecnologías ha facilitado la distribución de información, así como la presencia de empresas y entidades en Internet, lo que ha traído como inconveniente que estas estén expuestas a amenazas constantes por parte de los usuarios malintencionados. Las universidades son uno de los objetivos preferidos de los atacantes, debido a la gran cantidad de usuarios conectados a Internet. Un informe del Gobierno del Reino Unido reveló que 85 % de las universidades han sufrido ciberataques en el último año, superando a otros niveles educativos, como escuelas secundarias (63 %) y primarias (41 %), cifras alarmantes que destacan la vulnerabilidad de estas instituciones frente a amenazas cibernéticas (Delgado, 2023). Además, IT User Tech y Bussiness (2023) afirma que las agresiones más comunes a las universidades son los ataques phishing, lo que resulta 85 % de incidentes relacionados con rasomware, y 25 % de ataques anuales de DNS, con 90 %, y que los ataques DDoS han llevado a un costo promedio por hora de 40 000 USD/hora, mientras que estudios recientes del Centro Nacional de Ciberseguridad de Reino Unido (NCSC) reportan un aumento significativo en intentos de phishing dirigidos a instituciones educativas. Por ejemplo, en 2022, varias universidades en Estados Unidos experimentaron accesos no autorizados a sistemas internos que comprometieron información confidencial de estudiantes y empleados.

En una revisión de la gestión de incidentes en universidades cubanas, la cual influye en el enfrentamiento de los riesgos de ciberseguridad, se pudo identificar como problema que estos se realizan, mayormente, empleando métodos manuales, lo cual provoca demora en su respuesta y poca preparación de los especialistas para gestionar determinados incidentes, debido a que en ocasiones la fluctuación de especialistas es alta. No se tiene de forma precisa el procedimiento que se debe realizar cuando ocurre un incidente de seguridad, lo que trae como consecuencia que a veces los incidentes demoren varios días en solucionarse (Sánchez et al., 2022).

Por las razones anteriores, muchos de los ciberincidentes que ocurren en las universidades cubanas tienen efectividad y la Facultad de Turismo de la Universidad de La Habana no es ajena a esta realidad, por lo que enfrentar los riesgos de ciberseguridad resulta sumamente importante. En esas condiciones surge esta investigación, con el objetivo de evaluar mediante un índice sintético la ciberseguridad en la Facultad de Turismo (FTUR), de la Universidad de La Habana.

METODOLOGÍA

Para realizar esta investigación de tipo no experimental, transversal y con un enfoque descriptivo cuantitativo, se siguió el siguiente procedimiento metodológico (tabla 1).

Tabla 1. Procedimiento metodológico de la investigación

Etapas	Fases	Métodos y herramientas
Etapa 1: Planteamiento del problema de investigación.	Fase 1: Revisión de la literatura. Fase 2: Definición del problema y los objetivos.	• Revisión bibliográfica. • Análisis-síntesis.
Etapa 2: Diseño metodológico de la investigación.	Fase 1: Selección del diseño de la investigación. Fase 2: Selección del instrumento para evaluar la ciberseguridad, mediante un índice sintético de ciberseguridad.	• Consultas de búsqueda en Internet. • Revisión bibliográfica. • Consulta a expertos.
Etapa 3: Evaluación de la ciberseguridad, mediante un índice sintético.	Fase 1: Identificación de los especialistas en materia de ciberseguridad en FTUR. Fase 2: Caracterización de FTUR en cuanto a la ciberseguridad. Fase 2: Aplicación del Instrumento. Fase 3: Procesamiento y análisis de información.	• Trabajo de Campo. • Grupo focal. • Cuestionario. • Esquema lógico. • Método estadístico. • Excel. • SPPS. • RStudio.

(Fuente: Elaboración propia)

Para evaluar la madurez de ciberseguridad existen varios modelos (CMM, C2M2, NIST, Citigroup´s Information Security Evaluation, COBIT Maturity Model, CERT/CSO, entre otros). En esta investigación se optó por emplear el modelo de Ramírez (2016), porque ofrece un enfoque adaptado a las necesidades específicas de las organizaciones y empresas en el contexto latinoamericano e integra la mayoría de los modelos de madurez de ciberseguridad planteados anteriormente, permitiendo una evaluación más precisa y contextualizada de las capacidades de ciberseguridad. En el anexo 1 aparece la descripción de los ítems y las dimensiones propuestas para evaluar la madurez de ciberseguridad.

