ANÁLISIS DE SEGURIDAD BASADO EN LA ISO 27000 AL PROCESO DE ENSEÑANZA APOYADO POR HERRAMIENTAS TIC EN COLOMBIA FRENTE A LOS DESAFÍOS PRESENTADOS POR LA PANDEMIA PARA EL DESARROLLO DE ESTRATEGIAS Y MODELOS DE SEGURIDAD EN ENTORNOS DIGITALES

MIGUEL ANGEL PARRA MARTINEZ
CRISTIAN LIBARDO RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

ANÁLISIS DE SEGURIDAD BASADO EN LA ISO 27000 AL PROCESO DE ENSEÑANZA APOYADO POR HERRAMIENTAS TIC EN COLOMBIA FRENTE A LOS DESAFÍOS PRESENTADOS POR LA PANDEMIA PARA EL DESARROLLO DE ESTRATEGIAS Y MODELOS DE SEGURIDAD EN ENTORNOS DIGITALES

MIGUEL ANGEL PARRA MARTINEZ
CRISTIAN LIBARDO RIVERA

PROYECTO DE GRADO
MONOGRAFÍA PRESENTADA PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTORA DE TRABAJO DE GRADO
YENNY STELLA NUÑEZ ALVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 29 de mayo 2022

AGRADECIMIENTOS

Agradecimientos a todos los tutores, directores y personal en general de la Universidad Nacional Abierta y a Distancia UNAD, los cuales con su continuo trabajo nos permite realizar labores de aprendizaje y estudio, además de a cada uno de los profesionales y asesores, que, con su guía y acompañamiento constante, no habría sido posible alcanzar todos los objetivos propuestos.

Agradecimientos especiales a los tutores que nos apoyan en la elaboración de este trabajo y nos permiten cada día explorar más a fondo estos temas y tratarlos de la mejor manera.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE GRAFICOS

pág.

GLOSARIO

Accesibilidad: Son las condiciones que se incorporan dentro de una zona geográfica, implementados a través de herramientas tecnológicas, llevados a terrenos o lugares de difícil acceso.

Advertencia: Notificación que llega a un usuario buscando advertir de una perdida de datos o una vulnerabilidad en la red.

Amenaza: Evento que se lleva a cabo desde el exterior, ya sea una tercera persona u otra organización.

Antispam: Es un servicio que se implementa especialmente en correos no deseados, buscando que estos no afecten la seguridad del sistema ni moleste a los usuarios.

Antivirus: Es un software que protege los dispositivos de amenazas y filtraciones en la red, actúa en tiempo real y es autosuficiente ya que los virus los puede eliminar o enviar a cuarentena.

Ataques web: Es un tipo de vulnerabilidad que tiene como misión atacar páginas web de un cliente que generalmente se utilizan para atacar desde sitios externos.

Blacklist: Es una lista negra en la cual se pueden bloquear usuarios, IPs, dominios, MAC o direcciones de correo electrónico

Certificado: Son una prueba de identidad que tienen en su mayoría de veces las páginas web, por lo general estos certificados contienen nombre de usuario y claves públicas.

Ciberacoso: Se da a través de correos electrónicos generalmente, viene alojada con imágenes o contenido sensible que intenta agredir psicológicamente a personas.

Cibercrimen: Delitos informáticos que se llevan a cabo a través de la web, son conocidas como actividades ilegales ya que pueden afectar integridad de datos y personas.

Ciberseguridad: Conjunto de políticas que se utilizan con el fin de proteger información confidencial de usuarios y activos que tiene la empresa. Se utilizan diversos métodos para lograr este objetivo como métodos de investigación y desarrollo de buenas prácticas tecnológicas.

Cifrado: Es un método utilizado en los sistemas para encriptar información, se hace con el objetivo que personas ajenas o terceras no puedan tener acceso fácilmente a estos documentos y se cifra a través de claves difíciles de conseguir.

Conectividad: Sistema que se utiliza para unir dos partes interesadas, ya sea empresas, ciudades, países, etc., también se caracteriza por llevar servicio de internet a las personas.

Confidencialidad: Privacidad que se le asigna a documentos y archivos, los cuales un número determinado de personas puede tener acceso.

Contraseña: Cadena de valores que se utiliza para restringir el acceso a otras personas, en la cual guardan archivos confidenciales.
Disponibilidad: Conjunto de normas que permiten que información o archivos puedan estar utilizables al momento que otras personas requieran del mismo.
Exploits: Son las diferentes técnicas que se utilizan para vulnerar software, además de ello tiene como misión evadir la seguridad y atacar equipos de la red.
Filtración de datos: Momento en el cual queda a exposición información confidencial llevadas a cabo a través de ataques maliciosos y se realiza con fines delictivos.
Firewall: Se utiliza para bloquear conexiones entrantes y salientes de un sistema, suelen ser puertos los cuales se revisan para conocer el tráfico que se transporta por la red.
Grooming: Nueva tendencia de acoso y bullying hacia niños, se realiza a través de las redes sociales. Se da a través de comunicaciones entre una persona adulta que se hace pasar por niño con fines de satisfacción sexuales, incitando a la pornografía.
Gusanos: Son virus que se reproducen dentro de un equipo y pueden trasladarse de un sitio a otro sin problemas.
Hackear: Suplantar identidades de personas con la cual busca robar información, dinero u otros objetivos planteados por estas personas.
Integridad: Métodos sistemáticos que tienen como misión preservar la información de manera correcta y limpia.
Interconexión: Conexión de dos o más sitios que buscan interoperabilidad entre los dispositivos físicos y lógicos que se cuentan en la red.
Interferencia: Llevar a cabo otro tipo de conexiones o de dispositivos que no permitan la fluidez de datos y de información a través de una red.
Malware: Es un programa informático que tiene como misión incorporarse en medios magnéticos, como USB y CD, se consigue a través de mensajerías instantáneas o publicidad engañosa y solo se utiliza con el fin de cometer acciones delictivas.
Pharming: Herramienta que se utiliza para el desvío de información que transita por una red y tiene como finalidad mostrar un sitio espejo para que el usuario ingrese información personal y pueda ser captada por personas fraudulentas.
Phishing: Método que se utiliza para robar información confidencial de una persona que suelen ser tarjetas de créditos u otro tipo de información.
Pornografía infantil: Representaciones visuales o gráficas, la cual incluyen menores de edad que demuestran actividades sexuales y explicitas.
Radiocomunicación: Es la intercomunicación que se transmite por ondas eléctricas.
Red de acceso: Es la herramienta que permite una conexión entre la central de datos y los usuarios finales, buscando como beneficio la conexión a servicios requeridos, estos se llevan a cabo a través de medios como cables coaxiales o fibras ópticas.

Red troncal: Es un tipo de red que conecta las diferentes dependencias de una compañía y conecta diferentes tipos de dispositivos físicos para lograr una interconexión segura.

Rootkits: Es un tipo del malware que tiene como objetivo ejecutar códigos maliciosos dentro de una red y su mayor particularidad es que es indetectable en un equipo, además de esto realiza acciones sin el consentimiento del cliente.

Servicios de difusión: Son un tipo de comunicación que se realiza de manera unidireccional y en forma simultánea.

Sexting: Es la forma en que una persona toma una foto inapropiada de sí mismo y la envía a otras personas o la sube a internet.

Smishing: Es un método común de delitos informáticos y consiste en enviar información a usuarios pidiendo que ingresen a supuestos sitios web el cual tiene como finalidad insertar spyware en sus equipos sin que el usuario se dé cuenta de ello.

Spam: También es conocido como correo no deseado o correo basura, tiene como característica el envío de correos de manera idéntica a muchos destinatarios, se utiliza con el fin de infectar un equipo o utilizar otros equipos como métodos de propagación de ataques.

Spyware: Es una aplicación que se encarga de enviar a través de paquetes información confidencial de terceras personas. Estos datos pueden incluir desde información personal hasta cuentas bancarias de las mismas.

TICS: Se trata de un conjunto de dispositivos tanto de hardware como de software que permite la correcta transmisión de datos en formatos como voz, video e imágenes.

Telecomunicación: Es la transmisión y recepción de datos, señales o información que se puede transferir por diferentes medios como cable, ondas u otro elemento electromagnético.

Terminal: Es un dispositivo conectado a una red el cual busca proporcionar acceso a uno o más servicios.

Usuario: Es una persona a la cual se debe integrar dentro de un sistema y proporcionar los servicios necesarios para la operabilidad y la usabilidad de este.

Virus: Son programas informáticos que tienen autonomía propia y se reproducen por sí mismos, buscando alterar la manera en que un equipo funciona.

Vishing: Consiste en la realización de llamadas a las personas para solicitar datos personales e información bancaria, se da a través de voces de computadora semejantes a las que utilizan las entidades bancarias.

Vulnerabilidad: Es una propiedad que puede adquirir el sistema que busca afectar la integridad y confidencialidad de un sistema, se puede dar a través de diferentes medios, ya sean por terceras personas o a través de otras entidades.

Zona de cobertura: Es un sector que posee frecuencias especificas capaces de tener conectividad con otros sitios y se pueda establecer comunicación con otras estaciones de red.

RESUMEN

La educación virtual en Colombia ha tenido gran recibimiento desde su implantación, pero no ha sido sino hasta el año de la pandemia que se exigió su uso, por motivos de la reclusión y precaución de contagios, esto trajo consigo un crudo vistazo a la realidad, y con esto se hace referencia al nivel tan desigual que se tiene en cuanto a conocimiento en tecnología de la población, y ¿que trae esta desigualdad, sumada a el nivel de delincuencia que hay en el país?, pues un incremento en ciberdelincuentes.

La ciberdelincuencia viene en auge desde la última década, y estos criminales buscan victimas que no tengan demasiada experiencia, ni conocimientos, las personas que normalmente no tienen estos conocimientos se abstienen de usar las tecnologías, pero con esto que paso fueron un poco forzadas a utilizarlas.

Después de hacer un análisis de que tan segura fue la infraestructura usada para estos fines, que se puede hacer para mejorar y cuáles fueron los peores errores que se cometieron, todas estas dudas y más se deben solucionar para encontrar un punto de inicio y así aportar a que mejore el proceso y ayudar a que se tenga un método seguro que se pueda implantar en cualquier lugar para educar de forma segura a la población de forma virtualizada.

Esta monografía está basada en la educación en instituciones educativas de Colombia, se pretende manejar y conocer las diferentes herramientas TIC implementadas en ellas, especialmente las utilizadas en comunicación con estudiantes, basándose en la educación virtual. Además, se pretende estudiar el manejo de la información confidencial de una institución educativa, tanto información de estudiantes (sean menores de edad o mayores), como la de docentes, para salvaguardar la información y mitigar cualquier tipo de ataque a través de la normativa ISO 27000.

Palabras claves: Colombia, Educación virtual, Herramientas TIC, Pandemia, Seguridad informática.

ABSTRACT

Virtual education in Colombia has had a great reception since its implementation, but it was not until the year of the pandemic that its use was demanded, for reasons of seclusion and precaution of contagion, this brought with it a crude look at reality, and this refers to the unequal level that has in terms of knowledge in technology of the population, and what brings this inequality, coupled with the level of crime in the country, because an increase in cybercriminals.

Cybercrime has been on the rise since the last decade, and these criminals are looking for victims who do not have much experience or knowledge, people who normally do not have this knowledge refrain from using technologies, but with this that happened they were a little forced to use them.

After making an analysis of how safe the infrastructure was used for these purposes, what can be done to improve and what were the worst mistakes that were made, all these doubts and more must be solved to find a starting point and thus contribute to improve the process and help to have a safe method that can be implemented anywhere to safely educate the population in a virtualized way.

This monograph is based on education in educational institutions in Colombia, it is intended to manage and know the different ICT tools implemented in them, especially those used in communication with students, based on virtual education. In addition, it is intended to study the management of confidential information of an educational institution, both information of students (whether minors or adults) and teachers, to safeguard the information and mitigate any type of attack through the ISO 27000 standard.

Keywords: Colombia, Virtual education, ICT tools, Pandemic, Computer security.

INTRODUCCIÓN

La situación que se dio en los años 2020 y 2021 planteó un nuevo paradigma en el cual, la protagonista fue la tecnología, no solo la médica si no la de la informática y las comunicaciones.

La pandemia quedará como un evento de gran relevancia en la historia de la humanidad y aunque se podría hablar de las múltiples consecuencias y cambios que se dieron debido a esta emergencia sanitaria, en este documento se centrará la consecuencia que trajo al sistema educativo en todo el mundo, los cambios implementados el nuevo sistema educacional y los métodos de enseñanzas que trajo consigo nuevos desafíos y oportunidades.

La tecnología como se mencionaba fue fundamental en estos tiempos oscuros, iluminaban las rutas de la educación desde una cómoda y segura locación, debido al virus covid-19 se implementaron medidas seguras de comportamiento, se decidió permanecer un aislamiento y definir un distanciamiento prudencial, que después llevo a medidas de cuarentena obligatoria con toques de queda y demás, todo para evitar la propagación masiva de este virus en muchas ocasiones mortal.

Todas estas medidas y normativas hicieron que se dificultara el proceso de enseñanza y aprendizaje, por lo que, con la ayuda de las TI se dispuso de un nuevo paradigma educacional, el digital, haciendo que todo el proceso sea virtual, el aprendizaje, los procesos administrativos y cada aspecto que con antelación se hacía personalmente o mejor expuesto, físicamente.

Al virtualizar cada aspecto en la educación la transición trajo consigo múltiples problemas, pero también algunos beneficios como se explicará en el desarrollo del presente documento.

Pero al utilizar todo este tipo de tecnologías surgieron patrones de uso, o mejor métodos y herramientas preferidas por quienes la utilizaban sin mencionar, las apoyadas por organismos que incentivaban su uso y mejora de la experiencia digital.

La educación virtual no es nueva no viene del año 2020 o 2021, viene muchos años desarrollándose y usándose, pero fue hasta el 2020 que su uso se hizo masivo y necesario, debido a las condiciones ya descritas, por lo cual, aunque fuera una tecnología en uso no estaba preparada para soportar semejante cambio, de igual manera no fue en términos generales tan mal, y hubo varios países que destacaron más que otros en el proceso.

En este documento se explicará el proceso que le dio el país Colombia, sus desafíos, sus logros y su facilidad en la integración, o fallos y decepciones, dependiendo de su desempeño y del análisis realizado.

La realización de este documento es como se dijo anteriormente analizar la situación con respecto a la educación en Colombia pero centrándose en la seguridad de dichas tecnologías, estrategias y métodos utilizados para tal fin, y verificar los niveles de seguridad, para así plantear al final un método o practica seguras, de utilización segura y eficiente de estos sistemas basado claro está en os estándares de la normativa ISO 27000, para así ayudar con los procesos de educación virtual que es el nuevo paradigma educacional que nos dejó este periodo transicional debido a la pandemia.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En diciembre del año 2019, se descubrió el brote en Wuhan, China, de un virus desconocido hasta el momento, la OMS, recibió reporte de una clase de neumonía de origen desconocido que desde china se expandía con peligro y vertiginosamente por todo del mundo, ampliando el espectro de contagios por diferentes continentes.

Debido a las propiedades de fácil contagio, se entró en un estado de emergencia global y se declaró, pandemia y un estado de emergencia sanitario por causa del virus Covid-19, por este motivo se empezaron a tomar medidas progresivas en algunos lugares y en otros más inmediatas.

La medida más común que se empezó a tomar luego de ver la mortalidad de tal virus fue de aislar a las personas con una cuarentena, el objetivo de la cuarentena era evitar el contagio entre las personas infectadas y los que no lo estaban, puesto que en algunos periodos la enfermedad era asintomática por lo cual los contagios eran masivos en lugares públicos sin saber quién tenía el virus, lo cual trajo consigo cientos de contagios.

Luego de la cuarentena, las diversas restricciones y empezar los múltiples esfuerzos por encontrar una vacuna que le hiciera frente a este mal, empezaban a aparecer diferentes incógnitas, y preocupaciones menos mortales pero muy importantes, entre ellas la educación.

Con las cuarentenas, restricciones y demás la educación tuvo que dar un paso muy grande y complicado que fue virtualizarse, como ya no podía haber clases presenciales se optó por el uso de las tecnologías y se empezó la transición por las clases online o clases virtuales.

Esto fue global pues se habla de una pandemia, por lo cual afecta a todo el mundo, pero esta problemática afecta en diferente medida a las diferentes naciones del mundo, ya sea por preparación, tecnología, recursos, u otros aspectos la implementación de esta nueva forma de impartir la educación, era diferente para un país desarrollado europeo en comparación con uno subdesarrollado de algún lugar desfavorecido en América, por ejemplo.

Para el caso de Colombia, que tenía una infraestructura de telecomunicación funcional, pero en desarrollo, fue un reto el afrontar este nuevo paradigma, pero aun así tuvo que adaptarse e implementar este método de enseñanza para con sus ciudadanos.

Todo este cambio o transición trajo consigo muchos problemas e inconvenientes, pero del que se va a hablar en este documento es concretamente el problema de seguridad

de la información, pues la adopción de una nueva tecnología para su aplicación siempre trae consigo diferentes falencias en especial con los entornos seguros.
También es un reto poder tener a salvo la información personal de estudiantes, padres de familia y docentes, administración de información confidencial de estudiante incluido menores, hojas de vida, bases de datos de notas, plataformas educativas, softwares contables y demás, por esta razón es importante en una institución educativa contar con diferentes esquemas y jerarquizar a los usuarios de acuerdo con su rol dentro de la institución.
La utilización de diferentes técnicas o metodologías apoyados en la normativa ISO 27000, busca mitigar cualquier ataque a la institución educativa y salvaguardar la información contenida en los servidores y bases de datos. Además de ello, proporciona una adecuada administración a la red privada de la institución educativa, para disminuir el riesgo de ataque. Es importante tener en cuenta estas metodologías, para garantizar la conservación y privacidad de los datos que se mueven a través de la red interna de las instituciones y ajustarlas al nuevo método remoto para así manejar la misma seguridad.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo los estándares de la normativa ISO 27000 pueden contribuir a reducir el riesgo a la seguridad de la información en los procesos de enseñanza virtual apoyados en TIC en Colombia?

