25(2): 219-227, 2022
SCIÉNDO

Esta obra está publicada bajo la licencia
CC BY 4.0

REVISIÓN SISTEMÁTICA

# Seguridad en el uso de aplicaciones de mensajería instantánea de comunicación interna

## Security in the use of instant messaging applications for internal communication

**Keyly Esperanza Ortiz Noriega[1, *]; Jair Erinson Guevara Segura[1]; Alberto Carlos Mendoza De los Santos[1]**

1 Facultad de Ingeniería, Universidad Nacional de Trujillo, Av. Juan Pablo II s/n – Ciudad Universitaria, Trujillo, Perú.

*Autor correspondiente: **kortizn@unitru.edu.pe** (K. Ortiz).

Fecha de recepción: 08 04 2022. Fecha de aceptación: 19 05 2022.

**RESUMEN**

El objetivo de la investigación fue dar a conocer algunas consideraciones de seguridad para el uso de aplicaciones de mensajería instantánea de comunicación interna, recolectando información de los últimos diez años. El diseño de la investigación fue no experimental y con un enfoque descriptivo. Se realizó una revisión sistemática de diversas publicaciones nacionales e internacionales obtenidas en bases de datos confiables como Scielo, Google Académico, PubMed, IEEE Xplore y ScienceDirect. Los documentos se incluyeron de acuerdo al período de publicación y relación con el tema en estudio, se excluyeron aquellas publicaciones repetidas e incompletas. De las 60 publicaciones recolectadas en primera instancia se seleccionaron únicamente 24; encontrándose un total de 23 consideraciones generales de seguridad que, sometidas a un análisis, permitieron destacar a 5: capacitación de personal en temas de seguridad informática y de la información, y fomento de buenas prácticas; cumplimiento de buenas prácticas; uso de aplicaciones con cifrado de datos; y establecimiento de políticas de ciberseguridad. Finalmente, se concluyó que entre las consideraciones de seguridad en aplicaciones de mensajería instantánea para comunicación interna se incluyen técnicas de seguridad, prácticas individuales del personal y medidas adoptadas por la empresa, todas en conjunto, para una mejor gestión de la seguridad.

**Palabras clave:** Mensajería instantánea; empresa; seguridad; ciberseguridad; comunicación interna.

**ABSTRACT**

The objective of the research was to present some security considerations for the use of instant messaging applications for internal communication, collecting information from the last ten years. The research design was non-experimental and with a descriptive approach. A systematic review of various national and international publications obtained from reliable databases such as Scielo, Google Scholar, PubMed, IEEE Xplore and ScienceDirect was carried out. The documents were included according to the publication period and relationship with the subject under study, those repeated and incomplete publications were excluded. Of the 60 publications collected in the first instance, only 24 were selected; finding a total of 23 general security considerations that, subjected to an analysis, allowed to highlight 5: training of personnel in computer and information security issues, and promotion of good practices; compliance with good practices; use of applications with data encryption; and establishment of cybersecurity policies. Finally, it was concluded that the security considerations in instant messaging applications for internal communication include security techniques, individual personnel practices and measures adopted by the company, all together, for better security management.

**Keywords:** Instant messaging; business; security; cybersecurity; internal communication.

## INTRODUCCIÓN

Con el transcurrir de los años y la incorporación de nuevas y mejoradas tecnologías al mundo laboral, las empresas han debido, o deberían, tener en cuenta que el fin de incluirlas no es únicamente gestionar mejor algunos procesos y obtener mejores resultados cuantificables; sino también, a la

par, asegurar el cumplimiento de las metas de seguridad para garantizar que los datos confidenciales permanecerán siendo secretos y reservados. Sin duda, un aspecto que merece atención en ambientes organizacionales es la seguridad con la que se efectúa el proceso de comunicación interna, el que, según Calero (2020), es el medio para llevar a cabo las interacciones entre los colaboradores de una empresa y fomentar el intercambio de información entre los mismos. Para este autor, la comunicación interna se da en todas y cada una de las organizaciones, sin excepción, ya sea de forma intencional o no intencional, puesto que el ejercicio de las funciones de quienes laboran en una empresa requiere de interacción entre ellos continua y permanentemente.

Por otro lado, hablar de aplicaciones de mensajería instantánea, enfatizando el término, es departir de plataformas donde, en cuestión de segundos, se pueden enviar y recibir mensajes de texto o archivos de diferentes formatos y tamaños. De acuerdo con Calero (2020), la mensajería instantánea sirve para el envío de mensajes a uno o más destinatarios, quienes los reciben de manera inmediata y, de la misma forma, pueden contestar con prontitud; en otras palabras, estas aplicaciones agilizan la comunicación entre usuarios de una plataforma específica.

WhatsApp, por ejemplo, es una aplicación de mensajería instantánea muy eficaz que, de acuerdo con Ruíz (2020), años atrás podía presentar una desventaja en cuanto a la privacidad de los mensajes en entornos empresariales y se sugería, en lugar de esta aplicación, el uso de herramientas de comunicación corporativa que cumplan con los estándares de seguridad requeridos. Con el incremento de la demanda de seguridad, se llegó a implementar el cifrado de extremo a extremo para que nadie pudiera leer o escuchar lo que enviaban los usuarios; sin embargo, sigue teniendo limitaciones y es menester tener en cuenta recomendaciones si se desea usar para la comunicación interna.

