RIESGOS DE SEGURIDAD DE LA INFORMACIÓN QUE SE PRESENTAN AL USAR HERRAMIENTAS INFORMÁTICAS PARA EL DESARROLLO DE CLASES VIRTUALES POR PARTE DE DOCENTES Y ESTUDIANTES EN COLOMBIA.

HENRRY HARVEY HEREDIA NORIEGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO
2021

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN QUE SE PRESENTAN AL USAR HERRAMIENTAS INFORMÁTICAS PARA EL DESARROLLO DE CLASES VIRTUALES POR PARTE DE DOCENTES Y ESTUDIANTES EN COLOMBIA

HENRRY HARVEY HEREDIA NORIEGA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Yolima Mercado
Tutora de Curso
Katerine Márceles
Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO
2021

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Sincelejo., 31 Mayo 2022

DEDICATORIA

“Esta monografía esta dedica a mi hijo, que con las ganas de proporcionarle una mejor calidad de vida y que tenga un contesto mejor en su entorno, nos embarga la motivación de seguir adelante en los estudios académicos realizados en la preparación cada día de ser un mejor profesional preparado con calidad.

A mi madre que siempre ha sido uno de los motores de logros, para que sienta orgullo de sus hijos.”

AGRADECIMIENTOS

“Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.”

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

GLOSARIO

ACCESO: Se puede definir con la entrada para llegar a un lugar.

AMENAZAS: Es una acción donde se pone en peligro a una persona o un grupo en común, su lugar y ambiente.

AMENAZAS INFORMATICA: Es considerado un riesgo alto que está expuesto un individuo u organización a sufrir perdida de datos, daños o pérdida irrecuperable en sus sistemas de información.

ALUMNO: Es el individuo que está dedicada al aprendizaje por medio de un guía o tutor.

ATAQUE INFORMANTICO: Son los intentos que realiza un ciberdelincuentes al querer ingresar a una infraestructura de red por medio de medios digitales por medio de software maliciosos, ya sean virus, malware, troyanos, entre otros.

CÓDIGO MALICIOSO: Son códigos informáticos diseñados para crear vulnerabilidades en los sistemas permitiendo así la creación de puertas traseras, robo de datos y otros daños potenciales en los archivos y recursos informáticos.

CONFINAMIENTO: El término hace referencia de un aislamiento temporal en una población por eventos de salud o seguridad.

COVID-19: Es una enfermedad infecciosa que es causada por el coronavirus, que es una familia de virus que afecta las vías respiratorias.

DELITO INFORMÁTICO: Ciberdelito son acciones que van en contra de la leyes y normatividad que se realiza en los entornos informáticos o digitales, se considera delito informático a los ataques a los sistemas informáticos de personas o de entidades públicas o privadas que se ven afectadas por la sustracción de datos o intromisión a sus redes de computadoras sin autorización.

DIRECCIÓN MAC (MEDIA ACCESS CONTROL): Es el identificador único de un dispositivo de hardware de red que el fabricante asigna.

DOCENTE: Es una persona capaz de dirigir y guiar por medio de acciones encaminadas a la enseñanza a un grupo de individuos (alumnos o estudiantes) en temas específicos.

EDUCACIÓN: Es la formación impartida a un individuo para desarrollar sus capacidades morales, intelectuales y académicas con respecto a su costumbre, cultura y normas de convivencias establecidas por su comunidad.

E-LEARNIG: Es un término que se usa para referirnos al aprendizaje y enseñanza que se recibe de manera online, es decir por medio de internet y la utilización de la tecnología.

Que también se puede conocer como educación virtual, tele formación, formación a distancia o formación online.

INTRUSO INFORMATICO: Se puede considerar a una persona que ingresa sin autorización a una red de computadores o un aplicativo, script, archivo malicioso en una computadoras o red implantado con un fin lucrativo o para hacer algún daño.

INSTITUCIÓN EDUCATIVA: Una institución educativa es una organización formalmente constituida y conformada por grupos de alumnos, profesores y administradores que dirigen el proceso. En caminada a la formación de seres para el mañana de una sociedad bajo principios y valores.

KASPERSKY: Es una compañía internacional que se dedica a la seguridad informática, uno de sus productos destacados en Kaspersky antivirus que se convierte en una utilidad necesaria para los equipos de cómputos y la gran mayoría de dispositivos tecnológicos como servidores, *PCs* (Computadoras personales), *tablet*s, portátiles, entre otros.

MITIGAR: Es un verbo que se refiere o hace referencia a minimizar algo.

RAT (TROYANOS DE ACCESO REMOTO): Son aquellas aplicaciones que al parecer son originales o legales pero que en su estructura poseen malware que se pueden descargar en un dispositivo de manera involuntaria, una vez en el dispositivo el delincuente informantico puede tener control sobre el dispositivo ya infectado.

PANDEMIA: Es una epidemia que se extiende a nivel global ocasionada por una enfermedad infecciosa afectando gran parte de la población mundial.

PLATAFORMA VIRTUAL: Son aplicaciones o programas en internet que en el ámbito educativo es posible el desarrollo de cursos, módulos y material didáctico para el aprendizaje a distancia que pueda llegar a cualquier lugar.

RIESGOS: El riesgo consiste en la probabilidad que una amenaza llegue a convertiste en un desastre.

RIESGO INFORMÁTICO: Los riesgos informáticos son las diferentes exposiciones que pueden sufrir un individuo u organización como atentados y amenazas a su red o sistemas informáticos.

SEGURIDAD DE LA INFORMACIÓN: Son las diferentes medidas de prevención y de reacción de una organización para protegerse de ataques informáticos y resguardar los activos lógicos.

SITIO WEB: Conocido también como Portal Web es un conjunto de páginas web que están relacionadas en un dominio de internet dentro de la *World Wide Web*.

TIC (TECNOLOGIA DE LA INFORMACION Y LAS COMUNICACIONES): Son el conjunto de herramientas y recursos informáticos que permite poder realizar proceso complejos informáticos para poder obtener la trasmisión de la información.

TRAFICO DE RED: El término hace referencia a los datos que viajan o se transportan por una red de datos en un determinado. Cada uno de esos datos está dado por paquetes que son las unidades más pequeñas de datos trasmitida por la red.

VIDEOLLAMADAS: Son videoconferencia que se realizan por medio de una aplicación informática la cual consta de la interacción de dos o más usuarios que mantienen una comunicación sincrónica por voz o video.

VIRUS INFORMATICO: son segmentos de código que pueden infectar un sistema informático o una aplicación después que cumplan con alguna condición lógica o temporal.

VULNERABILIDAD: Se puede decir que es una combinación entre los riesgos y amenazad consistente las debilidades y exposiciones de su infraestructura que puede aprovechar un delincuente.

RESUMEN

Para el año 2020 a mediados del mes de marzo, Colombia comienza con el confinamiento a causa de la pandemia que es ocasionado por el virus *SARS-COV-2* y se hace necesario que los colegios, universidades, jardines, entre otros entes educativos se vieran en la necesidad de optar por la educación virtual y mediadas por las Tecnologías de la información y la comunicación (*TIC*), generando un cambio en la forma de impartir las clases, es así que tanto alumnos como docentes convierten salones de clases en aulas guiadas por la tecnología, utilizando las diferentes herramientas existentes en el mercado, tanto privativas como de libre acceso.

Los riesgos y amenazas a la seguridad informática en el año 2020 aumento considerablemente por la alta demanda de conectividad, en todos los sectores económicos. Las instituciones educativas se vieron enfrentadas a este fenómeno sin una preparación previa, tanto alumnos como docentes fueron enviados a sus viviendas para realizar sus actividades académicas interactuando aún más con los medios tecnológicos. Con esta monografía se busca generar recomendaciones para las buenas prácticas de seguridad informática permitiendo así poder salvaguardar la confidencialidad, disponibilidad e integridad de su información.

ABSTRACT

For the year 2020 in the middle of March, Colombia begins with the confinement due to the pandemic that is caused by the SARS-COV-2 virus and it is necessary for schools, universities, gardens, among other educational entities to see in the need to opt for virtual education and mediated by Information and Communication Technologies (TIC), generating a change in the way of teaching classes, so that both students and teachers convert classrooms into classrooms guided by technology, using the different tools on the market, both proprietary and freely accessible.

The risks and threats to computer security in 2020 increased considerably due to the high demand for connectivity, in all economic sectors. Educational institutions were faced with this phenomenon without prior preparation, both students and teachers were sent to their homes to carry out their academic activities, interacting even more with technological means. This monograph seeks to generate recommendations for good computer security practices, thus allowing to safeguard the confidentiality, availability and integrity of your information.

INTRODUCCIÓN

El virus *SARS-CoV-2* conocido por muchos como *COVID19* o Coronavirus, presente desde principios del año 2020 en todo el mundo y por cual la OMS (Organización mundial de la Salud) declaro pandemia, cambio el entorno y sectores económicos de manera inesperada.

Colombia comienza a registrar sus primeros pacientes infectados por coronavirus a principios del mes de marzo de 2020[1] y comienzan las alertas por las consecuencias ocasionadas en otros países orientales y occidentales. Los procesos de mitigación se hacen presentes y en muchos de estos países optan por un confinamiento en sus viviendas y todo tipo de restricciones para realizar actividades cotidianas, entre esas ir a las aulas de clases. Es así que Colombia al igual que muchos países opta por trasladar su educación a las casas guiada por la tecnología, la utilización de clases virtuales, plataformas educativas, herramientas interactivas, Videollamadas, mensajería instantánea, entre otros recursos tecnológicos que hicieran fácil el cumplimiento de la calidad de la educación en Colombia.

A las anomalías de la vida cotidiana y situaciones de todos los sectores económicos, también se suman ambientes nuevos de producción y la forma de realizar delitos, aparecen con mayor asiduo los ciberdelincuentes aprovechando la conexión a internet casi que total en la vida de las personas. Por medio de los celulares, *Tablet* y computadores se inicia una nueva forma de realizar actividades diarias como son las clases virtuales incluyendo desde los más chicos hasta los más grandes. Es enfrentarse a cambios inesperados ahora en una realidad sometida por un ciberespacio inhóspito de las cuales muchas personas tienen poco conocimiento de las amenazas que podían enfrentar y las herramientas apropiadas para combatirlas. Robo de identidad, clonación de páginas web, robo de información financiera, ingresos abusivos, *ciberbullying*, *sexting* entre otros delitos contemplados en la ley colombiana 1273 de 2009, comenzaron hacer más visibles en tiempos de confinamiento preventivo.

Los ciberdelincuentes aprovechan entonces las fallas de las aplicaciones e incauto actuar de las personas al momento de usar las *TIC* (Tecnologías de la Información y la Comunicación). El desconocimiento en muchas ocasiones de los usuarios finales, los convierte en la mayor vulnerabilidad para la seguridad de la información en cualquier entorno sea para una empresa o para una institución educativa.

[1] Minsalud.gov.co. [Sitio Web]. Colombia confirma su primer caso de COVID-19. [Consulta 21 septiembre 2021]. Disponible en:https://www.minsalud.gov.co/Paginas/Colombia-confirma-su-primer-caso-de-COVID-19.aspx

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La educación en tiempo de pandemia ocasionada por el virus del *COVID-19*, condujo a los colegios a migrar sus clases presenciales a la utilización de las *TIC* (tecnologías de la información y la comunicación) y al mismo tiempo generó que los niños, jóvenes y adultos se vieran en la necesidad de trasladar las clases presenciales a aulas virtuales guiadas por la tecnología. Con la ayuda del internet y herramientas informáticas, como plataformas educativas, programa para video conferencia, entre otras, han sido utilizadas para mitigar el impacto de trabajar desde casa. Los riegos en la educación al momento de navegar, buscar y compartir contenido ha sido uno de los talones de Aquiles de este nuevo proceso. Los delincuentes toman este momento como una oportunidad para poder realizar sus delitos, cambiando un poco su manera de operar, ya que también utilizan la tecnología para realizar actos en contra de los usuarios.

Existen reportes de sucesos sobre estudiantes que les hayan tenido que suspender la clase virtual por intromisión de personas compartiendo contenido sexual en las trasmisiones en vivo[2]. Los más pequeños como niños de nueve a diez años son los más propensos a estar visitando sitios web diferentes a las clases, tales como contenido de explotación sexual.

La normatividad colombiana castiga este tipo de actos indebidos mediante la ley 1273 de 2009, la cual modifica el código penal. Que refiere sobre la protección de la información y de los datos[3].

El aumento de ciberdelito estará en constante auge vertiginoso a medica que las personas no tomen conciencia de los riesgos que pueden existir y que puedan afectar su vida cotidiana.

[2] Elpais.com.co. [Sitio Web]. Trabajo y clases virtuales son blancos de los ciberdelincuentes. [Consulta 1 marzo 2021]. Disponible en: https://www.elpais.com.co/judicial/trabajo-y-clases-virtuales-son-blanco-de-los-ciberdelincuentes.html.
[3] Secretariasenado.gov.co. [Sitio Web]. Ley 1273 De 2009. [Consulta 1 marzo 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

1.2 FORMULACIÓN DEL PROBLEMA

En Colombia con la aparición del coronavirus *SARS-CoV-2*, los sectores económicos se vieron en la obligación de cambiar su forma de producción generando nuevas formas e intentando conservar las ya existentes. Es así que el gobierno nacional decreto confinamiento y hubo la necesidad de realizar teletrabajo y en el sector educativo realizar las clases virtuales. Esta nueva normalidad trajo consigo un aumento considerable en el uso de los recursos tecnológico y del internet como base fundamental para el trabajo desde casa. Las clases virtuales también forman parte de esta normalidad inesperada, con los diferentes riesgos existentes en el ciberespacio.

¿Cómo mitigar los riesgos y amenazas a las que se enfrentan docentes y alumnos al momento de utilizar herramientas informáticas como plataformas y videoconferencia para el desarrollo de clases virtuales?

2 JUSTIFICACIÓN

La protección de los datos personales se convierte en una necesidad que surge al mismo tiempo que la navegación por internet y la utilización de herramientas informáticas en línea o en la nube se hacen cada vez más necesaria en nuestro cotidiano vivir. En Colombia para el año 2020 a mediados del mes de marzo se comenzó a vivir el confinamiento por parte de la pandemia a nivel mundial generada por el virus *COVID-19*[4], esto ocasiono que la economía de los países cambiara mucho y la forma de realizar los trabajos y estudios. Entre estos sectores afectados fue el educativo, en Colombia la educación virtual ha tenido un gran crecimiento debido a que obligatoriamente ha sido utilizada como consecuencias de la pandemia.

Al momento de navegar en internet e ingresar a clases virtuales y utilizar las herramientas informáticas tanto por los docentes como los estudiantes, se exponen a riesgos informáticas, sin tener recomendaciones previas de navegación. Es por ello la importancia del análisis monográfico con el fin dar un amplio conocimiento de los riesgos existentes y maneras de poder mitigar este tipo de amenazas. Es por ello que se busca generar conciencia o cultura digital al momento de navegar en el internet, teniendo en cuenta la situación presentada por la pandemia ocasionada por el brote del virus *COVID-19* y a que los ataques informáticos se vieron en aumento durante este tiempo.

Para el primer semestre del año 2020, con un aumento del 59% de los delitos informáticos, evidencio el Centro Cibernético de la Policía Nacional de Colombia comparado con el mismo periodo del año 2019, esto debido a la gran demanda de la utilización de operaciones[5].

Según el informe evaluación, retos y amenazas a la ciberseguridad publicado en junio de 2021 por la cámara Colombiana de Informática y Telecomunicaciones *(CCIT)* y el Tanque de Análisis y Creatividad de las *TIC (TicTac)*, para el 2021 el cibercrímen se ha mantenido desde el año 2019 con una tasa de crecimiento continuo con un 35% con respecto al año 2020, lo cual equivale a más de 20.502 reportes de noticias de cibercrímenes, entre los ataques con mayor relevancia en Colombia son representados por el phishing, Ransomware y la fuga de información de datos personales[6].

---

[4] Coronaviruscolombia.gov.co. [Sitio Web]. Acciones tomadas por el Gobierno. [Consulta 24 septiembre 2021]. Disponible en:https://coronaviruscolombia.gov.co/Covid19/acciones/acciones-de-aislamiento-preventivo.html

[5] Portafolio.co. [Sitio Web]. Delitos informáticos, la otra pandemia en tiempos del coronavirus. [Consulta 28 febrero 2021]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642.

[6] Ccit.org.co. [Sitio Web]. Evaluación, Retos y Amenazas a al Ciberseguridad. [Consulta 24 septiembre 2021]. Disponible en:https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

La educación Colombia no es ajena a las brechas educativas, en muchas partes la conectividad puede decirse que es casi nulo lo cual afecta la manera de poder llegar los colegios y docentes a los alumnos, el aprendizaje se ve afectado de manera drástica. Esta problemática no es la única que se asoma al momento de pensar en la tecnología como medio viable desde que comenzó la pandemia para poder impartir clases. Los riesgos en el ciberespacio son otro problema que se suma a la gama de dificultades que han tenido que pasar las instituciones educativas, docentes, padres de familia y alumnos. Los ciberatacantes cada vez más aprovechan este auge tecnológico, los delitos han cambiado de ámbito debido a la gran cantidad de personas conectadas en el trabajo y estudios es por ello la importancia de conocer a que vulnerabilidades como usuarios se pueden mitigar.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

- Analizar los riesgos de seguridad de la información que se presentan al usar herramientas informáticas para el desarrollo de clases virtuales por parte de docentes y estudiantes en Colombia, con el fin de establecer buenas prácticas para el tratamiento de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos de seguridad de la información que se presentan al usar herramientas informáticas para el desarrollo de clases virtuales por parte de docentes y estudiantes en Colombia.

- Establecer las amenazas, vulnerabilidades e impactos de las herramientas informáticas más utilizadas para el desarrollo de clases virtuales por parte de estudiantes y docentes.