2 JUSTIFICACIÓN

La educación es fundamental para el desarrollo de los seres humanos, siempre ha sido el pilar fundamental de una buena sociedad, por lo tanto, es un tema de suma importancia a nivel mundial, y con la reciente tragedia mundial causada por la pandemia, los gobiernos del mundo tuvieron que hacer uso de la tecnología para seguir impartiendo educación a sus ciudadanos.

La educación virtual no es más que impartir enseñanzas por un medio digital, utilizando las Tecnologías de la información y comunicación (TIC), y desde la creación de los medios digitales se ha ido desarrollando y usando, pero con la pandemia, se centralizó como la única forma segura para los ciudadanos de obtener su educación.

La razón de su seguridad es que, ya que no se necesitaría contacto y todo seria de forma virtual, no había manera de que se propagara el virus además que no rompía las normas y medidas tomadas por los diferentes gobiernos en todo el mundo.

Esto se ideó para aliviar el entorno físico, pero se encuentra con el problema que se planteó en este documento y es que, al realizar esta transición a lo digital, no solo se debe soportar, sino que además se debe proteger dicho entorno, la seguridad es muy importante en este aspecto, las personas no están expuestas a un virus mortal, pero si a cientos de peligros virtuales que, aunque no dañen físicamente y traen afectaciones graves.

La infraestructura tecnológica que tenga cada país es muy importante en este aspecto, y concretamente en Colombia no se tiene la mejor infraestructura del mundo, pero tampoco la peor es más ni siquiera de América, pero aun así los desafíos siempre han sido muy grandes.

En Colombia la seguridad informática ha venido desde los últimos 5 años en aumento con la creación de organismos de control y de regulación, pero hay un problema que es evidente y es la educación, la cultura digital en Colombia es muy pobre en comparativa con su estructura general y su estatus como nación, lo que hace vulnerable a miles de nuevos usuarios sin mencionar la creciente ola de ciberdelincuencia.

Con la virtualización de la educación se hace uso de múltiples plataformas, y algunas son seguras pero otras no garantizan la seguridad, además de la utilización de otros medios que de no tener una buena configuración los hace vulnerables, y no se podía dejar de mencionar que hasta la organización más grande siempre tiene fallos de seguridad, por lo cual, nadie está seguro y con tantos nuevos usuarios se debe tener un plan de seguridad para solventar por lo menos la mayoría de amenazas posibles.

La mitigación de riesgos es fundamental y para esto es importante analizar el estado actual de uso de herramientas para la educación virtual y realizar una investigación sobre los métodos más seguros y las buenas prácticas para fomentar un buen método

en donde se pueda impartir educación de forma virtual de manera segura, tanto para los maestros como para los estudiantes y sus familias.

En algunos países se ha invertido bastante en la seguridad informática, ya que se entiende que la información es considerada el más valioso activo intangible, con el cual se cuenta en un sistema.

Por esta razón una de las recomendaciones principales es realizar acciones de prevención y predicción, haciendo uso de las normas ISO 27000 que permiten crear estrategias y métodos de seguridad efectivo en el sistema académico de una institución educativa.

En la última década se han incrementado de manera significativa los ataques a instituciones educativas, a su vez ha surgido la necesidad de mejorar en las maneras de resguardar los sistemas informáticos. Esta necesidad de protección se puede ver suplidas con la implementación de normas como la ISO 27000, la cual ofrece una gran variedad de normas enfocadas en la seguridad de la información e informática que se ajusta a los requerimientos de cada organización.

Bajo estos parámetros se busca utilizar diferentes estrategias y herramientas TIC para que ayuden a garantizar la confidencialidad y la privacidad de los datos, buscando la calidad educativa en las instituciones.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar la seguridad de la información e informática en los procesos de enseñanza virtual mediados por TIC, teniendo como referencia la ISO 27000, para el desarrollo de estrategias y modelos seguros en los entornos digitales en Colombia.

Analizar la seguridad de la información basado en la norma ISO 27000, a través del análisis de información, la cual conlleven a el desarrollo de estrategias y modelos seguros a nivel digital en Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar el panorama de seguridad en los procesos de enseñanza virtual, apoyados por las TIC, en Colombia durante los años 2020 y 2021, mediante la revisión de informes y reportes en los procesos de aprendizaje.
- Evaluar las principales herramientas tecnológicas utilizadas en los procesos de aprendizaje dentro de las instituciones educativas, permitiendo identificar el nivel de seguridad basado en los estándares ISO 27000.
- Valorar el grado de apropiación y seguridad sobre el uso de ambientes virtuales por parte del personal académico, mediante la consulta y comparación de informes asociados que permitan establecer el grado de conocimiento y manejo seguro de las herramientas digitales.
- Elaborar una estrategia de seguridad digital que reduzca la incidencia de riesgos informáticos generadas por el manejo de las principales plataformas y herramientas tecnológicas de las instituciones académicas en los procesos de aprendizaje teniendo como referencia las ISO 27000.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 La educación Virtual

Es la dinámica de impartir la enseñanza-aprendizaje realizada de forma virtual, se trata de un formato educativo no presencial, donde la educación a través de vías remotas tiene como función buscar espacios de capacitación y formación, con la cual se apoya de herramientas TIC, que sirven para impartir conocimiento a las personas.

En la educación virtual, se manifiestan diferentes factores que implica este tipo de educación, como es la flexibilidad y exigencias, se afecta factores como el entorno económico, social y político.[1]

"Es importante tener en cuenta que la educación virtual se relaciona con la educación a distancia, la cual nació a raíz de la necesidad de cobertura de calidad educativa a personas que, por distancia y tiempo, no pueden desplazarse hacia un centro de formación físico". [2]

"La educación a distancia apareció en el contexto social como una solución a los problemas de cobertura y calidad que aquejaban a un número elevado de personas, quienes deseaban beneficiarse de los avances pedagógicos, científicos y técnicos que habían alcanzado ciertas instituciones, pero que eran inaccesibles por la ubicación geográfica o bien por los elevados costos que implicaba un desplazamiento frecuente o definitivo a esas sedes".[3]

4.1.2 Historia de la educación a distancia

La educación a distancia es una de las ofertas educativas que más ha crecido desde su surgimiento, las primeras opciones educativas a distancia surgieron en Europa occidental y en América del norte durante el siglo XIX y principios del siglo XX, se ofrecía a través de correspondencia y se podía realizar desde cualquier lugar.

Tras la creación de la radio, y luego de la televisión, se empezó a impartir cursos y carreras a través de estos dos medios de comunicación masiva.

---

[1] MinEdu. La educacion virtual. [En línea] 2017. Disponible en: https://www.mineducacion.gov.co/1780/w3-article-196492.html?_noredirect=1

[2] GCFGlobal. El Futuro de la Educación y el papel de GCFGlobal. [En línea] 2021. Disponible en: https://edu.gcfglobal.org/es/educacion-virtual/el-futuro-de-la-educacion-y-el-papel-de-gcfglobal/1/

[3] Ibid.1

Después de la Segunda Guerra Mundial la educación a distancia se popularizó entre la población europea y norteamericana, ante la necesidad de adquirir conocimientos o desarrollar habilidades para poder ingresar al mercado laboral.

Este tipo de educación también incluyó el uso del teléfono, que sirvió como medio de apoyo en el proceso educativo. Luego aparecieron los casetes y videocasetes con contenido en formato de audio y video, que funcionaron como soportes para la educación a distancia.

Con el avance tecnológico y la creación de las computadoras, la educación a distancia comenzó a realizarse a través de disquetes y enciclopedias virtuales, pero no fue hasta el posterior desarrollo de internet que la educación a distancia se hizo masiva.

Así, se dejaron de lado los métodos de educación a distancia existentes y se comenzó a utilizar el correo electrónico, las videoconferencias y las plataformas virtuales para hacer llegar los contenidos educativos a una gran parte de la población mundial[4].

4.1.3 La educación a distancia en Colombia

La primera generación se caracterizó por la utilización de una sola tecnología y la poca comunicación entre el profesor y el estudiante. El alumno recibía por correspondencia los materiales impresos que le brindaban la información y la orientación para su procesamiento. Por su parte, el estudiante realizaba su trabajo en solitario, enviaba las tareas y presenta exámenes en unas fechas señaladas con anterioridad.

La segunda generación introdujo otras tecnologías y una mayor posibilidad de interacción entre el docente y el estudiante. Además del texto impreso, el estudiante recibía casetes de audio o video, programas radiales y contaba con el apoyo de un tutor (que no siempre era profesor del curso) al que puede contactar por correo, por teléfono o personalmente en las visitas esporádicas que éste hace a la sede educativa. En algunos casos cada sede tenía un tutor de planta para apoyar a los estudiantes.

Por último, la tercera generación de la educación a distancia se caracteriza por la utilización de tecnologías más sofisticadas y por la interacción directa entre el profesor del curso y sus alumnos. Mediante el computador conectado a una red

[4] Características. Educación a distancia. [En línea] 2021. Disponible en: https://www.caracteristicas.co/educacion-a-distancia/

telemática, el correo electrónico, los grupos de discusión y otras herramientas que ofrecen estas redes, el profesor interactúa personalmente con los estudiantes para orientar los procesos de aprendizaje y resolver, en cualquier momento y de forma más rápida, las inquietudes de los aprendices. A esta última generación de la educación a distancia se le denomina como "educación virtual" o "educación en línea".

Para definir la educación en línea parte de una concepción pedagógica que se apoya en las Tecnologías de la Información y Comunicación.

Algo que garantiza la calidad de la educación es la articulación coherente y armónica de un modelo educativo con dicha tecnología, pues una educación de calidad puede salir adelante con una “mala” tecnología; pero jamás por más que la tecnología sea excelente no podrá sacar adelante un proceso educativo de baja calidad.

Lo que se pretende es desarrollar este tipo de educación, de tal manera que se convierta en una opción real y de calidad para muchos colombianos que pueden encontrar en ella el espacio para formarse.[5]

4.1.4 Características de la educación a distancia

Las principales características de la educación a distancia son:

Distanciamiento físico

Existe una separación física entre el profesor y el alumno dentro de todo el proceso educativo. Esto permite que personas de diferentes puntos geográficos puedan acceder a una variada oferta educativa.

Uso de medios electrónicos

Se emplean plataformas virtuales, libros digitales, apuntes online, acceso a tutores, videos y material audiovisual para trasmitir conocimientos. Para ello resulta imprescindible una conexión a internet, que permita acceder a los soportes o plataformas en las que se encuentran los contenidos.

Uso de tutorías y apoyo estudiantil

En ciertas ocasiones, los estudiantes cuentan con un tutor online que los ayuda a evacuar dudas durante el proceso de aprendizaje. Los alumnos establecen contacto con sus tutores a través del correo electrónico o de plataformas virtuales.

[5] MinEdu. La educacion virtual. [En línea] 2017. Disponible en: https://www.mineducacion.gov.co/1780/w3-article-196492.html?_noredirect=1

Aprendizaje independiente
En este tipo de educación el estudiante es responsable de la organización de su tiempo de estudio. En algunos casos, debe asistir a clases pautadas en un día y horario específico.

Horarios flexibles
El estudiante puede acceder a los contenidos o realizar clases virtuales o trabajos en los horarios que tiene disponibles.

Comunicación bidireccional
Las plataformas de enseñanza permiten la comunicación bidireccional (entre docente y alumno) y la comunicación entre pares para la preparación de trabajos prácticos online, video conferencias, entre otras.

Enfoque tecnológico
El sistema de educación a distancia se apoya en los avances tecnológicos que permiten la evolución de esta metodología de enseñanza.

Optimización de tiempos
Cada estudiante emplea libremente su tiempo y forma de estudio. Esto permite ampliar la demanda de estudiantes dado que no deben suspender sus actividades diarias para concurrir a una institución.

Menor costo
La educación remota implica un menor costo para las instituciones educativas porque prescinde de aulas o material impreso. Además, los cursos que se imparten suelen ser más baratos que los de formato presencial y el alumno ahorra tiempo y dinero al no tener que trasladarse de un lugar a otro.

Alcance masivo
La masificación de internet permitió que todo aquel con un ordenador y conexión a internet pueda acceder a diversas opciones educativas, como cursos o posgrados de distintos puntos geográficos. Sin embargo, la actual brecha digital que existe en el mundo genera que no toda la población tenga acceso a este tipo de educación.[6]

[6] Características. Educación a distancia. [En línea] 2021. Disponible en: https://www.caracteristicas.co/educacion-a-distancia/

4.1.5 Educación a distancia y la pandemia

Debido a al coronavirus se está cambiando de forma muy abrupta la manera en que se imparte la educación, ya que la escuela y el hogar, ahora se convierten en el mismo lugar tras las necesarias regulaciones efectuadas.

Según la UNESCO, más de 861.7 millones de niños y jóvenes en 119 países se han visto afectados al tener que hacer frente a la pandemia global que nos ha sacudido este año.

Desafortunadamente, las escuelas que pueden ofrecer una experiencia académica virtual completa, con alumnos que cuentan con dispositivos electrónicos, profesores que saben cómo diseñar lecciones en línea funcionales y una cultura basada en el aprendizaje tecnológico, no son muchas.

"El mayor cambio que requiere el aprendizaje virtual es la flexibilidad y el reconocimiento de que la estructura controlada de una escuela no es replicable en línea", señala Noah Dougherty, director de diseño en la consultora de educación, Education Elements. Muchas preguntas surgen a raíz de las problemáticas que tienden a afectar de manera desigual a aquellos en desventaja.

Estas dificultades se replican mundialmente, no sólo en la educación básica, sino en miles de universidades que han tenido que cerrar sus aulas debido a esta crisis sanitaria. [7]

4.1.6 Informática segura

El objetivo de la seguridad informática es proteger los activos que están asociados con los elementos que integran un sistema informático. Para lograr un ambiente informático más seguro se puede decir que los elementos que integran un sistema informático son las tecnologías de información, la información, las personas o usuarios y los Inmuebles.

Se le puede aplicar en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

- La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de

[7] Tecnológico Monterrey. Educación en tiempos de pandemia: COVID-19 y equidad en el aprendizaje. [En línea] 2020. Disponible en: https://observatorio.tec.mx/edu-news/educacion-en-tiempos-de-pandemia-covid19

otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

- La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.

- La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.

- La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

- La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.[8]

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

Integridad: los activos o la información solo pueden ser modificados por las personas autorizadas y de la forma autorizada.

[8] Kaspersky. Ingeniería social: definición. [En línea] 2021. Disponible en: https://latam.kaspersky.com/

Confidencialidad: la información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.
Disponibilidad: los activos informáticos son accedidos por las personas autorizadas en el momento requerido.
Irrefutable (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.[9]

4.1.7 Tipos de ciber amenazas

Las amenazas a las que se enfrenta la ciberseguridad son tres:
El delito cibernético incluye agentes individuales o grupos que atacan a los sistemas para obtener beneficios financieros o causar interrupciones.
Estos son algunos de los métodos comunes utilizados para amenazar la ciberseguridad:

Malware
se refiere al software malicioso. Ya que es una de las ciber amenazas más comunes, el malware es software que un cibercriminal o un hacker ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia propagado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima, el malware puede ser utilizado por los ciberdelincuentes para ganar dinero o para realizar ciberataques con fines políticos.

Hay diferentes tipos de malware, entre los que se incluyen los siguientes:

- **Virus:** un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- **Troyanos:** un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
- **Spyware:** un programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- **Ransomware:** malware que bloquea los archivos y datos de un usuario, con la amenaza de borrarlos, a menos que se pague un rescate.
- **Adware:** software de publicidad que puede utilizarse para difundir malware.

[9]Ecured. Tipos de virus. [En línea] 2020. Disponible en: https://www.ecured.cu/EcuRed:Enciclopedia_cubana

- **Botnets:** redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.

Phishing

El phishing es cuando los cibercriminales atacan a sus víctimas con correos electrónicos que parecen ser de una empresa legítima que solicita información confidencial. Los ataques de phishing se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito y otra información personal.

Ataque de tipo "Man-in-the-middle"

Un ataque de tipo "Man-in-the-middle" es un tipo de ciber amenaza en la que un cibercriminal intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

Inyección de código SQL

Una inyección de código SQL (por sus siglas en inglés Structured Query Language) es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa. Esto le brinda acceso a la información confidencial contenida en la base de datos.

Ataque de denegación de servicio

Un ataque de denegación de servicio es cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales.

Malware Emotet

A finales del 2019, el Centro Australiano de Seguridad Cibernética advirtió a las organizaciones nacionales sobre la ciber amenaza mundial generalizada del malware Emotet. Emotet es un sofisticado troyano que puede robar datos y también cargar otros malware. Emotet se aprovecha de las contraseñas poco sofisticadas y es un recordatorio de la importancia de crear una contraseña segura para protegerse de las ciber amenazas.

Estafas románticas

En febrero del 2020, el FBI advirtió a los ciudadanos de EE. UU. que tuvieran cuidado con el fraude a la confianza que los cibercriminales cometen a través de sitios de

citas, salas de chat y aplicaciones. Los perpetradores se aprovechan de las personas que buscan nuevas parejas y engañan a las víctimas para que proporcionen sus datos personales. El FBI informa que las ciber amenazas románticas afectaron a 114 víctimas de Nuevo México durante 2019, cuyas pérdidas financieras sumaron 1 600 000 dólares.

Malware Dridex

En diciembre del 2019, el Departamento de Justicia de los Estados Unidos (DoJ) imputó al líder de un grupo de cibercriminales organizados por su participación en un ataque global del malware Dridex. Esta campaña malintencionada afectó al público, al gobierno, a la infraestructura y a las empresas de todo el mundo. Dridex es un troyano financiero que posee diferentes funcionalidades. Desde el 2014, afecta a las víctimas e infecta a las computadoras a través de correos electrónicos de phishing o malware existente. Es capaz de robar contraseñas, datos bancarios y datos personales que pueden utilizarse en transacciones fraudulentas, y ha causado pérdidas financieras masivas que suman cientos de millones de dólares. En respuesta a los ataques de Dridex, el Centro Nacional de Seguridad Cibernética del Reino Unido aconseja a las personas que “se aseguren de que los dispositivos estén actualizados y los antivirus estén activados y actualizados, y de que se realicen copias de seguridad de los archivos”.[10]

[10] Ecured. Tipos de virus. [En línea] 2020. Disponible en: https://www.ecured.cu/EcuRed:Enciclopedia_cubana

4.2 MARCO CONCEPTUAL

4.2.1 Ciberseguridad en tiempos de pandemia

El 2020 y el 2021 han sido años plagados de muerte y mucha desesperanza a causa de un virus que, aunque no muy mortal, si, muy contagioso, que ha llevado al mundo a declarar emergencia sanitaria global o también llamada pandemia, esto trajo consigo múltiples problemas, sociales, económicos, y más, pero que no nos competen en este momento, pues nos enfocaremos en uno en concreto, y es en el tecnológico y más específicamente, la ciberseguridad.

