Estudio analítico referente a usabilidad y seguridad de aplicaciones tecnológicas basadas en software para videoconferencia.

Analytical study on usability and security of technological applications based on videoconferencing software.

David Galarza G[1]. , Alexis Taco C[1]. ,Viviana Flores C[1]. y Jonathan Cahuasqui[2]

[1] Instituto Tecnológico Superior Quito Metropolitano. Carán N3-195 y Calle B (Nueva Tola 2) Quito, Ecuador., dgalarza@itsqmet.edu.ec, agtaco@itsqmet.edu.ec, vflores@itsqmet.edu.ec

[2]Universidad Tecnológica Israel, E4-142, Marieta De Veintimilla y Fco. Pizarro, Quito 170516, jcahuasqui@uisrael.edu.ec

ÉLITE 2020, VOL. (2). NÚM. (1)
ISSN: 2600-5875

Recibido: 11/10/2019
Revisado: 12/11/2019
Aceptado: 17/01/2020
Publicado: 04/04/2020

RESUMEN:

La videoconferencia es una herramienta tecnológica necesaria para cualquier ambiente educativo y social, especialmente utilizado en educación superior. El presente trabajo estudia el software encargado en entregar soluciones de videoconferencia. Esta analítica se realiza a nivel de usabilidad y seguridad, para lo cual es importante medir, desde la perspectiva de usabilidad, los siguientes criterios: accesibilidad, efectividad, eficiencia de uso, facilidad de aprendizaje, retención sobre el tiempo (curva de aprendizaje), tasa de error y satisfacción. Mientras que, desde la perspectiva de seguridad, los criterios a ser evaluados son: disponibilidad, confidencialidad e integridad. Balancear estas características de usabilidad con las de seguridad, conocidos como CIA estas últimas, es el indicador al cual se le prestara mayor atención debido a que la usabilidad es inversamente proporcional a la seguridad. Esta analítica permitirá definir el estado actual de las aplicaciones de videoconferencia más utilizadas identificando cuál de ellas mantiene criterios aceptables referentes a usabilidad y seguridad.

Palabras clave: videoconferencia, tiempo real, usabilidad, seguridad, streaming.

ABSTRACT:

Videoconferencing is a necessary technological tool for any educational and social environment, especially used in higher education. The present work studies the software in charge of delivering video conferencing solutions. This analysis is performed at the usability and security level, for which it is important to measure, from the usability perspective, the following criteria: accessibility, effectiveness, and efficiency of use, ease of learning, retention over time (learning curve), error rate and satisfaction. While, from a security perspective, the criteria to be evaluated are: availability, confidentiality and integrity. Balancing these usability features with security features, known as CIAs the latter, is the indicator that will be given the most attention because usability is inversely proportional to safety. This analysis will define the current status of the most used video conferencing applications, identifying which of them maintains acceptable criteria regarding usability and security.

Keywords: Videoconferencing, real time, usability, security, streaming.

INTRODUCCIÓN:

El software multimedia y audiovisual procesado en tiempo real es compuesto por un conjunto de herramientas que permiten la transmisión en vivo de información utilizando canales de comunicación tecnológicos y/o telemáticos. Este conjunto de herramientas informáticas es mayormente utilizado en educación superior superando medios de comunicación tradicional como el correo electrónico, chats o grupos de chats en aplicaciones que se ejecutan en teléfonos inteligentes, entre otros.

De acuerdo con lo dicho, las nuevas herramientas de video conferencia incorporan características que apoyan al proceso enseñanza-aprendizaje garantizando el esquema académico general, en este sentido, los individuos que interactúan en las plataformas de videoconferencia pueden preparar, compartir y manipular el material didáctico en tiempo real con la finalidad de satisfacer la necesidad de aprender, enseñar, aprender y generar conocimiento y desarrollar habilidades académicas. (Hernández Martín & Olmos Migueláñez, 2011)

El internet es fuente donde se busca y encuentra información de todo tipo ya sea fiable, filtrada, académica o completamente falsa, esta último es la mayoría. Las herramientas de video conferencia entregan información en tiempo real de manera que el individuo que las recibe es testigo de la presentación y creación de conocimiento fiable en ese momento y no solo es receptor de material académico enriquecido, sino también la procesa y puede participar con la finalidad de despejar sus dudas.

Las conferencias de video utilizando canales de internet se han vuelto necesarios y en algunos

casos oficiales para la transmisión de documentación académica, en la mayoría de los casos, considerando que se basa en una comunicación síncrona y bidireccional.

Los sistemas informáticos de video conferencia soportan así también procesos empresariales de manera que sustituyen reuniones o presentaciones deavances o hitos de un proyecto central de acuerdo con el giro del negocio. Por lo que es importante establecer y configurar a nivel de aplicación reglas de manera que la comunicación sea asertiva cumpliendo los objetivos esperados al utilizar las herramientas tecnológicas.