- Recomendar buenas prácticas de seguridad de la información para docentes y estudiantes, que le permitan salvaguardar la confidencialidad, disponibilidad e integridad de su información.

- Proponer buenas prácticas de seguridad de la información por parte de las instituciones educativas que permitan robustecer su infraestructura tecnológica.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Según las predicciones en la publicación “Kaspersky ofrece pronóstico de ciberseguridad 2021 para América Latina” del 19 noviembre 2020, da a conocer algunos pronósticos con respecto a la ciberseguridad.

Dmitry Bestuzhev, encargado de la dirección de investigación y análisis de Kaspersky para América latina, se pronuncia al respecto al año 2021 considerándolo desafiante por la proliferación de ataque y su sofisticación.

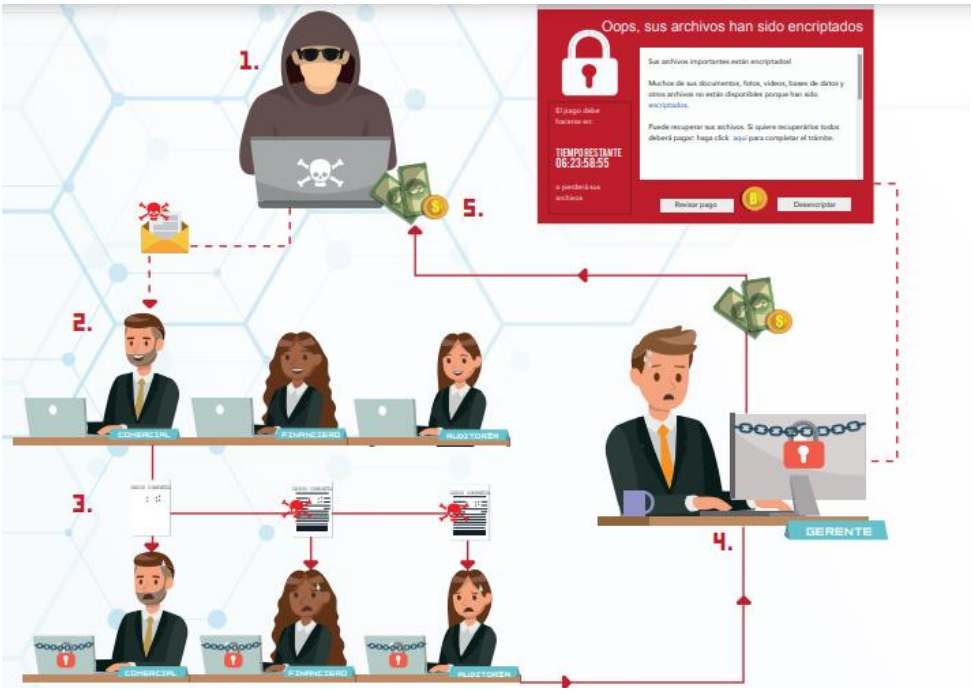
“La tendencia de realizar la mayoría de nuestras actividades en línea se mantendrá por lo menos hasta mediados del próximo año por cuestiones relacionadas con la pandemia, lo que significa tierra fértil para que los ciberdelincuentes continúen sus campañas de fraude, robo y extorsión. Es más, los ataques con mayor potencial de ganancias, aquellos que apuntan a empresas y entidades públicas, serán más coordinados y, por ende, más dañinos”[7].

Los ataques realizados por medio de malware como *Ransomware* dirigidos, para América latina la influencia de ciberdelincuentes de Europa Oriental ha tenido un gran aporte debido a que aumenta el desarrollo de estas amenazas la cual se asemejan a sus esquemas y es posible compararlos con grupos tales como, *Netwalker, Egregor, Sodinokibi*, *Ragnar Locker*, entre otros.

[7] Latam.kaspersky.com. [Sitio Web]. Kaspersky ofrece pronóstico de ciberseguridad 2021 para América Latina. [Consulta 21 septiembre 2021]. Disponible en: https://latam.kaspersky.com/about/press-releases/2020_kaspersky-ofrece-pronostico-de-ciberseguridad-2021-para-america-latina

Como se observa en la Figura 1, tenemos un ataque de Ransomware la cual es usado para cifrar la información y de esta manera realizar petición de dinero para su rescate.

Figura 1. Pasos de ataque Ransomware



Fuente: Evaluamos.com. [Sitio Web]. Tendencia Cibercrímen Colombia 2019 - 2020. [Consulta 25 abril 2021]. Disponible en: http://www.evaluamos.com/pdf/TENDENCIASCIBERCRIMEN.pdf.

Uno de los atractivos más recurrentes para los ciberdelincuentes serán las entidades financieras, generando ofertas por medio de contrataciones para el diseño y ataques, con la modalidad *"hacker for hire",* de esta manera las amenazas en el año 2021 son cada vez más cargadas de sofisticación utilizando todos los medios posibles para poder propagar y realizar intromisiones en los sistemas de información, redes de datos e incautos cibernautas. Además de esto la mirada hacia los dispositivos móviles se convierten en blancos para el uso de *RAT* (Troyano de acceso remoto) para Android con el objetivo de obtener un mayor ingreso sin mucho trabajo con respecto a los ataques tradicionales ha activos de escritorio.

El teletrabajo como herramienta para la continuidad del desarrollo laboral ocasionada en su gran parte por el virus *COVID-19*, la cual ocasionó el confinamiento y realizar labores desde casa, apunta a la diversificación de las técnicas de ataques con relativo aumento de las técnicas para robo de información confidencial (*Personally Identifiable Information*) de usuarios, convirtiendo también a las universidades y escuelas en objetivo.

El equipo de Kaspersky basado en estudios y experiencias durante el año 2020, centra las diferentes perspectivas y pronósticos sobre el tema de ciberseguridad para Latinoamérica[8].

Las tendencias a la criminalidad por los medios informáticos crecen vertiginosamente, en el “Informe de las tendencias del cibercrímen en Colombia (2019 - 2020)” presentado por varias entidades entre ellas la Policía Nacional expone por medio de cifras estadísticas la relevancia de los actos cibercriminales en Colombia, las técnicas y métodos que fueron denunciadas ante el centro cibernético Policial *CECIP* que en su total corresponden a 15.948 casos reportados para el año 2019. Teniendo en cuenta todo el crecimiento de riegos en el ciberespacio, se evidencia que los cibercriminales actúan de manera coordinada con recursos económicamente ilimitados derivado del ciberdelito[9].

En Colombia según las estadísticas los ataques que más recuren a su utilización por parte de los ciberdelincuentes encontramos, *malware, Ransomware*, ciberextorsiones y el uso de fraude por medio de *BEC (Business Email Compromise)* y otras técnicas y amenazas que afectan el ámbito sobre la seguridad de la información y por ende la productividad de las entidades de cualquier sector de la economía.
En Colombia el 90% de los ataques que afectan al sector productivo, utilizan la ingeniería social, de esta manera logran obtener información relevante y privada de los funcionarios y directivos y luego utilizan toda esta información para realizar suplantación de identidad, falsificación de correos y en otros casos poder realizar desvíos de dineros de a cuantas bancarias que están en su poder.

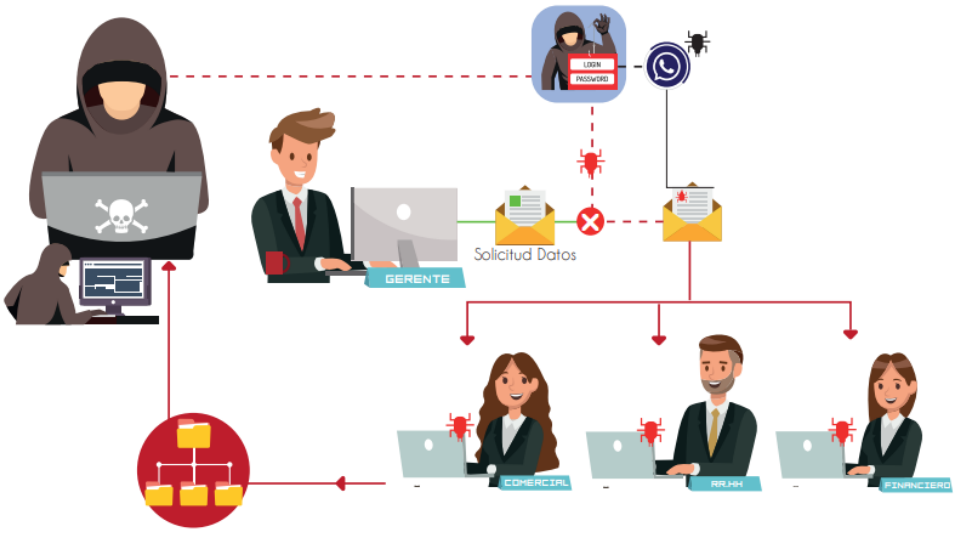
El *Phishing* es una de las técnicas que por medio de un correo los cibercriminales tienen la posibilidad de apoderarse de las cuentas de correo y desde allí poder enviar comunicados, solicitudes que en su mayoría son a los funcionarios que tiene las funciones de generar pagos o la realización de trasferencias bancarias. El atacante envía un correo electrónico falso suplantando alguna entidad oficial o privada solicitado el ingreso a una página donde se deben depositar o digitar datos de la empresa y así de esta manera el atacante obtiene la información.

[8] Latam.kaspersky.com. [Sitio Web]. Kaspersky ofrece pronóstico de ciberseguridad 2021 para América Latina. [Consulta 21 septiembre 2021]. Disponible en: https://latam.kaspersky.com/about/press-releases/2020_kaspersky-ofrece-pronostico-de-ciberseguridad-2021-para-america-latina

[9] Ccit.org.co. [Sitio Web]. Informe de las tendencias del cibercrimen en Colombia 2019 - 2020. [Consulta 22 septiembre 2021]. Disponible en:Ihttps://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

En la Figura 2, se evidencia el proceso en que el atacante obtiene la información por medio de correo electrónico

Figura 2. Esquema de ataque Por Phishing



Fuente: Ccit.org.co. [Sitio Web]. Informe de las tendencias del cibercrimen en Colombia 2019 - 2020. [Consulta 22 septiembre 2021]. Disponible en:Ihttps://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

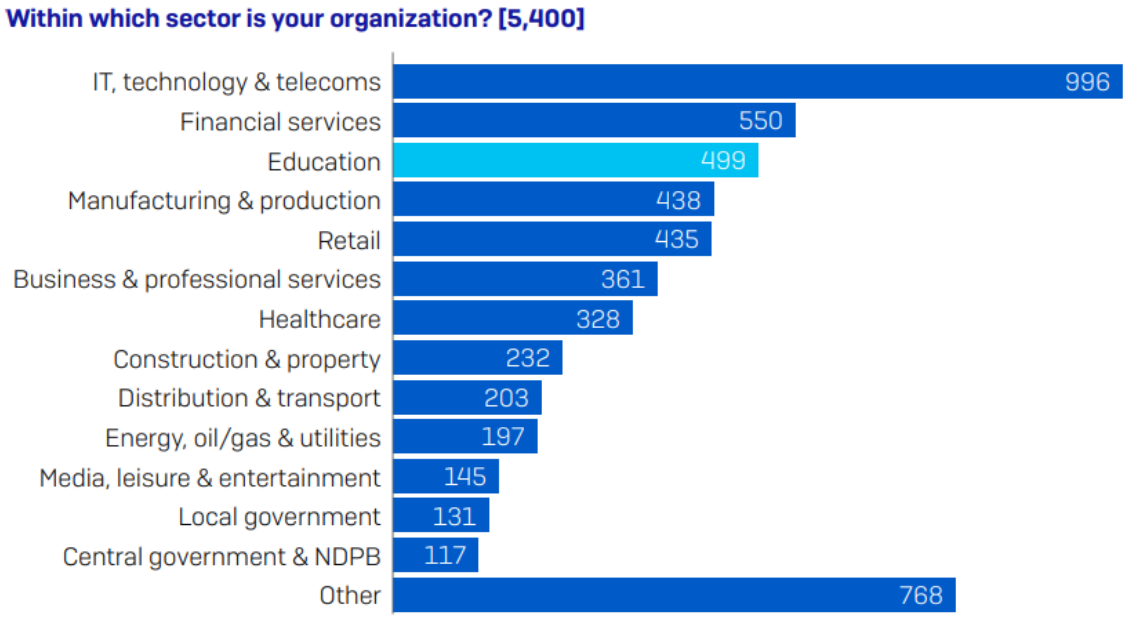
La empresa *Sophos* de *hardware y software* de seguridad, en el informe técnico publicado en julio de 2021 "*The State of Ransomware in Education 2021*"[10] revela el resultado que el sector más golpeado por ataques de Ransomware en el año 2020 fue el sector educativo, año de la pandemia mundial ocasionada por el virus *COVID -19*. El informe recoge un estudio entre casi 500 entidades educativas a nivel mundial confirmando esta vulnerabilidad a la cual se ve enfrentado el sector y amenaza cibercriminal a la cual están expuestas las instituciones educativas.

La encuesta realizada por *Vanson Bourne*, empresa experta en investigación de mercado de tecnología a nivel global. Los encuestados más o menos 5400 entre ellos 499 del sector educativo, esta encuesta fue aplicada entre enero y febrero de 2021.

[10] Sophos.com. [Sitio Web]. The State of Ransomware in Education 2021. [Consulta 22 septiembre 2021]. Disponible en: https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf

En la Figura 3, se muestra la cantidad de empleados encuestados de diferentes sectores económicos. Que para el sector educativo fueron 499 personas.

Figura 3. Sector en que se encuentra la Organización



Fuente: Sophos.com. [Sitio Web]. The State of Ransomware in Education 2021. [Consulta 22 septiembre 2021]. Disponible en: https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf

El resultado para el sector educativo con respecto a los 499 encuestados, ante la pregunta, “En el último año, ¿su organización ha sido atacada por Ransomware? [499 encuestados sobre educación]”, el 44% contestaron que sí. En la Figura 4, Es posible ver los resultados obtenidos.

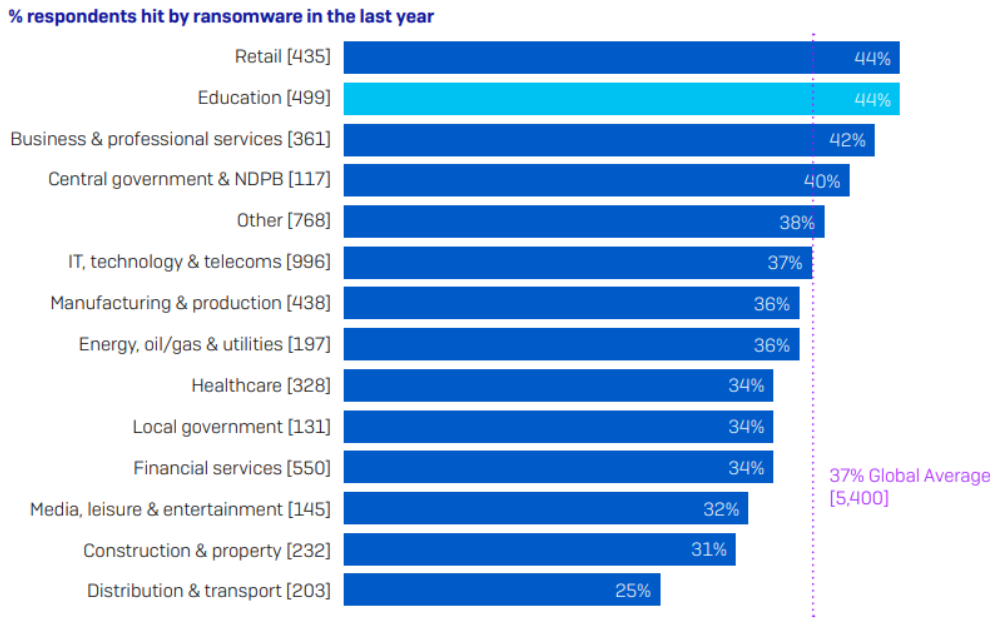
Figura 4. Establecimientos educativos afectados en el año 2020

Fuente: Sophos.com. [Sitio Web]. The State of Ransomware in Education 2021. [Consulta 22 septiembre 2021]. Disponible en: https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf

Con un 44% entidades afectadas por *Ransomware*, 33% no afectado en el año 2020 pero esperan ser afectados en el fututo y 22% no afectado en el 2020 y no esperan ser afectado en el futuro.

En la Figura 5, Es posible ver que en los sectores educativas y empresas minoristas prevaleció la concurrencia de ataques de *Ransomware*.

Figura 5. 5 % de afectados en el año 2020 por Ransomware



Fuente: Sophos.com. [Sitio Web]. The State of Ransomware in Education 2021. [Consulta 22 septiembre 2021]. Disponible en: https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf

El hecho de que el sector educativo sea uno de los más afectado es posible que se debe según el informe de *Sophos* a los presupuestos bajos en *TI* y ciberseguridad, equipos obsoletos con recursos bastantes limitados y se suma el poco conocimiento de los estudiantes ante el uso y buen comportamiento a la hora de navegar. Con la pandemia el panorama cambio un poco más ya que las instituciones no estaban preparadas para el aprendizaje de manera virtual y remota tanto para los estudiantes como los profesores.

El comportamiento en Colombia del ciberdelito según el informe evaluación, retos y amenazas a la ciberseguridad de junio de 2021 publicado por cámara Colombiana de Informática y Telecomunicaciones *(CCIT)* y el Tanque de Análisis y Creatividad de las *TIC (TicTac).* La cibercriminalidad sigue usando envió de correos electrónicos masivos

mediante la técnica de *phishing,* en su mayoría los mensajes están incluidos enlaces que redirigen al usuario a páginas web para recolección de datos personales con el objetivo del robo de identidad y suplantación, las víctimas son engañas con la utilización de las entidades con el fin de generar confianza.