En comparativa, con la evolución de la tecnología han surgido aplicaciones que han marcado tendencias en entornos empresariales y han sido empleados, específicamente, para la comunicación. De esta manera se ha empezado a dejar de lado, inclusive, el típico correo electrónico que no maneja un acuse de recibo y genera inconvenientes en la comunicación; para dar cabida a aplicaciones como HipChat, que está orientada a equipos de trabajos y empresas y permite el envío de mensajes y compartición de archivos manejando la encriptación de datos; Skype Empresarial, que ofrece mensajería, llamadas y videollamadas para miembros de organizaciones; y, entre otras, Slack, que permite mejorar la comunicación entre las áreas de una empresa y es promocionada como una aplicación segura y de fácil uso (García, 2017). Además, entre una de las ventajas sobresaliente de Slack se encuentra el que se puede integrar fácilmente a otras aplicaciones, llegando a generar provechosas oportunidades de mejoras y adaptaciones dependiendo de las necesidades de las empresas (Romero, 2020).

Adicionalmente, Joyanes (2017) menciona que la inclusión de Big Data, Cloud Computing y robots virtuales en el vocabulario habitual de las empresas es una clara evidencia del comienzo de una nueva revolución industrial (la cuarta) donde surgen o resurgen, a la vez, desafíos a nivel de seguridad ya que hay ciberataques que vulneran sistemas y destruyen la confidencialidad de datos empresariales. Así, entonces, queda claro que existen peligros constantes en la tecnología ya que esta se puede usar con fines maliciosos y se pueden producir robos de información, fraudes, propagación de virus, etc. Aunque a primera vista la mejor opción pareciera ser el abandono de plataformas que pueden ser vulneradas, debido a su utilidad estas no pueden simplemente rechazarse, pero las empresas pueden considerar estrategias de ciberseguridad.

Por ciberseguridad se entiende, de acuerdo al aporte de Astorga y Schmidt (2019), al conjunto de acciones que involucran la supervisión, el gobierno, la investigación, el mantenimiento y la defensa de la seguridad en la red. A su vez, Cano (2020) argumenta que implementar medidas de ciberseguridad será necesario para contrarrestar el efecto negativo de las tendencias emergentes al 2030, como los ciberataques y el cibercrimen.

Este estudio está justificado en que, a raíz de la evolución de las exigencias de las organizaciones a nivel de seguridad en el proceso de comunicación interna, también surgen nuevas consideraciones para preservar la inviolabilidad de la información manipulada por medio de aplicaciones de mensajería instantánea y resulta natural el querer ahondar o profundizar en este tema para tener la información suficiente para tomar medidas de prevención contra ciberataques. Las medidas preventivas requieren o necesitan de concientización por parte de las empresas, así se adoptan políticas o procedimientos para mitigar los riesgos de posibles ataques ya que, como lo recalca, las vulnerabilidades cibernéticas no son temporales; por lo tanto, requieren atención permanente (Caamaño y Gil, 2020).

La presente investigación tuvo como objetivo identificar consideraciones de seguridad para el uso de aplicaciones de mensajería instantánea de comunicación interna, para dar a conocer reflexiones de estudios al respecto, considerando un ambiente organizacional cambista donde, a la par con la evolución de la tecnología, las técnicas para vulnerar los sistemas también mejoran.

## METODOLOGÍA

La presente revisión sistemática de la literatura científica se realizó con el objetivo de reunir información suficiente y necesaria sobre un tema específico y adoptando un diseño de investigación no experimental y un enfoque descriptivo. Se revisó material documental de variadas fuentes válidas y confiables en la persecución de evidencias que den respuesta a la interrogante de esta investigación: ¿cuáles son las consideraciones de seguridad para el uso de aplicaciones de mensajería instantánea de comunicación interna?

### Estrategia de búsqueda

Cabe indicar que, para el proceso de búsqueda de información y para su futura selección, se consideraron términos como los siguientes: "mensajería instantánea", "empresa", "seguridad", "ciberseguridad", "comunicación interna", "recomendaciones de seguridad" y "buenas prácticas de seguridad" combinadas de diferentes formas, incluyendo, para algunos, la traducción al inglés.


**Figura 1**. Aplicación de criterios de exclusión para selección de publicaciones.

### Criterios de selección

Los artículos y tesis recopilados se analizaron de acuerdo a criterios de inclusión y exclusión. Aquellos artículos publicados entre los años 2012 y 2021 que, además, describen consideraciones de seguridad en aplicaciones de mensajería instantánea para comunicación interna fueron incluidos, y se descartaron aquellos artículos o tesis cuya información está desfasada o incompleta, y las investigaciones repetidas; no hubo exclusión por idioma. Se partió de un total de 60 documentos entre artículos y tesis con la siguiente distribución entre las bases de datos consultadas: Scielo, 3; Google Académico, 38; PubMed, 4; IEEE Xplore, 8; y ScienceDirect, 7. El resultado de la aplicación de los criterios de selección de publicaciones se muestra en la Figura 1.

### Extracción de datos

Para la extracción de datos se diseñó una tabla con 6 columnas diferentes: número de publicación, título de publicación, autor(es), revista, país y las consideraciones de seguridad rescatadas. Adicionalmente, se organizó otra tabla con la información correspondiente a las consideraciones generales identificadas en las publicaciones, a las que les corresponde un respectivo identificador que permite su vínculo o relación con la tabla 1.