Como se venía explicando el estado de emergencia o pandemia trajo consigo medidas para la contención de este virus que aquejaba al mundo entero, por sus características se decide estar en cuarentena, un estado de aislamiento social, un distanciamiento obligatorio, esto trajo como ya se explicó varios problemas en diferentes sectores, entre ellos la educación, pues las clases ya no se podrían hacer presenciales pues rompería las normas actuales de distanciamiento, por lo tanto se optó por la utilización de la tecnología y se decidió que ante las nuevas medidas ahora seria virtualizada la educación.

La educación Virtual no es más que utilizar las herramientas TIC para impartir las clases o enseñanzas, esto solucionaría el problema de contagio pues cada alumno y docente estaría en un lugar distante uno del otro, lógicamente como todo lo anterior, también trajo bastantes problemas consigo, uno de ellos es la ciberseguridad tal como se habló antes.

4.2.2 Cibercrimen y ciberseguridad

La ciberseguridad se refiere a la seguridad cibernética, todo lo referente a las TIC para resumir, pero no solo a los equipos, las infraestructuras y las configuraciones, también le compete las personas, tanto la prevención de cibercriminales como la preparación de los usuarios finales.

Ahora antes de entrar en el estado de la seguridad cibernética en este periodo de tiempo de pandemia, vamos a tener en cuenta el estado de la ciberseguridad antes de esta, pues es importante tener en cuenta que ya desde los últimos cinco años el ciber crimen ha tenido un auge muy preocupante para las comunidades del mundo, mientras la tecnología avanza y se hace cada vez mejor los cibercriminales parecen hallar más formas y métodos para su utilización malintencionada, lo que ha llevado a gobiernos mundiales realizar grandes inversiones en temas de seguridad, además de conformar organizaciones formadas por diferentes naciones para combatir el cibercrimen.

Todo estos esfuerzos han ido aumentando pero la cibercriminalidad no ha bajado tanto como se esperaría, al contrario cada vez va en aumento y con este escenario nos encontramos con la emergencia descrita, es muy preocupante saber que en un escenario tan desolador se hallan personas malintencionadas tratando de exponer a personas que luchan por seguir a pesar del estado del mundo actual, por eso es tan importante el proveer una seguridad a los ciudadanos que confían el estar seguros del mundo físico estando en el virtual, pero se encuentran con estos criminales que les pueden causar daños importantes, quizás no físicos pero si económicos y hasta de integridad.

4.2.3 Consecuencias

Una de las consecuencias evidentes de la pandemia ha sido la rápida transición a una vida digital, con lo cual los ciberataques se han disparado debido a la falta de preparación de los nuevos usuarios y a los peligros digitales, desde el comienzo de la crisis del virus Covid-19 los ataques de phishing han aumentado un 70% según Telefónica TECH, también esta fuente nos informa, que según los registros de las autoridades, durante la pandemia, el phishing y el smishing son los principales ataques utilizados por los criminales para ultrajar a los ciudadanos.

Las causantes, el incremento masivo de usuarios novatos, la desinformación y la falta de preparación, claramente al ser una emergencia fue un cambio muy trascendental e inmediato, pero según su nivel en el proceso cultura digital, el proceso de adaptación de cada nación varia.

Con las nuevas medidas tomadas por los gobiernos en la pandemia muchos ciudadanos a excepción de unos pocos fueron confinados y obligados a trabajar remotamente, desde sus casas o en lugares aislados, lo que trajo un aumento desproporcionado del uso de las TIC, y de herramientas de conexión como herramientas de control remoto, de video conferencias y de mensajería instantánea.
Para la educación no fue muy diferente al resto de la población, este nuevo paradigma afecto a un gran numero poblacional en todo el mundo, obligando a muchos a abandonar su modus vivendi, para buscarse la vida en este nuevo paradigma de vida, los campus por ejemplos tuvieron que ser desocupados haciendo a estudiantes a regresar a sus casa pero hubo muchos sin posibilidad de hacerlo debido a la situación mundial del lugar de su origen, pero la idea de los gobiernos era seguir impartiendo la educación de forma remota y con ayuda de las Tics.

Ignorando los problemas de muchos estudiantes, quienes no tenían posibilidad de acceso a estos medios digitales tan fácilmente, y múltiples problemas sociales surgidos

por la emergencia vivida, para quienes pudieron adoptar este nuevo método de enseñanza y educación tampoco fue muy fácil, después de todo salieron a la luz problemas de infraestructura y la desigualdad en conocimientos informáticos de la población general, entre otros.

4.2.4 Colombia y el nuevo paradigma

Concretamente en Colombia muchos de estos nuevos usuarios eran niños que acompañados por unos padres no muy afín a la tecnología fueron expuestos a este nuevo paradigma digital.

Como se explicaba anteriormente, con la educación se integraron al mundo digital usuarios habituales, algunos casuales y muchos nuevos, los cuales no fueron orientados a tener una sana y segura ciudadanía digital, simplemente se les alentó a digitalizarse, muchos con carencias en términos de seguridad, como equipos desactualizados o no protegidos, conexiones no seguras, escasez de protocolos básicos de ciberseguridad, todo esto a causa de la falta de concienciación sobre los peligros cibernéticos.

Los recursos utilizados por la educación virtual son herramientas de sistema de correo electrónico, foros de discusión, blogs, chat, conferencias tanto de voz como de video, uso de la nube y bibliotecas digitales, entre otros más imaginativos, pues hay que recordar que cada tutor realiza su clase según su criterio y los permisos de la institución a la cual pertenece.

Todas estas herramientas ayudan a dinamizar y a mejorar el proceso de aprendizaje del estudiante y le dan opciones de enseñanza a los maestros, pero todas son potenciales peligros para los usuarios si es que no saben navegar en internet, pues los peligros son cada vez mayores, muchas personas tienen una sensación falsa de seguridad por utilizar herramientas soportadas por grandes compañías a nivel mundial, pero la verdad es que, si hasta esas compañías están expuestas y tienen riesgo de ser atacadas, con toda las preparaciones e inversiones en seguridad, evidentemente un usuario normal también lo está.

4.2.5 Peligros y amenazas

Las personas naturales o usuarios normales del servicio de las TIC piensan que los ataques ocurren por navegar en sitios peligroso y hacer búsquedas complejas o específicas, lo cual en su mayoría es una mentira, incrementa el riesgo al exponerse más si pero la exposición es solo un factor, también piensan que a un ciudadano de a pie no le van a secuestrar los datos o le van a extorsionar o a realizar algún tipo de ataque, pero la verdad es que es posible, y es lo que ha estado ocurriendo, un claro

ejemplo es el uso de una base de datos de un centro educativo hackeado para hacer que sus estudiantes cayeran expuestos a múltiples ataques de phishing y smishing, causando daños económicos y de información muy importante, aunque es un ejemplo de un modo de ataque, ha sucedido en múltiples ocasiones.
Y no solo concierne a las instituciones, los usuarios también al solo tener algún tipo de exposición al mundo digital están en constante peligro ante una ciber amenaza, pero hablando de educación, se debe formar un ambiente seguro, para que los estudiantes se sientan seguros y puedan desarrollar sus actividades sin mayores inconvenientes que los generados por las cargas académicas.

Para esto es de suma importancia capacitar e instruir sobre buenas prácticas, sobre cultura segura, sobre la buena utilización de las TIC, además de concienciar sobre los peligros, las amenazas y los riesgos, al navegar en internet, e informar de los múltiples ataques existentes por lo menos concernientes a personas naturales para prepararse ante estos criminales y no caer como tantas víctimas que ya lo hicieron.

Todo tipo de seguridad busca como objetivo minimizar el riesgo con respecto a los accesos o el mal uso de la información, en el caso de la seguridad informática debemos manejar una buena gestión de riesgos, en donde se use medidas preventivas y correctivas como políticas y normas de seguridad que puedan proteger el sistema frente a un ataque o alteración de los datos suministrados allí.

4.2.6 Normas 27K

Las normas ISO 27000 nos sirven como punto de partida para establecer manuales de buenas prácticas con relación al SGSI o al sistema de gestión de seguridad de la información, todo lo relacionado con la ISO 27000 va encaminado a la mejora continua y a la mitigación de riesgos.

Esta norma describe los sistemas de gestión de seguridad de la información de forma general, incluyendo las normas ISO 27k, definiendo términos y definiciones explícitamente, al tener intenciones de implementar algunas de las normas de la familia ISO 27k debe tener en cuenta esta norma introductoria a la gestión de seguridad de la información, para una posterior implementación de las normativas.

A partir de las ISO se pude ser capaz de establecer, requisitos, manuales, guas, requerimientos y criterios de evaluación que ayudan a que el sistema de gestión de seguridad sea más estable y usable ante las empresas a desempeñar.

ISO 27001: Esta norma ISO se encarga de definir algunos requerimientos en el SGSI que sirven como punto de partida para implantar esta norma y que a su vez es certificable.

ISO 27002: Comprende un conjunto de buenas prácticas, las cuales contiene hasta 114 controles, divididos en 14 dominios y 35 controles de seguridad.

ISO 27003: La norma ISO 27002 ayuda a implementar de forma correcta el SGSI a través de una guía que ayuda a tener como base los aspectos importantes del SGSI.

ISO 27004: Se complementa con la definición de métricas, que ayudan a evaluar de forma eficiente el rendimiento del SGSI.

ISO 27005: Se define como se debe manejar la gestión de riesgos y que metodología se debe llevar a cabo de acuerdo con los sistemas de gestión de la información.

ISO 27007: Se toman los procedimientos necesarios para llevar a cabo auditorías internas y externar con el fin de poder verificar el funcionamiento y usabilidad, basado en la norma ISO/IEC-27001.

ISO 27008: Se utilizan diferentes controles del SGSI, para poder evaluar los mismos y conocer si son controles eficientes a la hora de mitigar riesgos.

ISO 27009: Se basa en añadir nuevos controles y van orientados a sectores específicos; se hace con el fin de buscar mejora en su implantación de objetivos.

ISO:27010: Esta norma ISO busca generar controles en cuestión de compartir información entre empresas u organizaciones. Se busca conocer que riesgos pueden aparecer y a su vez con que controles se pueden mitigar los mismos.

ISO 27013: Contiene una guía que ayuda a integrar las normas SGSI y la SGS, sirve en los casos de las empresas que utilizan ambas.

ISO27014: Esta enfocado en el gobierno de la seguridad de la información, ayuda a establecer principios que ayudes a monitorizar las actividades relacionadas con la seguridad de la información.

ISO 27016: La norma ISO 27016 va enfocada a la toma de decisiones en el ámbito económico y que se vean estrictamente ligadas a la gestión de la seguridad de la información en apoyo a la dirección principal de las empresas.

ISO 27017: Contiene una guía de 37 controles específicos para las empresas que prestan servicios cloud.
ISO 27022: Proporciona un modelo de referencia de procesos (PRM) para la gestión de la seguridad de la información.

ISO 27031: Brinda orientación sobre los conceptos y principios detrás del papel de la tecnología de la información y las comunicaciones para garantizar la continuidad del negocio.

ISO 27032: Aborda la Ciberseguridad o la seguridad del Ciberespacio, definida como la preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio.

ISO 27033: Proporciona una guía detallada sobre la implementación de los controles de seguridad de la red que se introducen en ISO 27002.

ISO 27034: Ofrece orientación sobre la seguridad de la información a quienes especifican, diseñan y programan o adquieren, implementan y usan sistemas de aplicación, en otras palabras, gerentes, desarrolladores y auditores de TI y de negocios y, en última instancia, los usuarios finales de las TIC.

ISO 27035: Amplía la sección de gestión de incidentes de seguridad de la información de ISO 27002.

ISO 27036: Es una norma de varias partes que ofrece orientación sobre la evaluación y el tratamiento de los riesgos de la información relacionados con la adquisición de bienes y servicios de los proveedores.

ISO 27039: Proporciona pautas para ayudar a las organizaciones a prepararse para implementar sistemas de prevención y detección de intrusiones (IDPS).

ISO 27040: Brinda orientación técnica detallada sobre cómo las organizaciones pueden definir un nivel apropiado de mitigación de riesgos mediante el empleo de un enfoque consistente y bien probado para la planificación, el diseño, la documentación y la implementación de la seguridad del almacenamiento de datos.

ISO 27550: Proporciona pautas de ingeniería de privacidad que tienen como objetivo ayudar a las organizaciones a integrar los avances recientes en ingeniería de privacidad en los procesos del ciclo de vida del sistema.

ISO 27554: Define el riesgo relacionado con la gestión de identidad con el fin de aplicar las directrices de gestión de riesgos de ISO 31000 en este campo.

ISO 27555: Contiene pautas para desarrollar y establecer políticas y procedimientos para la eliminación de información de identificación personal (PII).

ISO 27556: Brinda ayuda al implementar mecanismos de control de privacidad efectivos en los sistemas de TIC, el manejo de datos debe controlarse mediante la entrada de preferencias de privacidad por parte de los directores de PII, incluida la información de consentimiento.

ISO 27557: Proporciona pautas para la gestión de riesgos de privacidad organizacional.

ISO 27559: Proporcionará un marco no prescriptivo para identificar y mitigar los riesgos relacionados con la privacidad, como la repetición de información, etc. durante el ciclo de vida de los datos no identificados.

I**SO 27560:** Especifica una estructura de información interoperable, abierta y extensible para registrar el consentimiento de los titulares de datos personales o de los interesados para el procesamiento de datos.

ISO 27701: Especifica los requisitos y brinda orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de información de privacidad (PIMS) en forma de una extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad dentro del contexto de la organización.

4.3 MARCO CIENTÍFICO O TECNOLÓGICO

En medio de la educación a virtual se llevó a cabo diversas aplicaciones capaces de proporcionar herramientas a los docentes, para que el proceso educativo de los estudiantes se haga más interactivo y eficaz, algunos de ellos son:

Correo electrónico: Esta herramienta es utilizada en todos los ámbitos informáticos empresariales, pero llevándolo a cabo en el ámbito educativo, permite que exista una comunicación fluida entre los actores de aprendizaje (Docentes, estudiantes, coordinadores), permite enviar información de tipo gráfico y de texto; además de ello permite que haya una interacción donde se tenga una comunicación formal con otras personas.

Foros de discusión: El foro de discusión permite que exista una comunicación asertiva entre dos o más personas, en la cual existe una total interacción entre todos los participantes de este y permite que otras personas puedan leer opiniones o comentarios de un tema o asunto en especial.

Bitácora digital (Blog): Es un documento que se encuentre en línea y permite realizar publicaciones cronológicas de textos y artículos de varias personas o autores. Se puede considerar como un diario, donde el autor puede expresar sus opiniones, acerca de un comentario o un tema en especial. En la bitácora se permite expresar opiniones de la más reciente a la más antigua. Llevándolo a el ámbito de herramientas virtuales, es bastante importante, ya que los alumnos pueden publicar comentarios acerca de un tema en especial, el docente los puede leer, reaccionar y comentar el mismo, convirtiéndose en un dialogo preciso y de manera online.

Conversación escrita (Chat): Es uno de los métodos más sofisticados y utilizados en la virtualidad, ya que permite la comunicación simultanea entre dos o más personas, que pueden estar conectados a una red, ya sea de manera pública o privada; pero tiene la misma funcionalidad:

Audioconferencias: Es otro método de comunicación en directo con los receptores, permite llevar la voz de los interlocutores, se puede catalogar como una información formal del mensaje ya que se puede escuchar un mensaje no verbal, pero con el tono de la voz se puede dar a entender un significado o una profundización especial a un tema o un comentario en general.

Videoconferencias: Es el método más eficaz a la hora de transmitir mensajes en directo a los estudiantes, se debe tener un alto grado de presencialidad en la misma, ya que a través de ella los receptores pueden participar y a su vez el emisor puede responder a todas sus dudas. Su ventaja es que tanto el emisor como el receptor se pueden encontrar a millones de kilómetros, pero la información llega de manera óptima.

Nube educativa: El servicio de la nube proporciona un servicio tanto a docentes como a estudiantes, el cual permite que se pueda compartir, crear, revisar o descargar material educativo en un equipo que tenga conexión a internet en tiempo real. Se considera un sistema educativo autodidacta y dinámico.

Bibliotecas digitales: Son bibliotecas que se encuentran en la web. Para poder acceder a ellas se debe contar con acceso a internet; medios como las revistas y los periódicos están cambiando su método de transmitir información ya que ofrece una comodidad a nivel de consulta más sencilla que el mecanismo tradicional.

Su aplicación se puede hacer mediante diferentes proveedores o herramientas, a continuación, se mencionará las más usadas e importantes, y se describirán de forma breve.

Google

La compañía Google aparte de ofrecer servicio de correo electrónico ofrece una serie de herramientas que se asocian y engloban una suite muy útil para la educación virtual o a distancia. Entre ellas están:

Google for Education

Es una suite de Google para profesores y alumnado que proporcionan un conjunto de herramientas de fácil uso y acceso para usar en las clases o en cualquier momento del proceso educativo. Incluye varias herramientas de trabajo.

Gmail

Es el servicio electrónico de Google, su capacidad de almacenamiento es muy amplia, su interfaz amable es muy intuitiva y cómoda ayudando a tener mejor orden y ayuda a controlar el spam o correo no deseado.

Google Classroom

Es una aplicación enfocada a ayudar en el proceso de enseñanza virtualizada, permite la creación de aulas virtuales, permite distribuir tareas, así como evaluar contenidos y facilita la conexión entre profesores, padres y alumnos.

Google Drive
Es una herramienta en la nube propiedad de Google que permite almacenar hasta 15GB de forma gratuita, el cual permite acceder a estos archivos desde cualquier dispositivo que tenga sincronizado a la cuenta asociada, además cuenta con una suite ofimática online que permite crear, modificar y compartir documentos de forma eficiente.

Google Forms
Se trata de unas herramientas para la creación de formularios, sirve tanto para la creación de encuestas en línea o para realizar pruebas, que pueden ser retroalimentadas o evaluadas de forma muy simple y fácil.

