

Seguridad informática en la nube: percepción de los estudiantes de las carreras
de Bibliotecología de la Universidad de Costa Rica

Cloud security: perception of Library Science students at the University of Costa
Rica

Ginnette Guillén-Jiménez¹
Valeria Calvo-Chaves²

RESUMO

O presente artigo apresenta os resultados da pesquisa realizada sobre o conhecimento da segurança informática em nuvem por parte dos estudantes de ambos os bacharelados, tanto em Bibliotecas Educativas quanto em Ciências da Informação, da Escola de Biblioteconomia e Ciências da Informação da Universidade da Costa Rica, matriculados no I ciclo de 2024. Tratou-se de uma pesquisa de tipo exploratório e de abordagem mista, cuja população foi composta pelos estudantes da EBCI matriculados no bacharelado durante o I ciclo de 2024. Aplicou-se um questionário à população do estudo, que revelou que os estudantes pesquisados se encontram em nível avançado do bacharelado. Além disso, evidenciou-se a relação entre a ênfase do bacharelado cursado pelo estudante e seu conhecimento em segurança informática em nuvem. Ressalta-se a importância de integrar a segurança informática em nuvem no plano de estudos dos programas de bacharelado da escola.

Palavras-chave: proteção de dados; informática documental; indústria da informática; bibliotecas digitais.

RESUMEN

El presente artículo da a conocer los resultados de la investigación realizada sobre el conocimiento de la seguridad informática en la nube por parte de los estudiantes de ambos bachilleratos, tanto Bibliotecas Educativas como Ciencias de la Información, en la Escuela de Bibliotecología y Ciencias de la Información de la Universidad de Costa Rica matriculados en el I ciclo de 2024. Fue una investigación de tipo exploratoria de corte mixto, cuya población fueron los estudiantes de la EBCI matriculados en el bachillerato durante el I ciclo del 2024. Se aplicó un cuestionario a la población de estudio, que dió a conocer que los estudiantes encuestados se encuentran en un nivel avanzado del bachillerato, además se evidenció la relación entre el énfasis del bachillerato que cursa el estudiante y su conocimiento en seguridad informática en la nube. Se resalta la importancia de integrar la seguridad informática en la nube en el plan de estudios de los programas de bachilleratos de la escuela.

¹ Máster en Gerencia de Proyectos de Desarrollo por la Universidad de Costa Rica. ORCID: <https://orcid.org/0000-0001-5389-6195>. Correo electrónico: ginnette.guillen@ucr.ac.cr.

² Máster en Gerencia de Proyectos de Desarrollo por la Universidad de Costa Rica. Correo electrónico: valeria.calvochaves@ucr.ac.cr.



Palabras clave: protección de datos; informática documental; industria informática; bibliotecas digitales.

ABSTRACT

This article presents the results of research conducted on the knowledge of cloud information security among students from both Educational Libraries and Information Sciences bachelor's programs at the School of Library Science and Information Science of the University of Costa Rica, enrolled in the first semester of 2024. The research employed a mixed-method exploratory approach, focusing on the students enrolled in the bachelor's programs at the School of Library Science and Information Science at UCR during the first semester of 2024. A self-administered questionnaire was distributed to the study population. The results revealed that the surveyed students are at an advanced level in their bachelor's studies and demonstrated a relationship between the emphasis of the student's program and their knowledge of cloud information security. The importance of integrating cloud information security into the curriculum of the bachelor's programs at the EBCI.

Keywords: data protection; document management; IT industry; digital libraries.

Submetido em: 24 abr. 2025.

Aprovado em: 23 jul. 2025.

1 INTRODUCCIÓN

La seguridad informática en la nube es un tema que a través del tiempo ha tomado importancia dentro de los diferentes tipos de organizaciones, tanto públicas como privadas, de ahí que sea necesario que quienes se encuentren en las diferentes áreas que se ligan de una forma u otra a la tecnología requieran contar con nociones fuertes sobre las herramientas que se gestionan en la nube, así como la seguridad informática en ella.

En el campo de la bibliotecología, la nube se ha convertido en una herramienta clave para bibliotecas, centros de documentación y unidades de información, independientemente de su naturaleza. Estas instituciones la utilizan para ofrecer diversos servicios a su comunidad de usuarios, como el almacenamiento de archivos digitales, la difusión de servicios digitales, o proyectos masivos como el caso del proyecto colaborativo entre OCLC, *HathiTrust*, la Biblioteca de la Universidad de Nueva York y el consorcio RECAUDA, denominado “*CLOUD LIBRARY*”. Según Balagué (2011), este proyecto tenía como objetivo estudiar si la aparición de colecciones masivas de documentos digitalizados y su vinculación con almacenes



cooperativos de documentos impresos modificaría el modelo de negocio de las bibliotecas especializadas.

Por otro lado, Morales (2012) señala que la computación en la nube corresponde a un modelo que permite sentar las bases sobre la demanda de acceso a los datos, lo cual podría impactar a las bibliotecas y por ende a sus funcionarios. Pasqui (2010), señala que las unidades de información inevitablemente están cada vez más ligadas a la tecnología y por ende a su avance donde podrían ofrecer múltiples servicios en la red, como lo es el caso de los repositorios institucionales, bibliotecas digitales, entre otros.

De lo anterior es posible inferir que si la nube es utilizada por profesionales de la información, estos requieren conocer sobre la seguridad informática en la nube, para de esta manera desenvolverse adecuadamente dentro del entorno laboral, tal y cómo lo señala Morales (2012) cuando menciona que los estudiantes y profesionales de las carreras de bibliotecología deben de adquirir los conocimientos técnicos requeridos a nivel de funcionamiento y seguridad con el fin de desarrollarse en las oportunidades que presenta la nube para estas unidades de información.

Por lo tanto, es posible evidenciar que los servicios que se pueden brindar en la nube y ser aprovechados por el área de la bibliotecología es un tema que se ha estudiado con anterioridad y que no es ajeno a la profesión.

De acuerdo a Cabral Vargas (2018) la tendencia en los últimos años es la transición de los centros educativos universitarios hacia las herramientas digitales, es decir hacia las tecnologías de la información, como base para las actividades de investigación y educativas. Es decir, en los últimos años los centros educativos se han inclinado por las herramientas que ofrecen las tecnologías de información para continuar avanzando en materia educativa, esto incluye los servicios que se dan en las mismas contemplando a las bibliotecas y lo que en ellas se ofrece.

En ese sentido, realizar este estudio resulta importante ya que como lo han señalado Morales y Cabral Vargas en sus investigaciones, el crecimiento del uso de las herramientas en la nube ha sido exponencial, además, la implementación generalizada de servicios en la nube ha cambiado la manera en que se almacena, accede y comparte la información, imponiendo nuevos retos en términos de protección y gestión de datos sensibles así como la importancia de los mismos.

Por lo anterior, este estudio tiene como propósito analizar la percepción y el nivel de conocimiento sobre la seguridad informática en la nube entre estudiantes de los bachilleratos en Bibliotecología de la Universidad de Costa Rica (EBCI), matriculados en el I ciclo de 2024, considerando tanto el año de carrera como el énfasis cursado. Asimismo, busca identificar la formación recibida en esta materia, documentar el uso que hacen de los servicios en la nube y las medidas de seguridad que adoptan, así como explorar posibles diferencias entre perfiles académicos. Los hallazgos permitirán proponer recomendaciones para fortalecer la inclusión de contenidos sobre seguridad en la nube en el plan de estudios y para mejorar la difusión de las políticas institucionales sobre el manejo seguro de la información.