### Análisis de datos

Se procedió a comparar la información recopilada e identificar patrones entre los mismos. Además, se estableció una clasificación para las consideraciones de seguridad en base a los patrones previamente identificados y se obtuvieron consideraciones más importantes basadas en el número de ocurrencias y coincidencias entre la opinión de los autores.

## RESULTADOS Y DISCUSIÓN

Acorde a los criterios de inclusión y exclusión, se obtuvo las siguientes cantidades de fuentes o publicaciones por cada base de datos de revistas indexadas y repositorios de tesis: Scielo, 0; Google Académico, 16; PubMed, 2; IEEE Xplore, 2; y ScienceDirect, 4. Gráficamente, se obtuvo el resultado de la Figura 2, habiendo un total de 24 publicaciones.

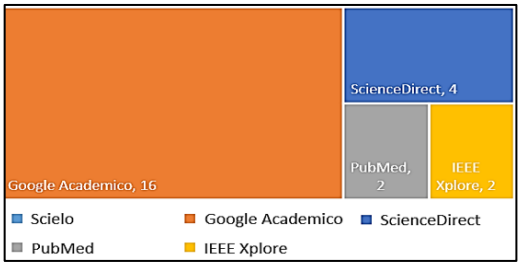


**Figura 2**. Número de documentos por base de datos consultada después de aplicar criterios de exclusión.

**Tabla 1**
Publicaciones analizadas a nivel nacional e internacional

| N° | Fuente | País | Consideraciones de seguridad |
|---|---|---|---|
| 1 | Ruíz (2020) | Perú | C-00, C-01, C-02, C-03, C-22 |
| 2 | Singh et al. (2021) | Irlanda | C-04 |
| 3 | Abiodun et al. (2020) | Malasia | C-05 |
| 4 | Ellewala et al. (2020) | Sri Lanka | C-01, C-04, C-06, C-07 |
| 5 | Ali y Alsaad (2020) | Irak | C-01, C-08 |
| 6 | Savolainen (2017) | Finlandia | C-03, C-09, C-22 |
| 7 | Cardozo y Celis (2021) | Colombia | C-01, C-03, C-09, C-10, C-11, C-22 |
| 8 | Valderrama (2018) | Colombia | C-03, C-09, C-22 |
| 9 | Moreno (2018) | Colombia | C-03, C-09, C-11, C-22 |
| 10 | Camino y Puente (2020) | Ecuador | C-00, C-01, C-03, C-09, C-10, C-11, C-12, C-13, C-14, C-22 |
| 11 | Hernández (2020) | Colombia | C-01, C-03, C-09, C-10, C-22 |
| 12 | Rodríguez y Sánchez (2019) | Ecuador | C-01, C-10 |
| 13 | Monsalve (2018) | Colombia | C-03, C-22 |
| 14 | Martínez y Blanco (2020) | Colombia | C-03, C-09, C-10, C-11, C-15, C-16, C-22 |
| 15 | Freire (2017) | Ecuador | C-03, C-10, C-11, C-22 |
| 16 | He y Zhang (2019) | Estados Unidos | C-03, C-22 |
| 17 | Ezra et al. (2020) | Israel | C-01, C-17 |
| 18 | Phillips y Tanner (2019) | Estados Unidos | C-03, C-10, C-18, C-22 |
| 19 | Segoro y Putro (2020) | Indonesia | C-01, C-07, C-19 |
| 20 | Nursalman et al. (2020) | Indonesia | C-01, C-20 |
| 21 | Xie et al. (2012) | Estados Unidos | C-21 |
| 22 | Cai y Wu (2018) | China | C-09, C-10, C-15 |
| 23 | Sigelman (2017) | Israel | C-01, C-10, C-15, C-16, C-17 |
| 24 | Curry (2013) | Estados Unidos | C-00, C-01, C-03, C-07, C-09, C-10, C-16, C-22 |

A partir de los documentos incluidos se organizó la tabla 1 con la información necesaria para su análisis como la fuente o autor(es), el país y las consideraciones o recomendaciones rescatadas.
En la Tabla 2 se muestra el listado de consideraciones generales de seguridad, cuyo identificador se incluye en la última columna de la primera tabla.
Así, se hizo seguimiento de la ubicación de las instituciones que referencian consideraciones de seguridad para el uso de aplicaciones de mensajería instantánea de comunicación interna en los últimos diez años. El resultado, considerando países, se muestra en la Figura 3.