Google Calendar
Es una aplicación muy útil que funciona como calendario que interconecta los dispositivos asociados ayudando en el proceso gestionando los horarios, las fechas de exámenes, de entregas, de eventos, etc.

Google Keep
Es una aplicación muy simple pero útil, que ayuda a crear notas, recordatorios, etiquetas, captura mensajes de voz convirtiéndolos en texto y compartiendo la información de forma ágil.

Google Hangouts
Se trata de un chat online en el cual se pueden interconectar hasta 10 personas en videoconferencia y en chat aproximadamente 100, puede utilizarse desde cualquier dispositivo conectado a la cuenta principal de correo de Google, y se usa para intercambiar opiniones y enviar lecciones a los alumnos.

Google Meet
Es una aplicativo de videollamada que permite conectar a múltiples usuarios, pudiendo conectarse ya sea por audio o por video, su capacidad puede llegar hasta a 250 usuarios con una versión de pago, permite no solo la posibilidad de dar las conferencias, sino que también de grabarlas, dejando un enlace en el cual se almacena la reunión, tiene un chat también en el cual se puede participar en tiempo real, compartir pantalla, audios, videos o archivos.

Microsoft
Esta compañía también ofrece una serie de soluciones a las necesidades de conexión y de ayuda a la educación virtual.

Outlook
Es el servicio de correo electrónico propiedad de Microsoft, tiene un sistema inteligente de bandeja de entrada que facilita la detección de correos importantes, es minimalista y de fácil acceso y cuenta con la opción de calendario, de asociación de contactos con plataformas como Skype y además algunos servicios y aplicativos muy importantes.

Microsoft OneDrive
Se trata de un servicio de almacenamiento online, que está asociada con el correo Outlook, en donde se pueden almacenar 5GB de archivos, permite compartir archivos y acceder a ellos desde cualquier dispositivo asociado.

Office 365
Es un servicio de Microsoft que ofrece una suite completa de Office online, en donde se permite crear documentos y archivos y trabajar de forma colaborativa además de compartirlos.

Microsoft Teams
Se trata de un complemento de Office 365 que permite chat, videoconferencias, notas, entre otras opciones, en donde se pueden conectar hasta 250 usuarios en tiempo real y compartir, pantalla, audios, videos y contenido variado, en un entorno amigable además de la realización de documentos con la ofimática de Office 365 en el mismo aplicativo, lo cual resulta bastante útil si se están desarrollando actividades conjuntas.

OneNote
Es un bloc de notas digital, en donde se puede tomar notas, recopilar información, y la compartirla e interactuar con esta.

Zoho
Es un aplicativo de gestión en la nube multiplataforma y ejecutable en la nube, tiene una suite ofimática en la cual se puede trabajar online, crear, modificar y compartir archivos y documentos, además cuenta con Zoho mail que se trata de un servicio de correo electrónico, en el cual trabaja con Zoho Workplace que se trata de un conjunto de aplicaciones de oficina considerados de los más seguros del mercado, también cuenta con funciones como videoconferencias, chat, calendario, programador de tareas, creador de notas y marcadores.

Yahoo! Mail Es un proveedor de servicio de correo electrónico que se destaca por su capacidad de almacenamiento su interfaz amigable, además de contar con una bandeja muy organizada, que permite crear filtros y carpetas para agrupar los correos recibidos.

WhatsApp

WhatsApp puede ser una herramienta motivadora y creativa en la vida diaria de los estudiantes. Puede crear más interacción en el aula de lo habitual. Esta herramienta, por tanto, puede ser muy amplia ya que proporciona, además de mensajes de texto, correos de voz, imágenes, fotos e incluso llamadas IP, conectividad IP con el teléfono instalado u otro dispositivo con el que quieras hablar. Como resultado, se puede aprovechar la popularidad de WhatsApp para expandir los canales a través de los cuales los maestros pueden crear respuestas más rápidas, claras y armoniosas para las interacciones diarias de los estudiantes. La idea es crear grupos para que los estudiantes puedan tener un papel más activo en el aprendizaje y al mismo tiempo facilitar la construcción de conocimiento entre ellos.

Dropbox

"El servicio de almacenamiento en línea más popular para guardar y compartir archivos. También ofrece la posibilidad de crear carpetas compartidas con otros usuarios y conectarse mediante aplicaciones desde distintos dispositivos".[11]

"Un espacio de alojamiento que dispone de diferentes herramientas para guardar archivos como documentos, imágenes o presentaciones. El almacenamiento no es su única función: permite sincronizar carpetas con compañeros de la docencia, estudiantes o familiares de estos; hablar con otros usuarios a través del sistema de comentarios y acceder desde distintos dispositivos".[12]

Skype

Es una de las aplicaciones más legendarias y utilizadas para realizar reuniones virtuales o retransmitir clases online, comunica bastante bien y aunque no tiene tantas herramientas como Zoom, la experiencia sonora y visual es bastante completa.[13]

Skype en clase

"Gracias a la función de chat integrada, es genial chatear con los estudiantes mientras les envía enlaces a recursos o tareas para trabajar con el maestro. Además,

[11] Educacion3.0. Herramientas educativas para organizar, crear y gestionar la labor docente. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-educativas-docentes-ahorrar-tiempo/

[12] Educacion3.0. Herramientas colaborativas para el aula. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-colaborativas-aula/

[13] ArteyAnimacion. Conoce las 7 mejores herramientas "gratis" para clases y reuniones virtuales 2021. [En línea] 2021. Disponible en: https://arteyanimacion.com/herramientas-clases-y-reuniones-virtuales/

recientemente se agregó la función para usarlo sin registro, por lo que no es necesario que los estudiantes ingresen sus datos: simplemente genere un código de 24 horas invitando a las personas a unirse a la clase. Además, cuenta con una opción de "Skype en Clase" diseñada para difundir conocimientos educativos".[14]

Zoom meeting

"Su versión gratuita ofrece opciones para programar reuniones de video y agregar temas de reunión. Luego envía un enlace URL para que el usuario se una al grupo; también incluye un botón "Invitar personas" para agregar más participantes.[15]

> La herramienta incluye un tablero virtual de escritura y dibujo, chats grupales, funcionalidad para compartir pantalla, grabación de reuniones y clases para monitoreo e integración de seminarios web con Facebook Live y Youtube Live. La opción gratuita permite que hasta 100 personas se unan a una reunión de equipo de 40 minutos, pero hay una opción que permite crear una cantidad ilimitada de nuevas reuniones, cada una con una duración de 40 minutos. También tiene una versión de pago que incluye más almacenamiento y servicios.[16]

Kahoot

"Se trata de una herramienta online que puede ser utilizada para enseñar por medio de juegos con formato de concurso. Puedes crear un concurso con distinta temática y tipos de actividades competitivas. Puedes crear una cuenta gratuita para tener acceso a las actividades y diseñar tu concurso. Entre las actividades están las preguntas de verdadero o falso y de selección múltiple. Tu cuenta gratuita admite hasta 50 personas".[17]

"Kahoot permite crear concursos de preguntas y respuestas que sirven para poner a prueba los conocimientos de los alumnos o que repasen los contenidos que ya se han trabajado en el aula. Existen cuatro tipos de test: concurso, puzle, debate o encuesta.

---

[14] HUBSPOT. Los mejores programas para videoconferencia. [En línea] 2021. Disponible en: https://blog.hubspot.es/sales/programas-videoconferencias

[15] Educación 3.0. Plataformas gratuitas para aprender a través de videoconferencias. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/plataformas-de-videoconferencia/

[16] BIBDIGITAL. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informatica. [En línea] 2007. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD1053.pdf

[17] EDTECH. 5 herramientas gratuitas para dinamizar tus clases virtuales. [En línea] 2021. Disponible en: https://pupitres.net/blog/5-herramientas-gratuitas-para-dinamizar-tus-clases%02virtuales

Los juegos se pueden proyectar en una pantalla haciendo a toda la clase partícipe y los estudiantes responden desde sus ordenadores o dispositivos móviles".[18]

Edmodo

"Una de las plataformas de aprendizaje más conocidas del mundo. Su objetivo es crear clases virtuales en las que los alumnos participen, colaboren y dialoguen, todo a través de un mero navegador".[19]

"Edmodo puede comunicar tanto estudiantes como docentes, pero a su vez puede comunicar familias, respecto a todo lo relacionado con la parte académica. Aparte de ello permite compartir fotos, proyectos, trabajos y actividades, que pueden ser visualizados por el personal académico, etc."[20]

Cerebriti

Es una aplicación que cuenta con un Directorio Activo extendido, que cuenta especialmente con miles de juegos disponibles que han sido creados previamente por maestros y organizaciones y dejados al público. Puede buscar su categoría por juego, tema, evento o palabra clave. Cerebriti comienza a jugar sin registro previo, solo visite el sitio web oficial. Sin embargo, si desea guardar los resultados de su estudiante, puede registrarse fácil y rápidamente. Otra gran cosa de esta herramienta es que, si se desea crear un juego con información propia, se puede usar plantillas editables para acelerar el proceso.[21]

"La sección Edu de Cerebriti permite evaluar las lecciones de una manera fácil y divertida: a través de juegos. Independientemente de si son creados por estudiantes o profesores de todo el mundo. También permite consultar el progreso de los estudiantes individuales por materia o materia".[22]

---

[18] Educación 3.0. Herramientas colaborativas para el aula. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-colaborativas-aula/

[19] Educación 3.0. Herramientas educativas para organizar, crear y gestionar la labor docente. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-educativas-docentes-ahorrar-tiempo/

[20] Ibid.20

[21] Cerebriti. cerebriti. [En línea] 2022. Disponible en: www.cerebriti.com

[22] Educación 3.0. 30 herramientas para la comunicación entre familias, alumnos y centro. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-comunicacion-familias-centros/

ClassDojo

Esta plataforma ayuda a mantener una comunicación fluida entre los estudiantes, los padres y el personal. ClassDojo alienta a compartir recursos de aprendizaje en el hogar a través de fotos, videos y mensajes en la plataforma. Asimismo, los docentes pueden incentivar a sus alumnos sobre cualquier habilidad o valor, ya sea el trabajo duro, la amabilidad, ayudar a los demás, etc. [23]

"Permite a los profesores gestionar a los estudiantes. asignando puntuaciones positivas y negativas para medir su comportamiento. Toda esta información es visible para los familiares y se puede establecer un canal de comunicación con ellos. Es divertido, fácil de usar, fácil de configurar y comenzar, y muy intuitivo. También permiten tanto maestro-alumno-padre interactúe a través de SMS y MMS y se pueden definir como Edmodo con una interfaz más fácil de usar, aunque con una funcionalidad más limitada".[24]

Genially

"Permite crear contenidos diferentes en los que la interactividad y la información ganan gran peso. Perfectos para usar en clase, enganchar a los chavales y explicar lecciones completas a golpe de imagen, es una de esas herramientas para crear infografías muy logradas y bien trabajadas que podemos usar en clase para ahorrar tiempo y esfuerzo, logrando grandes resultados".[25]

"Es una herramienta que permite a los docentes crear presentaciones de forma animada e interactiva para captar de mejor manera la atención de los estudiantes.
Esta herramienta cuenta con una biblioteca de plantillas que facilitan la creación del contenido animado de las presentaciones. Las plantillas se pueden encontrar según la temática que se desea representar, hace que el contenido de una materia cobre vida, generando mayor motivación al momento de prestar atención".[26]

---

[23] Wikipedia. Educación a distancia. [En línea] 2021. Disponible en: https://es.wikipedia.org/wiki/Educaci%C3%B3n_a_distancia

[24] Educación 3.0. 30 herramientas para la comunicación entre familias, alumnos y centro. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-comunicacion-familias-centros/

[25] Educación 3.0. Herramientas colaborativas para el aula. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-colaborativas-aula/

[26] EDTECH. 10 herramientas gratuitas para dinamizar tus clases virtuales. [En línea] 2021. Disponible en: https://pupitres.net/blog/10-herramientas-gratuitas-para-dinamizar-tus-clases%02virtuales

Padlet

"Herramienta gratuita para crear murales colaborativos de forma virtual. Profesores y alumnos pueden compartir enlaces y fotos en un entorno seguro. Les permite crear una URL personalizada y moderar los posts".[27]

"Permite la creación de distintos espacios en los que organizar el temario de una asignatura o compartir información adicional con los estudiantes. Son denominados 'muros' y, en ellos, los docentes pueden incluir toda la información que quieren presentar en clase con la ayuda de imágenes, enlaces y documentos. El hecho de que sea un espacio interactivo permite que en cada muro se genere participación en torno al tema expuesto".[28]

Esemtia

"Del Grupo edebé, es una plataforma integral que aborda todas las etapas educativas, desde Infantil a Formación Profesional. En el caso de esemtia school, las familias reciben información acerca del día a día de sus hijos. Ya sea vía web o a través de la aplicación esemtia Familias (gratuita para Android e IOS), consultan información diversa como eventos, anotaciones pedagógicas, galerías de fotos, mensajes, tareas para hacer en casa, posibles incidencias".[29]

"Ayuda a gestionar todas las actividades del aula, lo que facilita la organización de las tareas diarias del docente. Desarrollar ejercicios y secuencias didácticas, organizar grupos y tareas con etiquetas personalizadas, crear elementos de evaluación, diseñar rúbricas y compartir y sincronizar las calificaciones del alumnado son algunas de las funciones que incorpora la app".[30]

---

[27] Educación 3.0. Herramientas educativas para organizar, crear y gestionar la labor docente. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-educativas-docentes-ahorrar-tiempo/

[28] Educación 3.0. Herramientas colaborativas para el aula. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-colaborativas-aula/

[29] Educación 3.0. 30 herramientas para la comunicación entre familias, alumnos y centro. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-comunicacion-familias-centros/

[30] Educación 3.0. Herramientas colaborativas para el aula. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-colaborativas-aula/

LiveWebinar

"Permite organizar seminarios web, está basado en navegador, incluidas funciones interactivas como compartir pantalla, pizarra, encuestas y cuestionarios, opciones de marca, contenido a pedido, integraciones, interpretación de idiomas. Más de 50 funciones de interacción entre los participantes. Además de más de 1.500 componentes para elegir, que se pueden modificar y combinar libremente, para mantener los estándares de seguridad, incluido el cumplimiento de la normativa de protección de datos personales".[31]

Anymeeting

Esta plataforma permite tener una sala virtual, para esto se debe registrar e iniciar sesión. El número de participantes es libre 30 personas y se debe tener un correo electrónico primero para compartir la invitación. Se debe crear la sala y completar el formulario con 5 campos muy simples para obtener una sala de reuniones gratis. La plataforma es tan buena que incluso puede organizar seminarios para cursos universitarios. Es fácil de usar y el chat en vivo le permite integrar discusiones en línea o trabajo en equipo sin compartirlo con todos los participantes de la videoconferencia. También tiene una versión de pago que incluye más almacenamiento y servicios.[32]

Otras herramientas utilizadas en la educación virtual

EDpuzzle

EDpuzzle es una sugerencia para crear contenido educativo basado en videos. Ya sea que lo grabe o elija una de las plataformas educativas más utilizadas, como Khan Academy y YouTube, esta herramienta permite a los estudiantes y docentes crear contenido multimedia mucho más atractivo. Incluye la posibilidad de realizar comentarios (verbales o escritos) sobre lo explicado en el vídeo y realizar la pregunta perfecta para atraer a los alumnos.

GoConqr

GoConqr tiene una plataforma muy completa que puede aprovechar todo tipo de recursos. Idealmente, los estudiantes deberían poder matricularse y aprovechar los

[31] HUBSPOT. Los mejores 30 programas para videoconferencias en 2022. [En línea] 2021. Disponible en: https://blog.hubspot.es/sales/programas-videoconferencias

[32] BIBDIGITAL. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informatica. [En línea] 2007. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD1053.pdf

materiales disponibles públicamente pertenecientes a todo tipo de materias. Contiene material y formatos, como documentos, líneas de tiempo, mapas y gráficos.

TriviNet

Permite a los estudiantes pueden crear sus propios cuestionarios de trivia o jugar cuestionarios de trivia creados por otros. En cualquier caso, el profesor puede calificar y evaluar al alumno a través de las preguntas y respuestas de cada lección. Todos estos se pueden personalizar por tema, tema y nivel, y pueden crear un gran contenido con relativamente poco esfuerzo.

Prezi

Es una plataforma que sirve para crear contenido dinámico, acompañado de muchas transiciones para crear presentaciones muy atractivas, cómodas e intuitivas.

Code.org

Es una plataforma muy completa que fue creada para los niños de 3 a 4 años pueden aprender los conceptos básicos de la codificación. Code.org es una plataforma completamente gratuita, sus materiales son guiados y muy fáciles de seguir y completar, por lo que puedes aprender desde cero (casi) infinitamente. Los esquemas poplet y los mapas conceptuales del aula son muy útiles para ayudar a todo el estudiantado a comprender conceptos complejos.

Vyond

Ofrece una variedad de herramientas para crear videos animados con temas seleccionados por el usuario. Sus numerosas funciones le permiten elegir la duración, los diálogos, las escenas y los personajes que desea incluir en su montaje. También puede editar el fondo y cambiar las transiciones. Finalmente, los videos se pueden descargar o compartir a través de plataformas como YouTube y la nube. El grupo Together recopila algunos recursos ideales para profesores y recursos para ayudar a organizar el trabajo dentro y fuera del aula. [33]

ApliAula

Esta herramienta permite gestionar funciones de mensajería interna y documentos que a su vez permite ser compartidos a estudiantes.

Aula 1.

[33] Educación 3.0. 30 herramientas para la comunicación entre familias, alumnos y centro. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-comunicacion-familias-centros/

Su módulo de comunicación contiene información de todos los eventos, evaluaciones o anuncios asociados con la institución educativa, la familia o los maestros de la escuela. Permite enviar estos eventos a las personas implicadas de manera automática a la app.

Alexia

Esta plataforma multimedia promueve la relación con toda la comunidad educativa, y tanto los empleados como los estudiantes como la comunicación familiar. Como características interesantes es la existencia de los canales (web, aplicación, correo electrónico, SMS). Además, contiene temas de peticiones de entrevistas, cuestionarios y cifras educativas, etc.