La orientación por excelencia de las videoconferencias ha sido reuniones de negocios, grupos de investigación, conferencias magistrales y un conjunto de intercambio de información profesional, sin embargo, debido a la realidad actual de la presente pandemia, las herramientas decomunicación audio visual en vivo han subido la demanda en ambientes educativos medios y superiores. (Montesinos García, 2011)

El presente estudio propone realizar un análisis de usabilidad y seguridad a las herramientas de videoconferencia considerando que estas dos características son inversamente proporcionales como se presenta en la siguiente formula:

$$S \approx \frac{k}{U}$$

Donde S es el coeficiente de seguridad y U representa a usabilidad.

MARCO CONCEPTUAL

Las conferencias tecnológicas necesitan de toda una arquitectura informática y de telecomunicaciones para poder garantizar la comunicación. Se listan a continuación los elementos esenciales que forman en conjunto los conceptos que rodean al software para videoconferencia.

Internet

Se define al internet como una red informática que utiliza la telemática para transmitir datos e información.

Este criterio de comunicación de información inicia con el proyecto ARPNET en el cual se conectó en una misma red a dos campus universitarios, UCLA y SRI. La necesidad de trasmisión de datos aumentó exponencialmente no solo en la academia si no también en la ciencia donde los científicos de áreas exactas proponen un estándar denominado WWW que facilite la publicación de información relevante para sus investigaciones. (Gonzálvez Vallés, 2011)

Actualmente, se consideran tres etapas dentro de la evolución del internet las cuales se presentan en la siguiente tabla:

Etapa	Detalle
Web 1.0	Páginas web estáticas y con poca interacción con los usuarios. Presentación de información sin interacción desde el proveedor al consumidor.
Web 2.0	Es un ambiente para la creación de conocimiento, generación de contenidos, por lo que las páginas web deben ser dinámicas, usables e interactivas en donde los usuarios socializan información de otros usuarios.
Web 3.0	Ambientes de realidad aumentada, realidad virtual, inteligencia artificial, minería de datos, minería de texto, sociedades virtuales, búsquedas inteligentes, entre otros elementos.

Tabla 1: Evolución del internet. (Elaboración propia).

El internet es el pilar donde se fundamenta el funcionamiento del software para video conferencia.

Texto e hipertexto

Históricamente el texto es el ambiente que permite la transmisión de datos, información y conocimiento por excelencia que perdura a través del tiempo. Otros medios de comunicación como los visuales no han podido superar la trascendencia que el texto impone en la comunicación. (Lamarca Lapuente, 2011)

El hipertexto pretende superar el ecosistema que el texto plantea inicialmente, es por ello que para su difusión es necesario medios informáticos y telemáticos. Al texto sumamente expresivo y ampliamente difundido por medios de telecomunicación se le conoce como hipertexto que en la actualidad se le conoce como hipermedia, es decir, no solo transacciona datos o información en palabras escritas, si no también comunica a través de videos, imágenes en movimiento, interacción hombre máquina, entre otros. (Cantos Gómez et al., 2010)

La necesidad de comunicación en este contexto es de dos vías en las que coexisten la tecnología con la hipermedia, donde los medios informáticos y telemáticos soportan la infraestructura de divulgación informativa la cual sufre constantes cambios y evoluciona de manera exponencial, por lo que los cimientos deben adaptarse a criterios contemporáneos de hardware y software con el fin de garantizar y asegurar el principal objetivo por el cual existe el texto e hipertexto. (Lamarca Lapuente, 2011)

Media y multimedia

La arquitectura tecnológica es base fundamental para transmitir información almacenada, en reposo o en tiempo real, a esta característica se le conoce como media. Mientras que multimedia representa la variedad de canales tecnológicos por los cuales se puede comunicar o difundir información. Así se tiene como representación de multimedia a videos, imágenes, audio, texto, etcétera. (Steinmetz & Nahrstedt, 2011)

Los canales telemáticos facilitan esta transmisión de sistemas, debido a esto es imperioso alinear la infraestructura tecnología a las mejores prácticas para garantizar la difusión de la información. Si el objeto a ser transmitido ocupa más de dos canales de comunicación informática, se debe prestar especial atención a criterios de calidad tales como: usabilidad, disponibilidad, confidencialidad, integridad, concurrencia, entre otros. (Konert, 2015)

La comunicación multimedia es de gran ayuda a la academia ya que su transmisión es lo más cercano a una transmisión de conocimientos de forma presencial.

Sin embargo, conociendo este principio, la multimedia presenta las siguientes desventajas:

- Retroalimentación no puede ser entiempo real.
- Dudas o preguntas deben ser solventadas de forma presencial o consultadas al generador de la información en multimedia o al experto.
- No necesariamente se utiliza un lenguaje inclusivo a momento de transmitir la información.