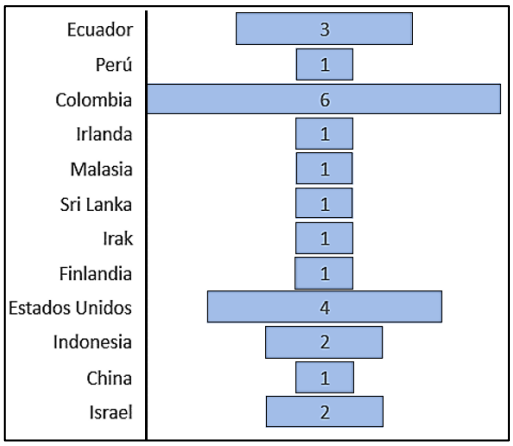


**Figura 3**. Número total de publicaciones por país

Adicionalmente, en la tabla 2, se presenta un listado de consideraciones generales de seguridad para el uso de aplicaciones de mensajería instantánea en empresas, las que han sido organizadas de acuerdo al contenido de las publicaciones incluidas. También se incorporó una categorización de acuerdo a la naturaleza de las consideraciones, siendo estas técnicas de seguridad, prácticas individuales del personal y medidas adoptadas por la empresa. En la última columna de la tabla 2 se incluye el conteo de ocurrencias en las publicaciones.
De acuerdo a lo plasmado en la Tabla 2, se han recopilado un total de 23 consideraciones generales de seguridad, muchas de las cuales comprenden consideraciones específicas y particulares de acuerdo a los autores. En cuanto a la consideración C-00, control de contenidos en equipos informáticos, Ruíz (2020), en acuerdo con Curry (2013), menciona que es indispensable realizar este tipo de tarea para evitar cualquier robo de información que, a largo plazo, perjudique a la empresa. Para regular el contenido al que puede acceder un usuario de la red, Santamaría et al. (2018) menciona que se deben segmentar las redes y los canales de datos.
Con respecto a la consideración C-01, uso de aplicaciones con cifrado de datos, más de un autor, entre ellos Ruíz (2020), Ellewala et al. (2020), Ali y Alsaad (2020), Cardozo y Celis (2021), Camino y Puente (2020) y Sigelman (2017), coincide en que esta técnica es necesaria para garantizar un nivel medio de seguridad en aplicaciones de mensajería o cualquier sistema de información. El cifrado de datos, para Carvajal (2019) , se refiere a la codificación de cierta información para evitar que este sea descifrado si llega a ser interceptado.
Por otro lado, en referencia a la consideración C-002, Ruíz (2020) opina que, para la adopción de correo electrónico o una aplicación de mensajería dentro de la

institución, se debe considerar la existencia de los dispositivos tecnológicos en todas las oficinas, lo que es natural puesto que es primordial, en una primera etapa, asegurarse de contar con los recursos necesarios para la inclusión de algo nuevo, si se está pensando implantar por primera vez una práctica como la descrita.

Adicionalmente, sobre la consideración C-03, capacitación de personal en temas de seguridad informática y de la información, y fomento de buenas prácticas, es de las consideraciones más importantes para autores como Savolainen (2017), Cardozo y Celis (2021), Valderrama (2018), Monsalve (2018), y He y Zhang (2019). Phillips y Tanner (2019), inclusive, han afirmado que los empleados suelen ser el principal punto de falla en la seguridad cibernética, por lo que consideran que la inversión en educación y concienciación del personal sobre el tema ayudaría grandemente a la mejora de la postura de seguridad de la empresa. Por su parte, Moreno (2018) añade que los planes de capacitación sobre buenas prácticas de seguridad deben ser periódicos y continuos.

La consideración C-04, uso de un mecanismo de mensajería segura respaldado por blockchain, hace referencia a una técnica de seguridad que, para Singh et al. (2021), proporciona confidencialidad y privacidad, incrementando la seguridad de las aplicaciones que, incluso, ya incluyen el cifrado de extremo a extremo. Blockchain es definido por Yaga et al. (2019) como un conjunto de libros contables digitalizados que se implementan de forma distribuida, como si se tratara de una cadena de bloques que no se pueden manipular. Según Ellewala et al. (2020), esta técnica garantiza seguridad a nivel empresarial. El uso de técnicas de seguridad también se evidencia en la consideración C-05, empleo del sistema de cifrado Honey encryption (HE) que, de acuerdo con Abiodun et al. (2020), ayuda a reforzar la seguridad de los sistemas de mensajería instantánea utilizando una clave correcta para descifrar un mensaje, pero en caso de que se ingrese una contraseña errónea, genera mensajes señuelo de apariencia válida cuyo propósito es confundir a un atacante y hacer que crea que ha logrado vulnerar el sistema de mensajería, lo que da tiempo para adoptar otras medidas. Asimismo, la consideración de contratos inteligentes y un modelo de prevención de pérdida de datos (C-06) es explicada por Ellewala et al. (2020) como una técnica de importancia para que los registros de datos sean inalterables y que, utilizando aprendizaje automático (Machine Learning), puedan garantizar la seguridad de la información. Este tipo de modelos, en afinidad con Gantiva (2021), tienen el propósito de detectar, supervisar y evitar la fuga de los datos en reposo, que son datos críticos que se respaldan y almacenan; datos en movimiento, que son observados por un proxy en el tráfico de red de mensajería instantánea, por ejemplo; y datos en uso, que son utilizados constantemente por los usuarios de una empresa.

En relación con la consideración C-07, empleo de autenticación multifactor, Ellewala et al. (2020), Segoro y Putro (2020), y Curry (2013) opinan que para ceder el acceso a una persona a un aplicativo esta debe haber demostrado ser quien dice ser en más de una prueba, de esa forma se evita la suplantación. Por otro lado, la inclusión de técnicas de privacidad que corresponde a la consideración C-08, se refiere a que las aplicaciones de mensajería deberían incluir técnicas de privacidad básicas como la negociación de mensajes, el bloqueo de contactos, si se considera necesario, y la destrucción de conversaciones de manera permanente, inclusive en servidores, para una mayor seguridad y privacidad (Ali y Alsaad, 2020).