Childcare On

Esta aplicación está orientada para ser administrada por los dueños de los centros o guarderías, jardines de infancia para dispositivos móviles que facilita la comunicación entre el personal, las familias y los educadores de estos centros (diseñada para el correcto manejo de los niños y la gestión eficaz del centro). Los padres siempre saben cómo les va a sus hijos.

Clickedu

Esta plataforma de gestión escolar en la nube contacta con colegios y familias a través de mensajes SMS, email, notificaciones, mensajes internos...información variada sobre notas, exámenes, calendarios online, notificaciones de tutores... Puedes conseguirla, consulta las citas disponibles para concertar una entrevista y descargar el certificado.

Dinantia

Esto permite que las escuelas y los maestros envíen mensajes a los teléfonos móviles de los padres y los estudiantes. El mensaje puede incluir preguntas para organizar la reunión, aprobar el viaje y realizar una breve prueba de estudiante. Las respuestas se reciben en tiempo real, reduciendo las tareas administrativas. También asume esa función desde cualquier dispositivo y notifica automáticamente a los padres de su ausencia.

DocCF 3.0

Los miembros de la familia pueden usar este software de gestión académica y administrativa para revisar la agenda escolar y las calificaciones de sus hijos en línea y recibir alertas por correo electrónico sobre ausentismo o medidas disciplinarias.

Mientras tanto, los niños también pueden ver sus calificaciones, calendarios escolares y bibliotecas.

Educamos

Los objetivos de esta plataforma de gestión desarrollados por SM son insertar la tecnología en el servicio de todos los procesos que se llevan a cabo en una escuela, y la comunicación con las familias no es una excepción. Fue considerado en la integración de todas las herramientas necesarias, como chats, espacios de trabajo, correos electrónicos externos, mensajes instantáneos, etc.

Educcare

La gestión académica, el campo financiero, el análisis y los resultados presupuestarios son las tres áreas disponibles para esta plataforma de gestión. En particular, el módulo de gestión académico consta de tres portales web, que son independientes, están perfectamente integrados en una sola base de datos: maestros, padres y secretaría. En particular, los portales solo para familias facilitan la comunicación con el centro y brindan acceso a la información más relevante e importante sobre su hijo.

Escolapp

Con esta aplicación, los padres pueden recibir notificaciones, tareas, notas y otra información en sus teléfonos inteligentes. En su caso, los profesores acceden a través de un navegador y envían notificaciones a todos los padres, a una sola clase o a un alumno en concreto. Las familias pueden consultar actividades en centros, cafeterías y rutas, comprar libros y uniformes, organizar actividades extraescolares y permitir excursiones.

Gestión aula

La aplicación web ofrece a los administradores una herramienta que permite crear un portal educativo, que a su vez permite tener una completa comunicación entre familias y alumnados. A través de esta aplicación se puede solicitar asesorías, acceso a información académico, descarga de tareas y programaciones.

Globaleduca

Contiene seis módulos educativos, el cual se destaca el módulo de la comunicación entre las familias, a través de un portal web. Tiene como valor adicional que contiene una app gratuita que sirve para teléfonos móviles tanto iOS como Android.

Goombook

Es una aplicación que interactúa a través de grupos, van segmentados, en padres de familia, estudiantes, docentes y administrativos. Actúa como una red social privada en la cual podrá comunicarse con los docentes a través de dispositivos como Skype, ya sea a través de chats o videollamadas.

Gqdalya

Es una plataforma que sirve para la gestión integral de centros educativos el cual componen distintos módulos y aplicaciones, se destacan en la mismas, servicios como: evaluaciones, informes, actividades. Permite la gestión de roles y permisos de padres, docentes y alumnos.

iEduca

Actúa como una plataforma de gestión que tiene como ventaja que es multi idioma, permite crear la comunidad educativa en general y se considera que es de gestión académico-administrativa. Contiene una app tanto para iOS y Android la cual facilita el acceso a la información y a revisión de diferentes temas como horarios y control de faltas.

iesFacil

Permite tener un canal de comunicación y de información directo con la institución, permite observar las observaciones que realizan los tutores en las evaluaciones, trabajos o notas de recuperación.

Lanshool

Es un sistema que trabaja bajo los servicios cloud y tiene como servicio principal la proporción de auditorías a distancia a través de la web, es compatible con estructuras P2P y sistemas operativos como Android y iOS.

Oduca

Los usuarios pueden acceder desde cualquier dispositivo y contiene en su suite las áreas principales de un centro educativo (Contable, administrativo, académico y portal de comunicación con padres de familia).

Phidias

Es una plataforma online que tiene como principal herramienta el sistema de mensajería para estudiantes y familias permite citar a reuniones a padres de familia, enviar reuniones y citaciones; además de ello enviar mensajes con archivos adjuntos.

RM Gestión académica

Se puede acceder desde cualquier dispositivo móvil, es una plataforma multiusuario que permite acceder a la misma desde cualquier lugar y en cualquier momento. Puede acceder a todos los servicios que presta la comunidad educativa tales como transporte y servicio de cafetería.

Saeko

Esta plataforma tiene como principal función, dar a conocer a los estudiantes y padres de familia, las actividades y calificaciones en tiempo real. También permite conocer los horarios de los estudiantes en las aulas de clase.

Sappschool

Es una aplicación móvil que envía notificaciones a través de un sistema de mensajería instantánea. Lo más innovador de esta aplicación es que todo lo relacionado con la web, los blogs, el calendario y la mensajería, lo integra en un solo sitio, buscando que toda la información enviada, no se duplique en otros sitios.

Shisinus.

Además, esta plataforma disponible en forma de teléfonos Android, tabletas y aplicaciones de iOS es óptima, permite compartir información con los padres de familia (por ejemplo, tareas, estadísticas, históricas, informes de comidas ...) En este sentido, esta información se registra en una agenda digital personalizable y ayuda a ser motivado. Incluye servicios de mensajería instantánea que brindan herramientas para enviar (y compartir) actividades, ejercicios de profundización y repetición de temas específicos que realizan los estudiantes.

TokApp school

Esta aplicación de mensajería móvil y de escritorio basada en la nube facilita que las escuelas se comuniquen con los estudiantes y los padres de una manera eficiente, segura y rentable a través de la mensajería instantánea. La escuela tiene una aplicación web que puede enviar todos los mensajes y los padres tienen una aplicación para recibir el mensaje. Y todo ello tiene efectos jurídicos en esa comunicación.

Weclass

Desarrollado por Telefónica Learning Services, este entorno virtual de aprendizaje incluye herramientas de autor para crear contenido y enriquecer el contenido

proporcionado por el editor. Hay un apartado solo para familias que cubre aspectos como las tutorías, la supervisión de los alumnos y las relaciones con el centro. [34]

WordPress

Una de las herramientas de blogs más populares. Esto permite a los estudiantes digitalizar su trabajo y a los profesores agregar TIC a sus clases.

Stormboard

Plataforma de colaboración para ayudar a organizar sesiones de lluvia de ideas. Al igual que otras herramientas, le permite compartir su pizarra para que todo su equipo pueda contribuir. Cada idea que agregue incluye un hilo de conversación de la persona que creó la idea.

Wetransfer

Una de las mejores formas de enviar documentos de gran tamaño (hasta 2 GB) a cualquier usuario a través de un enlace. Estos archivos no se archivan, solo se conservan durante unos días y luego se eliminan.

Mindmeister

Una aplicación de mapas mentales en línea que le permite capturar, desarrollar y compartir ideas visualmente. La herramienta está completamente basada en la web y no requiere descarga.

Storify

Un sitio web que crea una historia compatible con WordPress. Esto permitirá a los maestros digitalizar la entrega de tareas e inspirar a los estudiantes a presentar su trabajo en línea.[35]

Riot

Es compatible con dispositivos móviles iOS y Android, así como con Windows, macOS, Linux y versiones web. Permite realizar videoconferencias, llamadas de voz, intercambio de archivos y chatear desde cualquier dispositivo (computadora, tableta y teléfono móvil). Las comunicaciones de la plataforma son chats cifrados de extremo a extremo descentralizados para la privacidad.

---

[34] Educacion 3-0. Formas gratuitas para aprender a través de videoconferencias. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/plataformas-de-videoconferencia/

[35] Educación 3.0. Herramientas educativas para organizar, crear y gestionar la labor docente. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-educativas-docentes-ahorrar-tiempo/

Tango

Acepta videollamadas con hasta 300 personas y ofrece la posibilidad de enviar y recibir mensajes y archivos. Disponible para dispositivos móviles (de hecho, su uso está limitado a dispositivos con sistema operativo Android), tiene muchas opciones de privacidad y seguridad en lo que respecta al chat de la aplicación.

Videolink2.me

Gracias a su diseño fácil de entender, permite la planificación de lecciones enviando a todos los participantes un enlace que indica la fecha y la hora de la videoconferencia. Puede importar contactos a la página para facilitar la gestión de invitaciones. Incluye opciones de chat y pantalla compartida. [36]

Educaplay

EducaPlay es una plataforma de educación virtual que te permite crear actividades educativas utilizando contenido multimedia. Se enfoca en crear una comunidad con sus estudiantes, permitiéndoles motivarse mientras aprenden y se divierten. La plataforma permite la creación de diversos recursos de apoyo al aprendizaje virtual, como los que se muestran en la figura. La característica principal de esta herramienta es que permite a los docentes agregar contenido audiovisual (notas de voz, imágenes y texto) desde sus computadoras, lo que ayuda a promover una relación más estrecha entre docentes y alumnos, así como una sana participación en la lección. Se puede integrar con distintos LMS (Moodle).

Quizziz

Su principal atributo es crear preguntas interesantes individualmente para los estudiantes. Los maestros crean preguntas y proporcionan códigos para que los estudiantes participen. También puede usar preguntas de otros maestros a través de su biblioteca de pruebas.

AhaSlides

Es una herramienta en línea que le permite crear presentaciones interactivas y dinámicas para presentaciones en cursos virtuales. Una de las principales ventajas de esta herramienta es que le permite captar la atención de los estudiantes, por ejemplo, haciendo una pregunta en medio de la explicación de un tema en una diapositiva. La dinámica tiene lugar en cuatro sencillos pasos:

[36] HUBSPOT. Los mejores 30 programas para videoconferencias en 2022. [En línea] 2021. Disponible en: https://blog.hubspot.es/sales/programas-videoconferencias

- Cree una presentación: utilice un tema de su elección.
- Integra tus preguntas: Agrega preguntas relacionadas con el tema. Pueden contener texto e imágenes.
- Comentarios de la audiencia: los estudiantes escanean un código QR para abrir la aplicación y responder la pregunta. Además, pueden enviar respuestas en tiempo real a las presentaciones e incluso hacer preguntas en tiempo real.
- Obtenga actualizaciones en pantalla en tiempo real: a medida que los estudiantes envían sus respuestas, se muestran gráficamente en las diapositivas. Allí, puede aprovechar la oportunidad para dar a los estudiantes comentarios sobre sus respuestas. [37]

Mentemiter

Esta herramienta permite a los profesores crear presentaciones al estilo de Microsoft PowerPoint, pero con un giro interesante para agregar las preguntas deseadas a las diapositivas. Además, Mentemiter le permite ver los comentarios de los estudiantes, publicar nuevas preguntas, compartir respuestas, realizar concursos y crear nubes de palabras.

Peardeck

Esta herramienta permite a los docentes visualizar las respuestas de los alumnos en tiempo real, leer sus inquietudes o preguntas y conocer sus opiniones, facilitando así la retroalimentación en el aula o aula virtual. La herramienta incluye una biblioteca de plantillas proporcionada por Google para que el proceso de aprendizaje sea más interactivo y agradable para los estudiantes. Los profesores pueden agregar estas plantillas al principio, a la mitad o al final de una presentación como mejor les parezca.

Brainscape

Usando Brainscape, los estudiantes pueden revisar y recordar información que es importante para su aprendizaje a través de la repetición espaciada, lo que implica repetir conceptos nuevos o difíciles con tarjetas didácticas durante un período de tiempo determinado. Muchos estudios de ciencia cognitiva han demostrado que establecer intervalos de repetición es una de las formas más efectivas de retener el

[37]Wikipedia. Educación a distancia. [En línea] 2021. Disponible en: https://es.wikipedia.org/wiki/Educaci%C3%B3n_a_distancia

conocimiento, por lo que Brainscape permitirá a los estudiantes recordar conceptos tan importantes con mayor frecuencia en clase.[38]

Streaming por Redes sociales
Facebook y YouTube en vivo.
Son muy poderosas porque son herramientas de transmisión de video y ambas pueden interactuar con estudiantes o espectadores a través de mensajes de texto en forma de chat. En cualquier caso, puede usar su perfil de Facebook o canal de YouTube para chatear usando la opción de video en vivo. De esta forma podrás utilizar herramientas sencillas, no se necesita instalar nada y se pueden observar las grabaciones si el estudiante lo requiere.

Facebook Messenger
Sala de Facebook o Sala de Messenger. Te permite unirte a videollamadas grupales con hasta 49 personas, lo que Facebook llama "salas". Podrá abrir la sala desde Messenger, Facebook, Instagram Direct, WhatsApp o el Portal y podrá abrir la conexión para todos o bloquearla para evitar que se unan personas no invitadas. También puede eliminar participantes. En la sala, puede usar el filtro de realidad aumentada de Facebook y cambiar el fondo a virtual. Facebook tiene una vista de fondo extraña de 360 grados y está trabajando en filtros embellecedores y filtros diseñados para iluminar las habitaciones oscuras.

Instagram
Permite una videollamada de 4 personas desde la aplicación móvil.

Snapchat
Permite hasta 15 videollamadas simultáneas a través de la app.

Gruveo
Es una plataforma que presenta una versión free de 45 días o también pueden probar las herramientas de videoconferencia y reuniones en línea en la versión gratuita de WebEx. [39]

[38]Evirtualplus. WhatsApp como herramienta educativa. [En línea] 2017. Disponible en: https://www.evirtualplus.com/whatsapp-como-herramienta-educativa/

Proyecto Gutenberg

Desarrollada por Michael Hart en 1971, la biblioteca ofrece libros electrónicos gratuitos de libros que ya existen. Disponible en varios formatos como Kindle, EPUB e incluso en línea en formato ASCII, UTF-8 o HTML, todo el texto proporcionado es de dominio público cuando estos derechos han expirado o con el consentimiento del autor. Actualmente, cuenta con una colección de más de 60.000 libros.

Wikifuente

Proviene de la Fundación Wikipedia, destinado a contener texto original libre que ha sido publicado bajo una licencia GFDL, una licencia Creative Commons o en dominio público en el mismo sitio web, junto con traducciones a diferentes idiomas. Contiene más de 100.000 documentos de dominio público, todos en HTML.

Biblioteca de Harvard

La principal universidad de Estados Unidos digitalizará todos los documentos en manos de sus investigadores y los pondrá a disposición de todos. Como resultado, brinda acceso gratuito a miles de fotografías históricas, folletos, manuscritos, libros, partituras, mapas y otros materiales exclusivos de la Universidad.

Biblioteca de internet

Un proyecto de la Fundación Bancaja con acceso gratuito a 99.000 textos literarios, científicos y técnicos. Fue creado con tres objetivos en mente: facilitar la localización de contenido literario, técnico o científico que existe en Internet, ayudar a aumentar la cantidad de dicho contenido y alentar a los usuarios (estudiantes, profesores e internautas) en general a participar - a través de Internet.

Educatribu

Educatribu es una web que esta categorizados por nivel académico (Educación Infantil, Primaria, ESO, Grado y Formación Profesional), e incluye un espacio dedicado a la educación de adultos. Actualmente es muy poco el contenido disponible, aunque es intención de sus creadores alimentar el espacio con aportes y aportes de otros usuarios del sitio.

Maestroteca

---

[39] BIBDIGITAL. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática. [En línea] 2007. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD1053.pdf

Contiene una gran variedad de libros clásicos, también cuenta con un directorio de aplicaciones con enlaces a enciclopedias virtuales, diccionarios en línea, enlaces para trabajar habilidades básicas.

Wikilibros

Wikilibros incluye sitios de lectura relacionados con idiomas, física, química, matemáticas, ciencias sociales, informática. Este portal recopila textos educativos, libros de texto y libros de interés para la comunidad docente, siguiendo la filosofía de Wikipedia: estos textos pueden ser editados por usuarios, y su conocimiento ha contribuido a la creación de otras bibliografías.

Biblioteca de literatura infantil

Contiene un amplio catálogo de autores latinos y latinos dedicados a este tipo de literatura e incluye la "Biblioteca de Autor" con enlaces a webs de Jordi Sierra y Páginas de escritores como Fabra o Gloria Fuertes, permitiéndote visualizar su trabajo, leer algunos extractos.

Europeana

Esta biblioteca digital funciona desde 2008 y cuenta con el apoyo de los países de la Unión Europea. Ofrece cientos de materiales de diferentes países, como mapas, imágenes, libros y películas. [40](17)

Biblioteca Digital de México

La Dirección de Archivos Nacionales (AGN), la Biblioteca Nacional de Antropología e Historia (INAH), el Centro de Estudios Históricos Mexicanos CEHM-CARSO y el Consejo Nacional para la Cultura y las Artes (CONACULTA) han colaborado para crear un órgano multifuncional. biblioteca en México. Cada institución ofrece material histórico y cultural relevante de sus colecciones, y te invita a unirte a las numerosas bibliotecas y archivos mexicanos y extranjeros que atesoran importantes documentos de México.