Finalmente, el artículo se organiza en cuatro apartados: el primero presenta el marco teórico, el segundo describe la metodología, el tercero expone y analiza los resultados, y el cuarto plantea las conclusiones y recomendaciones.

2 MARCO TEÓRICO

El presente apartado ofrece los fundamentos conceptuales y antecedentes que sustentan la investigación. En este apartado se definen los principales términos relacionados con la computación en la nube y la seguridad informática, incluyendo nociones sobre la nube, el software, los servidores e internet, así como las prácticas y amenazas más comunes. Además, se presenta un repaso de estudios previos que abordan la relación entre la bibliotecología y el uso de la nube, identificando beneficios, retos y medidas de protección. Este sustento teórico permite comprender la relevancia del tema y proporciona el contexto necesario para interpretar los resultados obtenidos en el estudio.

2.1 La nube

De acuerdo con Microsoft (2024a) la nube es un término utilizado para describir una red mundial de servidores, donde cada uno tiene una función única. La nube no es una entidad física, sino una red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema, en otras palabras la nube es una metáfora, que se utiliza para describir la computación que se da por medio del internet a gran escala. La nube ofrece una serie de ventajas para el almacenamiento, la ejecución y el desarrollo de datos ya que en lugar de contar con

grandes cantidades de dispositivos y de *softwares* individualmente, esta permite acceder a los programas, archivos, documentos, entre otros, de forma remota.

De este modo, es posible comprender que la nube, entre muchas de sus ventajas, cuenta con un alto grado de flexibilidad, escalabilidad, eficiencia, fiabilidad y seguridad, este último concepto será tratado más adelante.

2.2 Software

Para comprender la información detallada en esta investigación, es importante definir qué es un *software*. Gómez Palomo y Moraleda Gil (2020) señalan que el *software* abarca no solo los programas que controlan el funcionamiento del sistema, sino también otros elementos como documentos, bases de datos y aspectos inmateriales, tales como los procedimientos de operación y mantenimiento. Es decir, incluye tanto componentes tangibles como intangibles, y funciona en conjunto con el *hardware*. Además, en el contexto actual, el acceso a programas a través de la nube, como es el caso de la suite Office 365, permite utilizarlos sin necesidad de instalación local en la computadora.

2.3 Servidor

Ahora bien, como ya se mencionó, la nube es una serie de servidores interconectados en la red o internet donde cada uno tiene una función específica, de ahí que sea importante definir en lo que consiste un servidor. Según López Cuevas y Miramontes Carpena (2024), los servidores son un equipo informático que está integrado en una red y ofrece servicios a otras computadoras clientes o usuarios. En esencia, se trata de una máquina de gran potencia que guarda los archivos necesarios para que diferentes sitios web sean accesibles en internet. Sin embargo, los servidores pueden referirse tanto al aparato físico como al *software* y su configuración varía según las necesidades del cliente o usuario.

Para efectos de esta investigación se tomará el servidor en red como concepto fundamental, dado que el estudio se centra en la seguridad informática en la nube y en los servidores donde opera.

2.4 Internet

Por otra parte, es esencial comprender el entorno en el que opera la nube. Uno de los elementos clave de este entorno es internet, que sirve como base para el funcionamiento de la nube y otros servicios en línea. Según lo expone Sevilla (2020), es una red masiva de redes, infraestructura de redes que conecta a millones de computadoras unidas de forma global.

Esos servidores que funcionan conectados entre ellos y que operan de acuerdo a las necesidades de los clientes y usuarios para conectarse entre sí, requieren de protocolos los cuales son de diversos tipos. Algunos de ellos son: transporte, almacenamiento y seguridad. A grandes rasgos, de acuerdo a lo descrito por SaludData (2023) un protocolo, desde el enfoque informático, es un conjunto de reglas que establece cómo deben interactuar los diferentes dispositivos en una red. Estas normas son fundamentales para asegurar una comunicación efectiva y sin inconvenientes, sin importar la ubicación espacial de los dispositivos.

Como se mencionó anteriormente, la nube permite a los usuarios acceder a diversos sistemas, *software* y suites ofimáticas desde cualquier ubicación y dispositivo. Este acceso se realiza mediante credenciales de usuario, es decir, cada persona cuenta con un ID y una contraseña únicos que le permiten ingresar a sus datos y servicios en la nube. Sin embargo, es posible que los datos corran peligro si no se cuenta con buenas prácticas de seguridad informática como lo son:

- a) El uso de contraseñas seguras. Microsoft (2024b) las define como las contraseñas que son largas con generalmente de 12 a más dígitos que incluyen letras mayúsculas, minúsculas, números y caracteres especiales;
- b) La verificación en dos pasos. De acuerdo a Google (2024a) es un método de identificación y autenticación que agrega un nivel de protección a sus datos en caso de que otro usuario quisiera acceder a sus cuentas por un robo de contraseña.

Aunque la nube ofrece comodidad y accesibilidad, la seguridad sigue siendo una prioridad. Las buenas prácticas mencionadas son esenciales para prevenir ataques y proteger la información personal y profesional de los usuarios en la nube.

El robo de contraseñas puede darse por diferentes motivos, una de ellas es el *phishing*, el cual de acuerdo a lo detallado por Medina Martínez, Cárdenas Osorio e Mejía Lobo (2021, p. 76) “se puede definir como un método usado para sustraer información y obtener beneficios económicos a partir de ello”. Esta modalidad de fraude es una de las más antiguas y recurrentes.

Por otro lado, para mantener la seguridad informática en la nube es necesario revisar la configuración de la privacidad en las cuentas que se albergan en ella para controlar quién o quiénes pueden acceder a la información y archivos. De acuerdo con Google (2024b) estos parámetros son de fácil uso y permite brindar a los usuarios transparencia en el uso y manejo de sus datos.

Además, es fundamental mantener actualizados tanto el *software* como las aplicaciones utilizadas para acceder a los servicios en la nube, ya que estas actualizaciones ayudan a prevenir la pérdida de datos al corregir las vulnerabilidades presentes en versiones anteriores o no actualizadas. Google (2024c) señala que es importante revisar el historial de actividad de la cuenta, con el fin de detectar cualquier actividad poco usual o no autorizada.

Por otra parte, es necesario realizar copia de seguridad de los datos que se almacenan en la nube, pues según Martínez (2019) las organizaciones tienen posibilidades de caer en riesgos cibernéticos, que son sucesos digitales causados por personas internas o externas a la organización. Entre los eventos destacados se encuentran el robo y la pérdida de información crucial para la organización, así como la pausa de funciones. Este tipo de riesgo se clasifica como un riesgo tecnológico y se incluye dentro del riesgo operacional de una organización. Por eso, las copias de seguridad son una medida de seguridad y protección de los datos utilizada a modo de prevención en caso de cualquier fallo, natural, humano o de seguridad.