Entre las modalidades está la violación de datos personales contemplada en el artículo 269F del código penal colombiano. El incremento fue de un 123% con respecto al año 2020. Con un 33% de incrementos con respecto al año 2020 se refleja la suplantación de sitios web con la finalidad de poder captar datos personales contemplado en el artículo 269G, las técnicas que son utilizadas son smishing, phishing y pharming. Otras de las modalidades que se reflejan en el informe que presenta aumento es el acceso abusivo a sistemas informáticos contemplado en el artículo 269A con un 28% respecto al año 2020[11].

[11] Ccit.org.co. [Sitio Web]. Evaluación, Retos y Amenazas a al Ciberseguridad. [Consulta 24 septiembre 2021]. Disponible en:https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

4.2 MARCO CONCEPTUAL

La pandemia por el virus del *COVID-19,* ocasiono muchos cambios en la vida de las personas, una de ellas es la utilización masiva del uso de la tecnología. Es por ello que las instituciones educativas también se vieron a la necesidad de adoptar las tecnologías de manera intempestiva, convirtiéndose en blanco fáciles para los riesgos del ciberespacio.

En esta etapa de pandemia mundial se convirtió en una necesidad aprender muchos conceptos que se pudieron usar en algunos momentos, masificándose en el año 2020 por motivos de fuerza mayor ocasionadas por el confinamiento que fue necesario debido a la pandemia por *COVID 19*. Entre los conceptos que más se popularizaron a nivel del sector educativo fue el uso de la palabra y utilización de aulas virtuales[12], que son los entornos digitales en las cuales es posible realizar intercambio de conocimiento, donde es posible realizar un aprendizaje por medio de la interacción de la tecnología con el hombre. Por medio del uso de las tecnologías y las herramientas informáticas es posible el desarrollo de clases virtuales.

Paralelamente a todo este cambio trascendental en la educación colombiana se presentaron inconvenientes ocasionados por la pronta implementación de mecanismos de educación no convencionales y de difícil acceso para algunos estudiantes como es de notar que muchos alumnos no poseían las herramientas necearías para poder recibir clases guiadas por la tecnología y aquellas instituciones y actores involucrados se enfrentarían aun flagelo que se pensaría que podía ser propio de empresas financieras y bancarias, los delincuentes cibernéticos comenzaron a enfocar sus esfuerzos al sector educativo, ya que fue blanco fácil para ellos. Recordemos que este sector fue uno de los que tuvo que “tirarse al agua sin salvavidas” y el riesgo ante ataques cibernéticos fueron más probables, ya que la mayoría de instituciones educativas no contaban con un plan de ciberseguridad para la protección a las infraestructuras tecnológicas con el fin de poder protegerse ante ataques maliciosos.
La proliferación de ataques al sector educativo para el año 2020 fue considerable – según informe “*The State of Ransomware in Education 2021*[13]” publicado en julio de 2021 de la empresa *Sophos* – los ciberdelincuentes inician su marcha enfocada en poder obtener información de todos los usuarios con mayores debilidades, tales como estudiantes, docentes y padres de familia con poco conocimiento en el área de la seguridad informática.

Los inminentes riesgos informáticos a la hora de navegar por el ciberespacio se intensificaron para todos los sectores de la economía con la implementación del trabajo

[12] EvolCampus. [Sitio Web] ¿Qué es un aula virtual y para qué se puede utilizar? [Consulta 15 marzo 2021]. Disponible en: https://www.evolmind.com/latam/blog/que-es-un-aula-virtual-y-para-que-se-puede-utilizar.

[13] Sophos.com. [Sitio Web]. The State of Ransomware in Education 2021. [Consulta 22 septiembre 2021]. Disponible en: https://www.sophos.com/es-es/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf.

en casa por medio de los medios tecnológicos, es allí en ese espacio donde comienza un asecho por parte de ciberdelincuentes. “El riesgo de una actividad puede tener dos componentes: la posibilidad o probabilidad de que un resultado negativo ocurra y el tamaño de ese resultado. Por lo tanto, mientras mayor sea la probabilidad y la pérdida potencial, mayor será el riesgo”[14]. Este concepto se puede tomar de manera generalizada para inspeccionar y hacernos una idea de lo que es un riesgo. Aun cuando el concepto de riesgo no difiere mucho del concepto de riesgo informático se maneja desde otro ambiente virtualizado, correspondiendo a los daños o peligros que puede entorpecer el correcto funcionamiento directo o resultado que se esperan de sistemas informáticos imposibilitando obtener los objetivos esperados.

Aunque no todo ha sido un choque abrupto que el sistema educativo entrara de repente al ámbito virtual, ha traído ventajas favorables convirtiéndose en oportunidades sobre la brecha de acceso a la conectividad y el uso de dispositivo por parte de estudiantes en condiciones desfavorables y de la misma manera a los docentes que tuvieron la necesidad de ser capacitados para sacar el mayor provecho posible de las herramientas informáticas, la tecnología y su uso no solo debería estar en la virtualidad sino también en la prespecialidad. Los gobiernos de los países les corresponden la tarea de fortalecer las capacidades de las instituciones educativas y a los docentes en el ámbito tecnológico.

“La educación de los niños y las niñas se perdió en un esfuerzo por proteger las vidas de toda la población del coronavirus”, dijo Martínez. “Para compensar su, los gobiernos deben estar a la altura del desafío y hacer que la educación sea gratuita y esté disponible para todos los niños y niñas del mundo[15]”

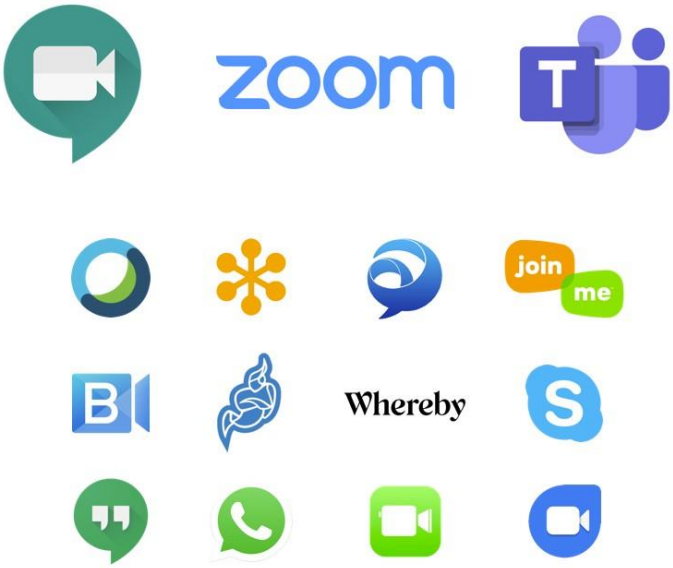
En el sector de la educación la utilización de plataformas virtuales o *LMS (Learning Management Systems)* como alternativa acogidas por las instituciones educativas con el objetivo de logar los procesos educativos, se convirtió en las nuevas aulas de clases y forma de educar.

En la Figura 6, es posible ver algunas herramientas gratuitas para clases y reuniones virtuales.

[14] Scielo.sld.cu. [Sitio Web]. Echemendía, Belkis. Definiciones acerca del riesgo y sus implicaciones. [Consulta 11 marzo 2021]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1561-30032011000300014.

[15] Hrw.org. [Sitio Web]. El grave impacto de la pandemia en la educación mundial. [Consulta 24 septiembre 2021]. Disponible en:https://www.hrw.org/es/news/2021/05/16/el-grave-impacto-de-la-pandemia-en-la-educacion-mundial

Figura 6. Herramientas de videollamadas



Fuente: medium.com/. [Sitio Web]. Plataformas educativas. [Consulta 25 abril 2021]. Disponible en: https://miro.medium.com/max/2400/1*vmWN_RB5PU4l6-ZDHvGe6g.jpeg

Estas herramientas tecnológicas de apoyo, se han convertido en alicientes para las instituciones educativas que no cuentas con una infraestructura robusta para poder logar su objetivo de impartir educación. A continuación, relacionamos algunas de ellas con sus características más relevantes[16].

- ***Whereby*****,** es una herramienta para realizar sesiones agiles al momento de usar el audito, video y compartir la pantalla. Además, con un chat muy flexible.

- **Jitsi,** herramienta para videoconferencias sin límite de participantes, es una de las grandes ventajas de esta aplicación que pueden interactuar con video, audio y mensajería multiplataforma.

- ***Meet,*** herramienta que se utiliza con cuentas de correo de Gmail, con acceso a 100 usuarios con video y audio en la suite básica, con una suscripción avanzada puede conectarse 250 personas al tiempo.

- ***Microsoft Teams,*** es una de las herramientas más robustas del mercado, pensada principalmente para reuniones empresariales, aunque hoy en día se usa

[16] Arte&Animación. [Sitio Web]. Conoce las 7 mejores herramientas "gratis" para clases y reuniones virtuales. [Consulta 15 marzo 2021]. Disponible en: https://arteyanimacion.com/herramientas-clases-y-reuniones-virtuales/

para impartir clases de manera remota. Con esta herramienta se logra tener todo el contenido en la pantalla de la videollamada, junto de salas de chat y posibilidades de video llamadas.

- ***Hangouts,*** herramientas que requiere una cuenta de correo Gmail para poder realizar las reuniones virtuales, con cuentas tradicionales de la suite de Gmail se podrán conectar 10 usuarios, con cuentas de empresa se puede tener 25 personas.

- ***Skype,*** es una herramienta usada para Videollamadas la cual puede ser como canal principal para clases o reuniones, se puede realizar video llamada de hasta 10 usuarios de forma gratuita, en casi cualquier tipo de dispositivo tecnológico, *Tablet*, móvil o *PC*.

- ***Anymeeting,*** Esta herramienta es necesario registrarse para su ingreso, la capacidad para l asistencia es de 30 personas de manera gratuita la cual se debe contar con los correos electrónicos de las personas a invitar.

- ***Streaming*** **por Redes sociales,** *YouTube* y *Facebook Live*, herramientas para compartir video en vivo por medio de su perfil o su canal, es posible que puedan interactuar con la audiencia o en su defecto estudiantes por el chat.

- **Zoom,** Aplicación para clases virtuales consideraba una de las más completas, es posible tener acceso a una pizarra virtual, dividir salas, generar encuestas en línea, entre otras. Además, tiene la funcionalidad de poder compartir la pantalla y poder realizar la grabación de las clases y de esta manera mantener un registro.

Las instituciones educativas de la misma forma que adoptan herramientas para el apoyo a las clases virtuales también tienen la necesidad de poder tener su contenido de aprendizaje en plataformas educativas para estudiar a distancia[17]

- ***Blackboard,*** una de las plataformas educativas a distancia con mayor acogida por prestigiosas instituciones de educación superior. Con mayor usabilidad que permite un manejo intuitivo a los usuarios y poder acceder a una educación con calidad en cualquier lugar o momento.

- ***Schoology,*** plataforma de carácter educativo gratuita, con las funcionalidades de poder realizar la programación de actividades en línea, compartir recursos didácticos e ideas.

[17] Universia.net. [Sitio Web].10 plataformas virtuales para estudiar a distancia. [Consulta 15 marzo 2021]. Disponible en: https://www.universia.net/pe/actualidad/orientacion-academica/10-plataformas-virtuales-estudiar-distancia-1141829.html

- ***Edmodo,*** plataforma web educativa interactiva que puede facilitar la interacción y comunicación virtual entre los padres, profesos y el alumno. También ejercicios de destrezas mentales e intelectuales.

- ***Moodle,*** considerada una de las plataformas más completas en el mercado a nivel de educación, es muy interactiva enfocada en el paradigma de la educación social constructivista.

- ***Twiducate,*** los alumnos y maestros pueden crear salas privadas para poder plantear sus ideas o realizar discusiones de temas educativos.

- ***Hootcourse,*** por medio de esta aplicación es posible la creación de clases virtuales por medio de las redes sociales validándonos por medio de nuestras cuentas sea de Facebook o Twitter y crear comentarios durante la sesión.

- **Edu 2.0,** es un LMS, sistema de gestión de aprendizaje con facilidades para poder implantar e-learning, disponibles para cualquier tipo de centro educativo sin importar el nivel con un centro de administración completo para maestros, estudiantes y padres de familia.

- **Teachstars,** plataforma pensada para profesores que se pueden realizar la programación de sus cursos, módulos y actividades. Por medio de esta aplicación es posible compartir contenido de redes sociales y revistas digitales.

4.3 ANTECEDENTES O ESTADO ACTUAL

- El 26 de marzo (2020) *Motherboard* en una de sus publicaciones da a conocer que una de las herramientas de videoconferencias como es *Zoom*, no tenía claridad para los datos que manejaba bajo el sistema operativo *IOS* "la app para este sistema operativo enviaba datos a Facebook, incluso si los usuarios de Zoom no tenían una cuenta en la red social"[18].

- El 1 de abril de 2020 *Zoom* en un comunicado manifiesta preocupación por los problemas de privacidad y seguridad que han presentado a los usuarios, por lo cual tomó medidas para solucionarlo y se suma otras amenazas a la aplicación por medio de los cibercriminales que de alguna manera aprovechan el interés de quienes utilizan la plataforma y de a las cuales son ajenos a la organización.[19]. publicado el 9 abril 2020.

- 3 abril de 2020, *CNN, (Dakin Andone)*. Las autoridades federales en estados unidos reportan la utilización de la técnica de *zoombombing*, que es el acoso cibernético ocasionada por troles o piratas informáticos sin identificación, encargados de utilizar un lenguaje inapropiado y compartir imágenes perturbadoras en video llamadas por medio de la plataforma zoom.
  "A fines de marzo, el FBI dijo en una persona o personas no identificadas se conectaron a la clase en línea de un maestro de escuela secundaria y gritaron una blasfemia, así como la dirección de la casa del maestro."[20]

- 30-abril-2020.*CyberArk Labs* encontró vulnerabilidades críticas en la plataforma *Microsoft Team* tanto para las versiones para navegadores y escritorio. La cual puede ser usado para robo de datos, poniendo en riesgo inminente la privacidad.[21].

- 2020, 15 de mayo. Redacción BLU Radio, una docente de inglés denuncia ataques de un Influencer que aparece en las redes sociales como 'Mantekoman' con el usuario

[18] Welivesecurity.com. [Sitio Web]. Zoom: problemas de seguridad y privacidad en la popular herramienta para videoconferencias. [Consulta 2 marzo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/03/30/zoom-problemas-seguridad-privacidad-popular-herramienta-videoconferencias/.
[19] Welivesecurity.com. [Sitio Web]. Un repaso por los últimos problemas de seguridad y privacidad que se descubrieron en Zoom. [Consulta 1 marzo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/04/09/repaso-ultimos-problemas-seguridad-privacidad-descubrieron-zoom/.
[20] CNN, español. [Sitio Web]. «Zoombombing», el FBI advierte que las llamadas de video por Zoom están siendo interceptadas. [Consulta 01 junio 2021]. Disponible en: https://cnnespanol.cnn.com/2020/04/03/zoombombing-el-fbi-advierte-que-las-llamadas-de-video-por-zoom-estan-siendo-interceptadas/
[21] RZ Redes Zone. [Sitio Web]. CyberArk Labs encuentra una vulnerabilidad en Microsoft Teams. [Consulta 07 marzo 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/cyberark-labs-vulnerabilidad-microsoft-teams/

de "*Iphone7*" que en clases virtuales de zoom compartió material pornográfico a menores de edad[22].

- Según datos de la Policía Nacional, citados por la firma Aon, los cibercrímenes más denunciados en 2019 por los colombianos tuvieron que ver con *phishing* (42%), suplantación de identidad (28%), envío de malware (14%) y fraudes en medios de pago en línea (16%). Todos estos fenómenos corren el riesgo de agudizarse en el marco de la cuarentena[23]. Publicado 27 de mayo de 2020.

- Para el año 2020 en Colombia según estadísticas del Gaula de la policía en un 130% creció el delito del *sexting* durante la cuarentena[24]. Publicado 2 de junio 2020.

- "En la ciudad de **Nueva *York*** estafadores están contactando a los padres pidiendo dinero para entregar un producto o servicio al estudiante para el aprendizaje virtual"[25].Publicado 21 de agosto 2020.

- David Oliveros, joven de 16 años estudiante de *Miami-Dade* confeso haber realizado 8 ciberataques con el fin de denegar servicios en las redes del distrito. Oliveros, confeso la autoría en los ciberataques de la cuales arruino el regreso a clases virtuales en el distrito escolar, "informaron las autoridades"[26]. Publicado 3 de septiembre de 2020

- Los cibercriminales, han encaminado sus ataques al regreso del colegio, ya que aprovechan que los profesores y alumnos continúen sus clases por medio de aulas virtuales, "Señala Mario García, director general de *Check Point* para España y Portugal. Por este motivo, ahora más que nunca la educación en conceptos básicos de ciberseguridad tanto a los alumnos como a sus familiares. Además, es fundamental que los equipos estén correctamente protegidos y que los colegios cuenten con una estrategia de protección sólida frente a las amenazas del mundo virtual", García[27]. Publicado 9 de septiembre 2020.

---

[22] Bluradio.com. [Sitio Web]. 'Influencer' que se infiltró con porno en clase a menores es universitario: profesora. [Consulta 26 abril 2021]. Disponible en: https://www.bluradio.com/judicial/influencer-que-se-infiltro-con-porno-en-clase-a-menores-es-universitario-profesora

[23] Semana.com. [Sito web]. *Estos son algunos riesgos cibernéticos durante la cuarentena*. [Consulta 2 marzo 2021]. Disponible en: https://www.semana.com/empresas/tecnologia/articulo/riesgos-ciberneticos-para-empresas-y-usuarios-durante-la-cuarentena/287040/.