Es por esto por lo que se debe prestar especial

Streaming de video

Se define al streaming de video como la transferencia usualmente de audio y video en la que el producto es pre procesado antes de ser recibido, así como los videoclips incrustados en páginas web. Ahora bien, se debe conceptualizar las características de archivos de video el cual hace referencia a una secuencia de imágenes fijas denominadas fotogramas. De manera que cuando los fotogramas son reproducidos crean la ilusión de movimiento. ("Video Basics WSA", 2016)

Las características principales de archivos de video se listan a continuación: (“T. Estudiantiles, M. Garc, and J.Oribe”, 2013)

- Tamaño de fotograma
- Relación de aspecto
- Velocidad de fotograma
- Tasa de bits
- Frecuencia de muestre de audio

Existen tres características fundamentales para hacer posible el streaming de video, los cuales se presentan en la tabla 2: (“T. Estudiantiles, M. Garc, and J.Oribe”, 2013)

Característica	Detalle
Métodos de transmisión de video	• Streaming tradicional: descarga y reproducción. • Video streaming: video en vivo • Descarga progresiva
Formatos de streaming de video	• VP9 • High Efficiency Video Coding (HEVC p H.265)
Dispositivos utilizados para la transmisión de streaming	• Smartphones • Smart TV • Computadoras personales y laptops

Tabla 2: Características fundamentales para el streaming de video. (Elaboración propia)

Videollamadas

La videollamada es un derivado de la videoconferencia sumamente necesario en el cual interactúan usuarios que pueden escucharse y verse al mismo tiempo y en vivo. Mientras la video llamada está en ejecución, los usuarios pueden compartir multimedia, así como también tienen la capacidad de compartir elementos de sus dispositivos como la compartición de escritorio o aplicaciones específicas, estas características son heredadas de la videoconferencia.

Para que la videollamada sea posible es necesario software e infraestructura de telecomunicaciones que soporten la transferencia de datos en tiempo real. En la actualidad, la mayoría de las aplicaciones de mensajería instantánea tiene

incorporado software de videollamada con el fin de agregar características de comunicación digital a las soluciones informáticas. Cuevas (Valencia, Rene & Añorve, Ana, 2013).

Los metadatos de audio y video son entregados de un usuario a otro dependiendo de su disponibilidad en una red local o en internet, si existe disponibilidad, el flujo de datos se envía directamente sin necesidad de pasar a través del servidor. En este caso, el servidor se encarga de viabilizar la conexión entre usuarios más no del envío de los metadatos que forman la videollamada.

Las diferencias que existen entre videoconferencia y videollamada como tal, se listan a continuación:

- La limitación de usuarios en la videollamada.
- La calidad del streaming es superior para la videoconferencia.
- La videollamada sugiere reuniones breves y semiformales, es por tal motivo que el software tiene ese comportamiento

Video conferencia

La videoconferencia es una tecnología contemporánea que entrega a los usuarios un conjunto de sistemas de comunicación digital bidireccional de video, audio, datos e información manteniendo una transacción simultanea e interactiva en tiempo real. Para garantizar el funcionamiento de esta solución tecnológica, la videoconferencia necesita de equipos especializados a nivel de hardware y software.

El objetivo principal de esta metodología tecnológica de comunicación en tiempo real es la compartición de información, intercambiar opiniones, crear, manipular y generar documentación en tiempo real con la participación de todos los involucrados si así lo necesitase la reunión, entre otras actividades. (Cabero Almenara, 2011)

La videoconferencia es efectiva siempre que se cumplan con los siguientes parámetros:

- Verificar si se cuenta con el software y hardware mínimo para realizar la video conferencia.
- Verificar los periféricos de audio y video para ser utilizados mientras dure la videoconferencia
- Verificar el número de participantes
- Verificar el tiempo de duración
- Configurar el software de videoconferencia luego de haber conocido el número de participantes y el tiempo

En la actualidad, existe diversas soluciones para videoconferencia las cuales soportan con los criterios mínimos para lograr una reunión digital efectiva.

Software para video conferencia

El software orientado a videoconferencia hace referencia al conjunto de sistemas informáticos que fueron diseñados para entregar las características definidas de las reuniones tele presenciales, entre los cuales tenemos empresas como: (Vidal Martínez & Camarena Gómez, 2017)

- Cisco
- Microsoft
- Zoom
- LogMein
- Google
- Adobe
- Huawei
- Enghouse Systems (Vidyo)
- TrueConf
- PGi
- Avaya
- ZTE
- Pexip
- BlueJeans
- StartLeaf
- Lifesize

Las soluciones de videoconferencia más destacadas según Gartner se presentan a continuación en la figura 1

Figure 1: Cuadrante mágico de video conferencias. (Gartner, 2019)

De acuerdo con Gartner, las soluciones de videoconferencia más utilizadas son las entregadas por Cisco, Microsoft y Zoom.