De esta forma, se obtiene una valoración de los indicadores, ponderada en función de las características de cada indicador, pero a la vez comparable entre ellos, para que posteriormente puedan ser sintetizados en índices dimensionales y estos en un índice general que responderá a la madurez de ciberseguridad de la Facultad de Turismo, a través del esquema lógico para el cálculo del índice sintético de ciberseguridad (ISC).

Pasos para el cálculo del índice sintético:

1. Parametrización de los indicadores propuestos, a partir de la información cualitativa y cuantitativa que se pueda extraer del análisis de cada uno de ellos en donde se desarrolla el estudio. Esta parametrización le determina a cada indicador un valor entre 1 y 5 puntos.

2. El valor de cada dimensión depende del valor medio de los indicadores que lo compongan, multiplicado por el peso asociado a dicha dimensión. El peso por dimensiones se distribuye a partir

del porciento que representen los indicadores que lo componen del total de indicadores en escala de 0 a 1. De esta forma, las dimensiones que posean mayor cantidad de indicadores tendrán asociado un mayor peso y por ende una mayor influencia dentro del cálculo del ISC.

3. El cálculo del ISC es la sumatoria de los valores ponderados de las dimensiones que lo compone.

El análisis permite reflejar la situación de ciberseguridad de la Facultad de Turismo, así como el estudio parcial de sus dimensiones, para poder incidir en las más afectadas. La escala de evaluación final del ISC se muestra en la tabla 2.

Tabla 2. Escala de evaluación

Valor del ISC	Evaluación de ciberseguridad
ISC [0;1]	Ciberseguridad muy baja
ISC (1; 2]	Ciberseguridad baja
ISC (2; 3]	Ciberseguridad media
ISC (3; 4]	Ciberseguridad alta
ISC = 5	Ciberseguridad muy alta

(Fuente: Elaboración propia).

El esquema lógico del índice sintético se muestra a continuación (figura 1):

Instrumento de Ciberseguridad planteado por Ramírez (2016)	Análisis por dimensiones	Análisis por ítems		Síntesis	Índice Sintético de Ciberseguridad (ISC)	
	Compromiso del gerente		2 ítems			0.06 x Isp
	Entendimiento de las obligaciones		1 ítems			0.03 x Isp
	Entendimiento de los riesgos de seguridad		1 ítems			0.03 x Isp
	Contramedidas esenciales de ciberseguridad		13 ítems			0.38 x Isp
	Reglas		1 ítems			0.03 x Isp
	Responsabilidades		1 ítems			0.03 x Isp
	Plan de supervivencia		2 ítems			0.06 x Isp
	Vigilancia		2 ítems			0.06 x Isp
	Políticas y procedimientos		2 ítems			0.06 x Isp
	Sistema de gestión		1 ítems			0.03 x Isp
	Tecnologías de seguridad		4 ítems			0.12 x Isp
	Educación		1 ítems			0.03 x Isp
	Conciencia		3 ítems			0.09 x Isp

Fig. 1 Esquema lógico para la construcción del ISC (Fuente. Elaboración propia, a partir de Ramírez, 2016).

RESULTADOS Y DISCUSIÓN

La Facultad de Turismo (FTUR) de la Universidad de La Habana cuenta con entre 40 y 70 trabajadores. Dispone de varias infraestructuras tecnológicas, como computadoras de escritorio, sitio web, aplicaciones, correo electrónico corporativo, enlaces de telecomunicaciones, varios dispositivos móviles, equipos de acceso inalámbrico, así como Internet, a través dispositivos móviles, mediante una red wifi y la cobertura de datos 4G o a partir del nodo UH con el uso de las computadoras de escritorio. A su vez, tiene un Sistema de Gestión de Seguridad de la Información, existe

al menos un cargo exclusivo para temas de seguridad de la información y se le concede una alta importancia tanto a usar buenas prácticas en ciberseguridad a la hora de realizar labores y a invertir en la seguridad de la información. Se considera que el centro puede ser objetivo de delincuentes o actitudes malintencionadas, para obtener información confidencial que, como centro de altos estudios, puede ser de interés para estudiantes, profesores y otros individuos, ya sea de la propia institución, de otras facultades o de otra procedencia. A partir del cuestionario aplicado en el grupo focal se obtuvo la información referente a los ítems y dimensiones de la ciberseguridad, como se detalla seguidamente.