[24] LaFM. [Sitio Web]. Sexting, el delito que ha aumentado más del 130 % en Colombia y que afecta principalmente a menores. [Consulta 07 de marzo 2021]. Disponible en: https://www.lafm.com.co/colombia/sexting-el-delito-que-ha-aumentado-mas-del-130-en-colombia-y-que-afecta-principalmente.

[25] Telemundoatlanta.com. [Sitio Web]. Montenegro, J. (*Aprendizaje virtual; autoridades alertan sobre algunos riesgos cibernéticos para los estudiantes*. [Consulta 2 marzo 2021]. Disponible en: https://www.telemundoatlanta.com/noticias/coronavirus/recursos/educacion_virtual/aprendizaje-virtual-autoridades-alertan-sobre-algunos-riesgos-cibern-ticos-para-los-estudiantes/article_4198f916-e369-11ea-80a2-dfabd373871e.html.

[26] Eluniversal.com.mx. [Sitio Web]. Estudiante arruina clases virtuales con ciberataques en Miami. [Consulta 07 marzo 2021]. Disponible en: https://www.eluniversal.com.mx/mundo/estudiante-arruina-clases-virtuales-con-ciberataques-en-miami.

[27] PCWorld, México. [Sitio Web]. Los ciberriesgos de la educación online (Y cómo evitarlos). [Consulta 07 marzo 2021].

- *TransUnion* en uno de los estudios reciente incluye a Colombia, informa que el '*phishing*', como uno de los delitos digitales principales en el mundo. "De acuerdo con el documento, el 27% de los consumidores encuestados dijeron haber sido víctimas de este tipo de estafa con temas relacionados con la pandemia."
  Un 21% de estudiantes contesta que fue víctima de ciertas formas de estafas por medio de enlaces legítimos de sitios web de comercio en línea y un 19% fue estafado por medio de fondos de recaudos de caridad[28.] Publicado el 15 de septiembre de 2020.

- En chicago, Estados Unidos. La policía capturo a un hombre luego que después en una plataforma virtual agrediera de manera sexual a una niña de 7 años, la información la dieron varios medios locales. En el afán de evitar esto la docente les decía que se desconectaran. Esto sucedió el 15 de octubre de 2020 aproximadamente a las 13:00 horas. La niña identifico al agresor y los uniformados procedieron la detención.[29]. publicado el 20 de octubre de 2020.

- La Comisión Federal de Comercio de Estados Unidos *(FTC*) informó que la plataforma "engañó a algunos usuarios que querían almacenar las reuniones grabadas en el almacenamiento en la nube de la compañía al afirmar falsamente que esas reuniones estaban encriptadas inmediatamente después de que terminara la reunión", pero realmente "algunas grabaciones supuestamente se almacenaron sin cifrar durante hasta 60 días en los servidores de *Zoom* antes de ser transferidas a su almacenamiento seguro"[30].Publicado 10 noviembre de 2020.

- En Quito, Ecuador el 13 de noviembre de 2020, el periodista Cristian Espinoza informa en el periódico El COMERCIO, una alumna expresa que, en un colegio de la capital, en el desarrollo de una clase virtual que se realizaba por videoconferencia la cual utilizaban zoom, alguien pudo infiltrarse y trasmitió contenido para adultos a los alumnos conectados, siendo estos menores de edad.[31]

- El centro cibernético de la policía en Colombia, informo que para el año 2020, las denuncias por victimas algún tipo de ciberdelito aumentaron en un 89% con respecto

Disponible en: http://pcworld.com.mx/los-ciberriesgos-de-la-educacion-online-y-como-evitarlos/

[28] Portafolio.co. [Sitio Web]. Delitos informáticos, la otra pandemia en tiempos del coronavirus. [Consulta 28 febrero 2021]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642.

[29] El Comercio. [Sitio Web]. *Alumnos presenciaron agresión sexual a una compañera de siete años durante una clase virtual*. [Consulta 2 marzo 2021]. Disponible en: https://www.elcomercio.com/actualidad/chicago-agresion-sexual-nina-clase/.

[30] Eltiempo.com. [Sitio Web]. *Las serias acusaciones contra Zoom por problemas en su seguridad*. [Consulta 2 marzo 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/zoom-es-senalada-de-enganar-sobre-la-seguridad-dentro-de-la-plataforma-548126.

[31] Elcomercio.com. [Sitio web]. Infiltrado mostró contenido para adultos durante clase virtual de un colegio de Quito; ¿Cómo evitar que esto ocurra? [Consulta 07 marzo 2021]. Disponible en: https://www.elcomercio.com/actualidad/infiltrado-contenido-adultos-clase-quito.html.

al año anterior, 45.104 para el año 2020 y 23.907 para el año 2019[32]. Publicado 15 de febrero 2021.

- El periódico el tiempo en sus versiones web para el día 28 de junio de 2021, “La universidad ha sido víctima de un ciberataque de seguridad, por el cual algunos de nuestros sistemas internos han sido comprometidos" universidad el Bosque. Las cuentas de *twitter*, sistemas informáticos, correos institucionales y pagina web fueron atacadas comprometiendo la información de la comunidad educativa[33].

[32] Elpais.com.co. [Sitio Web]. Trabajo y clases virtuales son blancos de los ciberdelincuentes. [Consulta 1 marzo 2021]. Disponible en: https://www.elpais.com.co/judicial/trabajo-y-clases-virtuales-son-blanco-de-los-ciberdelincuentes.html.
[33] Eltiempo.com. [Sitio Web]. Universidad El Bosque sufre ataque informático. [Consulta 22 septiembre 2021]. https://www.eltiempo.com/vida/educacion/universidad-el-bosque-sufre-ataque-informatico-599303

4.4 MARCO LEGAL

- **Ley 1273 De 2009**
  "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[34]. La ley está conformada por artículos de las cuales describe cada uno de los diferentes delitos informáticos que son castigados según la legislación colombiana, estipulando las diferentes multas de 100 a 1000 salarios mínimos vigentes mensuales y penas de presión contemplados que pueden ir de cuarenta y ocho (48) a noventa y seis meses (96).

  Esta ley aplica en el momento que el ciberdelincuente interceptan datos informáticos (art 269C), uso de software maliciosos como es el caso de malware y Ransomware (Art 269F), violación de los datos personales cuando se usa la técnica de *phishing* el atacante obtiene datos sin consentimiento (Art 269F) y la suplantación de sitios web (Art 269G)

- **Ley Estatutaria 1581 De 2012**
  "Por la cual se dictan disposiciones generales para la protección de datos personales"[35].Esta ley cubre todos los datos recolectados en las entidades públicas y privada la cual puede ser datos públicos, semiprivados, privados, sensibles, biométricos, de niños, niñas y adolescentes. Las entidades deben tener claro el uso de los datos dependiente de su clasificación ya que de ellos depende también su uso indebido genera sanciones impuesto por la superintendencia de industria y comercio.

  Las sanciones al incumplimiento de la norma ocasiones sanciones que pueden ser multas, cese de actividades, cierre de la empresa o entidad proporcional al grado de la infracción.

  Las instituciones educativas recolectan información públicos, semiprivados, privados, sensibles, biométricos, de niños, niñas y adolescentes, por lo tanto, deben garantizar que esa información no sea expuesta al pública, las entidades deber procurar que las personas sean conscientes que su información será tratada. Por medio de un consentimiento de tratamiento de datos personales los usuarios dan una autorización para tal fin contemplado en el artículo 3 de ley estatutaria 1581 de 2012.

[34] Secretariasenado.gov.co. [Sitio Web]. Ley 1273 De 2009. [Consulta 1 marzo 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.
[35] Secretariasenado.gov.co. [Sitio Web]. Ley estatutaria 1581 de 2012. [Consulta 14 abril 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

- **Ley 1928 De 2018**
  "Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest"[36].
  Esta ley es adoptada como medida legislativa con el fin de poder tipificar como delitos, pornografía infantil en sus ámbitos de producción, oferta, difusión, adquisición y posesión en medios de sistemas informáticos.

  Esta ley en sus "Títulos 1 delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, Titulo 2 delitos informáticos y Título 3 delitos relacionados con el contenido". Tipifica los delitos informáticos que son concurrentes por cibercriminales.

- **Decreto 1295 de 2010 Nivel Nacional**
  "Por el cual se reglamenta el registro calificado de que trata la Ley 1188 de 2008 y la oferta y desarrollo de programas académicos de educación superior"[37].
  Se encarga de reglamentar el registro calificado de la cual habla la ley 1188 de 2008 y oferta y el desarrollo de los diferentes programas académicos en instituciones de educación superior. Entre esos los estudios de programas virtuales.

  El decreto describe la manera de cómo deben estar estructurados los programas virtuales en instituciones de carácter superior, apoyados por las tecnologías.

- **Ley 1978 de 2019**
  "Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.

  En su artículo 3, "Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones". En este artículo busca garantizar la priorización del acceso a las tecnologías y comunicaciones, "en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad" [38].

[36] Normograma.mintic.gov.co. [Sitio Web]. Ley 1928 de 2018. [Consulta 14 abril 2021]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/ley_1928_2018.htm
[37] mineducacion.gov.co. [Sitio Web]. Decreto 1295 de 2010. [Consulta 20 abril 2021]. Disponible en: https://www.mineducacion.gov.co/1621/articles-229430_archivo_pdf_decreto1295.pdf
[38] Alcaldiabogota.gov.co. [Sitio Web]. Ley 1978 de 2019 Nivel Nacional. [Consulta 25 septiembre 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=85632

5 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN QUE SE PRESENTAN AL USAR HERRAMIENTAS INFORMÁTICAS PARA EL DESARROLLO DE CLASES VIRTUALES POR PARTE DE DOCENTES Y ESTUDIANTES EN COLOMBIA.

Los riesgos en las plataformas virtuales que son una de las herramientas más utilizadas en las en el apoyo de las instituciones educativas para impartir su enseñanza puede ser atribuibles a varios actores.

5.1 RIESGOS PROPORCIONADOS POR EL PROFESOR.

Los profesores, tutores, guías según sea la denominación de la institución educativas son los encargados de subir material (documentos, videos, audios, test, entre otros) en este punto existen dos riesgos inminentes el primero por derechos de autor donde se infrinja esta norma y la institución sea sancionada y el segundo subir material o enlaces con que contenga algún tipo de código malicioso es por ello que todos los elementos de la plataforma deben ser revidada de manera minuciosa.

Los encargados de los riesgos deben estar a cargo del centro educativo a través de un equipo interdisciplinario, ya que los profesores pueden ser transitorios.

5.2 RIESGOS PROPORCIONADOS POR LOS DIRECTIVOS Y ADMINISTRADORES DE LAS HERRAMIENTAS INFORMÁTICAS O PLATAFORMA VIRTUALES.

En este contexto otra persona se hace pasar por algún estudiante, suplantado la identidad y pueda enviar documentación infectada por algún tipo de malware por medio de los foros de la plataforma o chat de las Videollamadas.

La directiva es la encarda de la vigilancia de las inscripciones a los cursos y los estudiantes que estén avalados para participar de las clases de los cursos inscritos por esa persona.

Los administradores de las plataformas virtuales y demás herramientas informáticas como software de video llamadas que ayudan a impartir las clases virtuales tienen la responsabilidad de salvaguardar las credenciales de acceso al momento de delegar funciones.

5.3 RIESGO PROPORCIONADO POR LOS DESARROLLADORES.

El equipo de desarrollo debe mitigar los problemas en las plataformas educativas virtuales y herramientas informáticas (Mensajería, Videollamadas, foros, entré otros) y las fallas de seguridad. Es por ello que los desarrolladores deben conocer muy bien los ataques informáticos que hoy en día aqueja, por lo tanto, el código informático debe estar protegido.

5.4 RIESGOS PROPORCIONADOS POR LOS ESTUDIANTES.

Los estudiantes pueden ser de diferentes niveles de educación desde la primaria hasta los postgrados, en la cadena alimenticia de un ciberdelincuentes puede convertirse en la puerta de entrada para un ataque informático avanzado. Al momento de utilizar sus credenciales de acceso a una plataforma u otra utilidad destinada a recibir clases virtuales debe de tener precaución con el uso de la misma, debido a que es la manera más fácil de propiciar un ataque sin mucho esfuerzo por parte de un ciberdelincuente.

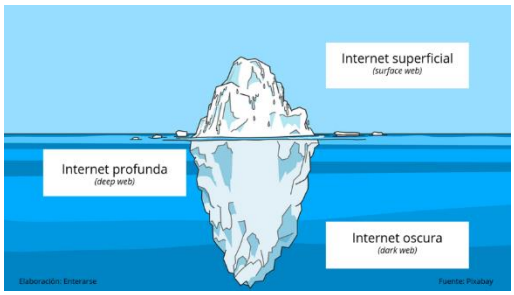
Los estudiantes deben de tener conocimiento sobre técnicas de ciberataques tales como el *phishing* ya que por medio está el estudiante puede ingresar a páginas parecidas a la plataforma de su institución e ingresar información confidencial.

5.5 RIESGOS SEGÚN LA INFORMACIÓN.

La información que existe en internet es amplia y por ello se puede presentar que la información sea falsa, inapropiada, novia, peligrosa e inmoral. Como es posible nombrar riesgos como violencia, racismo, xenofobia, terrorismo, pedofilia, drogas, entre otros. ***Dark Web***[39] (Internet Oscuro) *y* ***Deep Web*** (Internet profunda) son todas aquellas páginas que no está indexadas por los buscadores más populares, para acceder a este tipo de información es necesario utilizar otra red como *TOR (The Onion Router),* la cual permite ser difícilmente rastreable.

En la Figura 7, es fácil ver los diferentes niveles considerados en la web como son: Internet superficie *(Surface web),* internet profundo *(Deep web)* e internet oscuro *(Dark web).*

Figura 7. Niveles de la Web



Fuente: enterarse.com. [Sitio Web]. Lo más profundo del Internet: ¿qué son la Deep web y la dark web? [Consulta 01 mayo 2021]. Disponible en: https://www.enterarse.com/img-deeeep.png.

[39] INISEG, Instituto Internacional de Estudios en Seguridad Global. [Sitio Web]. Peligros de la Dark Web: el lado oscuro desconocido. [Consulta 01 mayo 2021]. Disponible en: https://www.iniseg.es/blog/ciberseguridad/los-peligros-de-la-dark-web/

5.6 RIESGOS QUE SE RELACIONAN CON INTERACCIÓN INTERPERSONAL.

La interacción interpersonal por medio electrónicos como mensajes de texto, chat, entre otros, son necesario al momento de realizar la educación virtual, aunque este tipo de comunicación se convierte en un factor de riesgo, ya que, los cibercriminales por medio de mensajes pueden enviar enlaces que aparentan legitimidad y de esta manera pueden obtener datos relevantes. La ingeniería social es una de las técnicas más utilizada en esta época de pandemia difundida por medio de los teléfonos.

El *Smishing* es uno de las técnicas donde el atacante envía un mensaje de texto al celular y el usuario debe intervenir para poder ser efectivo el ataque, en la Figura 8 es posible ver un ejemplo de la ingeniería social, por medio de un mensaje solicitan que la víctima se comunica a ciertos números de teléfonos para luego “obtener un premio”.

Figura 8. Utilización de Ingeniería social por medio de Smishing (Caso real)

Fuente: autor

5.7 RIESGOS REFERENTES A REPERCUSIONES ECONÓMICAS[40].

Internet proporciona un gran número de información. Spoofing es una de técnicas utilizada para suplantar sitios web y pharming consiste en redirigir la página legítima a otra falsa para que el usuario crea que está en la página que él digitó, estas dos prácticas son utilizada en su mayoría para que los usuarios ingresen datos financieros, convirtiéndose en una trampa para cualquier tipo de persona.

5.8 OTROS RIESGOS POTENCIALES.

- Las redes sociales se han convertido en una de las plataformas de mayor difusión a nivel mundial, los profesores en muchas ocasiones utilizan para realizar sus clases virtuales con la utilización de las mismas aun que es importante tener mucha precaución ya que es una red mundial y los datos brindados en ellas son en muchas ocasiones de carácter público y de la misma forma son plataformas muy asesinadas por ciberdelincuentes.

- El préstamo de dispositivos a los estudiantes representa un riesgo ya que al momento de usarlos la conexión a internet en su casa no es controlada, descarga de documentos, archivos, entre otros[41].

- Los ciberataques en uno de los riesgos con mayor prevalencia al momento de realizar actividades por internet, en especial las clases virtuales y la utilización de las plataformas educativas, ya que los estudiantes pueden ingresar a enlaces que pueden aparentar ser legítimos.

- La falta de experiencia y de conocimiento necesario en cuanto a la descarga de aplicaciones, ingreso a enlaces y descarga de archivos que puedan poseer software y código malicioso por parte de los dos actores estudiantes y profesores corresponde en un porcentaje alto al momento de infecciones de malware.

- los correos representan un potencial de riesgo tanto para docentes como alumnos ya que pueden existir, alteraciones de los mensajes, mensajes que puede ser falsificados*, Man in the medidle* (hombre en el medio)[42].

- La información contenida en los servicios en la nube, constituyen un riesgo inminente debido a que la información esta compartida en internet, mucho de las instituciones

[40] Elteimpo.com. [Sitio Web]. Estas son las prácticas más usadas de suplantación de sitios web. [Consulta 01 mayo 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/suplantacion-de-sitios-web-que-es-el-spoofing-y-pharming-568652

[41] redalyc.org. [Sitio Web]. Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. [Consulta 26 abril 2021]. Disponible en: https://www.redalyc.org/jatsRepo/1941/194161290017/html/index.html

[42] Recursosdigitales.anuies.mx. [Sitio Web]. Plataformas y recursos digitales ante la contingencia de la COVID-19. [Consulta 26 abril 2021]. Disponible en: https://recursosdigitales.anuies.mx/ciberseguridad-para-educacion-en-linea/

educativas utilizan servicios gratuitos para alojar archivos y compartirlos, llámense trabajos que contienen información de estudiantes, videos, entre otros.