Método

Para cuantificar la usabilidad y seguridad del software para video conferencia, fue necesaria incorporar herramientas que permitan gestionar e interpretar información.

Con el objetivo de medir la usabilidad, se han aplicado encuestas con las siguientes características:

- Número de estudiantes matriculados a los que se realizó la encuesta.
- Institución educativa de los estudiantes encuestados.
- Medición de usabilidad
- Medición de eficiencia
- Medición de accesibilidad
- Medición de efectividad

Se ha revisado literatura e investigaciones relacionadas a la seguridad en software de videoconferencia con el objetivo de contrastar esta información con el enfoque del presente trabajo.

Usabilidad

La usabilidad se refiere a la capacidad de un software de ser comprendido, aprendido, usado y ser atractivo para el usuario, en condiciones específicas de uso. Esta definición hace énfasis en los atributos internos y externos del producto, los cuales contribuyen a su funcionalidad y eficiencia. En este contexto, se ha considerado varios parámetros, los cuales son explicados a continuación:

- **Accesibilidad**

Accesibilidad de un software representa una característica con la cual cualquier persona independientemente de su condición física, social o económica pueda acceder a este software de video conferencia.

- **Eficiencia**

Eficiencia. Esta característica principal se refiere a la facilidad con la cual un usuario puede interactuar con otro usuario, para esta investigación sería para la interacción profesor - alumno.

- **Efectividad**

Efectividad de un software de videoconferencia a la rapidez con la cual el software reacciona a interacciones como encendido o apagado de micrófono y cámara o compartimiento de pantalla o archivos multimedia.

- **Seguridad**

El software para videoconferencia ofrece muchas ventajas, sin embargo, necesita cumplir con parámetros de seguridad que garanticen la confidencialidad, integridad y disponibilidad.

Common Vulnerabilities and Exposures CVE, es un habiente en línea que ofrece estadísticas en tiempo real de vulnerabilidades encontradas en diversas aplicaciones. Se ha utilizado esta herramienta para identificar las debilidades de seguridad presentes en los sistemas de software para video conferencia. (Common Vulnerabilities and Exposures, 2020). A continuación, se analiza cada elemento del CIA por herramienta más utilizada según Gartner.

Microsoft Teams

La siguiente tabla presenta las vulnerabilidades encontradas en el sistema para videoconferencia entregado por Microsoft ordenado por la calificación adquirida donde 10 es el puntaje más alto en vulnerabilidad y 0 el más bajo, es decir, no presenta vulnerabilidad.

CVE ID	Puntaje	Conf.	Integ.	Dispo.
CVE-2019-0971	9.0	Completo	Completo	Completo
CVE-2019-1072	7.5	Parcial	Parcial	Parcial
CVE-2019-1306	7.5	Parcial	Parcial	Parcial

Tabla 3: Puntaje de seguridad de Teams según CVE. (Elaboración propia)

Donde los ID de CVE tienen los siguientes significados:

- CVE-2019-0971: Existe una vulnerabilidad de divulgación de información cuando Azure DevOps Server y Microsoft Team Foundation Server no desinfectan adecuadamente una solicitud de autenticación especialmente diseñada para un servidor afectado, también conocido como 'Azure DevOps Server y Team Foundation Server Information Vulnerability'.

- CVE-2019-1072: Existe una vulnerabilidad de ejecución remota de código cuando Azure DevOps Server y Team Foundation Server (TFS) manejan incorrectamente la entrada del usuario, también conocido como 'Azure DevOps Server y Team Foundation Server Vulnerabilidad de ejecución remota de código'.
- CVE-2019-1306: Existe una vulnerabilidad de ejecución remota de código cuando Azure DevOps Server (ADO) y Team Foundation Server (TFS) no pueden validar la entrada correctamente, también conocido como 'Azure DevOps y Team Foundation Server Remote Code Execution Vulnerability'.

Cisco Webex

Las vulnerabilidades encontradas por CVE se presentan en la siguiente tabla:

CVE ID	Puntaje	Conf.	Integ.	Dispo.
CVE-2019-1939	9.3	Completo	Completo	Completo
CVE-2019-1636	9.3	Completo	Completo	Completo

Tabla 4: Puntaje de seguridad de Cisco Webex según CVE. (Elaboración propia)

Los ID propuestos y evaluados por CVE se detallan a continuación:

CVE-2019-1939: Una vulnerabilidad en el cliente Cisco Webex Teams para Windows podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en un sistema afectado. Esta vulnerabilidad se debe a restricciones inadecuadas en las funciones de registro de software utilizadas por la aplicación en los sistemas operativos Windows. Un atacante podría explotar esta vulnerabilidad al convencer a un usuario objetivo de que visite un sitio web diseñado para enviar información maliciosa a la aplicación afectada. Una explotación exitosa podría permitir que el atacante haga que la aplicación modifique archivos y ejecute comandos arbitrarios en el sistema con los privilegios del usuario objetivo.