Finalmente, la medida de seguridad informática en la nube que es altamente recomendada de acuerdo a Google, (2024c), es cerrar las sesiones de trabajo en dispositivos ajenos, ya que de esa forma nadie podrá iniciar sesión en las cuentas ni vulnerar los datos.

Como se ha demostrado a lo largo de este apartado, esta investigación aborda aspectos clave de la seguridad informática en la nube, destacando temas generales pero esenciales para cualquier futuro profesional que trabaje en un mundo cada vez más globalizado.

3 MARCO METODOLÓGICO

En este apartado se describe el enfoque metodológico adoptado para el desarrollo del estudio, el cual combina técnicas cualitativas y cuantitativas con un carácter exploratorio. Se detalla la población y la muestra seleccionada, el instrumento de recolección de datos utilizado, así como los procedimientos aplicados para garantizar la validez y confiabilidad de la información. Esta sección permite comprender cómo se estructuró la investigación y las razones por las cuales se eligió la metodología empleada.

3.1 Enfoque de la investigación

La investigación es de carácter exploratorio, que de acuerdo con Sampieri (2019) son aquellos que se realizan cuando el objetivo del estudio es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes con mayor amplitud.

Además, es de enfoque mixto ya que de acuerdo a Sampieri (2019), este tipo de investigación es la que mezcla métodos cualitativos y cuantitativos con el objetivo de contar con un panorama más amplio del fenómeno. En el caso particular de esta investigación se utilizaron métodos cuantitativos para recolección de datos como lo es el formulario y cualitativos como la revisión bibliográfica.

3.2 Población y muestra

La población objetivo de este estudio está compuesta por los estudiantes de la Escuela de Bibliotecología y Ciencias de la Información de la Universidad de Costa Rica, matriculados en el programa de bachillerato durante el primer ciclo de 2024, sumando un total de 400 estudiantes. Utilizando una fórmula de muestra probabilística con un margen de error del 5% y un nivel de confianza del 95%, se determinó que la muestra adecuada para el estudio sería de 62 estudiantes. Este enfoque se implementó para minimizar el margen de error y maximizar el nivel de confianza en los resultados obtenidos. A continuación, se detallan los cálculos y el procedimiento utilizado.

$$n = \frac{N \cdot Z^2 \cdot a/2 \cdot p \cdot q}{e^2(N-1) + Z^2 \cdot a/2 \cdot p \cdot q} \quad (1)$$

N = población

Z^2_{α} = estadístico para $\alpha = 95\% = 1.96$

e = error = $5\% = 0,05$

p = 0.5

q = 0.5

$$n = \frac{400 \cdot (196)^2 \cdot 0,5 \cdot 0,5}{(0,10)^2(400-1) + (196)^2 \cdot 0,5 \cdot 0,5} = 62 \quad (2)$$

3.3 Instrumentos

Para realizar esta investigación se utilizó el cuestionario autoadministrado, el cual consiste en una serie de preguntas abiertas y cerradas. El mismo se facilitó a los y las estudiantes por medio de correo electrónico y grupos de *whatsapp* y se configuró en línea como un formulario de Google; se buscó evaluar el nivel de conocimiento de los estudiantes sobre seguridad informática en la nube.

Por otro lado se hizo revisión bibliográfica con el fin de establecer los diferentes conceptos que se necesitan comprender y practicar por parte de los estudiantes de bibliotecología en materia de seguridad informática en la nube.

4 RESULTADOS

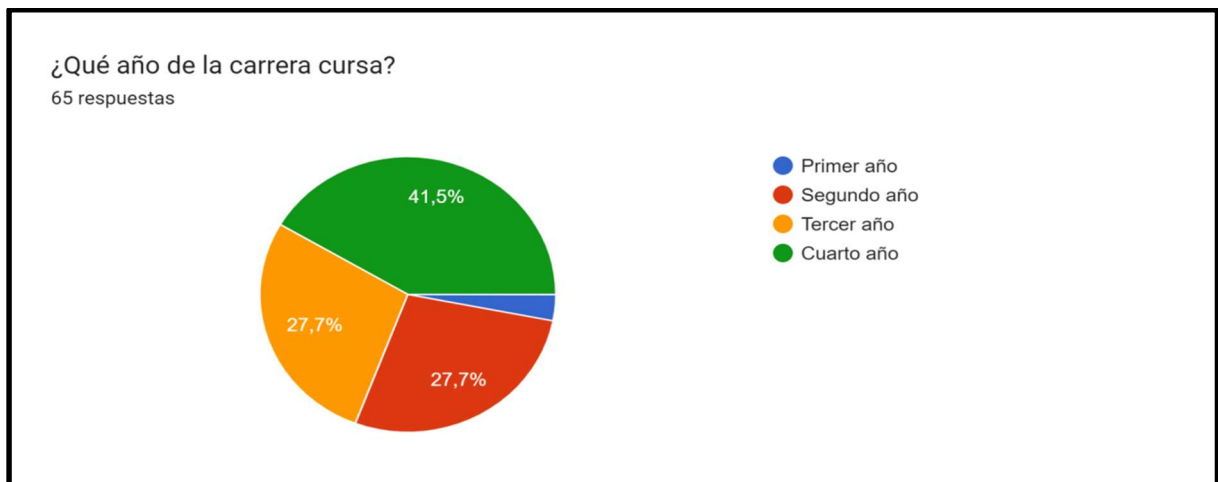
El presente apartado presenta los hallazgos derivados del análisis de los datos recopilados mediante el cuestionario autoadministrado y la revisión bibliográfica. Se incluyen tanto los resultados cuantitativos, representados en gráficos y tablas, como las tendencias cualitativas identificadas a partir de las respuestas abiertas. Los hallazgos se organizan en función de las variables de interés, como el año y énfasis de carrera, el nivel de formación recibida en seguridad en la nube, el uso de servicios y las prácticas de protección adoptadas por el estudiantado.

Los datos recopilados a través del cuestionario autoadministrado y la revisión bibliográfica fueron sometidos a un análisis exhaustivo que combinó técnicas estadísticas descriptivas con un enfoque de análisis temático de los datos cualitativos. Este análisis permitió una comprensión profunda del nivel de conocimiento de los estudiantes de bibliotecología y ciencias de la información sobre seguridad informática

en la nube. Para los datos cuantitativos, se emplearon herramientas estadísticas para examinar la distribución de respuestas y explorar posibles correlaciones entre variables. Por otro lado, los datos cualitativos se sometieron a una codificación y análisis temático para identificar patrones emergentes y temas significativos. La integración de estos enfoques permitió una interpretación completa de los resultados.

El cuestionario aplicado contó con una totalidad de 10 preguntas relacionadas a la seguridad informática en la nube, se obtuvo respuesta de 65 estudiantes que cursan los años de los bachilleratos de las carreras de bibliotecología en ambos énfasis, en donde mayoritariamente cursan el cuarto año de la carrera, tal y como se observa en el gráfico 1. De la población en estudio, el 3,1 % son de primer ingreso, el 27,7 % de segundo año; 27,7 % de tercero y 41,5 % de último año de bachillerato.