Biblioteca Digital ILCE

La Biblioteca Digital del ILCE es un portal que contribuye a la cultura brindando consultas gratuitas sobre colecciones, a su vez apoyo bibliográfico para el programa Red Escolar y el portal de educación SEPiens, ambos cuentan con ILCE. En 2001,

[40] Educacion 3.0. 15 bibliotecas on line para docentes. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/bibliotecas-on-line-docentes/

obtuvo Yahoo! Mejor en Ciencias Sociales en "Una Breve Historia de los Estados de la República Mexicana". http://bibliotecadigital.ilce.edu.mx/

Biblioteca Virtual Luis Arango

Esta biblioteca brinda documentos, contenidos e información principalmente sobre autores colombianos o colombianos. También encontrarás sitios web interactivos, exhibiciones en línea, proyectos temáticos y materiales educativos como Hemeroteca Histórica Digital, Mapas Históricos, Fonoteca Digital y más.
http://www.banrepculture.org/blaavirtual/indice. [41]

[41] IADB. Los Sistemas de Información y Gestión Educativa (SIGED) de América Latina y el Caribe: la ruta hacia la transformación digital de la gestión educativa. [En línea] 2021. Disponible en: https://publications.iadb.org/publications/spanish/document/Los-Sistemas-de-Informacion-y-Gestion-Educativa-SIGED-de-America-Latina-y-el-Caribe-la-ruta-hacia-la-transformacion-digital-de-la-gestion-educativa.pdf

4.4 MARCO LEGAL

En Colombia hoy en día el tema de legislación informática es un tema que no se ha consolidado de la mejor manera y solo se aplica en algunas ocasiones y son personas que no pertenecen a la rama del poder las que se eximen de estas penalidades. Además de ello no existe una consolidación de las diferentes partes de la sociedad, para que sean manejadas de la mejor manera (Comercial, administrativo, industrial, etc.). Para que esto se pueda llevar a cabo deben de realizarse procesos que lleven a los implicados a castigos reales, tanto para quien lo hizo como para quien lo induce a hacer, de este modo se debe empezar a buscar diferentes normatividades que ayuden a la legislación colombiana a hacer efectivos todos estos fraudes informáticos.
Para que esto se pueda llevar a cabo en Colombia se tienen varias problemáticas, una de ellas es el hacinamiento de presos que se tienen en las cárceles y además a ello la permisión que tiene la ley, lo que hace que se muestre más débil.

Hoy en día los delitos informáticos ocurren de manera frecuente y diaria en todos los sectores, en la educación es un tema muy tedioso y vertiginoso ya que se puede ver afectadas las instituciones educativas, desde el ámbito monetario hasta el ámbito social. Lo delicado de todo ello es que la información manejada y suministrada a las instituciones educativas es de carácter confidencial y peligroso, ya que se maneja información de menores de edad y esto tiene una doble responsabilidad, es por esto por lo que dentro de este marco legal especificaremos los ataques más frecuentes que se realizan en el interior de las organizaciones:

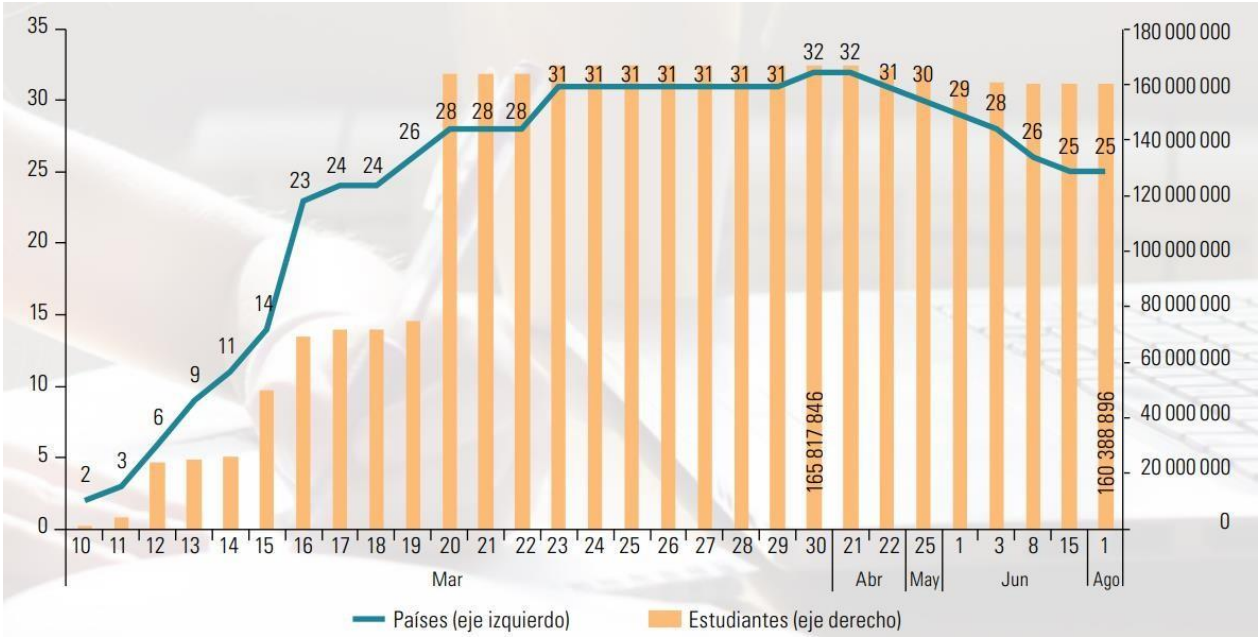
- **Sabotaje informático:** Este tipo delito tiene como misión destruir o modificar información a través de correos electrónicos, dentro de los organismos de control estatales se reportaron varios casos en el año, pero se apunta a que son muchos ataques más ya que en su mayoría no se reportan ante estas entidades.
- **Suplantación de identidad:** También se denomina delito de usurpación de estado civil o de identidad, básicamente se trata de apropiarse de una identidad de otra persona y se hace pasar por ella para poder obtener información confidencial de la persona. En Colombia se toma como delito esta suplantación cuando se toma la identidad de una persona real, si se hace ante un personaje ficticio no se tomaría como delito y todo quedaría en la impunidad.
- **Pornografía infantil:** Este es un delito que se ha vuelto común en este siglo, se trata de cometer actos sexuales con menores, filmando y creando videos en donde se están cometiendo actos considerados sexuales. Este es un acto que se comete en todo el mundo, se propaga a través de internet y se fomenta la venta de menores y el turismo sexual.

- **Interceptación ilícita de datos informáticos:** Trata el acto de interceptar o de obstruir datos sin autorización o de forma no legal, ya sea en su lugar de origen, de destino o dentro de un sistema informático, en Colombia este tipo de delito podría alcanzar una pena de los 36 a 72 meses.
- **Piratería:** Se puede considerar a la creación y/o distribución de las copias de productos registrados y protegidos por los derechos de autor.
- **Violación de datos personales:** Se da cuando el atacante roba, compra, vende, distribuye, divulga o utiliza datos personales que no son suyos y estén almacenados.
- **Daños informáticos:** Se puede considera delito si un individuo ajeno y sin autorización, ingresa a datos restringidos y privados, y altera, daña, modifica o elimina los datos informáticos.
- **Xenofobia:** Se trata de una manera de realizar acciones despectivas y de rechazo hacia un individuo o un conjunto de personas que compartan actividades en común, suele hacerse a través de redes sociales o páginas web de internet.
- **Phishing:** Este es considerado uno de los ciberdelitos más comunes en el mundo del internet, se trata que el atacante pueda conocer datos personales y confidenciales de los usuarios, principalmente datos donde existan cuentas bancarias o datos corporativos los cuales puedan afectar los datos de la misma, se hace con el fin de robar dinero o conseguir información sensible de la persona y este tipo de ataques se da a través de correos electrónicos, por esta razón la importancia de revisar los correos electrónicos, los remitentes de donde provienen y las bandejas de correos no deseados.
- **Spam:** Este también se envía con un enlace web que en ocasiones suelen ser propuestas de negocio, de amistad o algo parecido, para así instalar un software malicioso en el ordenador con el fin de obtener datos personales, bancarios, etc. Una de las modalidades también es el bombardeo de correo electrónicos y consiste en generar o causar la caída de un correo electrónico o de su servidor.
- **Acceso abusivo a un sistema informático:** Como su nombre lo indica se trata de un ingreso no autorizado que aprovecha las vulnerabilidades latentes en un sistema, para así obtener acceso a los sistemas de información o conseguir identificar debilidades en los procedimientos de seguridad; penalmente en Colombia esto podría tener una pena de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos vigentes legales.

5 ANÁLISIS DEL PANORAMA DE SEGURIDAD EN LOS PROCESOS DE ENSEÑANZA VIRTUAL, APOYADOS POR LAS TIC EN COLOMBIA DURANTE LOS AÑOS DE PANDEMIA

La enseñanza virtual o educación online, no es nueva y se había venido implementando en todo el mundo en los últimos 5 años aproximadamente con gran fuerza, pero no fue hasta la emergencia ocurrida a finales de 2019 y principios de 2020 que se decidió suplir la necesidad educativa del mundo con estas tecnologías y con estos métodos.
Desde antes del 2020 cuando tuvo su inicio brusco la pandemia mundial, ya muchos optaban por la educación a distancia, y la preocupación por la seguridad causaba malestar a la comunidad, pero al empezar las restricciones y en concreto las cuarentenas, en el mundo se tuvo que suplir la necesidad educativa con educación online, y todas las preocupaciones incrementaron de forma exponencial igual que los usuarios que la usaban.
En el gráfico siguiente se observa una estadística presentada por la UNESCO, en la cual se muestra el crecimiento exponencial de los estudiantes en los países de América latina y el caribe en un periodo de tiempo del 2020.

Gráfico 1. América Latina y el Caribe (33 países).2020



Fuente: CEPAL sobre la base de la UNESCO, (en línea). http://es.unesco.org/covid19/educationresponse

No es lo mismo tratar de proteger a mil estudiantes que a diez mil o un millón, y ese fue el fenómeno que se dió con la pandemia, en los años 2020 y 2021, se multiplicaron el número de usuarios de internet y con ellos los nuevos usuarios que buscaban tomar su

educación, pues no había ningún otro modo de tener sus clases sin arriesgarse a el creciente virus que ponía en emergencia sanitaria al mundo.
Teniendo en claro el escenario se puede deducir los problemas por el incremento de usuarios, el soportar tal cantidad de usuarios, las dinámicas estructurales de la educación que debía ser modificada y ajustada, pero también que los problemas que habían antes seguían estando, los peligros y vulnerabilidades de antes aún estaban presentes, solo que a una escala mayor, y que igual que antes los atacantes mejoran cada vez más los métodos de ataques, solo que esta vez tendrían más víctimas a los cuales atacar.
Este último puede ser el nuevo peor problema que surgió de este fenómeno, los nuevos usuarios y posibles víctimas de él cibercrimen, pero se debe enfocar en los problemas que conciernen concretamente en el área educativa y los problemas básicos para llegar a los que fueron surgiendo conforme se implementaba el nuevo sistema.

5.1 El sistema educativo actual y su articulación con la virtualización

Para comprender el nuevo que se implementó para continuar con el proceso y no detener de manera parcial, se optó por la educación virtualizada, como ya se había mencionado, y consiste en apoyar nuevas tecnologías de la información y de la comunicación (TIC), para realizar dichas labores de enseñanza, lo que significa que se anula la parte presencial y se remplaza con dispositivos interconectados vía internet para interactuar a través de ellos y poder recibir su educación por medio de este método.

El método es simple un anfitrión y muchos invitados, traducido a un docente y muchos alumnos, este método estructura no es nuevo y se venía dando desde el inicio de la educación virtual, solo que, en los años 2020 y 2021, se masificó, y se adoptó como el nuevo método de enseñanza dadas las circunstancias.

La seguridad en las instituciones educativas regulares antes de la pandemia se basaba en la presencialidad, se implementaban políticas, normativas y metodologías que consideraban la estructura interna y sus alrededores, pero no había estructuras o equipos externos, su funcionamiento era interno, por lo cual no estaban preparados para una educación a distancia básicamente.

Tanto los equipos como las plataformas a utilizar no son de su propiedad, entonces el control se hace muy vago y casi nulo, eso si no tienen un plan de contingencia, el cual deberían tener para satisfacer la nueva necesidad dada y seguir brindando seguridad a sus empleados y clientes, en este caso, a los docentes y alumnado.

Para las instituciones que tenían este sistema implementado, ofrecían desde antes formación a distancia o educación virtual, fue un poco más fácil el adaptarse ya que solo sería contemplar lo masivo de las nuevas integraciones y buscar robustecer el sistema actual además de implementar unas nuevas políticas que consideren la situación, pero aun así es muy difícil satisfacer los parámetros adecuados de seguridad que se espera de una institución educativa en una situación como esa.
Aun así, es una obligación de cada institución velar por sus activos, su personal y sus clientes, por lo que la búsqueda de un sistema seguro era parte de sus prioridades, aunque cabe aclarar que existen organizaciones que velan por el buen funcionamiento del sistema educativo, como lo es el SIGED o sistema de información y gestión educativa que intervienen en las operaciones de los sistemas educativos públicos, tanto para primario como para secundaria, y en esta época de pandemia también estuvo muy al pendiente de la nueva situación a la que se enfrentaba el sistema y de cómo enfrentar la situación.

5.2 Ataques al sector educativo

Lamentablemente para sorpresa durante la pandemia no fueron ni las instituciones financieras ni las de salud ni las de infraestructuras públicas, las principales víctimas de las malintencionadas acciones de los ciberdelincuentes, si no que fue el sector educativo, al digitalizar y virtualizar todo los procesos y el método de educación, sirvieron como objetivo al incrementar drásticamente la utilización de las redes.

En 2020, “Incluidos los costos de tiempo de inactividad, reparaciones y oportunidades perdidas, el ataque promedio de ransomware a 1.681 escuelas, colegio y universidades, costó a las instituciones educativas $ 2.73 millones, en USA, y a nivel mundial el 44% de las instituciones educativas fueron blanco de ataques”[42]. Según Byron Guerra miembro de la UDLA según su informe de instituciones en riesgo.

El objetivo puede llegar a ser como siempre monetario pero también puede ser de información, es de notar que las instituciones educativas maneja mucha información y esta no está generalmente puesta al público, además los proyectos que desarrollan e incluyan de utilidad no solo para la institución educativa sino para el desarrollo y el gobierno también pueden ser de gran valor e importancia, pero no queda hay otra no solo obtienen información con estos fines sino que también se aprovechan de la gran cantidad de información personal que poseen para realizar campañas como lo son las

[42] UDLA. Instituciones educativas en riesgo informático. [En línea] 2021. Disponible en: https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/?msclkid=5d356becc7e411ec8932597cb1a42872

conocidas campañas de phishing en donde por medio de correos spam, pueden a llegar a captar víctimas y engañarlas de algún modo para los beneficios del criminal y acosta de la integridad del usuario.

La educación fue muy golpeada por los ataques informáticos y el ataque protagonista fue el ransomware, según Sophos en su publicación "REvil a Kaseya que afectó a escuelas en todo el mundo, como por ejemplo en Nueva Zelanda, o los recientes ataques sufridos por varias universidades en España, Sophos, líder mundial en ciberseguridad de última generación, publica los resultados del estudio Sophos State of Ransomware in Education 2021".[43]
El estudio se hizo a nivel mundial en cuanto a seguridad de la información entre más de 500 instituciones se confirmaron las vulnerabilidades cibernéticas y las amenazas a las que se ve expuesto el sector.

5.3 Entre los principales resultados del estudio "Sophos State of Ransomware in Education 2021"

Nivel de ataques

Durante el 2020 se registró el mayor nivel de ataques con un 44%, porcentaje que supera unos 7 puntos en el porcentaje mayor en los demás sectores.

Coste del ataque

El impacto financiero reportado fue catastrófico según los resultados del informe, en el 2020 la media de coste fue 2,34 millones de euros, contando el tiempo del personal, de inactividad, el coste de la red, de los dispositivos, las oportunidades u opciones perdidas, el pago de los rescates, superando así la cantidad de perdida comparándola también con los demás sectores, además de un 48% superando la media global.

Cifrado de datos

Para el cifrado la tasa de éxito es buena, consiguiendo un 58% siendo superior a la mitad y a la media mundial que es del 54%.

Detención del ataque

En el caso de la detección realmente es más bajo de la media siendo esta del 39%, pero no es la peor solo dos puntos menos siendo del 37%, se supone que es debido a la escasez de recursos, limitaciones en presupuestos y tecnologías disponibles.

[43]SOPHOS. Sophos State of Ransomware in Education 2021. [En línea] 2021. Disponible en: https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/?msclkid=d137c220c7ef11ec84a62436ee0fc7c7

Ataques extorsivos

Según estudios de Sophos, los ataques extorsivos han tenido un gran aumento, en donde no cifran los datos, sino que se roban los datos para luego amenazar con publicarlos si es que no se les paga un rescate por ellos, puesto que supone menos esfuerzo para los criminales, esta modalidad alcanzo el 5% de las instituciones que fueron atacadas.

Pago de rescate

Lamentablemente el sector educativo es uno de los más propensos a recibir ataques en donde pidan rescate, el porcentaje alcanza un 35% de los afectados cedieron a las exigencias, superado por otros sectores como el de la energía y servicios públicos con un 43% y la administración con un 42%, la presión a la continuidad es una de las principales razones por las cuales se cede a este tipo de situaciones, y con la enseñanza online ha aumentado.

Coste del rescate

El promedio, aunque está por debajo de la media mundial situado en 145.856 euros, es muy alto para el sector siendo en promedio de 96.238 euros.

Recuperación de datos

Para revisar los datos se tiene que tener en cuenta las cifras las cuales dejan con un 98% de instituciones que recuperaros sus datos, lo cual sería reconfortante de no ser por los siguientes datos o cifras que son que el 35% de estos recuperando mediante pago alcanzan a rescatar una media de 68% de los datos, y solo el 11% que pagaron recuperaron en totalidad sus datos, también podemos rescatar que un 55% recuperaron sus datos por medio de copias de seguridad y un 8%mediante otros métodos.

El sector

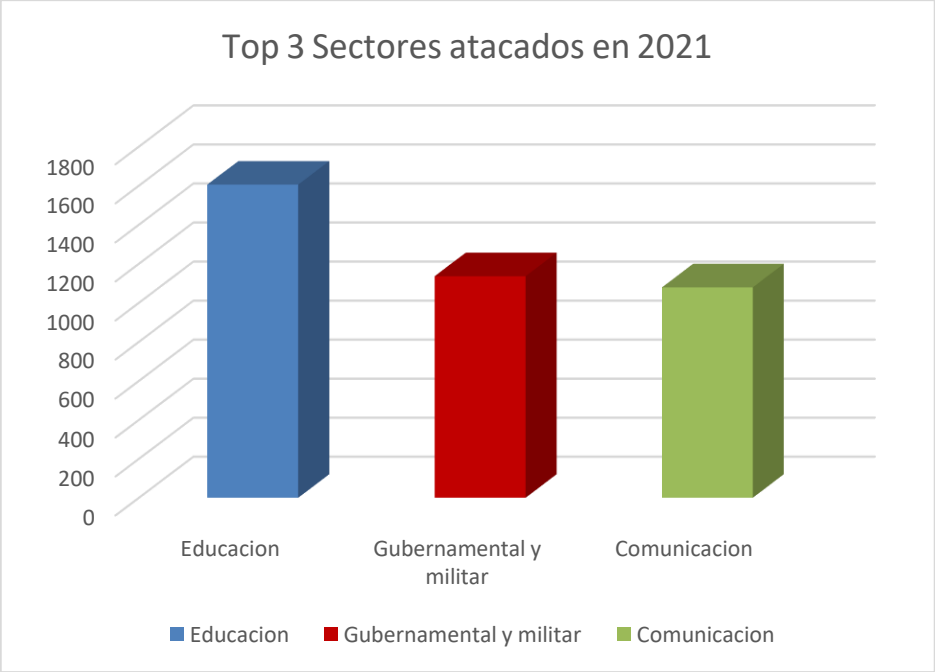
Para el sector según las instituciones encuestadas y que no han sido atacadas, un 61% de estos cree que serán atacados en el futuro, y ya que las principales razones son la notificación y la frecuencia, con el 46% y el 42% respectivamente, son casi imposible de detener.