CVE-2019-1636: Una vulnerabilidad en el cliente de Cisco Webex Teams, anteriormente Cisco Spark, podría permitir que un atacante ejecute comandos arbitrarios en un sistema de destino. Esta vulnerabilidad se debe a las rutas de búsqueda inseguras utilizadas por el URI de la aplicación que se define en los sistemas operativos Windows. Un atacante podría explotar esta vulnerabilidad al convencer a un usuario objetivo de que siga un enlace malicioso. La explotación exitosa podría hacer que la aplicación cargue bibliotecas desde el directorio al que apunta el enlace URI. El atacante podría usar este comportamiento para ejecutar comandos arbitrarios en el sistema con los privilegios del usuario objetivo si el atacante puede colocar una biblioteca diseñada en un directorio que sea accesible para el sistema vulnerable.

Zoom

CVE presenta un listado de vulnerabilidades presentadas en la siguiente tabla:

CVE ID	Puntaje	Conf.	Integ.	Dispo.
CVE-2004-0680	10	Completo	Completo	Completo
CVE-2018-15715	7.5	Parcial	Parcial	Parcial
CVE-2019-13567	6.8	Parcial	Parcial	Parcial

Tabla 5: Puntaje de seguridad referente a Zoom según CVE. (elaboración propia)

Los ID establecidos por CVE para evidenciar las debilidades informáticas en Zoom se describen a continuación:

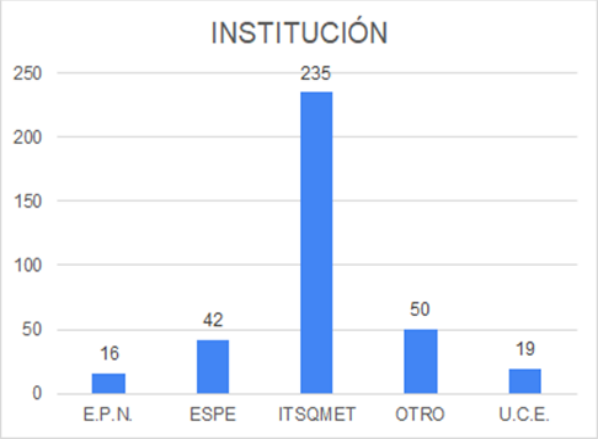
- CVE-2004-0680: El módem ADSL Zoom X3 tiene un terminal que se ejecuta en el puerto 254 al que se puede acceder utilizando la contraseña de administración HTML predeterminada, incluso si la contraseña se ha cambiado para la interfaz HTTP, lo que podría permitir a los atacantes remotos obtener acceso no autorizado.
- CVE-2018-15715: Los clientes de zoom en Windows (antes de la versión 4.1.34814.1119), Mac OS (antes de la versión 4.1.34801.1116) y Linux (2.4.129780.0915 y posteriores) son vulnerables al procesamiento de mensajes no autorizados. Un atacante remoto no autenticado puede falsificar mensajes UDP de un asistente a la reunión o un servidor Zoom para invocar la funcionalidad en el cliente objetivo. Esto permite al atacante eliminar a los asistentes de las reuniones, falsificar mensajes de los usuarios o secuestrar pantallas compartidas.
- CVE-2019-13567: Zoom Client antes de 4.4.53932.0709 en macOS permite la ejecución remota de código, una vulnerabilidad diferente a CVE-2019- 13450. Si el demonio ZoomOpener (también conocido como el servidor web oculto) se está ejecutando, pero el Cliente Zoom no está instalado o no se puede abrir, un atacante puede ejecutar código de forma remota con una URL de inicio creada con fines malintencionados. NOTA: ZoomOpener es eliminado por la Herramienta de eliminación de malware de Apple (MRT) si esta herramienta está habilitada y tiene el MRTConfigData 2019- 07-10.

DISCUSIÓN DE RESULTADOS:

Para la presente investigación se realizó una encuesta que evalúe a estudiantes de varias instituciones educativas acerca de su preferencia en cuestión a los softwares de videoconferencia utilizados.

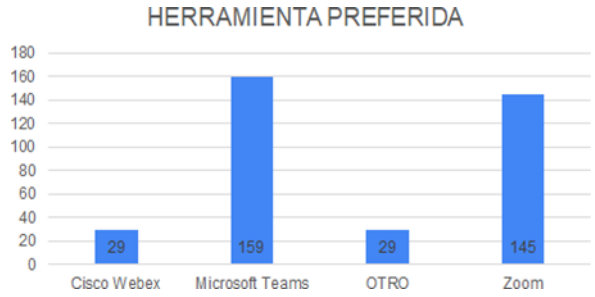
Las principales herramientas analizadas son Microsoft Teams, Cisco Webex y Zoom.