Entre las medidas adoptadas por la empresa se tienen la consideración C-09, protección de computadora contra malware, y C-10, establecimiento de políticas de ciberseguridad. La primera, de acuerdo con Savolainen (2017), consiste en realizar prácticas como mantener el sistema operativo, navegador y complementos actualizados siempre; habilitar el firewall permanentemente; usar los privilegios de administrador solo en situaciones que lo ameriten; protegerse de la red de área local que se utilice; mantener el enrutador actualizado y habilitar software de protección confiable. La segunda, considerando la opinión de Rodríguez y Sánchez (2019), se refiere a políticas de seguridad enfocadas principalmente a la clasificación y al aseguramiento de la información dado que en las pymes se puede identificar un alto número de activos considerados como confidenciales. Freire (2017), adiciona que tales políticas deben describir las responsabilidades, privilegios y restricciones del usuario e informar sobre las sanciones por su violación o incumplimiento.

Por otro lado, la consideración C-11, creación de copias de seguridad periódicas y permanentes, es planteada por autores como Cardozo y Celis (2021), Camino y Puente (2020), y Martínez y Blanco (2020), quienes lo recomiendan para el resguardo de los activos de información críticos e importantes para el negocio. Por otra parte, el uso alternativo de espacios de almacenamiento de información en nube, correspondiente a la consideración C-12, es mencionada por Hernández (2020), e indica

que su propósito es evitar el uso de unidades externas en los equipos de la institución para evitar el ingreso de malware que se pueda propagar por medio de aplicaciones de mensajería.

En cuanto la consideración C-13, adopción del ISO 27001, Camino y Puente (2020) argumentan que el propósito de este estándar internacional es implementar un sistema que se asegure de gestionar la seguridad de la data sensible y confidencial de la empresa. El ISO 27001, es de los estándares más usados a nivel empresarial para el resguardo de la seguridad informática; sin embargo, como lo enuncia Talib et al. (2012), este tipo de normas suele ser adoptado, principalmente por empresas dedicadas a la gestión de información de otras empresas o particulares ya que resulta costoso y requiere de personal experto.

Otra medida que pueden adoptar las organizaciones es la de la verificación del estado de la seguridad de la red y de los usuarios simulando ataques de ingeniería social (C-14), que según la opinión de Camino y Puente (2020), ayuda a comprobar si los protocolos están funcionando y establecer buenas prácticas de seguridad. Enriqueciendo la definición de ingeniería social, Hernández y Storchak (2018) comentan que se refiere al acto de manipular y engañar a alguien para conseguir que lleve a cabo ciertas acciones como brindarle información o acceso a información confidencial; en tal sentido, el elemento humano de las empresas es el más comprometido y vulnerable.

La consideración C-15, limitación del acceso a información considerando roles y permisos de usuarios, resulta importante, de acuerdo con Martínez y Blanco (2020), porque la definición clara de la información que cada persona puede manejar dentro de la organización previene del acceso no deseado a información crítica y divulgación de esta por canales como aplicaciones de mensajería. La ejecución de auditorías periódicas a nivel de personal interno y, si es posible, a nivel externo (C-16), igualmente es considerada de gran importancia. Martínez y Blanco (2020) también opinan que se deberían realizar este tipo de auditorías para identificar, describir y evidenciar el cumplimiento de las políticas de seguridad y las vulnerabilidades a las que están expuestas todos los sistemas, no solo aquellos orientados a la comunicación.

**Tabla 2**
Consideraciones de seguridad generales rescatadas de las publicaciones incluidas

| Id | Consideración general | Categoría | N° de ocurrencias |
|---|---|---|---|
| C-00 | Control de contenidos en equipos informáticos. | Medida adoptada por empresa | 3 |
| C-01 | Uso de aplicaciones con cifrado de datos. | Técnica de seguridad | 12 |
| C-02 | Verificación de existencia de equipos suficientes para emplear aplicaciones de mensajería en oficinas. | Medida adoptada por empresa | 1 |
| C-03 | Capacitación de personal en temas de seguridad informática y de la información, y fomento de buenas prácticas. | Medida adoptada por empresa | 13 |
| C-04 | Uso de un mecanismo de mensajería segura respaldado por blockchain. | Técnica de seguridad | 2 |
| C-05 | Empleo del sistema de cifrado Honey encryption (HE). | Técnica de seguridad | 1 |
| C-06 | Consideración de contratos inteligentes y un modelo de prevención de pérdida de datos. | Técnica de seguridad | 1 |
| C-07 | Empleo de autenticación multifactor. | Técnica de seguridad | 3 |
| C-08 | Inclusión de técnicas de privacidad. | Técnica de seguridad | 1 |
| C-09 | Protección de computadora contra malware. | Medida adoptada por empresa | 9 |
| C-10 | Establecimiento de políticas de ciberseguridad. | Medida adoptada por empresa | 10 |
| C-11 | Creación de copias de seguridad periódicas y permanentes. | Práctica individual del personal | 5 |
| C-12 | Uso alternativo de espacios de almacenamiento de información en nube. | Medida adoptada por empresa | 1 |
| C-13 | Adopción del ISO 27001. | Medida adoptada por empresa | 1 |
| C-14 | Verificación del estado de la seguridad de la red y de los usuarios simulando ataques de ingeniería social. | Medida adoptada por empresa | 1 |
| C-15 | Limitación del acceso a información considerando roles y permisos de usuarios. | Medida adoptada por empresa | 3 |
| C-16 | Ejecución de auditorías periódicas a nivel de personal interno y si es posible a nivel externo. | Medida adoptada por empresa | 3 |
| C-17 | Uso de aplicaciones de mensajería orientadas a organizaciones. | Medida adoptada por empresa | 2 |
| C-18 | Establecimiento del plan de continuidad del negocio. | Medida adoptada por empresa | 1 |
| C-19 | Prevención de robo de información con cifrado híbrido. | Técnica de seguridad | 1 |
| C-20 | Uso de un algoritmo de cifrado simétrico (AES) con un algoritmo de firma digital (ECDSA). | Técnica de seguridad | 1 |
| C-21 | Implementación del mecanismo de protección de red HoneyIM. | Técnica de seguridad | 1 |
| C-22 | Cumplimiento de buenas prácticas. | Práctica individual del personal | 13 |