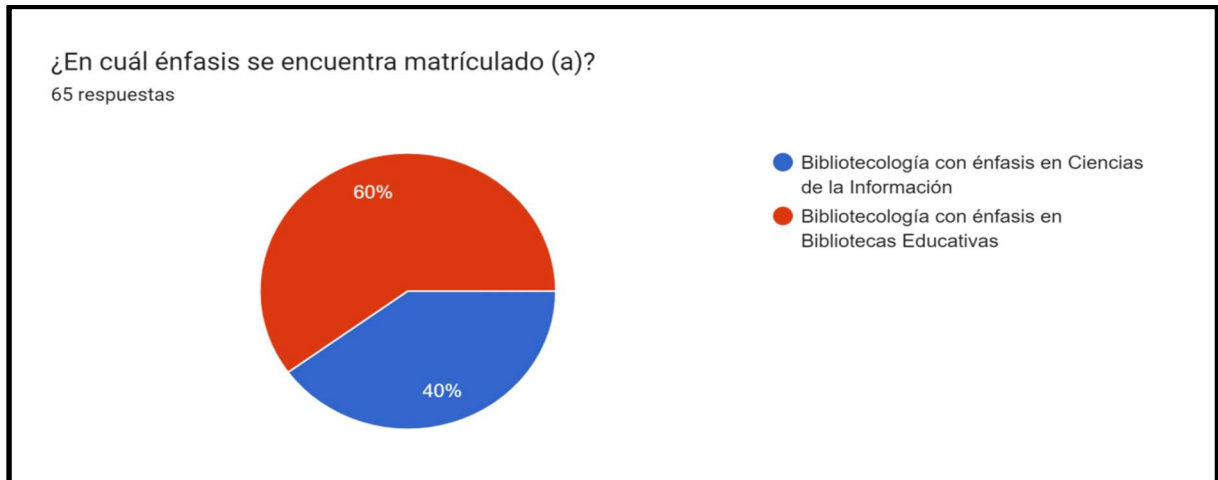
Gráfico 1 – Años de estudio universitario de la muestra encuestada



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

En relación con el énfasis en el que se encontraba matriculada la muestra se obtuvieron 65 respuestas de las cuales un 60 % se encontraba matriculado en el énfasis en Bibliotecas Educativas. Esta respuesta indica que la mayoría de la muestra estaba matriculada en un énfasis que, por su naturaleza, no aborda en profundidad las temáticas relacionadas con la informática. Por otra parte, el bachillerato en Ciencias de la Información, como se indica en la malla curricular que deben completar los y las estudiantes, se incluyen cursos como Estructura de bases de datos y Redes y sistemas de información. En estos cursos, el personal docente hace abordajes sobre la seguridad informática en los servicios en la nube.

Gráfico 2 – Distribución de énfasis de matrícula entre encuestados



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Por otra parte, cuando se preguntó al estudiantado sobre ¿Qué entiende por seguridad informática en la nube y cuál cree que es su importancia en el ámbito de la bibliotecología y ciencias de la información?, la mayor parte de ellos respondieron que la seguridad informática en la nube se relaciona con la protección y almacenamiento de datos y que la misma se relaciona con la carrera de bibliotecología desde el almacenamiento de los mismos y dar la seguridad a estos datos. Aunque no todos los encuestados responden al énfasis más relacionado a la tecnología, los estudiantes tienen, sin importar su énfasis, nociones básicas de qué es la seguridad informática en la nube y sus objetivos. En la tabla 1 se muestran algunas de las respuestas de la población estudiantil, se establecieron 7 categorías en las que se dividieron los comentarios obtenidos de la pregunta 2 del formulario.

Tabla 1 – Comprensión sobre la seguridad informática en la nube y su importancia en la bibliotecología

Categorías de respuesta	Ejemplos textuales de las respuestas obtenidas
Definición general de seguridad informática en la nube	"Es una disciplina que asegura la información." "La seguridad informática en la nube es la protección de archivos y datos." "Es una forma de guardar y almacenar datos en un lugar aparte."
Importancia en Bibliotecología y Ciencias de la Información	"Es importante en el ámbito de la bibliotecología porque permite almacenar y proteger todo tipo de recurso informativo." "En Bibliotecología es importante para la gestión de la información digital." "En bibliotecología es importante por la adopción de tecnologías basadas en la nube para gestionar grandes cantidades de datos digitales."
Ventajas del almacenamiento en la nube	"Guardar información y poder accederla en cualquier lugar." "Toda la información debe quedar almacenada en un lugar seguro." "Entiendo que los documentos siempre van a estar resguardados en la nube, por si se daña el dispositivo en el cual los tenemos."
Confidencialidad y privacidad de los usuarios	"Garantiza que la información sobre los usuarios se mantenga a salvo." "Proteger la privacidad de los usuarios, mantener la integridad y disponibilidad de la información en todo momento." "Que no ingresen terceros a la nube personal."
Medidas, herramientas y mecanismos de seguridad	"Un muro de contingencia basado en código para identificar archivos maliciosos o entradas sin permiso." "Conjunto de barreras de protección al que solo el usuario dueño del perfil puede tener acceso." "Un REcaptcha que se encarga de proteger la nube de supercomputadoras que prueban combinaciones de contraseñas."
Percepción de riesgos, responsabilidades y respaldo	"Es importante porque al no ser archivos físicos, cuando se sube a una nube lo que se espera es que se guarden ahí para no almacenarlos dentro de la computadora." "En una época en la que cada vez se utilizan más los medios digitales, es necesario tener todas las medidas de seguridad posibles en caso de cualquier eventualidad." "Permite respaldar documentos importantes y tener un entorno de trabajo más seguro con los compañeros."
Opiniones personales y analogías prácticas	"Imagino que tiene que ver con proteger la información que se sube en nubes como Google Drive para evitar el robo de información." "En mi experiencia, para una empresa que no se filtre información sensible o de investigación o de fórmulas de construcción de productos." "Es como una disciplina que se encarga de resguardar los datos que se almacenan en las nubes."

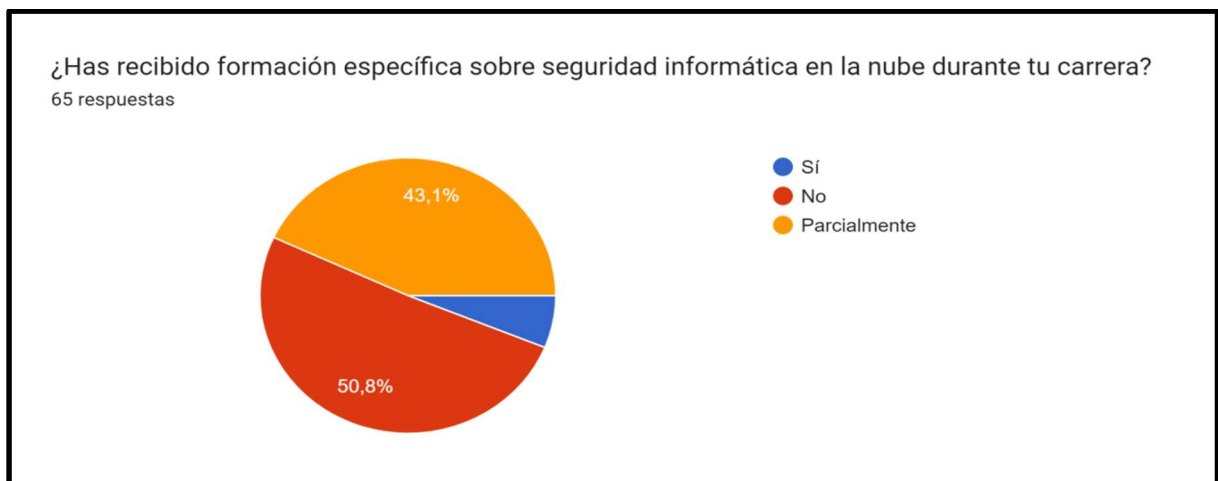
Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Se puede observar que a pesar de haber sido una pregunta concreta sobre la comprensión de la seguridad informática y su importancia en el área de la