Se realizó la encuesta a 362 personas de distintos institutos de educación superior y universidades, distribuidos de la siguiente manera como se muestra en la figura 3:



Herramienta de videoconferencia

Una vez realizada la encuesta, la cual tenía entre sus primeras preguntas "¿Cuál de estas herramientas prefiere usted para realizar una videoconferencia?" se obtuvo los siguientes resultados:



Como se puede observar en la figura 4, la opción preferida por los estudiantes para realizar videoconferencia es Microsoft Teams con un 43.8% de los votos seguido por Zoo, con el 39.9%.

Usabilidad

La pregunta hecha a los encuestados fue la siguiente:

"La usabilidad se refiere a la capacidad de un software de ser comprendido En cuestión de usabilidad, ¿cuál de los considera que es más usable?"

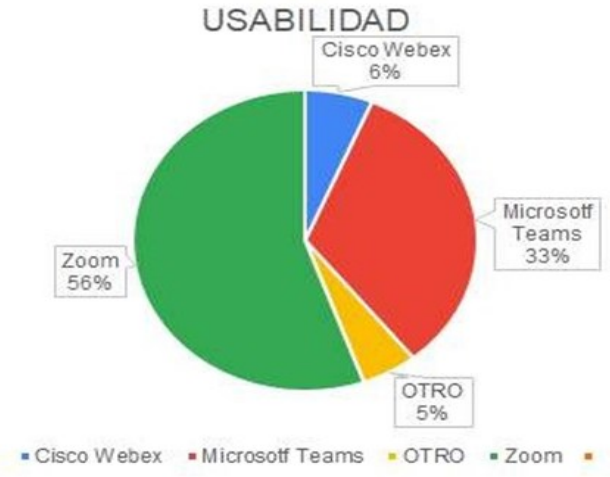


Figure 5. Gráfico de Pastel. Usabilidad de los softwares de videoconferencia.

El software más usable según los estudiantes encuestados es Zoom con un 56% seguido de Microsoft Teams con un 33%.

Accesibilidad

La pregunta realizada a los estudiantes fue:

"Accesibilidad de un software representa una característica con la cual cualquier persona independientemente de su condición física, social o económica pueda acceder a este software de video conferencia. En este contexto ¿Cuál considera usted que es el software de videoconferencia que es más accesible?"

Pregunta que arrojó los siguientes resultados al realizar la encuesta a los 362 estudiantes:

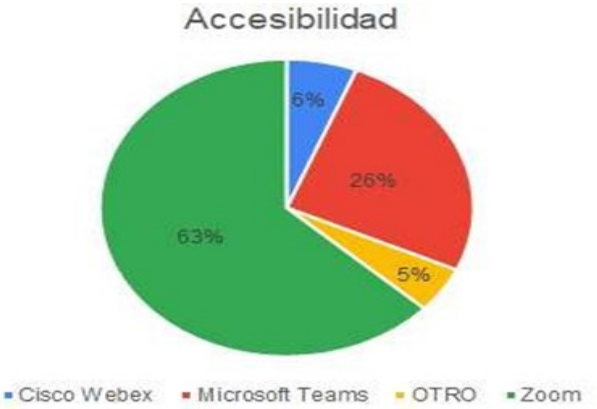


Figure 6. Gráfico de Pastel. Accesibilidad de los softwares de videoconferencia.

Como se puede observar en el gráfico de Pastel, el software más accesible a consideración de los estudiantes encuestados es Zoom con un 63% de preferencia, seguido de Microsoft Teams con un 26% de preferencia.

Eficiencia

La pregunta hecha a los encuestados fue la siguiente:

"Eficiencia. Esta característica principal se refiere a la facilidad con la cual usted puede interactuar con el usuario, en este caso la interacción profesor

- alumno. En este contexto, ¿cuál considera usted que es el software de videoconferencia más eficiente?"

Figure 7. Gráfico de Pastel. Eficiencia de los softwares de videoconferencia.

En cuestión de Eficiencia, el preferido vuelve a ser Zoom, con un 48% vs un 39% de MicrosoftTeams

Efectividad

La pregunta hecha a los encuestados fue la siguiente:

"Efectividad de un software de videoconferencia a la rapidez con la cual el software reacciona a interacciones como encendido o apagado de micrófono y cámara o compartimiento de pantalla o archivos multimedia. ¿En este contexto, cuál considera usted que es el software más efectivo?"

Figure 8. Gráfico de Pastel. Efectividad de los softwares de videoconferencia

En esta pregunta, según la experiencia de los encuestados, el software de videoconferencia que presenta una mayor efectividad es el de Zoom con un 46%, vs Microsoft Teams que lo sigue con un 40%.

Cuantificación

.Los encuestados, evaluaron cada uno de los softwares de videoconferencia (Microsoft Teams, Cisco Webex y Zoom), con la siguiente escala:

- Extremadamente bueno: 10 puntos
- Muy bueno: 8 puntos
- Bueno: 5 puntos
- Nada malo: 3 puntos
- Malo: 0 puntos.