Dimensión 1. Compromiso de la alta dirección de FTUR

La alta dirección siempre lidera y apoya las iniciativas de seguridad de la información compatibles con la estrategia y misión de la organización, promueve las acciones que se deben realizar, plantea las buenas prácticas, concientiza a profesores y otros trabajadores de la facultad, escucha sugerencias y propuestas, y resguarda la información mediante salvas. Casi siempre asegura que se tengan los recursos suficientes para el desarrollo de las iniciativas en seguridad de la información. No se cuenta con un presupuesto fijo para invertir en términos de ciberseguridad, lo que limita la implementación de medidas adecuadas de protección. Tampoco se dispone de un personal lo suficientemente capacitado o especializado en ciberseguridad, lo que deja vulnerabilidades en los sistemas de información. Los sistemas operativos de las computadoras se actualizan automáticamente y con ello la seguridad de Windows. Se tiene una PC para hacer las salvas de la información.

Dimensión 2. Entendimiento de las obligaciones

Casi todos los trabajadores y profesores conocen las obligaciones contractuales, legislativas y regulatorias que exigen requerimientos de seguridad de la información, pero no se conoce a profundidad cada una de ellas por todo el personal de la facultad.

Dimensión 3. Entendimiento de riesgos de seguridad

Casi siempre se conocen y revisan periódicamente los riesgos en seguridad de la información a los cuales se está expuesto, pero no se tiene un proceso sistemático para identificar riesgos de seguridad, lo que puede dejar expuestos varios puntos críticos sin protección adecuada. No se realiza una evaluación detallada de los riesgos, lo que impide una comprensión clara de la gravedad de las amenazas y cómo deben abordarse.

Dimensión 4. Contramedidas esenciales de seguridad

Se tienen definidos claramente los procesos de control del personal antes de la contratación, durante el empleo y después de la terminación del contrato, para preservar la seguridad de la información de la facultad. El acceso a las instalaciones y los sistemas es restringido; la recepcionista de la instalación constantemente controla el acceso de las personas, permitiendo solo la entrada a estudiantes, profesores y trabajadores. Para conectarse a las redes de Internet de las computadoras de la facultad se necesita una cuenta de usuario y para la instalación de los software se requiere la contraseña de administrador, que la posee solo el personal autorizado. Algunas computadoras inician sesión con el usuario principal sin solicitar contraseñas, lo cual es un riesgo; la información confidencial que exista puede ser obtenida, manipulada y eliminada por individuos malintencionados.

La institución desde el punto de vista constructivo se encuentra en óptimas condiciones para enfrentar los desastres naturales que ocurren casi siempre, como ciclones o tormentas tropicales, tornados u otro tipo de evento meteorológico. Se conoce todo el procedimiento que se debe seguir en caso de que estos fenómenos ocurran, para

resguardar la integridad de los recursos y activos de la facultad. Se lleva un control de los equipos entrantes y salientes de manera automatizada. Cada uno de los ordenadores de escritorio de la facultad tiene instalado un antivirus, el cual es controlado y actualizado por un personal dedicado a esta actividad.