bibliotecología, además los y las estudiantes dieron respuestas sobre las ventajas que brindan, mencionaron datos sobre la confidencialidad y privacidad que ofrece a los usuarios; indicaron medidas, herramientas y mecanismos de seguridad, entre otros comentarios personales. Pero se puede apreciar, que todos muy oportunos y acertados sobre la temática que se aborda en el estudio.

Sin embargo, aunque tienen conocimientos básicos, la mitad de la muestra indica que durante su carrera ha recibido nula formación sobre la seguridad informática en la nube, tal como se expone en el gráfico 3. Sin embargo, existe un 43,1 % que indica que parcialmente han recibido, lo cual coincide con el 40 % de los estudiantes que pertenecen al énfasis de ciencias de la información; lo anterior quiere decir que estos estudiantes tienen mayor familiarización con la temática ya que dentro de sus cursos han recibido formación de este tipo aunque sea de una forma parcial.

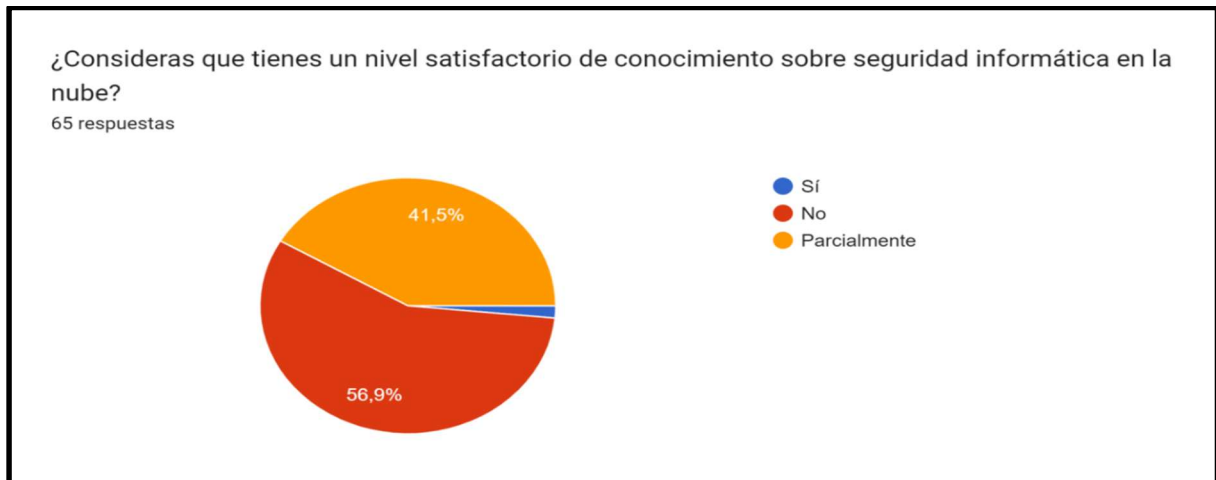
Gráfico 3 – Formación en Seguridad Informática en la Nube durante la carrera



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Por otro lado, este mismo fenómeno se repitió al consultar a la muestra sobre si considera que cuenta con un nivel satisfactorio de conocimiento sobre seguridad informática en la nube, tal y como se observa en el gráfico 4.

Gráfico 4 – Percepción del nivel de conocimiento en Seguridad Informática en la Nube



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Tomando en cuenta que existen básicamente las mismas proporciones en relación con el énfasis de la carrera que cursan los estudiantes encuestados, es posible que exista una relación directa entre el énfasis de ciencias de la información y el conocimiento en materia de seguridad informática en la nube y los conocimientos adquiridos en el plazo de su carrera.

Por otro lado, aunque no todos los encuestados cuentan con conocimientos sobre seguridad informática en la nube, el 72 % confirma utilizar servicios alojados en la nube regularmente y un 20 % afirma utilizarlos ocasionalmente. Esto refleja que usan los servicios y que por ende, es necesario que cuenten con dichos conocimientos.

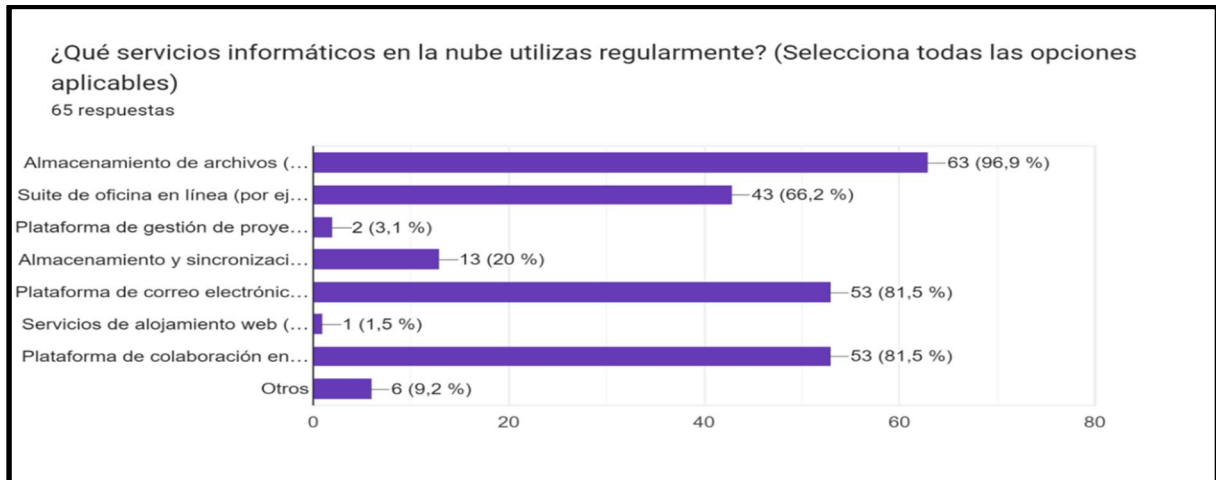
Gráfico 5 – Uso de servicios en la nube para almacenamiento y acceso a información académica



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Además, se determina que la mayoría de los encuestados utilizan servicios informáticos en la nube, siendo las funciones de almacenamiento de archivos, sincronización y colaboración en documentos las más frecuentes, tal como se evidencia en el gráfico 6. Estos hallazgos coinciden con lo señalado por una encuesta de *GoodFirms* de aproximadamente 600 usuarios globales de servicios en la nube: el 94 % utilizó *Google Drive*, el 64 % utilizó *Dropbox*, el 39 % utilizó *OneDrive*, y el 38 % utilizó *iCloud* (Howarth, 2024). Cifras que también son corroboradas por un análisis en *Cloudwards* (2025) que reporta el 94.44 % para *Google Drive*, 66.20 % para *Dropbox*, 39 % para *OneDrive* y 38 % para *iCloud*.