- Las nuevas tecnologías que comienzan a surgir y hacer parte de la vida cotidiana, *IoT* (Internet de las cosas) es adaptables a la vida asistida por la tecnología, hacen parte de ello, *Smart TV*, relojes, manillas y altavoces inteligentes. La utilización de los dispositivos *IoT* en nuestras vidas cada vez es mayor y su utilización en diferentes actividades también. Teniendo en cuenta que esta tecnología ha sido atacada con mayor relevancia[43].

- Ataque Día 0 *o Zero Day*, son las vulnerabilidades de las aplicaciones o dispositivos tecnológicos que no han sido identificadas y los cibercriminales aprovechan esta brecha de seguridad para poder realizar sus crimines.

Los riesgos en el ciberespacio siempre van a estar presente, los usuarios son propensos a generar errores y no tener precaución al momento de navegar y utilizar las herramientas digitales disponibles para su educación y trabajo. Se suma a esto las diferentes amenazas que son persistentes ya que es al igual que en el mundo físico también al mundo digital lo aquejan también males sobre delitos cibernéticos.

5.9 ALGUNOS RIESGOS AL USAR APLICACIONES DE VIDEOLLAMADAS[44]

La gran utilización de estas herramientas, ha llamado la atención a que las miradas se tornen a este tipo de plataformas. Este tipo de situación conlleva a conocer factores de riesgos que mitiguen los riesgos a reducir incidentes de ciberseguridad.

- la perdida, robo, divulgación de información financiera o personal es posible que ocurra al momento de usar aplicaciones de videollamas, esto ocasionado por el cifrados inseguros, a su vez es posible mitigar con el uso de herramientas que realicen el cifrado de extremo a extremo (*E2EE, end-to-end encryption).*

- Es posible que ocurran extorsión luego de escuchar toda una conversación, luego de que un ciberdelincuente haya ingresado a la conferencia con el interés de conocer más fondo sobre usuarios conectados realizando *Bombing.*

- Receso de las actividades académicas por un lapso de tiempo considerable que puede verse representado en días por medio del ataque de denegación de servicio

[43] INISEG, Instituto Internacional de Estudios en Seguridad Global. [Sitio Web]. Lista de 15 consejos de Ciberseguridad para tener una vida cibersegura. [Consulta 01 mayo 2021]. Disponible en: https://www.lisainstitute.com/blogs/blog/lista-consejos-ciberseguridad-vida-cibersegura

[44] Incibe_, Instituto Nacional de Ciberseguridad. [Sitio Web]. Videollamadas: riesgos asociados a su uso y recomendaciones de seguridad. [Consulta 7 marzo 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/videollamadas-riesgos-asociados-su-uso-y-recomendaciones-seguridad.

(DoS), estos ataques consisten en sobrecargar por muchas peticiones la plataforma de videoconferencia con el fin de que no se pueda acceder al servicio.

5.10 TÉCNICAS EN CIBERSEGURIDAD PARA MITIGAR RIESGOS[45]

- Autenticación por medio de los dos pasos, se limita y mitiga en acceso a usuarios sin la debida autorización, correspondiente a filtros de la privacidad.

- Crear una lista blanca de sitios *web* y aplicaciones para los profesores y alumnos de las cuales puedan visitar y acceder con confianza al momento de descargar o navegar.

- Limitar la cantidad de administradores en un sistema, de esta manera la exposición será menor y que puedan realizarse cambios, controlando la seguridad.

- Realizar segmentación de la red, es posible que un intruso tenga acceso a la red, pero de esta manera solo tendrá el acceso a una parte de la red y el resto estará seguro.

- Bloquear las puertas traseras, el acceso de usuarios tercero puede abrir puertas traseras a los cibercriminales.

- Realizar respaldo de la información relevante e importante.

- Actualización del sistema operativo y realización de auditoria periódica verificando que el sistema esté protegido.

[45] Magisnet.com. [Sitio Web]. Los seis riesgos de internet para los centros educativos. [Consulta 2 marzo 2021]. Disponible en: https://www.magisnet.com/2019/11/los-seis-riesgos-de-internet-para-los-centros-educativos/.

6 AMENAZAS, LAS VULNERABILIDADES E IMPACTOS DE LAS HERRAMIENTAS INFORMÁTICAS MÁS UTILIZADAS PARA EL DESARROLLO DE CLASES VIRTUALES POR PARTE DE ESTUDIANTES Y DOCENTES.

6.1 AMENAZAS EN LA EDUCACIÓN VIRTUAL[46] .

La educación en nuestros días ha cambiado de manera vertiginosa debido a las consecuencias de la pandemia por el virus *COVID – 19*, para el año 2020 las instituciones educativas trasladaron las clases a la virtualidad y ello trajo la utilización masiva de la tecnología y la conexión a internet.

En el mundo digital también existen peligros y riesgos. Estos son variables que se han ido incrementando y al mismo tiempo las vulnerabilidades también han ido creciendo, en la tabla 1, se pueden observar las más relevantes.

Tabla 1 Principales Amenazas en la Educación Virtual

Principales Amenazas	Descripción
Violación de la confidencialidad	Personas no autorizadas que de alguna manera fraudulenta obtienen acceso sin autorización a los activos a un sistema de *E-learning.*
Violación de la integridad	Personas no autorizadas que se apropian de un activo por medio de acceso ilegitimo de las *plataformas E-learning.*
Denegación de servicio	Interrupción del tráfico entre la plataforma e-learning y los usuarios al momento de intentar ingresar de manera legítima.
Uso ilegitimo	Usuarios legítimos que poseen accesos con privilegios por medios fraudulentos.
Programas maliciosos	Son línea códigos que pueden hacer daños a otro software o programas informáticos.
Repudio	Negar la participación de alguno de los usuarios de la plataforma *E-learning.*
enmascaramiento	Cuando el ciberdelincuentes de alguna manera puede esconder su identidad utilizando usuarios legítimos.
Análisis de trafico	Técnica de escaneo de puertos y tráfico, la cual puede dar bastante información al atacante.

Fuente: repository.usc.edu.co. Repositorio Universidad Santiago de Cali. [Sitio Web]. Plataformas E-Learning, sus riesgos y amenazas. [Consulta 25 abril 2021]. Disponible en:

[46] repository.usc.edu.co. repositorio Universidad Santiago de Cali. [Sitio Web]. Plataformas E-Learning, sus riesgos y amenazas. [Consulta 25 abril 2021]. Disponible en: https://repository.usc.edu.co/bitstream/handle/20.500.12421/1733/PLATAFORMAS%20E-LEARNING.pdf?sequence=1&isAllowed=y

https://repository.usc.edu.co/bitstream/handle/20.500.12421/1733/PLATAFORMAS%20E-LEARNING.pdf?sequence=1&isAllowed=y

Tabla 1. (Continuación)

Principales Amenazas	Descripción
Ataque de fuerza bruta	Intentos posibles que el atacante realiza para poder conseguir los accesos de usuarios a la plataforma *E-learning*.
Secuestro de información.	Malware dedicados a encriptar la información de un sistema informático y luego el ciberdelincuentes pide una recompensa por descifrar la información.

Fuente: repository.usc.edu.co. Repositorio Universidad Santiago de Cali. [Sitio Web]. Plataformas E-Learning, sus riesgos y amenazas. [Consulta 25 abril 2021]. Disponible en: https://repository.usc.edu.co/bitstream/handle/20.500.12421/1733/PLATAFORMAS%20E-LEARNING.pdf?sequence=1&isAllowed=y

6.2 SEGÚN SU FUNCIÓN LAS AMENAZAS TAMBIÉN PUEDEN CLASIFICARSE[47]

- ***Spoofing****,* Suplanta la identidad de un *PC* (Computador Personal) o algún dato del mismo como su dirección *MAC* (Control de acceso a medios).

- ***Sniffing****,* es una técnica que se encarga de analizar y monitorear todo tráfico para capturar información en la red.

- **Conexión no autorizada,** se utiliza para buscar puertas traseras o agujeros sean en un servidor o equipo de cómputo, con el fin de realizar una conexión no autorizada.

- ***Malware,*** son todos aquellos programas con una finalidad de realizar daño a un sistema informático o infraestructura de red con el fin de obtener un beneficio por medio de la información captada.

- ***Keyloggers,*** Son software o hardware que permiten captar todo lo que el usuario digita o teclea, incluso pueden llegar a realizar la captura de la pantalla.

- **Denegación de Servicio,** Es una interrupción de servicios ofrecidos por medio de un servidor o red informática, conocida también como DoS *(Denial of Service*).

- **Ingeniería social,** es la obtención de la información de una organización o persona con fines delictivos, los ejemplos de mayor difusión son el spam y phishing.

[47] Universidad Internacional de valencia. [Sitio Web]. ¿Qué es la seguridad informática y cómo puede ayudarme? [Consulta 11 marzo 2021]. [5]disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme.

- ***Phishing,*** Consiste en un engaño a los usuarios por medio de suplantación de identidad de una página web u organismo privado o gubernamental.

6.3 AMENAZAS EN LA SEGURIDAD INFORMÁTICA AL MOMENTO DE UTILIZAR LAS TIC (TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN) EN EL ÁMBITO DE LA EDUCACIÓN.[48]

- ***Hackers,*** Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas, pero sin motivación económica o dañina.

- ***Sniffers,*** Expertos en redes que analizan el tráfico para obtener información extrayéndola de los paquetes que se transmiten por la red.

- ***Lammers,*** Chicos jóvenes sin grandes conocimientos de informática pero que se consideran a sí mismos hackers y se vanaglorian de ello.

- **Ciberterrorista:** Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y saboteadores informáticos.

- **Programadores de virus:** Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.

6.4 PRINCIPALES VULNERABILIDADES EN LAS CLASES VIRTUALES[49].

En muchas ocasiones los ciberdelincuentes aprovechan las situaciones en que los estudiantes y profesores aumentan su búsqueda de información por internet la cual pueden ingresar a información fraudulenta.

- Muchas veces los estudiantes y profesores descargan información y aplicaciones de las páginas no oficiales lo cual son legítimos, pero con código malicioso.

- Las redes sociales (*Twitter, YouTube y Facebook),* son muy apetecidas por los estudiantes e incluso profesores las utilizan para difundir clases, aun cuando también son las predilectas de los ciberdelincuentes para difundir los malware.

[48] [Sitio Web]. ¿Qué es la seguridad informática y cómo puede ayudarme? [Consulta 11 marzo 2021]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme.

[49] Mibolsillo.com. [Sitio Web] ¿Tienes clases virtuales? Podrías ser víctima de ciberdelincuentes. [Consulta 26 abril de 2021]. Disponible en: https://www.mibolsillo.com/tecnologia/Tienes-clases-virtuales-Podrias-ser-victima-de-ciberdelincuentes-20200926-0014.html

- Tanto estudiantes y profesores, por el hecho de poder cumplir con sus compromisos y los cronogramas establecidos, se ven en la necesidad de conectar al internet en cualquier lugar que estén para no perder la clase virtual, en muchas oportunidades realizan conexiones a internet de redes públicas o empresariales dispuestas a los clientes.

- Los equipos tecnológicos deben estar actualizados en sus sistemas operativos y también las aplicaciones para videoconferencias deben estar descargada las últimas versiones desde las páginas oficiales.

- Compartir las credenciales de acceso por parte de estudiantes en redes o grupos de mensajería instantánea con el fin que otras personas puedan ingresar a las clases virtuales[50].

- Una de las vulnerabilidades que poseen los estudiantes y docentes al momento de utilizar plataformas, recursos digitales y servicios en la nube es guardar las contraseñes en los navegadores, constituyéndose así en una puerta abierta para que los ciberdelincuentes puedan obtener todas las credenciales de acceso a los diferentes portales y sitios web. En mucho de los casos los dispositivos que usan los estudiantes son de sus padres, ellos también tienen esta mala práctica por lo tanto es posible que haya información guardada de portales bancarios.

6.5 IMPACTO SOBRE NUESTROS DISPOSITIVOS.

Los dispositivos móviles (Celulares y Tablet) son en su mayoría la herramienta tecnológica de muchos de los estudiantes, las cuales a su vez son el blanco potencial de ciberdelincuentes para ser infectados con malware y poder así de esta manera tener acceso a todos sus archivos e incluso por tener ingreso a un sistema completo.

- Los usuarios de los dispositivos móviles acostumbran a dejar sus credenciales de acceso almacenadas, datos relevantes en la galería de imágenes, al igual que notas de contraseñas, entre otros. En caso de robo o pérdida resultarían un blanco con mayor porcentaje de acceso a la información.

- Siendo los más pequeños y personas desprevenidas la vulnerabilidad más relevante a la exposición de ataques, es posible que en ciertos momentos descarguen app (Aplicación móvil) de tipo maliciosa, la cual puede ser posible que se eliminen o utilicen los datos de los dispositivos sin consentimiento del propietario.

- Las redes *WiFi* Publicas, pueden ser convertidas en una telaraña para atrapar incautos navegantes de internet, debido a que no es posible saber que personas esté

[50] welivesecurity.com. [Sitio Web].10 consejos para proteger la información de instituciones educativas. [Consulta 26 abril 2021]. Disponible en: https://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/

conectada, es así que nuestro dispositivo móvil seria la puerta predilecta para la entrada el ciberdelincuentes.

6.6 VULNERABILIDADES EN APP DE VIDEOCONFERENCIAS[51].

Los diferentes recursos que existente en el mercado de la tecnología que han sido utilizadas en las clases virtuales para crear aulas virtuales sincrónicas, en algún momento en el trascurso de la utilización masiva de ellas en el tiempo de pandemia, han experimentado vulnerabilidades soportada por denuncias de los usuarios y entidades especializadas que han encontrado serias fallas al momento de ser utilizadas. No tener tanto conocimiento en el manejo de ellas, genero al principio de pandemia del COVID-19 que las vulnerabilidades y riesgos fueran mayor, debido a que los usuarios no proporcionaban de manera correcta los controles necesarios de seguridad y este desconocimiento conllevo a que se utilizara plataformas poco comunes y sin mucho soporte por sus proveedores, ocasionando un sin número de dificultades tanto para los administradores de las reuniones como para los participantes.

Google meet, Skype, Zoom, Microsoft Teams, WhatsApp, GoToMeeting, Webex de Cisco, entre otras, herramientas o aplicaciones que mitigan el impacto de la pandemia al no poder reunirse de manera presencial para evitar el contagio del nuevo coronavirus. Las entidades educativas adoptaron la tecnología de forma rápida por medio de plataformas educativas y videollamadas, aunque con ello se aumentó el riesgo ser atacados por delincuentes cibernéticos que han cambiado el modo de operar y su mirada giró hacia las personas en teletrabajo, estudiantes y docentes.

Los ciberdelincuentes buscan la parte más débil de la cadena alimenticia en el ciberespacio, se puede considerar que los más débiles pueden ser los menores de edad y personas con poco conocimiento en tecnología y es allí donde los delincuentes realizan sus investigaciones llamado como ingeniería social y apechar esta vulnerabilidad. Son eslabones importantes claves para que un ciberdelincuentes tenga el poder a la hora obtener información relevante.

- **Vulnerabilidades en *WhatsApp*.** Al igual que otras utilidades para la comunicación, la mensajería instantánea ha realizado un gran aporte a las clases virtuales con la facilidad de su utilización a su favor *WhatsApp* ha logrado recortar distancia e intercambio de información. Aunque este auge también ha traído consigo mayor interés para los delincuentes del ciberespacio que han encontrado la manera de poder tener acceso a las conversaciones.

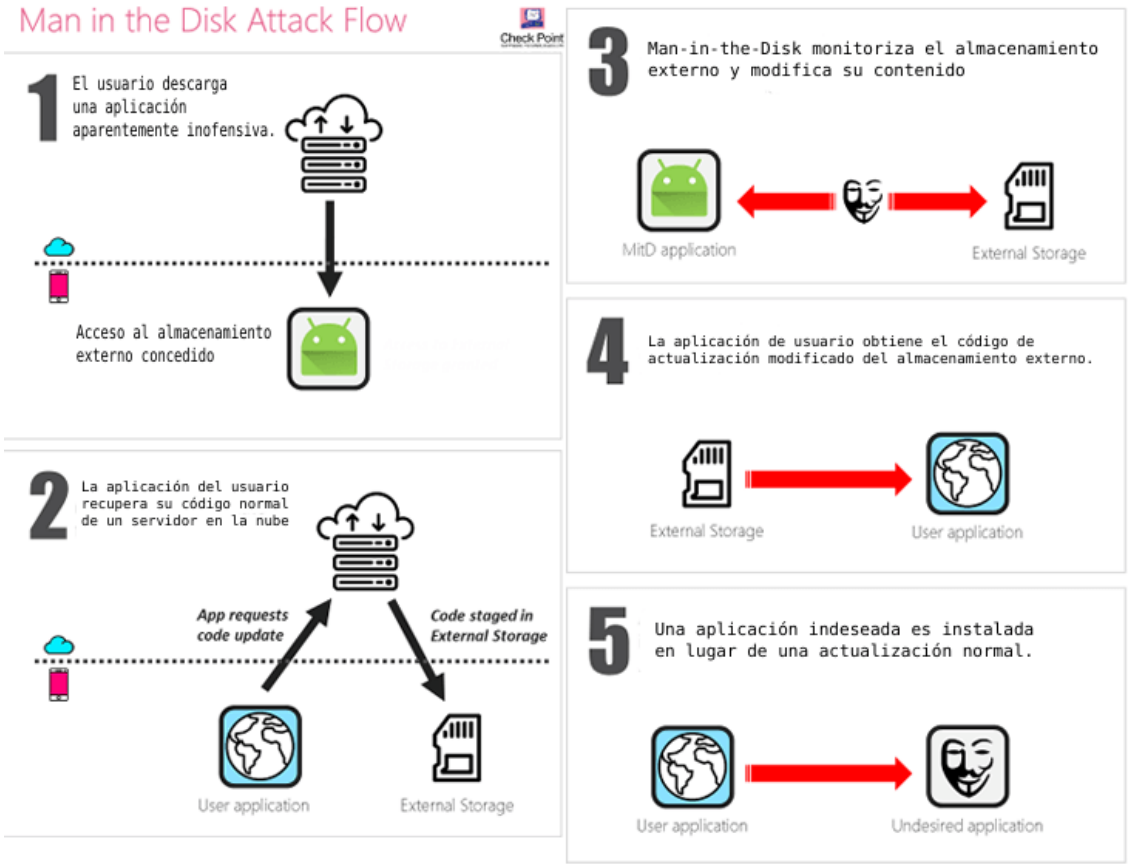
    - *Man in the Disk*, es uno de los ataques que permite *WhatsApp* en los dispositivos con sistema operativo Android, el atacante es capaz de poder instalar un malware

[51] Kaspersky.es. [Sitio Web]. Los problemas de las aplicaciones de videoconferencia. [Consulta 12 septiembre 2021]. Disponible en: https://www.kaspersky.es/blog/videoconference-software-security/22549/

en el dispositivo, según sean los permisos del dispositivo y de esta manera es posible el acceso a la información del almacenamiento externo.