En un cambio de tema, de acuerdo con Sigelman (2017), la tendencia de "trae tu propia nube" (BYOC) ha sido un gran riesgo en la última década por promover el uso de aplicaciones de mensajería personales que se basan en la nube y que se pueden vulnerar a nivel de seguridad tanto por ataques externos, como por el mismo mal uso que les puede dar el personal al compartir información confidencial de manera irresponsable. Por esta razón, para potenciar la seguridad de la información de las empresas, este autor propone la adopción de medidas preventivas como el manejo de aplicaciones de mensajería instantánea dedicadas al resguardo de información empresarial que cumplan con requerimientos como la encriptación y el cifrado de datos avanzado. La consideración C-17, uso de aplicaciones de mensajería orientadas a organizaciones tiene su sustento en la opinión de este autor. Además, Ezra et al. (2020), reconoce que las organizaciones tienen requerimientos particulares y se puede encontrar la aplicación de mensajería que mejor se adapte a estas. Por ejemplo, para compartir información confidencial entre médicos de una clínica se puede optar por una aplicación de mensajería denominada Siilo, que es gratuita y encriptada separada de cualquier medio personal.

Phillips y Tanner (2019), con respecto a la consideración "establecimiento del plan de continuidad del negocio" (C-18) argumentan que se debe tener en cuenta ya que involucra, en primera instancia, estar familiarizados con las amenazas cibernéticas comunes que enfrentan las organizaciones y las consecuencias del filtrado de datos, para elaborar un plan de prevención y uno de continuidad en caso de que las amenazas de seguridad se manifiesten. Siempre es mejor prevenir, pero nunca está demás contar con un plan de contingencia.

Acerca de la consideración C-19, prevención de robo de información con cifrado híbrido, Segoro y Putro (2020) recalcan que las aplicaciones de mensajería instantánea todavía son vulnerables al robo de cuentas, por ello recomiendan implementar un cifrado híbrido y autenticación de dos factores, llegando a incluir, incluso, tecnologías como código QR y reconocimientos de huella dactilar para inicios de sesión. Vivanco et al. (2019), sobre el cifrado híbrido, hace mención del uso de dos esquemas de cifrado, uno de llave pública y otro de llave privada, lo que eleva su seguridad en comparación con el cifrado estándar. El uso de un algoritmo de cifrado simétrico (AES) con un algoritmo de firma digital (ECDSA) que es la consideración C-20, también aporta con tecnologías de seguridad y para Nursalman et al. (2020), ya que la mensajería instantánea abre la puerta a un sin número de delitos, se debe seguir esta recomendación ya que es uno de los métodos correctos para mantener la seguridad de los datos. Acerca del cifrado simétrico García et al. (2018) indican que requieren de una clave única tanto para el proceso de cifrado, como para el descifrado y que combinado con hash y firma digital son un éxito garantizando seguridad en transmisiones y almacenamiento de información.

Adicionalmente, Xie et al. (2012), plantean que la mensajería instantánea es uno de los vectores de ataque de malware más utilizado debido a su popularidad, por lo que, en un entorno empresarial, es requisito que el servidor de mensajería se encuentre dentro de la red protegida, lo cual se puede conseguir con HoneyIM (C-21), que es un mecanismo de detección y supresión de malware de mensajería instantánea y que ofrece reportes sobre intentos de vulneración y mecanismos de recuperación de sistema avanzados. De acuerdo con Zobal et al. (2019), esta técnica se basa en Honeypots que tienen la ventaja de detectar ataques de manera confiable, sin generar falsos positivos como otras herramientas; sin embargo, no puede sustituir a otras medidas.

Finalmente, la consideración C-22, cumplimiento de buenas prácticas, de acuerdo con Moreno (2018), abarca la creación y actualización frecuente de contraseñas que protegen la identidad y seguridad de los empleados, el reporte inmediato de actividad sospechosa a quien corresponda, la verificación de la legitimidad de las páginas cuyo link llega por medio de mensajes, la protección de la información al no compartir datos confidenciales de la empresa por redes de mensajería pública, el uso de software con licencia provisto por la organización o descargado de páginas oficiales, la toma de precaución ante llegada de mensajes cuyo remitente no pertenece a la organización, entre otros.