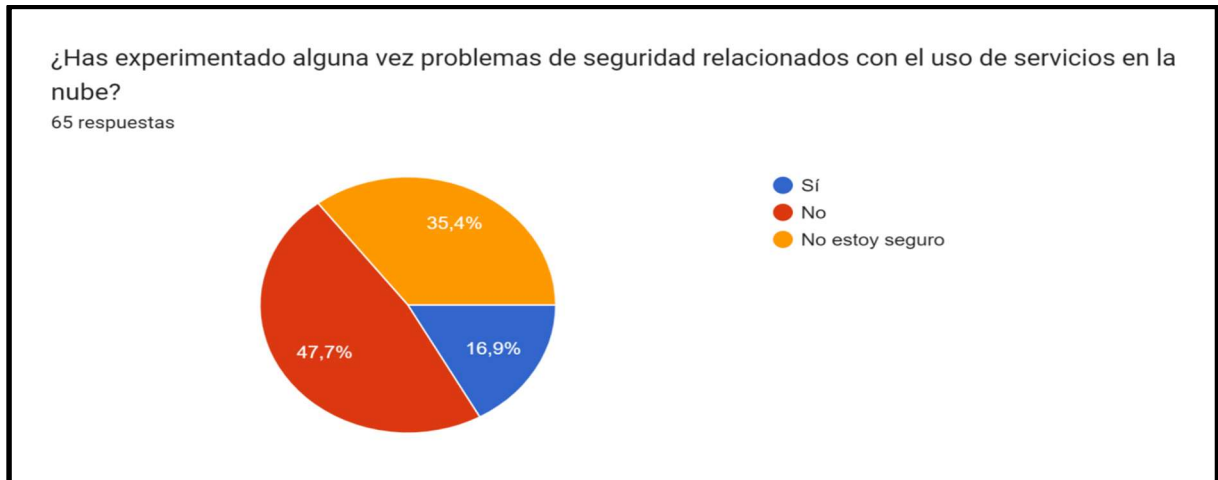
Gráfico 6 – Servicios en la nube utilizados regularmente



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Por otra parte, al consultar a los participantes sobre si han enfrentado problemas relacionados con el uso de los servicios en la nube en materia de seguridad, el 47,7 % respondió que no, un 35,4 % indicó que no está segura, y un 16,9 % afirmó que sí ha tenido inconvenientes, tal como se observa en el Gráfico 7. Esta tendencia resulta consistente con lo reportado por Omoshalewa (2025), quien, en un estudio similar, encontró que el 31,8 % de los encuestados reconoció haber experimentado incidentes de seguridad vinculados al uso de servicios de almacenamiento en la nube durante el año anterior. Lo anterior evidencia que, si bien una proporción importante de usuarios no identifica directamente problemas de seguridad, estos sí se presentan con relativa frecuencia en contextos de uso generalizado.

Gráfico 7 – Experiencia con problemas de seguridad en servicios en la nube

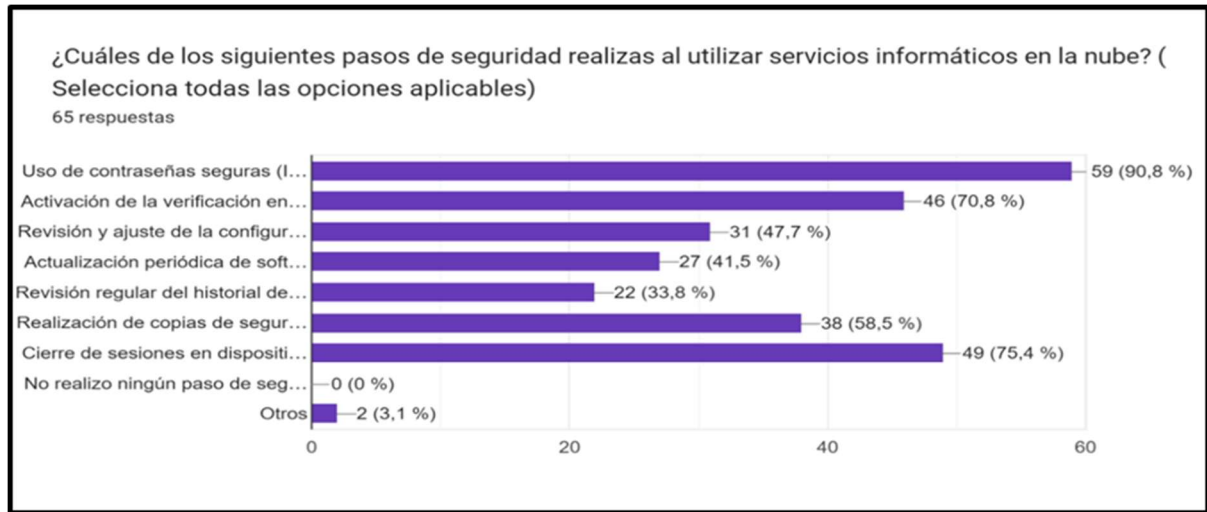


Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

En el Gráfico 8, se detallan las prácticas de seguridad digital adoptadas por los encuestados al utilizar servicios informáticos en la nube. Para ésta pregunta se presentó una lista de 8 opciones para que las personas seleccionaran las más utilizadas. Se incluyó el uso de contraseñas seguras, la activación de la verificación en dos pasos, revisión y ajuste de la configuración de privacidad; actualización periódica de software y aplicaciones, revisión regular del historial de actividad de la cuenta; realización de copias de seguridad de los datos almacenados y cierre de sesiones en dispositivos ajenos.

Entre estas destacan el uso de contraseñas seguras, la verificación en dos pasos y el cierre de sesión en dispositivos ajenos. Tales acciones contribuyen a que sus cuentas y la información almacenada no sean vulneradas, lo cual explica la baja incidencia de experiencias negativas reportadas en términos de seguridad.