Según las declaraciones de Ricardo Mate, director de Sophos, debido a los presupuestos ajustados y lo anticuada de las estructuras de TI en las instituciones educativas, limitan y la pobre cultura segura que se tiene hacen que se tenga una mayor exposición hacia estos delitos.

> “Todo esto supone un aumento en la exposición al riesgo en cualquier año, pero la pandemia sufrida en 2020 provocó que los centros educativos tuvieran que cambiar, con poca antelación, a entornos de aprendizaje virtuales, con muy poco tiempo para pensar en la seguridad o para proporcionar formación básica en ciberseguridad a todos los nuevos usuarios remotos. Esto aumentó significativamente la vulnerabilidad del sector y los ciber atacantes no tardaron en aprovechar la oportunidad, dejando a sus víctimas con el enorme golpe financiero de tener que reconstruir la infraestructura de TI desde cero”.[44]

A continuación, se mostrará el gráfico No 2 que indica el top 3 de sectores más atacados en el año 2021, en Colombia, Según un informe publicado por el CCIT “Tendencias cibercrimen Colombia 2019-2020”, todo esto para enseñar el panorama de los sectores más afectados, y teniendo en cuenta que el sector en el cual se centra, el educativo, es el más atacado, se debe tomar en cuenta las posibles amenazas y el riesgo al que se enfrenta.

Gráfico 2. TOP 3 Sectores atacados

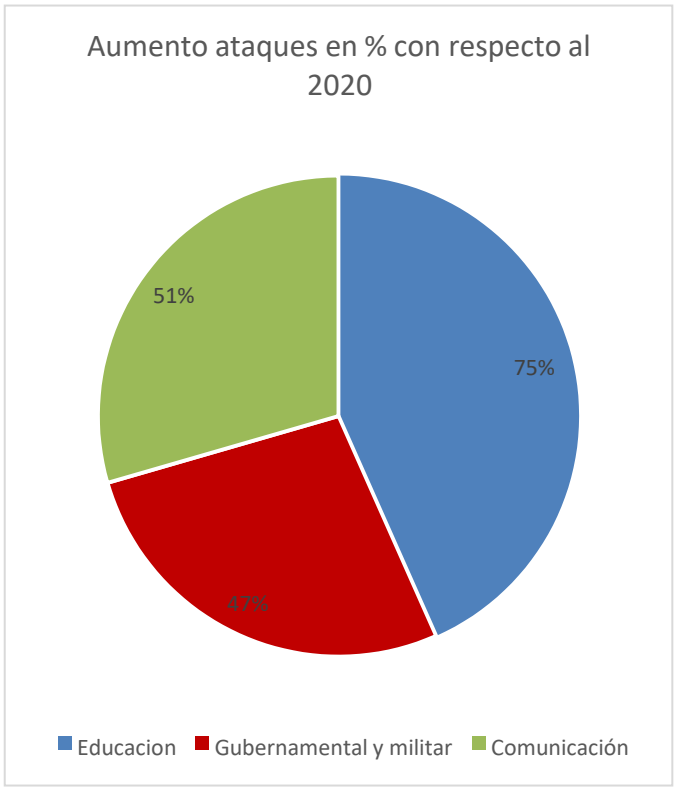


Fuente: Propia. basado en el informe “Tendencias cibercrimen Colombia 2019-2020” del CCIT.

[44] SOPHOS. Sophos State of Ransomware in Education 2021. [En línea] 2021. Disponible en: https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/?msclkid=d137c220c7ef11ec84a62436ee0fc7c7

En el siguiente grafico No 3 se muestra el aumento de ataques en el 2021 a los sectores más atacados con respecto al 2020, en Colombia, Según un informe publicado por el CCIT “Tendencias cibercrimen Colombia 2019-2020”, esto para enseñar el panorama de los sectores en cuanto a la progresión en inseguridad.

Gráfico 3. Aumento ataques



Fuente: Propia. basado en el informe “Tendencias cibercrimen Colombia 2019-2020” del CCIT.

“Aunque el aumento fue realmente generalizado, en diciembre los ataques añadidos atribuidos a las vulnerabilidades de Log4j contribuyeron efectivamente a elevar las cifras. También ha habido un aumento del 57% en el impacto del ransomware en las redes corporativas y del 59% en los robos de información”. Según Dembinsky desde Check Point Software Technologies[45].

Log4j es un marco de registro gratuito y de código abierto de apache utilizado en muchos proveedores de servicios, en el año 2021 fue descubierta y ha empezado a ser

[45] Computerworld. El sector educativo, acosado por los ciberataques en 2021. [En línea] 2021. Disponible en: https://cso.computerworld.es/cibercrimen/el-sector-educativo-acosado-por-los-ciberataques-en-2021

mitigada, pero con esta vulnerabilidad hace que se ejecute el código de forma remota, por lo que el ataque su alcance y efecto depende de su utilización.
Otro hallazgo hecho por el informe de Check Point también es las regiones más atacadas en 2021, siendo África con 1582 ataques y Asia-Pacífico con 1353 ataques, con un aumento del 13% y 25% respectivamente con respecto al 2020.

5.4 Los entornos digitales, peligros y amenazas

Primero que todo para continuar se explicará que es cada uno de los términos:
EVA significa entornos virtuales de aprendizaje, se trata de un espacio educativo que se encuentra alojado en la nube, el cual está conformado por un conjunto de herramientas TIC que permiten la interacción de forma remota entre los involucrados en el proceso de enseñanza, enfocándose más en el desarrollo personal e independiente de cada estudiante.
AVA significa Ambientes virtuales de aprendizaje, y se trata de una aplicación que permite la comunicación pedagógica con los estudiantes a distancia, OVA significa Objetos virtuales de aprendizaje, y se trata de las herramientas que se utilizan como recursos digitales pedagógicos en un ambiente de aprendizaje, y permiten la transmisión del conocimiento.

También tenemos los sistemas de gestión de contenidos (CMS) y los sistemas de gestión del conocimiento (LMS), son aplicaciones con múltiples herramientas que se utilizan para los procesos de enseñanza-aprendizaje de forma online, con las cuales se incorpora un método de enseñanza en el cual se gestiona este sistema y se utilizan para su gestión y revisión, controlar y siempre mejorar dicho proceso.

Ahora se tratará los problemas de seguridad que pueden o han afectado a estos instrumentos, herramientas o métodos de ejercer la enseñanza, como se explicó se trata de ayudas al método de enseñanza virtual y a distancia, cada uno explica de que se componen los entornos de aprendizaje digital y como se complementan para suplir y quizás hasta mejorar los procesos de enseñanza presencial mostrando y utilizando un nuevo paradigma de transmisión de los conocimientos o enseñanza y educación.

Equipos inseguros, se referiere a los equipos que están trabajando remotamente, como lo hace la educación a distancia, estos equipos pueden estar en peligro o riesgo por alguna vulnerabilidad por diversos factores, y puede ser la entrada de distintos ataques hacia la organización.

Softwares maliciosos, se trata de la utilización de aplicaciones no confiables, las cuales pueden generar un alto riesgo a la organización.

Outside firewall, esto se trata de trabajar o utilizar una conexión fuera de la permitida o fuera del firewall establecido por las políticas de la organización.
Update fail, como su nombre lo indica se trata de las actualizaciones, las cuales siempre se deben tener al día o pueden explotar alguna vulnerabilidad que aún no se parchea.
Gestión APP, se trata de la configuración adecuada a una aplicación que se utiliza, la cual puede tener riesgos y vulnerabilidades desconocidas para quien la usa por lo tanto se tiene que configurar de manera adecuada y segura.

Perdidas o robos, tal como se intuye se trata de la pérdida no deliberada de un activo o un robo directamente, con lo cual la información del dispositivo es pérdida de forma parcial o total.

E-mail y mensajes, los correos son indispensables y los mensajes otra forma de comunicación muy utilizada, existen métodos de ataque que utilizan estos métodos para infectar o contactar de forma maliciosa para causarle algún daño a la integridad de las personas.

Dispositivos de almacenamiento de datos externo, esta clase de dispositivos son muy usados y populares en la actualidad por lo cual es uno de los métodos que se utilizan para atacar a las organizaciones.

Saturación VPN, si se da el caso de un uso del VPN que se trata de una red virtual privada, para lograr cumplir los objetivos de la enseñanza, se debe tener en cuenta la cantidad de usuarios y las áreas, para tener un control sobre la conexión pues puede sufrir saturación.

Acceso a sistemas críticos, dicho acceso se tiene que verificar y ajustar pues no fue diseñada en su mayoría a una modalidad virtual o de acceso remoto, pues el peligro aumenta de forma exponencial con cada nuevo acceso externo.

FAKEDNS, se trata de un problema que consiste en que la institución educativa debe manejar una gran cantidad de usuarios utilizando un servicio web, pues se suele confundir al redirigirse un conjunto de usuarios con un ataque DNS y puede causar la caída de sitios web, servicios y servidores.

Response time, cuando ocurre un incidente hay generalmente un grupo encargado para reaccionar a estos, además de un plan de mitigación, contingencia y de respuesta, para que esto sea lo menos perjudicial posible se debe tener un tiempo de respuesta muy rápido o de ser posible inmediato o los daños pueden llegar a ser catastróficos.
Amenaza zero day, se trata de vulnerabilidades que se explotan antes de ser descubiertas y se creen métodos de mitigación.
Ciberataques, de esto si se tiene constancia, y es que la taza de crímenes informáticos sube conforme la tecnología mejora, con lo cual no hay sistema totalmente seguro, pues siempre hay un riesgo de que un criminal efectúe un ciberataque contra la organización, con lo cual es un peligro y una amenaza vigente, a la cual se está expuesto cualquier organización o persona natural.

Políticas y normativas, es muy importante saber que, si se tienen unas políticas y unas normativas que no son compatibles y no soportan el trabajo o actividad a distancia, virtual o digital, se tienen que actualizar y ajustar de inmediato desde que se considere el trasladarse al medio digital y online.

Internet y el factor humano, es de lo más evidente y más importante y se trata de la red mundial o internet y del factor humano, lo que quiere decir de la conducta humana y el ambiente en internet, el ambiente en internet no suele ser muy hostil pero en la parte de interfaz pues siempre hay un peligro al estar en internet pues hay muchos peligros y gente malintencionada, maneras cada vez más creativas para engañar y estafar a las personas sin olvidar los criminales que hacen daño integro a los usuarios, siempre hay que saber navegar en la red y hay métodos seguros además de las buenas prácticas y allí entra el factor humano, por eso son un solo apartado, quien hace uso del servicio de internet son las personas y ellas son las que mayormente cometen la imprudencia que afecta con la seguridad de las organizaciones, es el más vulnerable, por lo tanto se le tiene que capacitar en la gestión de su propia seguridad y así no afecte a la de la organización.

Según Sabnis, S., Verbruggen, M., Hickey, J. and McBride, A. J.[46], menciona algunos aspectos para la aplicación de seguridad en entornos virtuales: clasificación del tráfico e información real entre máquinas virtuales, mecanismos de autentificación y controles de acceso robustos, controles para el acceso y la operación, corrección de

[46] Sabnis, S., Verbruggen, M., Hickey, J. and McBride, A. J. (2012), Intrinsically Secure Next-Generation Networks. Bell Labs Tech. J., 17: 17–36. doi: 10.1002/bltj.21556. Disponible en: https://revista.seguridad.unam.mx/numero-20/seguridad-inform%C3%A1tica-en-entornos-virtuales

vulnerabilidades e instalación de actualizaciones de seguridad, así como configuración de auditoría y escaneo de vulnerabilidades.

La tabla número 1 que se muestra a continuación, enseña los ataques más comunes a entornos digitales según el ECUADORIAN SCIENCE JOURNAL VOL. 5 No. 1, sacado en el 2021, describiendo cada uno de los ataques con una definición dada por expertos en el tema.

Tabla 1. Ataques más comunes a un entorno virtual

ATAQUES MAS USADOS A ENTORNOS VIRTUALES	
De Disponibilidad	
DNS	Este tipo de ataque busca bloquear el servidor enviando una gran cantidad de solicitudes hasta hacerlo colapsar, y provocar un fallo en el sistema.
De Autenticación	
Ruptura de autenticación y gestión de sesión	Se trata de una usurpación de identidad, pues el cibercriminal usa las credenciales de acceso de un empleado para acceder y se apodera de la cuenta imposibilitando el acceso.
Comunicación no segura	Cuando se realiza una transmisión se tiene que velar por su seguridad, usando encriptación, canales seguros y verificaciones que impidan que un usuario no autorizado intervenga o sustituya a uno de los receptores o emisores.
De Confidencialidad	
Almacenamiento criptográfico no seguro	Se refiere a cuando no se realiza encriptación a la información sensible almacenada, pues puede ser susceptible a robos o perdidas.
Referencia directa	Generalmente los e-learning usan referencias a objetos directamente a interfaces web, por lo cual no hay comprobaciones de autorización por lo cual debe ser confidencial.
Fuga de información y respuesta inadecuada a errores	Se trata de la divulgación sin consentimiento de datos sensibles o filtración de los mismo ya sea por un error humano o de programación.
De Diseño	
Predicción de contraseñas y de los nombres de usuarios	Para este tipo de ataques se usa la intuición y la astucia de los atacantes para predecir o adivinar la

	contraseña o nombre de usuario mediante el análisis y la prueba de ideas referentes que pueden llegar a ayudar a descubrir algunas de estas.
Secuestro de sesión	Se trata de una interceptación del trámite de comunicación entre los clientes y servidores, generalmente se realizan solicitudes HTTP en donde por cookies quedan valores que pueden ser utilizados, por ejemplo, Moodle maneja 2 valores de identificación MoodleSession y MoodleSessionTest, que se almacenan en la cabecera del mensaje.
Fijación de la sesión	Se da cuando un atacante logra interceptar y acceder a una petición http como usuario anónimo y ser partícipe.
De Integridad	
Desbordamiento de búfer	Se da cuando no se limita el tamaño de validación en los datos almacenados por búfer, ocasionando el desbordamiento.
Cross Site Request Forgery	Se da cuando un atacante engaña a un usuario para que ingrese a una página de terceros para así aprovecharse de sus credenciales e ingresar al servidor causando daños y perjuicios.
Cross Site Scripting	Se trata de una inyección de java script malicioso en sitios web que capturan las sesiones usadas por la víctima en el navegador.
Fallo de restricciones de acceso URL	Se da cuando mediante medios de análisis e intuición, logran dar con la dirección URL que se utiliza en los procesos para acceder y realizar acciones no autorizadas o dañinas.
Defectos de inyección	Se trata de un ataque a las BD en donde por medio de inyección SQL y códigos maliciosos obtienen acceso a la información almacenada.
Ejecución de archivos maliciosos	Las plataformas de LMS no tienen la posibilidad aun de controlar el contenido que se puede llegar a usar por lo tanto pueden contener contenido malicioso o dañino por lo cual se debe comprobar de otras maneras.

Fuente: Propio, Basado en el informe de ECUADORIAN SCIENCE JOURNAL VOL. 5No. 1, MARZO-2021

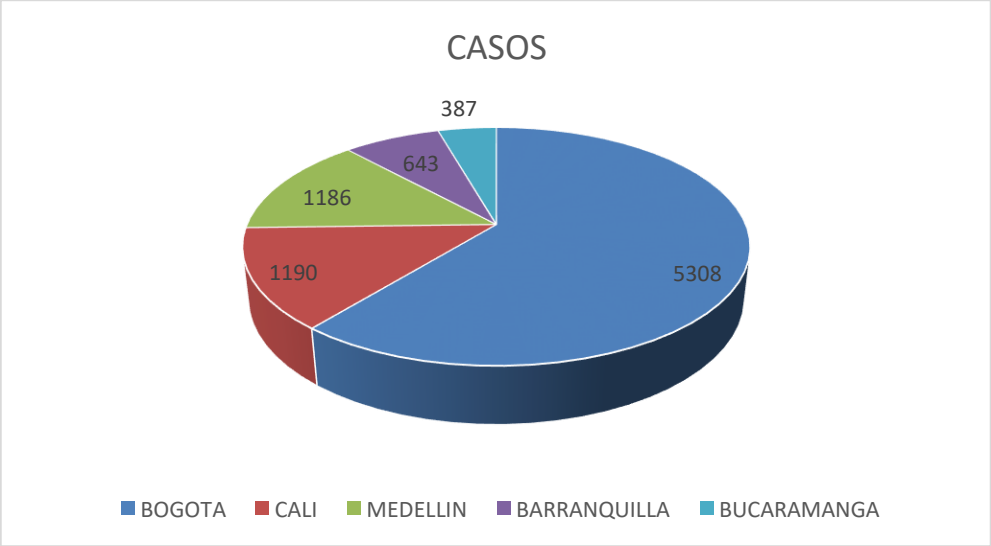
5.5 Cibercrimen

El ciber crimen o la ciber delincuencia según el FBI, en los últimos años ha dejado pérdidas de casi 12.000 millones de dólares en el mundo, a través de diferentes

modalidades, mencionado en una publicación, “Tendencias del Cibercrimen en Colombia 2019-2020” del 2019 hecha por la cámara colombiana de informática y telecomunicaciones.
En Colombia, según la fiscalía general de la nación, “el monto de pérdidas está entre 120 millones a 5.000 millones de pesos, dependiendo del tamaño de la empresa afectada”[47].