Las consideraciones que se han enumerado incluyen reflexiones que pueden ser consideradas por las organizaciones para prevenir ataques que vulneren la seguridad de la información que manejan.

Con base a los resultados identificados se elaboró el gráfico de la figura 4, que muestra las consideraciones de seguridad para el uso de aplicaciones de mensajería instantánea en un entorno laboral cambiante ordenadas, de mayor a menor, de acuerdo al número de ocurrencias encontradas, el que se rige en base al número de publicaciones incluidas en el estudio.

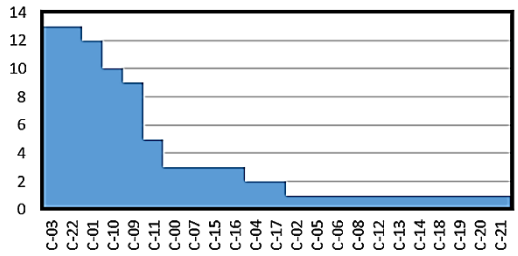


**Figura 4**. Consideraciones de seguridad ordenadas por número de ocurrencias.

Así, se puede apreciar que las consideraciones con más coincidencias son la C-03 (capacitación de personal en temas de seguridad informática y de la información, y fomento de buenas prácticas), C-22 (cumplimiento de buenas prácticas), C-01 (uso de aplicaciones con cifrado de datos) y C-10 (establecimiento de políticas de ciberseguridad). Cabe resaltar que estas consideraciones de seguridad corresponden con las tres categorías establecidas: técnicas de seguridad, prácticas individuales del personal y medidas adoptadas por la empresa.

## CONCLUSIONES

Las publicaciones analizadas indicaron que para el uso de aplicaciones de mensajería instantánea en una organización o empresa es necesario tener presente ciertas consideraciones de seguridad, las que pueden corresponder con técnicas de seguridad, prácticas individuales del personal o medidas adoptadas por la empresa. El análisis de coincidencias entre las distintas investigaciones que se han incluido en esta revisión sistemática permitió identificar consideraciones más relevantes que otras. Así, de las 23 consideraciones generales, 5 fueron nombradas en un mayor número de publicaciones y se establecieron como primordiales. Estas consideraciones fueron: capacitación de personal en temas de seguridad informática y de la información, y fomento de buenas prácticas (C-03), cumplimiento de buenas prácticas (C-22), uso de aplicaciones con cifrado de datos (C-01) y establecimiento de políticas de ciberseguridad (C-10). De esta manera se evidenció que las técnicas de seguridad, las prácticas individuales del personal y las medidas adoptadas por la empresa se deben considerar, en conjunto, para garantizar una mayor seguridad y confidencialidad de la información. La reflexión resulta útil para el uso de aplicaciones de mensajería e, incluso, otros sistemas de información empresarial.

Debido a los cambiantes retos a nivel de seguridad empresarial, es importante seguir ahondando en el conocimiento de consideraciones de este tipo. Inclusive, se puede llegar a elaborar un plan de acción para afrontar riesgos de seguridad con base en estos resultados.

## REFERENCIAS BIBLIOGRÁFICAS


Abiodun, E. O., Jantan, A., Abiodun, O. I., y Arshad, H. (2020). Reinforcing the Security of Instant Messaging Systems Using an Enhanced Honey Encryption Scheme: The Case of WhatsApp. *Wireless Personal Communications, 112*, 2533–2556.

Ali, R. M., y Alsaad, S. N. (2020). Instant messaging security and privacy secure instant messenger design. *IOP Conference Series: Materials Science and Engineering, 881*, 012117.

Astorga, C., y Schmidt, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Educare, 23*(3), 1-24.

Caamaño, E. E., y Gil, R. d. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional. *Novum, 1*, 61–80.

Cai, Y., y Wu, F. (2018). Data Security Framework for Electric Company Mobile Apps to Prevent Information Leakage. *Procedia Computer Science, 139*, 280–286.

Calero, M. A. (2020). WhatsApp y la comunicación interna en la empresa Promart de Santa Clara, 2019 (tesis de pregrado). Universidad Cesar Vallejo.

Camino, E. S., y Puente, E. D. (2020). *Análisis y evaluación de la seguridad en la red de la Unidad Educativa Salesiana Cardenal Spellman, utilizando herramientas de Ingeniería social, y recomendar medidas preventivas (tesis de pregrado)*. Universidad Politécnica Salesiana

Cano, J. J. (2020). Retos de seguridad/ciberseguridad en el 2030. *Sistemas,* (154), 68-79.

Cardozo, C. F., y Celis, J. F. (2021). Estudio de seguridad en dispositivos móviles con sistema operativo Android (tesis de pregrado). *Universidad Autónoma de Bucaramanga*. Universidad Autónoma de Bucaramanga

Carvajal, C. C. (2019). La encriptación de datos empresariales: ventajas y desventajas. *Recimundo, 3*(2), 980-997.

Curry, S. J. (2013). Instant-Messaging Security. En *Computer and Information Security Handbook* (págs. 721–735). Elsevier.

Ellewala, U. P., Amarasena, W. D., Lakmali, H. V., Senanayaka, L. M., y Senarathne, A. N. (2020). Secure Messaging Platform Based on Blockchain. *2020 2nd International Conference on Advancements in Computing (ICAC)*. IEEE.