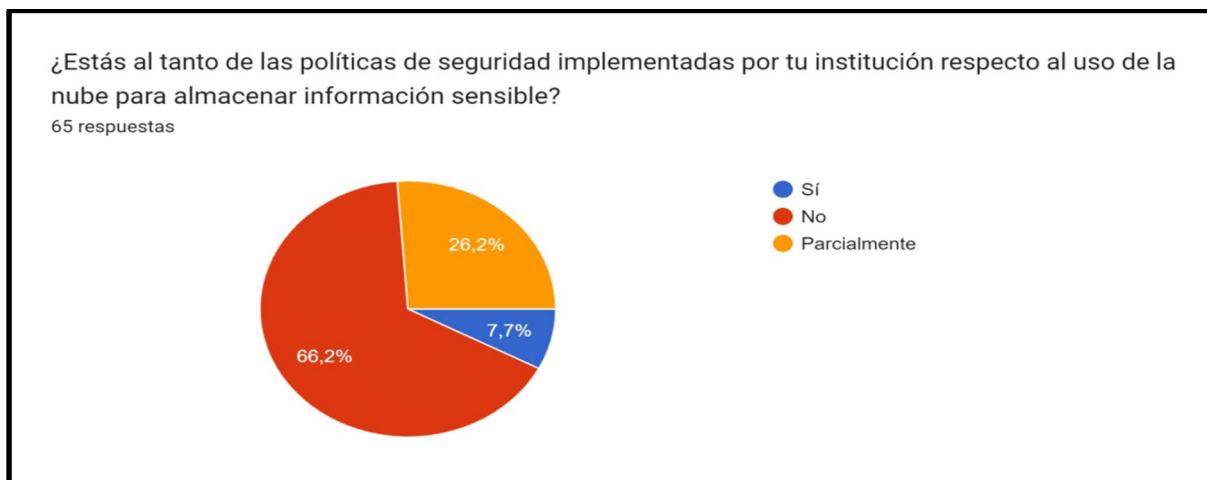
Gráfico 8 – Seguridad al utilizar servicios en la nube



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

Finalmente, al preguntar a los encuestados sobre su conocimiento en políticas de seguridad implementadas por la universidad sobre el uso de la nube para almacenar información sensible, el 66,2% indica no conocerla, según lo evidenciado en el gráfico 9. Sin embargo, el principal factor podría radicar en la falta de difusión de este tipo de información o bien que los estudiantes no revisan sus correos electrónicos ni los medios oficiales. La Unidad de Riesgos y Seguridad del Centro de Informática de la Universidad de Costa Rica (2022), especificó en su página web las recomendaciones de seguridad necesarias para el uso de los servicios informáticos en la nube, dicha página se encuentra disponible para el público en general y especializado. Esto refleja que la casa de enseñanza sí ha tenido iniciativas y las ha divulgado en la comunidad universitaria.

Gráfico 9 – Nivel de conciencia sobre políticas de seguridad en la nube



Fuente: elaboración propia a partir de las respuestas del cuestionario autoadministrado Apéndice A (2024).

5 CONSIDERACIONES FINALES

Este apartado aborda y sintetizan los principales hallazgos de la investigación, destacando las relaciones encontradas entre el perfil académico del estudiantado y su conocimiento en seguridad informática en la nube. Se identifican las áreas de fortaleza y las brechas de formación, así como las oportunidades para mejorar la enseñanza y la difusión de políticas institucionales relacionadas con la seguridad digital. Asimismo, se plantean recomendaciones que buscan fortalecer las competencias del estudiantado y garantizar un uso seguro y responsable de los servicios en la nube en el ámbito bibliotecario.

Los datos muestran que la mayoría de los encuestados se encontraban en el cuarto año de su carrera, lo que sugiere que representan un grupo significativo de estudiantes avanzados en su formación académica. Además, se observa que la mayoría estaban matriculados en el énfasis en Bibliotecas Educativas, lo que indica una mayor concentración en áreas no directamente relacionadas con la tecnología de la información.

A pesar de esto, los resultados muestran que la mayoría de los estudiantes tienen nociones básicas sobre seguridad informática en la nube, aunque la formación específica en este tema durante su carrera es limitada. Sin embargo, se observa una correlación entre aquellos estudiantes que pertenecen al énfasis más asociado a la tecnología y la recepción parcial de formación en seguridad informática en la nube.

Esto sugiere que los programas de estudio pueden influir en el nivel de conocimiento sobre esta materia.

Es interesante destacar que a pesar de la falta de formación específica, la gran mayoría de los encuestados utiliza regularmente servicios en la nube para almacenar y acceder a información académica. Esto plantea la necesidad de que los estudiantes adquieran conocimientos sobre seguridad informática en la nube para proteger adecuadamente sus datos y la información sensible.

Aunque la mayoría de los encuestados no informa haber enfrentado problemas de seguridad relacionados con el uso de servicios en la nube, la implementación de prácticas de seguridad como el uso de contraseñas seguras y la verificación en dos pasos sugiere una preocupación por mantener la seguridad de sus cuentas en la nube. Esto puede explicar en parte la baja incidencia de problemas de seguridad reportados.

Sin embargo, los resultados también muestran una falta de conciencia sobre las políticas de seguridad implementadas por la universidad en relación con el uso de la nube para almacenar información sensible. Esta falta de conocimiento puede deberse a una falta de difusión de esta información por parte de la institución o a una falta de atención por parte de los estudiantes a los canales de comunicación oficiales.

Para finalizar, los resultados destacan la importancia de integrar la seguridad informática en la nube en el plan de estudios de los programas de bibliotecología y ciencias de la información, especialmente para aquellos estudiantes que no se centran en áreas relacionadas con la tecnología. Además, subrayan la necesidad de aumentar la conciencia sobre las políticas de seguridad entre los estudiantes para garantizar una mejor protección de la información sensible.

REFERENCIAS

BALAGUÉ, S. Cloud-computing en las bibliotecas: los servicios bibliotecarios en nube podrían optimizar la gestión de las colecciones impresas?. Blok de Bid, 2011. Disponible em: <https://www.ub.edu/blokdebid/es/content/cloud-computing-en-las-bibliotecas-los-servicios-bibliotecarios-en-nube-podr%C3%ADan-optimizar-la>. Acceso em: 20 maio 2024.

CABRAL VARGAS, B. Consideraciones para el almacenamiento de archivos digitales en la nube informática en bibliotecas universitarias. **Investigación Bibliotecológica**, México, v. 32, n. 74, p. 55-75, jan./mar. 2018. Disponible em: <http://rev-ib.unam.mx/ib/index.php/ib/article/view/57909>. Acceso em: 11 ago. 2025.



CLOUDWARDS. Cloud computing statistics and trends. Cloudwards, 2025. Disponível em: <https://www.cloudwards.net/cloud-computing-statistics/>. Acesso em: 11 ago. 2025.

GÓMEZ PALOMO, S. R.; MORALEDA, E. A. G. **Aproximación a la ingeniería del software**. 2. ed. [S. l.]: Editorial Universitaria Ramón Areces, 2020. 332 p.

GOOGLE. Cómo activar la verificación en 2 pasos. Ayuda de Cuenta de Google, 2024a. Disponível em: <https://support.google.com/accounts/answer/185839?hl=es>. Acesso em: 11 ago. 2025.

GOOGLE. Controles de privacidad. Centro de seguridad, 2024b. Disponível em: <https://safety.google/intl/es/privacy/privacy-controls>. Acesso em: 11 ago. 2025.

GOOGLE. Encuentra, controla y borra la información de tu cuenta de Google. Ayuda de Cuenta de Google, 2024c. Disponível em: <https://support.google.com/accounts/answer/7660719?hl=es-419>. Acesso em: 11 ago. 2025.

HOWARTH, J. 34 amazing cloud computing stats 2024. Exploding Topics, 2024. Disponível em: <https://explodingtopics.com/blog/cloud-computing-stats>. Acesso em: 11 ago. 2025.

LÓPEZ CUEVAS, A. J.; MIRAMONTES CARPENA, R. P. Diseño de sitios web con WordPress. In: CENTRO DE INVESTIGACIÓN Y DESARROLLO. **Compilación de investigaciones em ciencias sociales: diversidad cultural y convivencia**. v. 1, n. 7, 7. ed. [S. l.]: CID Editorial, 2024. cap. 3, p. 54-72. Disponível em: https://doi.org/10.37811/cli_w1071. Acesso em: 11 ago. 2025.