Arrojando para las 362 personas encuestadas, los resultados mostrados en la siguiente tabla:

	VOTOS		
CALIFICACION	ZOOM	CISCO	TEAMS
EXTREMADAMENTE BUENO	40	30	66
MUY BUENO	193	126	171
BUENO	101	168	106
NADA MALO	21	25	13
MALO	7	13	6
TOTAL, DE VOTOS	362	362	362

Tabla 6: Cuantificación de los softwares de videoconferencia, según la encuesta realizada.

Los puntos obtenidos por cada software de videoconferencia son los siguientes:

ZOOM	2512
CISCO	2223
TEAMS	2597

Tabla 7: Cuantificación de los softwares de videoconferencia, según la encuesta realizada.

Obteniendo un promedio sobre 10 puntos de:

	PROMEDIO
ZOOM	6,94
CISCO	6,14
TEAMS	7,17

Tabla 8: Cuantificación de los softwares de videoconferencia, según la encuesta realizada.

Resultado mostrado en la siguiente figura:

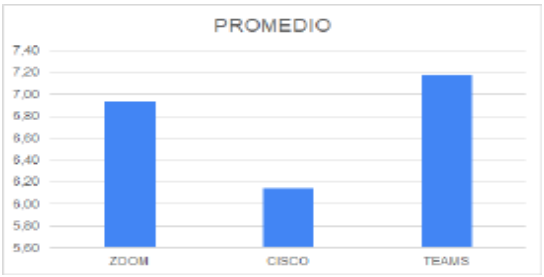


Figure 9: Promedio de puntuación para cada software según la encuesta realizada.

Con lo cual se puede concluir que a pesar de que se ha establecido que para el usuario, aunque el software Zoom sea considerado más usable en cuanto a efectividad, fiabilidad y eficiencia; al momento de cuantificar cada uno de los programas, el ganador con mejor puntuación es Microsoft Teams.

4.7. Recomendación de encuesta

Se realizó la siguiente pregunta: ¿Cuál de las tres plataformas recomendaría para videoconferencia?, obteniendo los siguientes resultados:

Figure 10: Software recomendado para realizar videoconferencia según los estudiantes encuestados.

DISCUSIÓN DE RESULTADOS:

A continuación, se presentan los resultados obtenidos al analizar la seguridad de los sistemas Teams, Webex y Zomm para video conferencia.

Los resultados de Microsoft Teams con respecto a las debilidades de seguridad encontradas en el software para videoconferencia, evidencian que una de las vulnerabilidades tiene un puntaje 9, mientras que dos de ellas tienen

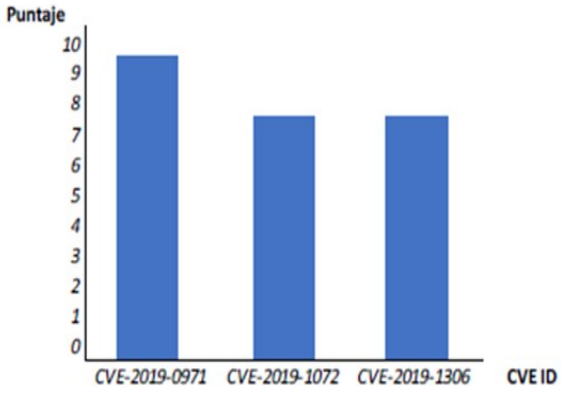


Figure 11: Resultados del puntaje de vulnerabilidades Microsoft Teams. (Elaboración propia)

Mientras que los resultados de Cisco Webex referente a las debilidades de seguridad encontradas en el software orientado a videoconferencia, evidencian que dos de las vulnerabilidades tienen puntaje 9.3, lo que se interpreta es que el sistema de videoconferencia es vulnerable si se ejecutan los vectores de ataque recomendados por los ID CVE (descritos en el capítulo anterior), como muestra la siguiente imagen:

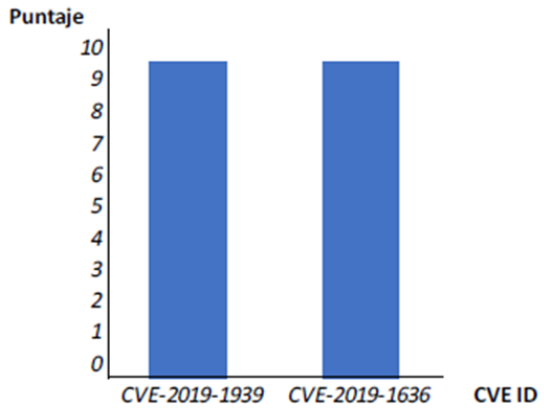


Figure 12: Resultados del puntaje de vulnerabilidades Cisco Webex. (Elaboración propia)