Diariamente se hacen copias de respaldo de la información importante en la máquina del especialista en seguridad informática. Los acuerdos de confidencialidad con los proveedores se firman a través de un convenio y contrato por ambas partes. Se hace ese registro, seguimiento y revisión de los servicios de los proveedores, mediante un software que trabaja el especialista de economía. La facultad tiene y mantiene un inventario completo y actualizado de todos sus activos de información, incluyendo hardware, software, datos y documentos importantes. La institución dispone de un esquema de clasificación de la información bien definido, que categoriza los datos según su sensibilidad y criticidad. Se tienen procedimientos documentados para la gestión de medios, que incluyen directrices claras para el almacenamiento, manejo y acceso a los medios que contienen información sensible. Las normas establecidas por el Ministerio de Educación Superior establecen claramente las políticas definidas para el teletrabajo y el manejo de dispositivos móviles, que incluyen directrices sobre el uso seguro de teléfonos inteligentes, tablets y laptops, para acceder a la información de la institución. Hay establecidas reglas para la instalación de software: se requiere disponer la contraseña del rol de administrador. No se realizan acciones, por ejemplo, como preguntar el nombre del software que se desea instalar en caso de solicitar al administrador su ayuda para proceder con las instalaciones.

Dimensión 5. Reglas

Existen políticas de seguridad de la información bien definidas y documentadas, que abarcan todos los aspectos de la gestión y protección de la información y los datos.

Dimensión 6. Responsabilidades

Se tienen algunos roles y responsabilidades asignadas para la seguridad de la información, pero no se cumplen en su totalidad.

Dimensión 7. Plan de supervivencia

La institución tiene un plan de continuidad del negocio documentado y actualizado, que detalla los procedimientos y las medidas que se deben seguir en caso de una interrupción significativa de las operaciones por desastres naturales u otro evento inusual. Tiene un procedimiento documentado y bien definido para la gestión de incidentes de seguridad de la información, que detalla los pasos a seguir desde la identificación hasta la resolución del incidente.

Dimensión 8. Vigilancia

Los eventos de seguridad se monitorean y evalúan. Existen auditorías internas para la seguridad de la información.

Dimensión 9. Políticas y procedimientos

En cuanto a las personas dedicadas a la seguridad de la información, existe al menos un cargo exclusivo para temas de seguridad de la información. Se dispone de un sistema de gestión documental específico para la seguridad de la información, que permite el almacenamiento, organización y acceso controlado a toda la documentación relevante.

Dimensión 10. Sistema de gestión

Se tiene un sistema de gestión de seguridad de la información que proporciona herramientas importantes, para llevar a cabo de manera segura el manejo de los datos e información relevante.

Dimensión 11. Tecnologías de seguridad

Hay presencia de controles criptográficos, se hacen análisis y gestión de vulnerabilidades y se tiene una arquitectura de red segura y políticas de desarrollo seguro.

Dimensión 12. Educación

Cuentan con un plan de conciencia y capacitación en ciberseguridad, el cual involucra a cada uno de los miembros de la organización. Además, como parte del plan de estudios de la Licenciatura en Turismo se imparte un tema dedicado a la ciberseguridad en la asignatura Informática, duarnte el primer año de la carrera.

Dimensión 13. Conciencia

Consideran importante y se valora mucho la seguridad de la información para las actividades de la facultad. A su vez, se tiene en cuenta que es conveniente tener buenas prácticas en seguridad de la información a la hora de manipular información de la empresa.

A continuación, en la figura 2, se muestra cómo se evaluaron desde la perspectiva de los investigadores los ítems y las dimensiones que integran el índice sintético de ciberseguridad de la Facultad de Turismo.