En la Figura 9, se evidencias los pasos que realiza un ciberatacante para poder realizar la técnica de *main in the Disk* sobre un sistema operativo *Android* de un dispositivo móvil.

Figura 9. Man in the Disk



Fuente: Unaaldia.hispasec.com. [Sitio Web]. Un fallo en WhatsApp permite ataques Man in the Disk. [Consulta 04 junio 2021]. Disponible en: https://unaaldia.hispasec.com/2021/04/bug-de-whatsapp-vulnerable-a-ataques-man-in-the-disk.html

- Suplantación de identidad, por medio de un mensaje donde pide que se envié un código de *SMS* (Servicio de mensajes cortos). Los delincuentes una vez obtienen los números de telefónicos, descargan WhatsApp e inician el proceso de validación en su *smartphone* pidiendo la confirmación que llega a la víctima por medio de un mensaje. Una vez que la cuenta está en manos de los ciberdelincuentes suplantan la identidad de la víctima y en ese momento comienzan a enviar mensajes solicitando ayudas económicas.

Todas las personas están en riesgo de sufrir algún tipo de ataques, en la Figura 10, el secretario de gobierno de Bogotá, Luis Ernesto Gómez, sufrió un ataque en su cuenta de *WhatsApp* el día 5 de abril de 2021 y por medio de su cuenta de *Twitter* lo manifestó.

Figura 10. Suplantación de identidad

Fuente: Lafm.com.co. [Sitio Web]. Hackearon WhatsApp de Luis Ernesto Gómez, secretario de Gobierno de Bogotá. [Consulta 06 junio 2021]. Disponible en: https://www.lafm.com.co/bogota/hackearon-whatsapp-de-luis-ernesto-gomez-secretario-de-gobierno-de-bogota

- **Vulnerabilidades en *Google Meet y Google Duo*.** Estas dos herramientas de ofrecen los servicios de videollamas, realiza la recopilación de información de los diferentes datos de los usuarios, lo que puede ocasionar daños en los datos sensible en los diferentes sectores especialmente en el comercial.

- **Vulnerabilidades en *Slack*.** Aplicaciones que permite crear conversaciones que es posible mostrarse en una ventana, la cantidad de participantes es de 15 usuarios al tiempo. Una de los principales inconvenientes es que permite la integración de aplicaciones de terceros de las cuales la seguridad no le pertenece a *Slack* y no maneja un cifrado de externo a extremo.

- **Vulnerabilidades en Microsoft *Team*.** Es una aplicación integrada al paquete ofimático *office* 365, diseñada principalmente para trabajo en equipo empresariales. Aun que Microsoft acostumbra a realizar las actualizaciones contantes y parchar sus

vulnerabilidades de manera rápida, *"Microsoft has fixed a subdomain takeover vulnerability in its collaboration platform Microsoft Teams that could have allowed an inside attacker to weaponize a single GIF image and use it to pilfer data from targeted systems and take over all of an organization's Teams accounts*. (Ya fue corregida)[52]".

- **Vulnerabilidades en *Skype* Empresarial 2019**. Precede a *Microsoft Team* sigue usándose, por ser considerado más practico por algunos usuarios, aun que permite la ejecución remota de código – CVE -2021-26422[53] - (ya corregida[54]). La aplicación estará soportada para la versión empresarial server 2019 hasta octubre de 2025.

- **Vulnerabilidades en *WebEx Teams y WebEx Meetings*.** en marzo del 2020 cisco como proveedor parcheo dos de sus vulnerabilidades las cuales podían ejecutar código de forma remota. En ***WebEx Teams*** para el año 2019 existía una brecha que posibilitaba la ejecución de comando como si fuera un usuario.

- **Vulnerabilidades en *Zoom*.** Aplicación que ha surgido de manera vertiginosa a raíz de la pandemia. *Zoom* anunció que implemento un cifrado de externo a extremo, no está aún del todo claras las políticas de uso ya que el descifrado lo realiza en sus servidores y en un país diferente a su origen.

  Los usuarios de los dos sistemas operativos de mayor amplio uso a nivel de usuarios final informaron de sucesos con sus cuentas, la cual permitía a atacantes robar datos de las cuentas de los ordenadores (Solucionado)[55] y además en *MacOS* los delincuentes podían tomar el control de los dispositivos[56].

  Además de la cantidad de noticias sobre la interrupción en las clases virtuales y videoconferencias sin restricciones donde podían troles publicar contenido inadecuado y poder realizar comentarios entre otros, estas dos vulnerabilidades se corrigen por medio de una buena configuración.

---

[52] Threatpost.com. [Sitio Web]. Single Malicious GIF Opened Microsoft Teams to Nasty Attack.[Consulta 12 Septiembre de 2021].Disponible en:https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/

[53]Cve.mitre.org. [Sitio Web]. CVE-2021-26422. [Consulta 18 noviembre 2021]. ¿Disponibilidad en:https://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2021-26422.

[54] Support.microsoft.com. [Sitio Web]. Descripción de la actualización de seguridad de Skype Empresarial Server y Lync Server: 11 de mayo de 2021 (KB5003729). [Consulta 18 noviembre 2021]. Disponible en:https://support.microsoft.com/es-es/topic/descripción-de-la-actualización-de-seguridad-de-skype-empresarial-server-y-lync-server-11-de-mayo-de-2021-kb5003729-3a6def2e-4b74-480e-bf24-fbec151f10a0

[55] Pcworld.com. [Sitio Web]. Update: Zoom issues fix for UNC vulnerability that lets hackers steal Windows credentials via chat. [Consulta 12 septiembre 2021]. Disponible en: https://www.pcworld.com/article/3535373/report-hackers-can-steal-windows-credentials-via-links-in-zoom-chat.html

[56] Forbes.com. [Sitio Web]. Zoom Users Beware: Here's How A Flaw Allows Attackers To Take Over Your Mac Microphone And Webcam. [Consulta 12 septiembre 2021]. Disponible en: https://www.forbes.com/sites/kateoflahertyuk/2020/04/01/zoom-users-beware-heres-how-a-flaw-allows-attackers-to-take-over-your-mac-microphone-and-webcam/

6.7 IMPACTO DE LAS HERRAMIENTAS INFORMÁTICAS EN LAS CLASES VIRTUALES.

Los cierres de escuelas e instituciones educativas enfrentadas a la realidad de la educación virtual en plena pandemia, ocasiono desigualdad precisamente en el uso de la tecnología y de las herramientas tecnológicas enfocadas a la educación.

- Los docentes comenzaron a usar herramientas tales como *Zoom, meet, Microsoft teams,* plataformas educativas y con ello experimentaron sucesos inesperados, en donde se vieron afectados por la intromisión de ciberdelincuentes a sus clases virtuales ocasionando temor de volver a ingresar a sus aulas virtuales.

  Una de las afectaciones negativas es el uso excesivo de la tecnología ya que sus clases son realizadas por dichas herramientas, es por ello que al pasar mucho tiempo conectados a sus despóticos (Ordenadores, Tablet o televisión) dejan a un lado la realidad y de esta manera se les hace difícil la interacción social[57].

- Estar frente a una pantalla en sus clases virtuales los alumnos generaron niños más pasivos, al igual que la interacción física con los demás compañeros interfiere en el desarrollo saludable.

[57] Scp.com.co. [Sitio Web]. Tecnologías digitales y los niños, efectos positivos y negativos. [Consulta 29 octubre 2021]. Disponible en:https://scp.com.co/actualidad-pediatria-social/tecnologias-digitales-y-los-ninos-efectos-positivos-y-negativos/

7 BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA DOCENTES Y ESTUDIANTES, QUE LE PERMITAN SALVAGUARDAR LA CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD DE SU INFORMACIÓN.

Con el fin de mitigar la pérdida de información al momento de estar conectados en las clases virtuales y evitar algunas intromisiones sin autorización o pérdida de información es conveniente seguir ciertas recomendaciones:

7.1 PARA EL REGRESO A LAS CLASES VIRTUALES[58].

- Dar clic a los enlaces de fuentes oficiales o seguras al momento de acceder a las plataformas virtuales de la institución educativa, las cuales haya sido enviada por la persona anfitriona de la clase virtual. Ya que pueden ser víctimas de phishing por medio de enlaces recibidos por correo.

- Tener claves robustas en las cuentas de usuarios, debido a que las contraseñas sencillas son muy fáciles de descifrar por parte de los cibercriminales, tales como: admin, 123456, 0000, nombre del hijo, fecha de cumpleaños, entre otras.

- No se recomienda compartir información confidencial por las herramientas online que estén utilizando en el momento de los encuentros virtuales.

7.2 PARA LOS PADRES Y MADRES QUE ESTÁN ENFRENTE DEL PROCESO EDUCATIVO DE SUS HIJOS.

- Dedicar un tiempo para los hijos y hablar de ataques como es el phishing, para que no den clic en correos antes de consultarle a ellos.

- Adquirir conocimientos básicos en ciberseguridad es necesario debido a la proliferación de delitos informáticos sobre robo de datos.

- Fomentar un pensamiento crítico a niños, niñas y jóvenes sobre la información obtenida en internet y que ellos puedan analizar su contenido.

- Las bromas que realizan online sobre comentarios de manera hiriente es necesario explicar a los hijos que no está bien. Ya que puede convertirse en un Ciberacoso.

- Los dispositivos tecnológicos (Ordenadores, portátiles, celulares, Tablet, entre otros) no deben estar desatendidos sin ningún tipo de vigilancia, ya que, en manos de los cibercriminales, ellos pueden usarlos y asumir la identidad de una niña o niño.

[58] PCWorld. [Sitio Web]. Los ciberriesgos de la educación online (Y cómo evitarlos). [Consulta 21 abril 2021]. http://pcworld.com.mx/los-ciberriesgos-de-la-educacion-online-y-como-evitarlos/

- Establecer los controles parenterales en los dispositivos tecnológicos estableciendo en su configuración la seguridad y privacidad para sitios web sobre compartir información.

  Las clases virtuales se convierten en una forma de normalidad y al igual tanto docente como estudiantes deben seguir aplicando las mismas normas que en un salón de clase físico.

7.3 DOCENTES ANTES Y DESPUÉS DE ENTRAR A CLASES VIRTUALES[59].

- El docente antes de entrar a su sesión virtual debe de protegerla por medio del ID sin que tenga que publicarlo en alguna red social, se recomienda enviarlo solo a los que van a participar de las clases virtuales.

- Realizar lista de personas autorizadas para las clases virtuales y muy recomendado pasar la lista como su estuvieran el aula física.

- En lo posible colocar contraseñas al acceso del aula virtual la cual está destinada para la clase virtual asignada.

- Mantener apagado el audio y video de los participantes y demás herramientas de la aplicación utilizada.

- Deshabilitar el chat entre los participantes de manera privada, solo debe quedar uno general para evitar mensajes individuales.

- Si es posible bloquear la sesión a la clase virtual una vez se esté seguro que estén todos los participantes que a los cuales se les entrego ID de ingreso o enlace de acceso.

- Tener actualizada la plataforma educativa actualizada a la última versión con el fin de poder obtener correcciones de seguridad.

- Modificar las configuraciones por defecto, logrando una configuración personalizada y con mayor robustez.

- Se debe compartir pantalla solo la ventana donde está la información pertinente en el momento de la clase virtual, más no todo el escritorio. Ya que es posible que se pueda ver información confidencial que este en el escritorio.

[59] t13.cl. [Sitio Web]. Cómo realizar clases online seguras: consejos para evitar el Zoombombing o gate-crashing virtual. [Consulta 21 abril 2021]. Disponible en: https://www.t13.cl/noticia/nacional/como-realizar-clases-online-seguras-consejos-evitar-zoombombing-o-gate-crashing-virtual

- Si la clase virtual es grabada debe ser informada a los participantes de esta acción debido a que quedan datos biométricos almacenados (Rostro, ojos, fisionomía, entre otros).

7.4 SEGURIDAD DE LA NAVEGACIÓN EN TODA LA WEB

- Si es una *web* de recursos académicos, verificar si posee certificado de seguridad *htpps* y un candado en color verde.

- Revisar si existen opiniones de otros usuarios en recursos académicos online consultados.

- Tener habilitada la doble autenticación de contraseñas en las cuentas de usuarios de correo, plataformas, entre otros.

- Usar el sentido común al momento de navegar en la web.

- Evitar las compras sin permisos, supervisando de manera periódica cuando los hijos utilicen los dispositivos y estén conectados en las clases virtudes.

- Al no estar al frente de los dispositivos no dejar abiertas las sesiones de correos, plataformas, aplicaciones online, entre otros.

7.5 CIBERSEGURIDAD EN EL HOGAR.

- Protege con cifrados avanzados las claves de los dispositivos que proporcionan redes de internet *WiFi*.

- Cambiar las contraseñas predeterminada de los dispositivos que proporcionen conexiones *WiFi* en el hogar.

- No compartir las claves de las redes *WiFi* con otras personas ajenas al hogar.

- Estar alertas antes llamadas de supuestas empresas legales donde soliciten datos sensibles sobre algún servicio que posea.

- Desactivar la opción de compartir ubicación de los dispositivos tecnológicos a menos que sea necesario utilizar esta opción.

- Evitar envió de información por medio de formularios en línea de dudosa procedencia.

7.6 PROTECCIÓN DEL AULA VIRTUAL CON LA HERRAMIENTA *ZOOM*.

Es una de la herramienta tecnológica que ha hecho que tanto alumnos como profesores hayan logrado una rápida migración a la enseñanza virtual y es por esta razón se hace necesario tener en cuenta medidas de seguridad para su utilización60.

- En zoom es posible realizar el bloqueo del aula virtual, al igual que cerrar la puerta del aula de clase cuando ya tocó el timbre para el cambio de clase.

- Controlar el uso compartido de la pantalla, los profesores tienen la posibilidad de bloquear el uso de compartir la pantalla para evitar que los alumnos puedan presentar contenido que no está estipulado en la clase.

- Habilitar la sala de espera, la cual costa de dos opciones, la primera opción permite poner en espera todos los participantes para que pueden ser admitidos de uno en uno, la segunda opción es participantes invitados únicamente los usuarios registrados pueden ingresar sin espera mientras que lo que no están registrados quedan en la sala de espera.

- Restricción de uso del chat, el profesor tiene la posibilidad de bloquear el uso del chat para sus alumnos no puedan enviar mensajes privados, aun cuando el profesor puede quedar interactuando con todos ellos.

- Eliminar participantes, el profesor puede eliminar a las personas que no están invitadas o no hacen parte de la clase por medio de la lista de participantes, dando clic sobre él y le muestre la opción eliminar entre otras.

7.7 PROGRAMACIÓN DE LA CLASE CON ZOOM.

Al momento de programar una clase virtual la herramienta tecnológica Zoom dispone de opciones de protección para reuniones virtuales.

- Solicitud de registro con el fin de poder revisar los correos inscritos y así de esta manera poder evaluar qué tipo de participantes están inscritos.

- Usar *ID* de las reuniones aleatoriamente, con esta práctica se crean reuniones más seguras.

- Usar contraseña para proteger el aula virtual, compartir la clave con los alumnos por medio del correo institucional para que solo los que participaran puedan ingresar.

[60] Zoom. [Blog]. Prácticas recomendadas para proteger su aula virtual. [Consulta 02 junio 2021]. Disponible en: https://blog.zoom.us/es/best-practices-for-securing-your-virtual-classroom/

- Permitir solo usuarios autenticados, con el fin que solo los miembros de la institución educativa que estén registrados en a la cuenta Zoom pueden ser validados.

- Deshabilitar la opción de unirse antes del anfitrión, deshabilitando esta opción es posible que solo se puedan unir a la clase virtual cuando el profesor los admita. Les aparecerá un mensaje “La reunión está en espera de que acceda el anfitrión”

- Durante la clase virtual los profesores pueden deshabilitar el video y silenciar los alumnos.

7.8 RESTRICCIONES USANDO *GOOGLE MEET*[61].

Es uno de los servicios para videollamas que ofrece Google, se ha popularizado en medio de la pandemia, también utilizado en las clases virtuales para cualquier nivel de la educación.

- Es necesario contar una cuenta activa de *Google*.

- No es necesario la instalación de algún software, *plugin* o herramienta adicional en el navegador de internet para su utilización.

- Limita la cantidad de participantes a la videollamadas, al igual que no es posible el ingreso a ella antes de los 15 minutos de la hora asignada.