MARTÍNEZ, N. L. **Ciberseguridad y riesgo operacional en las organizaciones**. 2019. 74 f. Trabajo de fin de máster (Maestría en Ciberseguridad) – Universidad Pontificia Comillas, Madrid, 2019. Disponível em: <https://repositorio.comillas.edu/xmlui/handle/11531/42317>. Acesso em: 11 ago. 2025.

MEDINA MARTÍNEZ, J. J.; CÁRDENAS OSORIO, C. H.; MEJÍA LOBO, M. Análisis del phishing y la ley de delitos informáticos en Colombia. **Cuaderno de investigaciones: semilleros andina**, [s. l.], n. 14, p. 75-79, 2021. Disponível em: <https://revia.areandina.edu.co/index.php/vbn/article/view/1948>. Acesso em: 11 ago. 2025.

MICROSOFT. Qué es la nube?. Azure, 2024a. Disponível em: <https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-the-cloud/>. Acesso em: 11 ago. 2025.



MICROSOFT. Qué es la protección con contraseña?. Seguridad de Microsoft, 2024b. Disponível em: <https://www.microsoft.com/es-es/security/business/security-101/what-is-password-protection>. Acesso em: 11 ago. 2025.

MORALES. M. M. F. Computación en la nube para automatizar unidades de información. **Revista Bibliotecas**, [s. /], v. 30, n. 1, jan./jun. 2012. Disponível em: <https://www.revistas.una.ac.cr/index.php/bibliotecas/article/view/3894/19794>. Acesso em: 11 ago. 2025.

OMOSHALEWA, A. A. Cloud data security: an empirical study of user awareness, perceived risks and protective measures. **World Journal of Advanced Research and Reviews**, [s. /], p. 1185-1192, 2025. Disponível em: <https://journalwjarr.com/content/cloud-data-security-empirical-study-user-awareness-perceived-risks-and-protective-measures>. Acesso em: 11 ago. 2025.

PASQUI, V. Cloud Computing and libraries: illusion or opportunity?. **JLIS.it**, [s. /], v. 1, n. 2, p. 277–304, 2010. Disponível em: <https://www.jlis.it/index.php/jlis/article/view/355>. Acesso em: 11 ago. 2025.

SALUDDATA. Lenguaje digital: un viaje al mundo del protocolo informático. SaludData, 2023. Disponível em: <https://saluddata.com/protocolo-informatico>. Acesso em: 11 ago. 2025.

SAMPIERI, R. H. **Metodología de investigación**. México: McGraw-Hill Interamericana de España S.L., 2019.

SEVILLA ROBLES, M. A. **Resumen sobre internet**. [S. /]: UDG, 2020. 59 p. Disponível em: <https://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/3088?mode=full>. Acesso em: 11 ago. 2025.

UNIVERSIDAD DE COSTA RICA. Centro de Informática. Unidad de Riesgos y Seguridad. Servicios en la nube (cloud). Centro de Informática da Universidad de Costa Rica, 2022. Disponível em: https://ci.ucr.ac.cr/servicios-en-nube-cloud?utm_source. Acesso em: 11 ago. 2025.



APÉNDICE A – INSTRUMENTO CONOCIMIENTO DE LA SEGURIDAD INFORMÁTICA EN LA NUBE

El propósito de este cuestionario es recopilar información que contribuya a determinar el conocimiento que poseen los estudiantes matriculados en el primer ciclo del 2024, en los bachilleratos en Bibliotecología de la Universidad de Costa Rica, este trabajo forma parte de una investigación del curso SC103 Introducción a la Informática de la Universidad Fidélitas

Las respuestas y opiniones de los participantes serán de gran valor para este estudio. La información proporcionada permitirá obtener una comprensión más precisa sobre el conocimiento en el área de la seguridad informática en la nube por parte de los estudiantes.

Es importante destacar que todas las respuestas serán tratadas con la más estricta confidencialidad y sólo se utilizarán con fines académicos y de investigación. Los datos recopilados se analizarán de forma agregada y no se divulgará ninguna información personal identificable.

Si tienen alguna pregunta o inquietud adicional, no duden en comunicarse con el equipo de investigación.

Agradecemos su colaboración.

1. ¿Qué año de la carrera cursa?

- a) Primer año;
- b) Segundo año;
- c) Tercer año;
- d) Cuarto año.

2. ¿En cuál énfasis se encuentra matriculado (a)?

- a) Bibliotecología con énfasis en Ciencias de la Información;
- b) Bibliotecología con énfasis en Bibliotecas Educativas.

3. ¿Qué entiende por seguridad informática en la nube y cuál crees que es su importancia en el ámbito de la bibliotecología y ciencias de la información?



4. ¿Ha recibido formación específica sobre seguridad informática en la nube durante tu carrera?

- a) Sí;
- b) No;
- c) Parcialmente.

5. ¿Consideras que tienes un nivel satisfactorio de conocimiento sobre seguridad informática en la nube?

- a) Sí;
- b) No;
- c) Parcialmente.

6. ¿Utilizas regularmente servicios en la nube para almacenar o acceder a información relacionada con tu área de estudio?

- a) Sí, regularmente;
- b) No;
- c) Ocasionalmente.

7. ¿Qué servicios informáticos en la nube utilizas regularmente? (Selecciona todas las opciones aplicables)

- a) Almacenamiento de archivos (por ejemplo, Google Drive, Dropbox);
- b) Suite de oficina en línea (por ejemplo, Google Workspace, Microsoft Office 365);
- c) Plataforma de gestión de proyectos (por ejemplo, Trello, Asana);
- d) Almacenamiento y sincronización de contraseñas (por ejemplo, LastPass, 1Password);
- e) Plataforma de correo electrónico en línea (por ejemplo, Gmail, Outlook.com)
- f) Servicios de alojamiento web (por ejemplo, AWS, Azure);
- g) Plataforma de colaboración en tiempo real (por ejemplo, Google Docs, Microsoft Teams);
- h) Otros.

8. ¿Has experimentado alguna vez problemas de seguridad relacionados con el uso de servicios en la nube?

- a) Sí;
- b) No;
- c) No estoy seguro.

9. ¿Cuáles de los siguientes pasos de seguridad realizas al utilizar servicios informáticos en la nube? (puede seleccionar más de una opción)

- a) Uso de contraseñas seguras (Incluyen entre 10 y 12 dígitos, con mayúsculas, minúsculas y símbolos);
- b) Activación de la verificación en dos pasos;
- c) Revisión y ajuste de la configuración de privacidad;
- d) Actualización periódica de software y aplicaciones;
- e) Revisión regular del historial de actividad de la cuenta;
- f) Realización de copias de seguridad de los datos almacenados;
- g) Cierre de sesiones en dispositivos ajenos;
- h) No realizó ningún paso de seguridad;
- i) Otros.

10. ¿Estás al tanto de las políticas de seguridad implementadas por tu institución respecto al uso de la nube para almacenar información sensible?

- a) Sí;
- b) No;
- c) Parcialmente.