Ezra, O., Toren, A., Tadmor, O., y Katorza, E. (2020). Secure Instant Messaging Application in Prenatal Care. *Journal of Medical Systems, 44*.

Freire, K. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de Ciberseguridad (tesis de pregrado). *Universidad Católica Santiago de Guayaquil.*

Gantiva, C. C. (2021). Análisis de soluciones DPL (Prevención de perdida de datos) como estrategia para la seguridad de la información en organizaciones colombianas (tesis de pregrado). Universidad Nacional Abierta y a Distancia UNAD.

García, G. P. (2017). Diseño de sistema de gestión de proyectos para PYME (tesis de maestría). Universidad Técnica Federico Santa María.

García, R., Lotzin, G., Cabrera, L., Puente, M., y Méndez, O. (2018). AES como Estándar Internacional de Cifrado. *Tecnología educativa, 5*(8), 65-70.

He, W., y Zhang, Z. (. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce, 29*, 249–257.

Hernández, A., y Storchak, S. (2018). Sistema para la detección de ataques phishing utilizando correo electrónico. *Revista telemática, 17*(2), 60-70.

Hernández, Y. (2020). Análisis y diseño de un mecanismo de cifrado de correo electrónico para garantizar y proteger la información enviada de las pymes (tesis de pregrado). *Universidad Nacional Abierta y a Distancia - UNAD*.

Joyanes, L. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). *Cuadernos de estrategia*, 19–64.

Martínez, J. A., y Blanco, L. X. (2020). Recomendaciones de buenas prácticas de ciberseguridad en Pymes para la generación de soluciones de detección de intrusos usando Snort (tesis de pregrado). *Universidad Autónoma de Bucaramanga*.

Monsalve, J. Y. (2018). Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos). *Universidad Piloto de Colombia*.

Moreno, Y. H. (2018). Prácticas básicas de seguridad informática y la importancia de un programa continuo de actualización de todos los sistemas de información. *Universidad Piloto de Colombia*.

Nursalman, M., Judie, P. R., y Ashshiddiqi, A. (2020). Implementation of AES and ECDSA for Encrypted Message in Instant Messaging Application. *2020 6th International Conference on Science in Information Technology (ICSITech)*. IEEE.

Phillips, R., y Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of business continuity y emergency planning, 12*, 224–232.

Rodríguez, J. E., y Sánchez, D. F. (2019). *Plan de sensibilización, comunicación y capacitación para minimizar los riesgos informáticos en la facultad de ciencias informáticas (tesis doctoral)*. Universidad Laica "Eloy Alfaro" De Manabi.

Romero, I. A. (2020). Sistema de gestión de recuperaciones de información para la empresa Cloner SPA (tesis de pregrado). Universidad Técnica Federico Santa María.

Ruíz, C. P. (2020). Uso de los canales digitales de comunicación interna en las organizaciones públicas y privadas de Lima, 2020 (tesis de pregrado). USMP.

Santamaría, T. M., Bravo, F. G., Lagos, G., y González, V. (2018). Infraestructira informática para dar soporte a un sistema de streaming de audio y video en la Universidad de Guayaquil. *Revista pedagógica de la Universidad de Cienfuegos, 14*(62), 101-105.

Savolainen, V. (2017). Job applicant's information security–Instant messaging applications as a part of virtual recruitment (tesis de pregrado). Obtenido de https://www.theseus.fi/handle/10024/139727

Segoro, M. B., y Putro, P. A. (2020). Implementation of Two Factor Authentication (2FA) and Hybrid Encryption to Reduce the Impact of Account Theft on Android-Based Instant Messaging (IM) Applications. *2020 International Workshop on Big Data and Information Security (IWBIS)* (págs. 115-120). IEEE.

Sigelman, O. (August de 2017). Personal cloud-based apps: the new insider risk. *Computer Fraud y Security, 2017*, 10–12.

Singh, R., Chauhan, A. N., y Tewari, H. (2021). Blockchain-Enabled End-to-End Encryption for Instant Messaging Applications. *Cornell University*. Obtenido de https://arxiv.org/abs/2104.08494

Talib, M. A., El Barachi, M. K., y Ormandjieva, O. (2012). Guide to ISO 27001: UAE case study. *Issues in Informing Science and Information Technology, 7*, 331-349.

Valderrama, J. E. (2018). Pentesting "prueba de penetración" para la identificación de vulnerabilidades en la red de computadoras en la Alcaldía del municipio de Cantón del San Pablo, departamento del Chocó (tesis de pregrado). *Universidad Nacional Abierta y a Distancia - UNAD*.

Vivanco, M. V., Benítez, V. H., Moreano, G. V., y Benítez, Á. G. (2019). Evaluación del rendimiento de comunicaciones entre las plataformas Java y. NET utilizando un cifrado híbrido. *Ciencia Digital, 3*(2.6), 141-161.

Xie, M., Wu, Z., y Wang, H. (2012). Secure instant messaging in enterprise-like networks. *Computer Networks, 56*, 448–461.

Yaga, D., Mell, P., Roby, N., y Scarfone, K. (2019). Blockchain technology overview.

Zobal, L., Kolář, D., y Fujdiak, R. (2019). Current State of Honeypots and Deception Strategies in Cybersecurity. *ICUMT*, 1-9.