- Las personas notificadas por el calendario de Google pueden ingresar si realizar la solicitud de aceptación, a diferencia de los que no tienen invitación, deben enviar la invitación y ser admitidos por el moderador de la reunión.

- Los organizadores de las reuniones o videollamas tienen la posibilidad de gestionar los controles de seguridad según sea necesario.

- Los datos que se manejan de los usuarios participantes son cifrados en el momento de envió y de las grabaciones de *meet* que se almacenan en el servicio de *Google Driver*.

7.9 REUNIONES SEGURAS CON GOOGLE *MEET.*

- Es recomendable no divulgar los enlaces de las reuniones en redes sociales, o foros que sean públicos.

- Verificar que los participantes que comienzan a unirse sean conocidos.

[61] Nubalia.com. [Sitio Web]. Medidas de Google Meet para mantener tu seguridad y privacidad. [Consulta 6 junio 2021]. Disponible en: https://nubalia.com/medidas-google-meet-mantener-seguridad-privacidad/

- Activar o desactivar el “Acceso rápido” de las opciones de seguridad según sea el caso. Si ve anormalidad en la reunión lo más adecuado utilizar los controles de seguridad por parte del moderador en *Google Workspace for Education Fundamentals*[62].

- La información personal no debe ser compartidas en las videollamas o reuniones, tales como contraseñas, numero de cuentas de bancos o los números de tarjetas de crédito.

- Se recomienda la utilización de la verificación de credenciales de dos pasos para evitar que la cuenta sea usurpada.

7.10 CONTROLAR QUIEN LLEGA A LA REUNIÓN CON *MICROSOFT TEAMS*[63].

- Realizar la configuración de la sala de espera disponible en las opciones de reuniones, pueden ser usuarios que se unen directamente y usuarios que van a sala de espera.

- Las reuniones estructuradas, son las que la persona administradora o moderadora tiene la posibilidad de controlar la experiencia de los asistentes, permitiendo o no el uso de cámara, micrófono, participación en el chat, compartir pantalla, admitir a otros asistentes, hacer que otros participantes puedan ser moderadores, entre otras opciones.

- Administrar los roles de los participantes en una reunión con Microsoft Teams. Se puede contar con organizador, moderador y asistente, es importante desde el principio realizar la configuración de cada rol para evitar contratiempos en medio de la reunión.

[62] Support.google.com. [Sitio Web]. Agrega a otras personas a una videollamada de Google Meet o quítalas. [Consulta 6 junio 2021]. Disponible en: https://support.google.com/meet/answer/9303164?hl=es-419&co=GENIE.Platform=Desktop

[63] Docs.microsoft.com. [Sitio Web]. Seguridad y Microsoft Teams. [Consulta 14 junio 2021]. Disponible en: https://docs.microsoft.com/es-es/microsoftteams/teams-security-guide.

8 BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN POR PARTE DE LAS INSTITUCIONES EDUCATIVAS QUE PERMITAN ROBUSTECER SU INFRAESTRUCTURA TECNOLÓGICA.

Las instituciones educativas en Colombia en la pandemia provocada por el *COVID-19* se vieron en la necesidad de usar diferentes herramientas tecnológicas y plataformas educativas para poder suplir la necesidad de impartir sus clases, pero ahora de manera virtual.

La crisis de salud mundial y la inmediatez del momento hizo que muchas instituciones a nivel educativo en Colombia que no tenían definido una infraestructura tecnológica y reglamentada una educación virtual, tomaron de internet plataformas educativas gratuitas sin tener en cuenta las medidas necearías sobre la ciberseguridad.

8.1 CIBERSEGURIDAD EN LA INSTITUCIÓN EDUCATIVA[64].

- Adquirir antivirus licenciados con opción de actualización automática, asegurando que los equipos portátiles y otros dispositivos que proporciona a sus alumnos en préstamo, evitando que puedan descargar malware.

- Establecer fuertes perímetros en línea, la institución educativa debe de tener o establecer *Gateway y firewall* que proteja la red escolar y el acceso no autorizado.

- Asegurarse de los proveedores de las plataformas educativas proporcionadas por terceros.

- Las instituciones educativas deben de monitorear sus sistemas de manera continua para evitar un ciberataque.

- Capacitar a todas las personas (Estudiantes, docente, administrativos, dirección.) que hacen parte de las instituciones educativas, con el fin que toma de conciencia sobre la ciberseguridad online y buen comportamiento seguro en internet.

- Evitar envió de correo que tengan relación con actividades académicas por medio del correo personal, es recomendable hacer uso de los correos internos de la plataforma educativa o de correos institucionales.

[64] PCWorld. [Sitio Web]. Los ciberriesgos de la educación online (Y cómo evitarlos). [Consulta 21 abril 2021]. http://pcworld.com.mx/los-ciberriesgos-de-la-educacion-online-y-como-evitarlos/

- Realizar la viabilidad para la implementación de un Sistema de Gestión de la seguridad informática (*SGSI*).

- Proporcionar el menor privilegio posible, no todos los funcionarios del área de *TI* o administrativos deben tener acceso a las plataformas que maneja la institución sin interferir en las labores de sus funcionarios.

- Las instituciones educativas deben proporcionar a sus estudiantes listas blancas de bases de datos de recursos bibliográficos, recursos digitales y aplicaciones web las cuales sea necesario acceder a ellas y descargar información o archivos. Por medio de portales como https://www.virustotal.com/ es posible escanear archivos, url y búsqueda, con la cual es posible estar más seguros de que nuestra información no se vea comprometida.

- Desactivar o bloqueo de credenciales de acceso al momento que profesores y estudiantes no hagan parte de la institución y si los términos de retiro no son los mejores procurar cancelar todos los accesos de manera inmediata[65].

- Realización de análisis de seguridad por medio de metodologías de Testing y así poder encontrar vulnerabilidades.

8.2 TECNOLOGIA RECOMENDADA PARA ROBUSTECER LA INFRAESTRUCTRUA RECNOLOGICA EN SEGURIDAD INFORMATICA.

Es posible proponer una infraestructura tecnológica tanto a nivel de software y hardware para robustecer la seguridad de la seguridad en una institución de carácter educativa. tal es el caso de dispositivos físicos que contrarresten los intentos de ingresos a los datos e información almacenada en los dispositivos tecnológicos de las instituciones educativas.

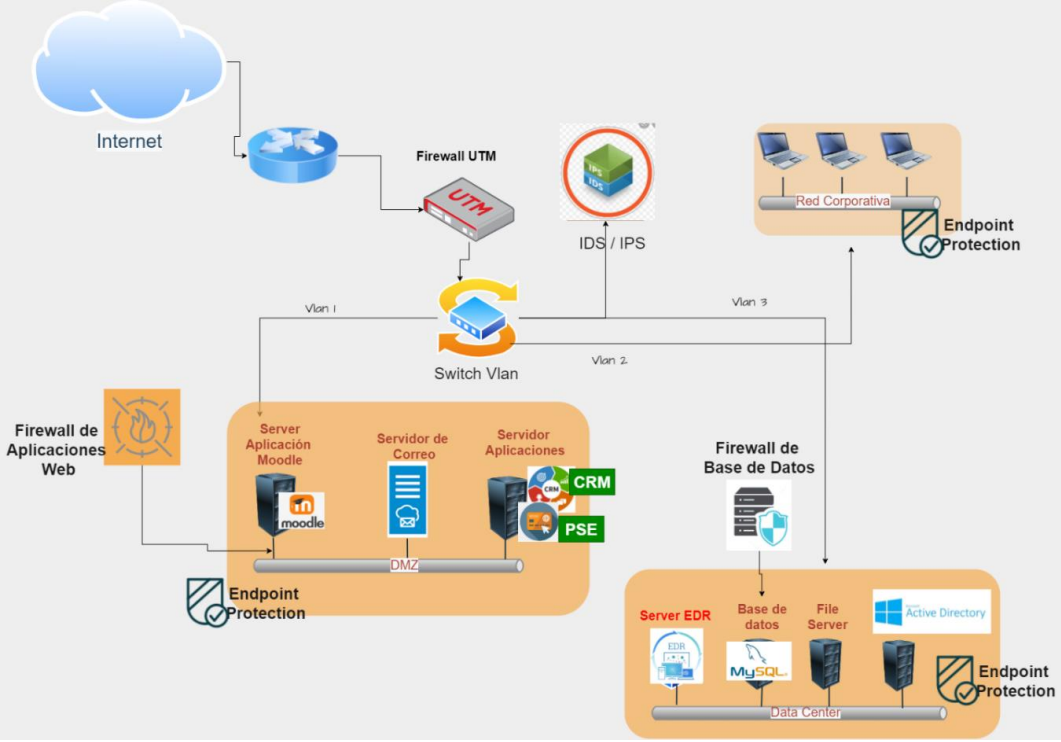
8.2.1 Propuesta para la infraestructura de seguridad

- Segmentación de red por medio de un *Switch* capa 3.
- *Firewall UTM* capa 7.
- *Firewall* de aplicaciones *Web.*
- *Firewall* de base de datos.
- *EDR (Endpoint Detection Response).*
- *IPS* (Sistema de prevención de intrusos) /*IDS* (Sistema de detección de intrusos).

[65] welivesecurity.com. [Sitio Web].10 consejos para proteger la información de instituciones educativas. [Consulta 26 abril 2021]. Disponible en: https://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/

la seguridad de las instituciones educativas genera seguridad para sus usuarios externos e internos. En la figura 11, se evidencia una posible infraestructura para la seguridad informática de una institución educativa utilizando elementos apropiados para la red.

Figura 11. Diagrama de la Topología



Fuente. Autor.

8.2.2 Justificación técnica a la propuesta tecnológica de seguridad.

Se fortalece el filtrado de paquetes desde internet por medio del firewall *UTM* con el fin de tener un control más preciso de los datos que provienen desde internet, este sería el primer filtro para la infraestructura.
Se implementará la segmentación de red con el fin dividir la red corporativa para poder realizar controles con más rigurosidad en cada segmento, además se anota que si en el caso que algún atacante ingrese a la red no tenga acceso a toda la infraestructura. De la misma manera se usa una *DMZ* con el fin de dividir los servidores que prestarán servicios salientes hacia internet, siendo así estos servicios que tendrán la interacción con la red interna.
Los firewalls de aplicaciones web y de bases de datos se encargarán directamente en cada uno de los servidores asignados con el fin de filtrar peticiones a las aplicaciones y a la base de datos. Al igual que los *IPS/IDS* se enfrentarán de forma pasiva o activa a las amenazas que posiblemente pueden atacar o afectar el funcionamiento de la

infraestructura. Por último, se propone un sistema de *EDR (Endpoint Detection Response)* la cual estará reforzando las diferentes estaciones de trabajo que hacen parte de la red, con el fin de detectar amenazas y riesgos.

Hablar de seguridad informática y ciberseguridad en las instituciones educativas, es importante para poder contrarrestar y mitigar los ataques que un ciberdelincuente puede realizar a una infraestructura o directamente a los actores que interactúan en las clases virtuales o la utilización de plataformas educativas sea de manera sincrónica o asincrónica. Cada actor que participa es un eslabón importante en esta cadena, resulta ser un efecto domino al momento de algún evento criminal hecho por ciberdelincuentes.

9 CONCLUSIONES

A partir de este trabajo se lograron determinar las siguientes conclusiones después del desarrollo de los objetivos específicos propuestos.

- En el primer objetivo específico, tenemos los diferentes riesgos informáticos que puede tener un estudiante al usar herramientas de internet o de video llamas, como son: pedida parcial o total de información personal, rodo de identidad, chantajes o extorciones, daño a su estado financiero, daño en su imagen por medio de suplantación de identidad, entre otros daños a nivel personal, económico y de imagen. Cada uno de ellos generan impacto totalmente negativo en una persona ya que son promovidos por personas que se dedican a la ciberdelincuencia la cual buscan favorecerse por lo general económicamente.

- Las vulnerabilidades son una gran brecha para la seguridad informática entre ellas es posible nombrar, las claves predeterminas en los dispositivos, la no actualización de los sistemas operativos o aplicaciones para realizar actividades educativas o de video llamadas, violación en la confidencialidad, los dispositivos en manos de personas que tiene poco conocimiento y dan clic indiscriminadamente. Detrás de todo esto existen personas que hacen posible que se cumplan cada uno de los posibles incidentes de los cuales conforman las amenazas, de los que se pueden nombrar; hacker, ingeniería social, *spoofing*, entre otros. Un incidente informático genera un impacto negativo o nefasto en un estudiante, institución educativa, de las cuales puede ocasionar que el estudiante deserte o en la continuidad del negocio en nuestro caso es posible que sea vulnerados los datos personales de todos los actores.

- Considerante las vulnerabilidades, amenazas e impacto que existen al momento de usar herramientas informáticas o de video llamadas para el desarrollo de clases virtuales y en la cuales está en juego la información, se recomienda que en las instituciones educativas exista catedra de seguridad informática para potencializar el conocimiento de estudiantes, profesores y hasta de los padres de familia, ya que estamos en un mundo globalizados y con cambios beligerantes que nos conlleva a tener cambios contantes de hábitos y forma de economías nuevas, tales como virtualidad en la educación. Es importante que se apliquen las recomendaciones que se han logrado plasmar en el desarrollo del objetivo 3, las cuales es posible mencionar entre ellas, no compartir información confidencial y financiera en las clases online, adquirir conocimientos básicos sobre la ciberseguridad, establecer controles parenterales para los menores de edad, proteger los dispositivos que proporcionan internet con protocolos y claves robustas, entre otros que conlleve a mitigar los acceso abusivos al momento de usar dichas herramientas usando conexiones “De confianza”

- Las instituciones educativas de cual índole de formación, es necesario que estén preparadas para enfrentarse a la virtualidad y los cambios educativos que mundialmente se vienen presentando. También tienen la obligación generar los cambios de mentalidad en todos los actores del sector. desarrolladas en el objetico 4 de las cuales se pueden destacar, el uso de dispositivos perimetrales de seguridad, monitoreo continuo en su red de datos y sistemas. Capacitaciones periódicas a los docentes, padres de familia y alumnos, evitar uso del correo personal para interactuar, fortalecer sus procesos con un Sistema de Gestión de la seguridad informática (*SGSI*), entre otros y de esta manera generar seguridad a padres y alumnos del uso de herramientas tecnológicas aportadas por la institución y evitar que existan intrusiones en sus sistemas.

10 RECOMENDACIONES

- Las instituciones educativas en Colombia tanto públicas como privadas deben garantizar la capacitación a docentes, padres de familia y estudiantes en los temas referentes a seguridad de la información, por medio de cátedras informáticas y ayudas visuales (Folletos, revistas, *blog*, entre otros) con el fin de fortalecer los conocimientos en temas relacionados en la ciberseguridad y poder mitigar los impactos a posibles ataques cibernéticos.

- Los equipos institucionales que se dan en son de préstamos a los estudiantes deben mantenerse actualizado los sistemas operativos, tales como: computadoras, *smartphone, tablets*, entre otros que se usan para clases virtuales, por medio de los parches que las empresas proveedores de software lanzan, tal es el caso de Windows, MacOs o Linux al igual que las herramientas para video llamadas como son: *Zoom, Microsoft Team, google Chrome* y demás que se utilicen.

- Los tutores o docentes deberían brindar a sus estudiantes listas blancas o web grafía segura para realizar las consultas, una vez hayan sido comprobadas por medio de algunas utilidades en línea tales como: www.virustotal.com/gui/home/upload, www.hybrid-analysis.com/ y sitecheck.sucuri.net/, con el fin de garantizar una navegación confiable.

- Los docentes o tutores deberían entregar recomendaciones a padres y alumnos sobre el uso de claves seguras con doble factor de autenticación y robustas en todos sus dispositivos, herramientas y plataformas que usan para las clases virtuales y al mismo tiempo la comprobación de las mismas en páginas sugerida tales como: https://password.kaspersky.com/es/, https://ciberprotector.com/comprobador-de-contraseña/ y https://password.es/comprobador/, con el objetivo de evitar que ciberdelincuentes puedan descifrar fácilmente las contraseñas.

- Las instituciones educativas que contraten proveedores de tecnología para la adquisición de herramientas informáticas (Plataformas educativas) serán las encargadas de brindar la mayor seguridad y confiabilidades en los productos ofertados a sus alumnos, por ende, será necesario comprobar la fiabilidad de los mismos por medio de personas expertas en el campo de la ciberseguridad.

11 BIBLIOGRAFÍA

Alcaldiabogota.gov.co. [Sitio Web]. Ley 1978 de 2019 Nivel Nacional. [Consulta 25 septiembre 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=85632

Arte&Animación. [Sitio Web]. Conoce las 7 mejores herramientas “gratis” para clases y reuniones virtuales. [Consulta 15 marzo 2021]. Disponible en: https://arteyanimacion.com/herramientas-clases-y-reuniones-virtuales/

Aulasiena.com. [Sitio Web]. González, S., educativos, P., Virtual, C., Virtual, F., & Virtual, F. Seguridad en Internet para profesores: entrevista a Vanessa González. Aula Siena. [Consulta 2 marzo 2021]. Disponible en: https://aulasiena.com/seguridad-en-internet-para-profesores-entrevista-vanessa-gonzalez/.

Blog.zoom.us. [Sitio Web]. Prácticas recomendadas para proteger su aula virtual. [Consulta 02 junio 2021]. Disponible en: https://blog.zoom.us/es/best-practices-for-securing-your-virtual-classroom/

Bluradio.com. [Sitio Web].’Influencer’ que se infiltró con porno en clase a menores es universitario: profesora. [Consulta 26 abril 2021]. Disponible en: https://www.bluradio.com/judicial/influencer-que-se-infiltro-con-porno-en-clase-a-menores-es-universitario-profesora

Business Insider México. [Sitio Web]. Consejos de ciberseguridad para un retorno a clases virtuales seguro. | Noticias pensadas para ti. [Consulta 2 marzo 2021]. Disponible en: https://businessinsider.mx/consejos-ciberseguridad-retorno-clases-en-linea-virtuales/.