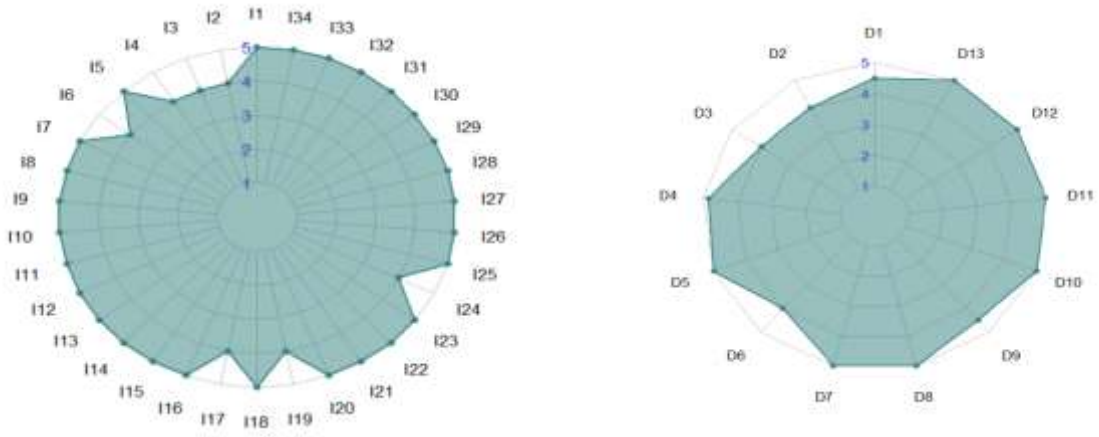

Fig. 2 Evaluación de los ítems y dimensiones del índice sintético (Fuente. Elaboración propia en RStudio).

Los resultados del análisis cuantitativo arrojan un panorama alentador en términos de ciberseguridad para la Facultad de Turismo (FTUR) de la Universidad de La Habana. El 79,4 % de los ítems evaluados alcanzaron la calificación más alta de 5 puntos, mientras que el restante 20,6 % obtuvo una calificación alta de 4 puntos, situando a la institución en un nivel de madurez elevado, con un Índice Sintético de Ciberseguridad (ISC) de 4,84 puntos. Sin embargo, el estudio también identifica áreas críticas que necesitan atención prioritaria para alcanzar un nivel óptimo de ciberseguridad.

Principales puntos débiles identificados:

- Entendimiento de las obligaciones:
  - Aunque los trabajadores y profesores están conscientes de las normativas que rigen la seguridad de la información, el conocimiento profundo de las obligaciones contractuales, legislativas y regulatorias es limitado, lo que genera un riesgo significativo de incumplimiento y exposición a sanciones legales.
- Entendimiento de los riesgos de seguridad:
  - La revisión de riesgos se realiza de forma periódica, pero no existe un proceso sistemático y detallado para identificar, evaluar y mitigar los riesgos de seguridad. Esto puede dejar puntos críticos sin protección adecuada frente a amenazas emergentes.
- Responsabilidades:
  - Si bien se han asignado roles y responsabilidades en materia de seguridad de la información, estos no se cumplen en su totalidad. Además, la falta de un especialista dedicado a liderar y coordinar los esfuerzos de ciberseguridad representa una debilidad estratégica.

CONCLUSIONES

El cálculo del Índice Sintético de Ciberseguridad (ISC) permitió evaluar de manera objetiva el estado de la ciberseguridad en la Facultad de Turismo de la Universidad de La Habana, evidenciando tanto sus fortalezas como sus áreas de mejora.

La Facultad de Turismo cuenta con una infraestructura tecnológica adecuada y políticas definidas que sustentan un nivel de ciberseguridad elevado. Además, el compromiso de la alta dirección, el monitoreo de eventos de seguridad y la implementación de contramedidas esenciales fortalecen la protección de los datos e información sensibles.

Es necesario profundizar en el conocimiento de las normativas contractuales, legislativas y regulatorias por parte del personal. Se debe implementar un proceso sistemático para la identificación y gestión de riesgos es crucial para prevenir vulnerabilidades, así como se requiere designar un especialista en ciberseguridad que pueda liderar y supervisar las acciones necesarias para mantener la protección y la resiliencia de la facultad.

El estudio demuestra que mantener un nivel alto de ciberseguridad es esencial para prevenir la pérdida de información sensible y garantizar la continuidad de las operaciones en un entorno digital cada vez más amenazante.

La Facultad de Turismo debe priorizar las acciones correctivas en las áreas identificadas como débiles, reforzando la capacitación, la asignación de recursos y la implementación de medidas sistemáticas para seguir avanzando hacia la excelencia en ciberseguridad. Estas acciones no solo mejorarán su nivel de protección, sino que también servirán como modelo de referencia para otras instituciones académicas en Cuba.

AGRADECIMIENTOS

Se le reconoce de manera especial a cada uno de los colaboradores del grupo focal de la Facultad de Turismo, de la Universidad de La Habana, que proporcionó información valiosa para llevar a cabo la investigación.