Finalmente, los resultados de Zoom con respecto a las debilidades de seguridad encontradas en el software para videoconferencia, evidencian que una de las vulnerabilidades tienen un puntaje 10, lo cual es el máximo puntaje para una debilidad de seguridad, mientras que dos de ellas tienen puntaje 7.5 y 6.8, lo que sugiere que el sistema de videoconferencia es vulnerable si se ejecutan los vectores de ataque recomendados por los ID CVE (descritos en el capítulo anterior), como muestra la siguiente imagen:

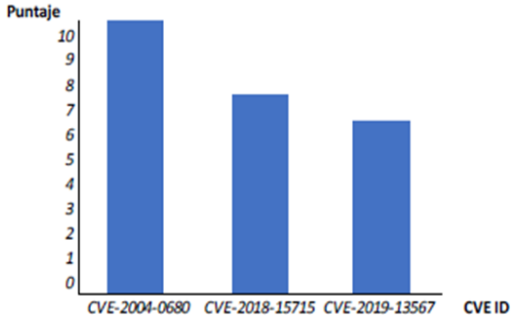


Figure 13: Resultados del puntaje de vulnerabilidades Zoom. (Elaboración propia)

Los sistemas para video conferencia sometidos a evaluación de seguridad informática presentaron vulnerabilidades las cuales pueden ser explotadas ejecutando vectores de ataques.

CONCLUSIONES:

- Los sistemas de video conferencia tienen al menos una vulnerabilidad critica, la cual puede derivar en ataques informáticos generando captura de información o perdida de esta.
- Los ataques para explotar las vulnerabilidades encontradas en los sistemas para video conferencia deben ser ejecutados utilizando los vectores de ataque sugeridos, sin embargo, para lanzar estos vectores de ataque se requiere alto conocimiento informático.
- Algunas de las vulnerabilidades presentadas involucran al individuo como eje fundamental que permitirá ejecutar los vectores de ataque afectando directamente al software de video conferencia.
- Según las encuestas realizadas a estudiantes de varias instituciones de educación superior, su preferencia y recomendación para un software de videoconferencia, es principalmente Zoom y Microsoft Teams.
- En cuanto a Usabilidad, Efectividad, Eficiencia, y Accesibilidad, a consideración de los encuestados, la muestra de estudiantes tiene una preferencia por Zoom, es decir se sienten más cómodos utilizando dicha herramienta, a pesar de que como se mostró en el análisis de vulnerabilidad Zoom es más vulnerable ante vectores de ataque cibernético.
- Según las encuestas realizadas, también se puede concluir que al momento de calificar los softwares de videoconferencia de una manera cuantitativa y cualitativa, el software acreedor a una mejor puntuación es Microsoft Teams, a pesar de que en otras preguntas realizadas a los encuestados, se sentían más cómodos utilizando Zoom.

REFERENCIAS BIBLIOGRAFÍCAS:

1. Cabero Almenara, J. (2011). Nuevas tecnologías enla formación flexible y a distancia. Universidad de Sevilla.

2. Cantos Gómez, P., Martínez Méndez, F., & Moya Martínez, G. (2010). Hipertexto y documentación. Universidad.

3. Common Vulnerabilities and Exposures (2020).CVE security vulnerability database. Security vulnerabilities, exploits, references and more. Retrieved 17 June 2020, from https://www.cvedetails.com/.

4. Cuevas Valencia, Rene & Añorve, Ana. (2013). Herramientas de videoconferencia aplicadas en la educación en nivel superior. Tesis pregrado.

5. Gonzálvez Vallés, J. (2011). La Web 2.0 y 3.0 en su relación con el EEES. Visión Libros.

6. Hernández Martín, A., & Olmos Migueláñez, S. (2011). Metodologías de aprendizaje colaborativo a través de las tecnologías.Ediciones Universidad de Salamanca.

7. Konert, J. (2015). Interactive Multimedia Learning. Springer International Publishing.

8. Lamarca Lapuente, M. (2011). Del texto al hipertexto. Hipertexto.info. Retrieved 10 June 2020, from http://www.hipertexto.info/documentos/text_ hipertex.htm.

9. Montesinos García, A. (2011). La Videoconferencia como instrumento probatorio en el proceso penal. Marcial Pons.

10. Steinmetz, R., & Nahrstedt, K. (2011). Multimedia fundamentals. PHI Learning.

11. Estudiantiles, M. Garc, and J.Oribe, La realidad actual del streaming de video. El streaming tradicional vs alternativas actuales, pp. 285–297, 2013.

12. Vidal Martínez, A., & Camarena Gómez, B. (2017). Evolución y análisis de una experiencia de utilización de videoconferencia de sala y de escritorio. Retrieved 15 June 2020, from http://dx.doi.org/10.12795/pixelbit.2015.i47.0 4.

13. Video Basics WSA. Wsa.wikidot.com. (2016). Retrieved 15 June 2020, from http://wsa.wikidot.com/tbm:video-basics.