Caivirtual.policia.gov.co. [Sitio Web]. Tendencias Cibercriminales en Colombia 2019 - 2020. [Consulta 25 abril 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

ccce.org.co. [Sitio Web]. INFORME PRIMER TRIMESTRE 2021. [Consulta 23 octubre 2021]. Disponible en:https://www.ccce.org.co/wp-content/uploads/2017/06/Estudio-trimestral-ecommerce-01-CCCE-vf_compressed.pdf

Ccit.org.co. [Sitio Web]. Evaluación, Retos y Amenazas a al Ciberseguridad. [Consulta 24 septiembre 2021]. Disponible en:https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

Ccit.org.co. [Sitio Web]. Informe de las tendencias del cibercrimen en Colombia 2019 - 2020. [Consulta 22 septiembre 2021]. Disponible en:https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Colaboracion.dnp.gov.co [Sitio Web]. Documento CONPES 3854. [Consulta 26 abril 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf

Computing. Sitio Web]. La videoconferencia, ante el reto de la ciberseguridad. [Consulta 7 marzo 2021]. Disponible en: https://www.computing.es/seguridad/opinion/1109164002501/videoconferencia-reto-de-ciberseguridad.1.html

Coronaviruscolombia.gov.co. [Sitio Web]. Acciones tomadas por el Gobierno. [Consulta 24 septiembre 2021]. Disponible en:https://coronaviruscolombia.gov.co/Covid19/acciones/acciones-de-aislamiento-preventivo.html

CNN, español. [Sitio Web]. «Zoombombing», el FBI advierte que las llamadas de video por Zoom están siendo interceptadas. [Consulta 01 junio 2021]. Disponible en: https://cnnespanol.cnn.com/2020/04/03/zoombombing-el-fbi-advierte-que-las-llamadas-de-video-por-zoom-estan-siendo-interceptadas/

Cve.mitre.org. [Sitio Web]. CVE-2021-26422. [Consulta 18 noviembre 2021]. ¿Disponibilidad en:https://cve.mitre.org/cgi-bin/cvename.cgi? name=CVE-2021-26422.

Cybermap.kaspersky.com. [Sitio Web]. Mapa en tiempo real de amenazas cibernéticas Kaspersky. [Consulta 2 marzo 2021]. Disponible en: https://cybermap.kaspersky.com/es/stats.

Docs.microsoft.com. [Sitio Web]. Seguridad y Microsoft Teams. [Consulta 14 junio 2021].
Disponible en: https://docs.microsoft.com/es-es/microsoftteams/teams-security-guide

ElComercio. [Sitio Web]. Alumnos presenciaron agresión sexual a una compañera de siete años durante una clase virtual. [Consulta 2 marzo 2021]. Disponible en: https://www.elcomercio.com/actualidad/chicago-agresion-sexual-nina-clase/.

Elcomercio.com. [Sitio web]. Infiltrado mostró contenido para adultos durante clase virtual de un colegio de Quito; ¿Cómo evitar que esto ocurra? [Consulta 07 marzo 2021]. Disponible en: https://www.elcomercio.com/actualidad/infiltrado-contenido-adultos-clase-quito.html.

Elpais.com.co. [Sitio Web]. Trabajo y clases virtuales son blancos de los ciberdelincuentes. [Consulta 1 marzo 2021]. Disponible en: https://www.elpais.com.co/judicial/trabajo-y-clases-virtuales-son-blanco-de-los-ciberdelincuentes.html.

Elteimpo.com. [Sitio Web]. Estas son las prácticas más usadas de suplantación de sitios web. [Consulta 01 mayo 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/suplantacion-de-sitios-web-que-es-el-spoofing-y-pharming-568652

Eltiempo.com. [Sitio Web]. La educación virtual en Colombia, entre retos, ventajas y desventajas. [Consulta 28 febrero 2021]. Disponible en https://www.eltiempo.com/vida/educacion/como-esta-la-educacion-virtual-en-colombia-530024.

Eltiempo.com. [Sitio Web]. Las ciberamenazas de las que más debe cuidarse este año. [Consulta 2 marzo 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cuales-son-los-mayores-riesgos-en-seguridad-informatica-y-como-prevenirlos-457980.

Eltiempo.com. [Sitio Web]. Las serias acusaciones contra Zoom por problemas en su seguridad. [Consulta 2 marzo 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/zoom-es-senalada-de-enganar-sobre-la-seguridad-dentro-de-la-plataforma-548126.

Eltiempo.com. [Sitio Web]. Universidad El Bosque sufre ataque informático. [Consulta 22 septiembre 2021]. https://www.eltiempo.com/vida/educacion/universidad-el-bosque-sufre-ataque-informatico-599303

Eluniversal.com.mx. [Sitio Web]. Estudiante arruina clases virtuales con ciberataques en Miami. [Consulta 07 marzo 2021]. Disponible en: https://www.eluniversal.com.mx/mundo/estudiante-arruina-clases-virtuales-con-ciberataques-en-miami.

Enterarse.com. [Sitio Web]. Lo más profundo del Internet: ¿qué son la Deep web y la Dark web? [Consulta 01 mayo 2021]. Disponible en: https://www.enterarse.com/img-deeeep.png

Evaluamos.com. [Sitio Web]. Tendencia Cibercrimen Colombia 2019 - 2020. [Consulta 25 abril 2021]. Disponible en: http://www.evaluamos.com/pdf/TENDENCIASCIBERCRIMEN.pdf

EvolCampus. [Sitio Web]. ¿Qué es un aula virtual y para qué se puede utilizar? [Consulta 15 marzo 2021]. Disponible en: https://www.evolmind.com/latam/blog/que-es-un-aula-virtual-y-para-que-se-puede-utilizar.

Forbes.com. [Sitio Web]. Zoom Users Beware: Here's How a Flaw Allows Attackers to Take over Your Mac Microphone and Webcam. [Consulta 12 septiembre 2021]. Disponible en: https://www.forbes.com/sites/kateoflahertyuk/2020/04/01/zoom-users-beware-heres-how-a-flaw-allows-attackers-to-take-over-your-mac-microphone-and-webcam/

Hrw.org. [Sitio Web]. El grave impacto de la pandemia en la educación mundial. [Consulta 24 septiembre 2021]. Disponible en:https://www.hrw.org/es/news/2021/05/16/el-grave-impacto-de-la-pandemia-en-la-educacion-mundial

Incibe_, Instituto Nacional de Ciberseguridad. [Sitio Web]. Videollamadas: riesgos asociados a su uso y recomendaciones de seguridad. [Consulta 7 marzo 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/videollamadas-riesgos-asociados-su-uso-y-recomendaciones-seguridad.

INISEG, Instituto Internacional de Estudios en Seguridad Global. [Sitio Web]. Lista de 15 consejos de Ciberseguridad para tener una vida cibersegura. [Consulta 01 mayo 2021]. Disponible en: https://www.lisainstitute.com/blogs/blog/lista-consejos-ciberseguridad-vida-cibersegura

INISEG, Instituto Internacional de Estudios en Seguridad Global. [Sitio Web]. Peligros de la Dark Web: el lado oscuro desconocido. [Consulta 01 mayo 2021]. Disponible en: https://www.iniseg.es/blog/ciberseguridad/los-peligros-de-la-dark-web/

Kaspersky.es. [Sitio Web]. Los problemas de las aplicaciones de videoconferencia. [Consulta 12 septiembre 2021]. Disponible en: https://www.kaspersky.es/blog/videoconference-software-security/22549/

Magisnet.com. [Sitio Web]. Los seis riesgos de internet para los centros educativos. [Consulta 2 marzo 2021]. Disponible en: https://www.magisnet.com/2019/11/los-seis-riesgos-de-internet-para-los-centros-educativos/.

Medium.com/. [Sitio Web]. Plataformas educativas. [Consulta 25 abril 2021]. Disponible en: https://miro.medium.com/max/2400/1*vmWN_RB5PU4l6-ZDHvGe6g.jpeg

Mibolsillo.com. [Sitio Web] ¿Tienes clases virtuales? Podrías ser víctima de ciberdelincuentes. [Consulta 26 abril de 2021]. Disponible en: https://www.mibolsillo.com/tecnologia/Tienes-clases-virtuales-Podrias-ser-victima-de-ciberdelincuentes-20200926-0014.html

Mineducacion.gov.co. [Sitio Web]. Decreto 1295 de 2010. [Consulta 20 abril 2021]. Disponible en: https://www.mineducacion.gov.co/1621/articles-229430_archivo_pdf_decreto1295.pdf.

Mineducacion.gov.co. [Sitio Web]. Ley 1188 de 2008. [Consulta 14 abril 2021]. Disponible en: https://www.mineducacion.gov.co/1621/articles-159149_archivo_pdf.pdf

Minsalud.gov.co. [Sitio Web]. Colombia confirma su primer caso de COVID-19. [Consulta 21 septiembre 2021]. Disponible en:https://www.minsalud.gov.co/Paginas/Colombia-confirma-su-primer-caso-de-COVID-19.aspx

News.sophos.com. [Sitio Web]. La educación fue el sector más golpeado por el Ransomware en el año de la pandemia. [Consulta 22 septiembre 2021]. Disponible en:https://news.sophos.com/es-es/2021/09/02/la-educacion-fue-el-sector-mas-golpeado-por-el-ransomware-en-el-ano-de-la-pandemia/

Normograma.mintic.gov.co. [Sitio Web]. Ley 1928 de 2018. [Consulta 14 abril 2021]. Disponible en: https://normograma.mintic.gov.co/mintic/docs/ley_1928_2018.htm

Nubalia.com. [Sitio Web]. Medidas de Google Meet para mantener tu seguridad y privacidad. [Consulta 6 junio 2021]. Disponible en: https://nubalia.com/medidas-google-meet-mantener-seguridad-privacidad/

LaFM. [Sitio Web]. Hackearon WhatsApp de Luis Ernesto Gómez, secretario de Gobierno de Bogotá. [Consulta 06 junio 2021]. Disponible en: https://www.lafm.com.co/bogota/hackearon-whatsapp-de-luis-ernesto-gomez-secretario-de-gobierno-de-bogota

LaFM. [Sitio Web]. Sexting, el delito que ha aumentado más del 130 % en Colombia y que afecta principalmente a menores. [Consulta 07 de marzo 2021]. Disponible en: https://www.lafm.com.co/colombia/sexting-el-delito-que-ha-aumentado-mas-del-130-en-colombia-y-que-afecta-principalmente

Latam.kaspersky.com. [Sitio Web]. Kaspersky ofrece pronóstico de ciberseguridad 2021 para América Latina. [Consulta 21 septiembre 2021]. Disponible en: https://latam.kaspersky.com/about/press-releases/2020_kaspersky-ofrece-pronostico-de-ciberseguridad-2021-para-america-latina

Obsbusiness.school. [Sitio Web]. OBS presenta "El mercado del e-learning crecerá cada año un 7.6% hasta 2020”. [Consultado 24 de septiembre 2021]. disponible en: https://www.obsbusiness.school/blog/obs-presenta-el-mercado-del-e-learning-crecera-cada-ano-un-76-hasta-2020

PCWorld, México. [Sitio Web]. Los ciberriesgos de la educación online (Y cómo evitarlos). [Consulta 07 marzo 2021]. Disponible en: http://pcworld.com.mx/los-ciberriesgos-de-la-educacion-online-y-como-evitarlos/

Pcworld.com. [Sitio Web]. Update: Zoom issues fix for UNC vulnerability that lets hackers steal Windows credentials via chat. [Consulta 12 septiembre 2021]. Disponible en: https://www.pcworld.com/article/3535373/report-hackers-can-steal-windows-credentials-via-links-in-zoom-chat.html

Portafolio.co. [Sitio Web]. Delitos informáticos, la otra pandemia en tiempos del coronavirus. [Consulta 28 febrero 2021]. Disponible en: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642.

Recursosdigitales.anuies.mx. [Sitio Web]. Plataformas y recursos digitales ante la contingencia de la COVID-19. [Consulta 26 abril 2021]. Disponible en: https://recursosdigitales.anuies.mx/ciberseguridad-para-educacion-en-linea/

Redalyc.org. [Sitio Web]. Corda, María Cecilia; Viñas, Mariela; Coria, Marcela Karina. Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. [Consulta 11 marzo 2021]. https://www.redalyc.org/pdf/3505/350553375007.pdf

Redalyc.org/ [Sitio Web]. Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. [Consulta 26 abril 2021]. Disponible en: https://www.redalyc.org/jatsRepo/1941/194161290017/html/index.html

Repository.usc.edu.co. repositorio Universidad Santiago de Cali. [Sitio Web]. Plataformas E-Learning, sus riesgos y amenazas. [Consulta 25 abril 2021]. Disponible en: https://repository.usc.edu.co/bitstream/handle/20.500.12421/1733/PLATAFORMAS%20E-LEARNING.pdf?sequence=1&isAllowed=y

RZ Redes Zone. [Sitio Web]. CyberArk Labs encuentra una vulnerabilid.ad en Microsoft Teams. [Consulta 07 marzo 2021]. Disponible en: https://www.redeszone.net/noticias/seguridad/cyberark-labs-vulnerabilidad-microsoft-teams/

Semana.com. [Sito web]. Estos son algunos riesgos cibernéticos durante la cuarentena. [Consulta 2 marzo 2021]. Disponible en: https://www.semana.com/empresas/tecnologia/articulo/riesgos-ciberneticos-para-empresas-y-usuarios-durante-la-cuarentena/287040/.

Secretariasenado.gov.co. [Sitio Web]. Ley 1273 De 2009. [Consulta 1 marzo 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

Secretariasenado.gov.co. [Sitio Web]. Ley estatutaria 1581 de 2012. [Consulta 14 abril 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Scielo.sld.cu. [Sitio Web]. Echemendía, Belkis. Definiciones acerca del riesgo y sus implicaciones. [Consulta 11 marzo 2021]. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1561-30032011000300014.

Scp.com.co. [Sitio Web]. Tecnologías digitales y los niños, efectos positivos y negativos. [Consulta 29 octubre 2021]. Disponible en:https://scp.com.co/actualidad-pediatria-social/tecnologias-digitales-y-los-ninos-efectos-positivos-y-negativos/

Support.google.com. [Sitio Web]. Agrega a otras personas a una videollamada de Google Meet o quítalas. [Consulta 6 junio 2021]. Disponible en: https://support.google.com/meet/answer/9303164?hl=es-419&co=GENIE.Platform=Desktop

t13.cl. [Sitio Web]. Cómo realizar clases online seguras: consejos para evitar el Zoombombing o gate-crashing virtual. [Consulta 21 abril 2021]. Disponible en: https://www.t13.cl/noticia/nacional/como-realizar-clases-online-seguras-consejos-evitar-zoombombing-o-gate-crashing-virtual

Telemundoatlanta.com. [Sitio Web]. Montenegro, J. (Aprendizaje virtual; autoridades alertan sobre algunos riesgos cibernéticos para los estudiantes. [Consulta 2 marzo 2021]. Disponible en: https://www.telemundoatlanta.com/noticias/coronavirus/recursos/educacion_virtual/aprendizaje-virtual-autoridades-alertan-sobre-algunos-riesgos-cibern-ticos-para-los-estudiantes/article_4198f916-e369-11ea-80a2-dfabd373871e.html

Threatpost.com. [Sitio Web]. Single Malicious GIF Opened Microsoft Teams to Nasty Attack.[Consulta 12 Septiembre de 2021].Disponible en:https://threatpost.com/single-malicious-gif-opened-microsoft-teams-to-nasty-attack/155155/

Vinculotic.com. [Sitio Web]. Riesgos educación virtual COVID-19: cómo evitarlos. [Consulta 2 marzo 2021]. Disponible en: https://vinculotic.com/educacion/riesgos-educacion-virtual-covid19/.

Unaaldia.hispasec.com. [Sitio Web]. Un fallo en WhatsApp permite ataques Man in the Disk. [Consulta 04 junio 2021]. Disponible en: https://unaaldia.hispasec.com/2021/04/bug-de-whatsapp-vulnerable-a-ataques-man-in-the-disk.html

Universia.net. [Sitio Web].10 plataformas virtuales para estudiar a distancia. [Consulta 15 marzo 2021]. Disponible en: https://www.universia.net/pe/actualidad/orientacion-academica/10-plataformas-virtuales-estudiar-distancia-1141829.html

VpnMentor, keeping you Safe online. [Sitio Web]. Guía de ciberseguridad para profesores: Lo que hay que saber. [Consulta 26 abril 2021]. Disponible en: https://es.vpnmentor.com/blog/guia-de-ciberseguridad-para-profesores-todo-lo-que-necesitas-saber-en/

welivesecurity.com. [Sitio Web].10 consejos para proteger la información de instituciones educativas. [Consulta 26 abril 2021]. Disponible en: https://www.welivesecurity.com/la-es/2014/07/08/10-consejos-proteger-informacion-instituciones-educativas/

Welivesecurity.com. [Sitio Web]. Un repaso por los últimos problemas de seguridad y privacidad que se descubrieron en Zoom. [Consulta 1 marzo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/04/09/repaso-ultimos-problemas-seguridad-privacidad-descubrieron-zoom/.

Welivesecurity.com. [Sitio Web]. Zoom: problemas de seguridad y privacidad en la popular herramienta para videoconferencias. [Consulta 2 marzo 2021]. Disponible en: https://www.welivesecurity.com/la-es/2020/03/30/zoom-problemas-seguridad-privacidad-popular-herramienta-videoconferencias/.

Www3.gobiernodecanarias.org. [Sitio Web]. Control de Errores - Gobierno de Canarias. [Consulta 2 marzo 2021]. Disponible en: http://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/riesgos/.