REFERENCIAS

Delgado Martorell, S. (2023, diciembre 14). El 85% de las universidades ha sufrido ciberataques en el último año. La Razón. https://www.larazon.es/emergente/85-universidades-sufrido-ciberataques-ultimo-ano_20231214657aa7b029f31800017626e2.html

Ganesan, R., Jajodia, S., Shah, A., y Cam, H. (2016). Dynamic scheduling of cybersecurity analysts for minimizing risk using reinforcement learning. ACM Transactions on Intelligent Systems and Technology (TIST), 8(1): 1-4. https://doi.org/10.1145/2882969

Granma (29 de mayo de 2024). Cuba fortalece su ciberseguridad como una labor prioritaria. https://www.granma.cu/cuba/2024-02-03/cuba-fortalece-su-ciberseguridad-como-una-labor-prioritaria

IT User Teach y Business (2023, noviembre 21). El sector de la enseñanza superior continúa a la cabeza de los ciberataques. https://www.ituser.es/seguridad/2023/11/el-sector-de-la-ensenanza-superior-continua-a-la-cabeza-de-los-ciberataques

Jaiyen, S., y Sornsuwit, P. (2019). A New Incremental Decision Tree Learning for Cyber Security based on ILDA and Mahalanobis Distance. Engineering Journal, 23(5): 71-88. http://dx.doi.org/10.4186/ej.2019.23.5.71

Ministerio de Ciencia, Innovación y Universidades. (2024). El Gobierno lanza 32 cátedras universidad-empresa en Inteligencia Artificial y ciberseguridad que movilizarán cerca de 50 millones de euros. https://www.universidades.gob.es/el-gobierno-lanza-32-catedras-universidad-empresa-en-inteligencia-artificial-y-ciberseguridad-que-movilizaran-cerca-de-50-millones-de-euros/

Nowersztern, A., Paz, S., Kagelmacher, D., Berenfus, F. C., Libedinsky, P., Ribagorda, A., Tapiador, J., Fuentes, J. M. D., y González, L. (2021). Programa formativo en ciberseguridad para América Latina y el Caribe. IDB Publications. https://doi.org/10.18235/0003659

Ramírez Montealegre, B. J. (2016). Medición de madurez de ciberseguridad en pymes colombianas, Tesis Doctoral, Universidad Nacional de Colombia. https://repositorio.unal.edu.co/handle/unal/57956

Sánchez, Y., Barrera, D., y Reyes, Y. (2022). Metodología para la gestión de ciberincidentes en las universidades cubanas. Revista Cubana de Ciencias Informáticas, 16(4): 101-113. http://scielo.sld.cu/pdf/rcci/v16n4/2227-1899-rcci-16-04-101.pdf

Torres, C., Joshua, D., Mata, P., y Joel, A. (2024). Evaluación de las buenas prácticas de ciberseguridad en los estudiantes universitarios: un estudio en la Universidad Politécnica Salesiana sede Guayaquil, Tesis de grado, Universidad Politécnica Salesiana. http://dspace.ups.edu.ec/handle/123456789/27867

Universidad de León (2024). Máster Universitario en Investigación en Ciberseguridad (online). https://www.unileon.es/estudiantes/oferta-academica/masteres/mu-investigacion-ciberseguridad-online

Universidad Rey Juan Carlos (2024). Ingeniería de la ciberseguridad. https://www.urjc.es/estudios/3100-ingenieria-de-la-ciberseguridad

Valencia, A., Bermeo, M. C., Acevedo, Y., Garcés, L. F., Quiroz, J., Benjumea, M. L., y Patiño, J. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. Revista Ibérica de Sistemas y

Tecnologías de la Información (Risti), 225-239. https://www.proquest.com/openview/a2803956d6c8a33be891343ca536dde9/1?pq-origsite=gscholar&cbl=1006393

Venter, I. M., Blignaut, R. J., Renaud, K., y Venter, M. A. (2019). Cyber security education is as essential as "the three R's". Heliyon, 5(12): 1-8. https://doi.org/10.1016/j.heliyon.2019.e02855

Von Solms, R., y Van Niekerk, J. (2013). From information security to cyber security. Computers y Security, 38: 97-102. https://doi.org/10.1016/j.cose.2013.04.004