El gráfico a continuación muestra el top Colombia en casos por ciberdelincuencias en donde se ha denunciado, en promedio unas 60 denuncias diarias, según el estudio de “tendencias cibercrimen Colombia”, liderado por el programa Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) del Tanque de Análisis y creatividad de las TIC (TicTac) que junto con la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional.

Gráfico 4. Casos Top Colombia



Fuente: Propia. Basado en el informe “Tendencias cibercrimen Colombia 2019-2020” del CCIT.

La dinámica actual del Cibercrimen en Colombia muestra un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades de ciberseguridad. A través de los canales de atención a empresas y ciudadanos dispuestos por parte de la Policía Nacional fueron registrados 30.410 casos durante el 2019.

[47] CCIT. Hasta 5.000 millones de pesos pierde una empresa por cada ataque cibernético. [En línea] 2019. Disponible en: https://www.ccit.org.co/noticias/hasta-5-000-millones-de-pesos-pierde-una-empresa-por-cada-ataque-cibernetico/

- Del total de los casos registrados, 17.531 fueron denunciados como infracciones a la ley 1273* de 2009 por parte de las víctimas, esta cifra corresponde al 57% del total de casos informados.

- Respecto al 2018 las denuncias disminuyeron un 5.8 % tras una variación negativa de 1.130 casos.

- El 45% del total de denuncias por ciberdelitos en el país se hace a través de la aplicación A Denunciar. Desde julio de 2017 se han recibido un total 24.711 denuncias por ciberdelitos en esta plataforma virtual.

- 12.879 incidentes cibernéticos es decir un 43% de los casos reportados en 2019, fueron gestionados sin que se llegara a instaurar una denuncia ante la fiscalía general de la Nacional.

- Esta cifra representa un incremento del 54% respecto del 2018, cuando fueron gestionados 8.363 casos.

- Los incidentes más reportados en Colombia siguen siendo los casos de Phishing con un 42%, la Suplantación de Identidad 28%, el envío de malware 14% y los fraudes en medios de pago en línea con 16% Los delitos que más afectan a los colombianos.

- El principal interés de los Cibercriminales en Colombia se basa en la motivación económica y la posterior monetización de las ganancias generadas en cada Ciberataque.

- El delito informático más denunciado en Colombia es el Hurto por medios informáticos con un total de 31.058 casos, los cibercriminales saben que el dinero está en las cuentas bancarias y por eso buscan comprometer los dispositivos utilizados en la interacción entre usuarios y banca.

- En segundo lugar, se encuentra la Violación de datos personales con 8.037 casos. Este dato revela que la segunda amenaza en Colombia para empresas y ciudadanos es el Robo de Identidad.

- El tercer delito más denunciado es el acceso abusivo a sistema informático con 7.994 casos, y esto se explica en razón a que, en las fases primarias de los

Ciberataques, los cibercriminales buscan comprometer los sistemas informáticos logrando ganar el acceso a los mismos.

- En cuarto lugar, con 3.425 casos se encuentra la transferencia no consentida de activos, conducta criminal que facilita al atacante sustraer el dinero o transferir valiosos activos financieros de las víctimas Las Money Mules prestan su nombre o su cuenta bancaria para recibir transferencias de dinero producto de la actividad ilícita de los cibercriminales.

- Las Money Mules o mulas monetarias se convierten en el eslabón primario de la cadena criminal del Cibercrimen, perciben generalmente un 10% a 15% del total de ganancias.

- Algunos pueden ser engañados con esquemas de teletrabajo y las redes del Cibercrimen pueden estar en otros continentes.

- Finalmente, en quinto lugar, se sitúa el delito de Uso de Software Malicioso con 2.387 casos.

5.6 Estados por ciudades

La concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados.

Esta cifra se refiere a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia las PYMES, entidades financieras y grandes compañías con asiento en estas ciudades. [48]

[48] CCIT. Tendencias del Cibercrimen en Colombia 2019-2020. [En línea] 2019. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

6 EVALUACIÓN DE SEGURIDAD A HERRAMIENTAS TECNOLÓGICAS USADAS EN PROCESOS EDUCATIVOS BASADO EN LAS ISO 27000

En estos últimos dos años se han llevado a cabo diversos eventos adversos, los cuales han afectado de manera significativa la rutina de la vida, es por esto que la pandemia ha hecho que se cambie la manera de ver y de aprender en la educación, es decir, los métodos de enseñanza, la virtualidad, el aislamiento, son algunos temas que cambiaron drásticamente pero que a partir de esto, se ha podido implementar diferentes herramientas tecnológicas que han servido para el proceso de enseñanza de los estudiantes y jóvenes. A partir de esto se revisará la seguridad implementada en cada una de ellas y el impacto que ha tenido en la educación virtual.

La educación en el siglo XXI ha tenido que mostrar más flexibilidad, se ha tenido que mostrar de manera más personalizada hacia los estudiantes, buscando que los mismos puedan desarrollar distintas competencias y se puedan relacionar mediante comunidades de aprendizaje virtual, esto se hace como el objetivo que el estudiante pueda construir conocimiento colaborativamente y por supuesto tenga la capacidad de trabajar en equipo.
Ante la urgencia sanitaria ocasionada en estos últimos años, se ha tenido que llevar la educación al extremo digital, esto en gran manera fue un gran avance ya que se está logrando que exista una cobertura más amplia en todo el territorio colombiano. Por lo pronto se debe trabajar en la transformación de las diferentes plataformas educativas, en su seguridad e interacción con el estudiante.

Las TIC son diferentes herramientas que se utilizan para administrar y compartir información mediante diferentes aplicaciones tecnológicas. Mediante las TIC se evidencia que el trabajo colaborativo fomenta a la participación de los estudiantes, así mismo compartir ideas y propuestas; algo que no se permitía antes, donde no eran plataformas interactivas, sino que sólo ofrecían contenidos estáticos.

Para que la educación virtual pueda ser llevada a cabo de manera satisfactoria, se deben tener en cuenta varios puntos y estándares en la educación: el sistema del currículo, la metodología utilizada para llevar a cabo los procesos de evaluación, pedagogía, los diferentes canales de comunicación que se desean llevar a cabo. Basado en esto se toma en consideración que herramientas tecnológicas cumplen con estas condiciones y a su vez poseen la seguridad necesaria para que los ambientes virtuales sean los más adecuados para los estudiantes.

En los ambientes virtuales se deben tener en cuenta 3 pilares importantes, los cuales garantizan a los estudiantes un aprendizaje optimo: el contenido de las clases, la pedagogía utilizada y el tipo de tecnología que se va a implementar; con estos tres pilares se facilita la creación de los EVA y ayuda a que la educación se lleve a cabo de manera eficaz.

Para que el aprendizaje virtual sea llevado a cabo de manera efectiva, se debe comprender que el conocimiento debe ser inducido de manera aplicable al aprendizaje basado en las mallas curriculares, en los objetivos, en el tiempo, en la escritura del material, donde se busca crear una interfaz educativa, capaz de mostrar las capacidades presenciales de la educación, dirigidas a la virtualidad.

Las instituciones educativas no estaban preparadas para realizar clases de manera virtual, al ser de esta manera, se debió preparar todo un sistema completo para que tanto los estudiantes como los docentes, se adapten a un proceso formatico completo, donde se busca que los docentes puedan acompañar a los estudiantes en su proceso formativo. Por otra parte, se esperaba que el estudiante asumiera una actitud más proactiva, donde debía de elevar su compromiso académico en pro a su aprendizaje. La forma en que se debía diseñar las clases virtuales era de manera organizada, donde se debía promover la participación e interacción de alumnos y a su vez que el estudiante tenga claras las metas que debe alcanzar al cursar las asignaturas correspondientes.

La planificación que se debe llevar a cabo en las clases virtuales debía tener como factor principal que la información a proporcionarse a los estudiantes debía llegar de manera rápida y efectiva, buscando la pluralidad en las diferentes herramientas digitales y que las clases fueran llevadas a cabo de manera diversa.

Se debe tener en cuenta que el material didáctico que se diseña o que se selecciona debe ser el más adecuado, teniendo en cuenta a la población que se va a llevar a cabo el mismo. Además de ello se debe establecer los valores cuantitativos y cualitativos que ayuden a evaluar los procesos educativos de los estudiantes, a su vez el docente debe promover el desarrollo de destrezas en la comunicación en la búsqueda de la información y en el aprendizaje autónomo.

A continuación, se entrará a evaluar cada plataforma, definida categóricamente y se entrará a revisar temas de ventajas y desventajas; además de ello el nivel de seguridad basado en la experiencia en el uso que se le dieron a las mismas.

- **Plataformas de comunicación**

Como primera medida se examinará las plataformas de comunicación más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de estas.

Tabla 2. Plataformas de comunicación

Nombre aplicación	**Resumen**	**Nivel de seguridad**	**Ventajas**	**Desventajas**	**Norma y lineamientos**
Microsoft teams	Para el concepto de muchos expertos es la herramienta más completa que se tiene dentro de las más útiles y optimas, posee muchísimos beneficios, posee a la plataforma de Outlook 365 y su versión premium o licenciada permite muchos beneficios, como crear equipos, canales, programar actividades en calendario, eventos masivos con capacidad para más de 6000 personas, es segura, tiene usuarios registrados con su mismo dominio, lo cual permite manejar y monitorear todos los estudiantes y saber que realizan en sus clases. Permite crear tareas y cuestionarios y grabar las clases.	Este es un punto bastante importante ya que permite guardar las grabaciones de manera privada, lo cual garantiza una privacidad y seguridad alta en el mismo	Como ventaja se encuentran la organización de canales y equipos, el cual privatiza y ordena mejor las aulas de clase virtuales.	Su única desventaja es que de acuerdo con el plan que se adquiere, las grabaciones tienen un tiempo de caducidad de 20 días.	Aplica los lineamientos de la norma ISO 27001 y en la ISO 27018, que trata de la protección de la información almacenada en la nube. La gestión de contraseñas y la política de privacidad de la información, esta administrada de la mejor manera.
Zoom	Es una aplicación que trae muchas controversias. Al principio que estaba llevando a cabo la virtualidad en las instituciones educativas, a través de diferentes medios de comunicación se	Su nivel de seguridad se muestra que es bajo, de acuerdo con los estándares de privacidad y de datos proporcionados a la red.	Como ventaja se muestra que es una aplicación sencilla y ágil de manejar en su versión free, se puede tener una cantidad de minutos determinado en	Como desventaja se muestra que, en su auge, la compañía mostró que los datos personales de los usuarios estaban siendo	La gestión de la información personal, la gestión de la seguridad de las contraseñas y las políticas de privacidad son algunos de los beneficios de

	mostraron evidencias que la plataforma no tenía ningún tipo de privacidad en la información de los clientes, se estaba vendiendo y filtrando a empresas terceras, motivo por el cual no se recomendaba en su momento implementar en instituciones educativas		esta versión, pero se muestra como una plataforma estable	expuestos y filtrados a otras empresas.	esta plataforma. Se evidencia que existe un aporte significativo en la norma ISO 27001 del 2013, la cual tiene una certificación a nivel de controles de seguridad y en la gestión de la mejora continua en los procesos que se llevan a cabo dentro de la aplicación.
Google Meet	Es una aplicación web que permite conectar a varios usuarios a través del navegador, trabaja con el centro de mensajería Gmail.	Se considera una plataforma segura, ya que proporciona niveles altos de seguridad en cuestión de que, si un usuario quiere acceder a una clase, debe permitir que el administrador de la sala permita o cancele el ingreso.	Como ventajas se tiene la pluralidad de plataformas, se puede acceder desde dispositivos móviles o desde computadores y las funciones son similares en ambos dispositivos	Como desventajas se encuentra que, a diferencia de otras plataformas, no se puede consolidar clases de manera que los archivos o grabaciones puedan estar disponibles sin necesidad de enviar enlaces a los participantes	Aplica los lineamientos de la norma ISO 27017 hace un gran aporte a nivel de controles tanto para proveedores como clientes. Esta norma ayuda a que los datos compartidos en la aplicación sean transmitidos de manera segura el cual está respaldado por un sistema de gestión por certificados de confianza.
Web Room	Es una aplicación web que permite crear salas hasta de 12 personas de manera simultanea	Proporciona un nivel de seguridad adecuado, posee espacios de trabajo adecuados y propicios para la enseñanza	Como ventajas se tiene la posibilidad de compartir pantalla y conectar a los 12 usuarios de manera simultanea	Como desventajas se tiene que, al tener la posibilidad de compartir documentos, la autoría de los documentos pasaría a hacer	Esta plataforma educativa obtuvo la certificación en la norma ISO 27001 como gran aporte en su gestión en la seguridad de la información,

				parte de la administración del software	además se evidencia que su plataforma contiene documentación y soportes necesarios que pueden garantizar tanto a clientes como empleados la integridad y el manejo de vulnerabilidades.
Hangouts	Es una herramienta que permite conectar a varias personas a través de una sala, donde permite compartir contenido de YouTube, gráficos, foros y se puede compartir documentos entre los usuarios conectados.	Posee un nivel alto de seguridad frente a lo que se desea manejar.	No posee un límite de tiempo en conexión por videoconferencia	Tiene unas funciones limitadas u otras que tienen otras aplicaciones que también son free.	Dentro de la plataforma Hangouts, es una suite que posee Google y cuenta con certificación ISO 27001, a su vez permite que los datos proporcionados por los clientes, como son los datos de audio y video, sean manejados a través de un sistema de gestión de integridad de datos.
Google duo.	Es una aplicación que funciona con conexión de extremo a extremo y permite conectar a los usuarios a través de llamadas o videollamadas. Su seguridad es buena ya que garantiza su comunicación a través del cifrado extremo a extremo	Tiene un nivel de seguridad medio alto, tiene niveles de seguridad óptimos pero la imagen y grabación de estas hacen propiedad de la empresa anfitriona.	Se cuentan con videollamadas de extremo a extremo, asegurando una conexión confiable entre dos personas.	Se debe instalar de manera correcta en el dispositivo a utilizar.	La plataforma Google duo hace parte de la suite que tiene Google y cuenta con certificación en la norma ISO 27018 que cuenta con estándares que dan garantía a la privacidad y protección a la información de identificación personal. Además,

					proporciona distintos controles de seguridad que ayudan a la protección de datos personales.
Skype	Es una herramienta que ha ido en una baja continua, ya que se creó Microsoft teams, pero sigue siendo una herramienta bastante interesante, se puede realizar videollamadas en calidad HD, se pueden conectar hasta 100 clientes en una misma llamada,	Posee un nivel de seguridad alto.	Como ventajas es que cuenta con una versión free que permite la conexión segura entre usuarios.	Microsoft creó a teams y las funciones de Skype han quedado limitadas frente a la creación de teams,	Se puede evidenciar que la búsqueda de usuarios es bastante fácil de encontrar. Finalmente, Skype no cuenta con un cifrado de extremo a extremo, lo que puede causar que Microsoft pueda ver todos los mensajes y archivos contenidos en ese chat, no se evidencia que la aplicación cuente con alguna certificación en norma ISO 27000 que pueda garantizar la fiabilidad y confidencialidad de la información.

Fuente: Propia – Basado en el análisis a estas plataformas de comunicación

- **Plataformas de evaluación**

Se entrará a identificar las plataformas de evaluación más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de esta.

Tabla 3. Plataformas de evaluación

Nombre aplicación	**Resumen**	**Nivel de seguridad**	**Ventajas**	**Desventajas**	**Norma y lineamientos**
Schoology	Es una plataforma	Muestra un	Como ventaja	Para	Esta plataforma

	gratuita que tiene como funciones la programación de actividades y evaluaciones para ser compartido por un curso virtual.	nivel de seguridad alto, el cual se evidencia que el manejo de la información y los recursos inmersos en ello poseen una seguridad adecuada	se tiene que es una herramienta que posee material educativo, el cual se puede manejar de manera virtual o puede servir como complemento de manera presencial	proporcionar acceso a un grupo de estudiantes, debe pagarse por un plan full que tenga más funciones.	cuenta con un sistema de autenticación doble, lo que hace que el acceso a la misma sea más seguro, ya que para el inicio de sesión se hace a través de un código QR y se requieren dos pasos de autenticación para ingresar a la misma, garantiza algo de seguridad a través de MFA y el SSO. No se encuentra registrado si cuenta con certificación en la norma ISO 27001.
CoFFEE	Es una plataforma de código abierto que tiene como principal factor la preparación de foros, mapas mentales, exámenes, etc.	Es una plataforma que se considera poco segura, ya que se considera que es un software de código abierto, es decir que puede ser modificado o personalizado de acuerdo con cada usuario como lo desee poner	Como ventajas se tiene que cuenta con varias herramientas, las cuales permiten realizar una buena planeación a las clases.	Como desventajas se tiene que es un software de código abierto, pueden ocurrir problemas en la filtración de información o de datos del personal académico y educativo.	No se encuentra registrado si la herramienta cuenta con certificación en norma ISO 27001.
Tiching	Es una plataforma utilizada especialmente para la educación a nivel preescolar y se puede organizar la información por carpetas o asignaturas.	Posee una seguridad nivel medio, ya que se debe compartir información o documentos de estudiantes y podrían llegar a ser públicos, es	Como ventaja se encuentra que los estudiantes pueden trabajar de manera libre en la realización de actividades y trabajos propuestos por el personal	Como desventajas se tiene que es una plataforma que tiene varios recursos gratuitos y por otros se debe pagar para obtener	No se encuentra registrado si la herramienta cuenta con certificación en norma ISO 27001.

		delicado ya que la información de menores de edad se debe preservar de la mejor manera.	académico.	acceso completo a ellos.	
Classlife	Es una plataforma catalogada todo en uno, tiene muchas herramientas que van desde básica primaria, hasta la educación superior	Tiene un nivel de seguridad bastante alto, cuenta con muchas herramientas que pueden ayudar a potenciar el ámbito educativo de manera confiable.	Como ventaja se cuenta con la pluralidad de herramientas y funciones capaces de solventar todo tipo de necesidades educativas de cualquier instancia.	Como desventaja es que los términos de servicio no especifican los niveles de seguridad en el tratamiento de datos.	Dentro de esta plataforma, se encuentran varios parámetros a nivel de seguridad, como es la actualización de datos en tiempo real, la centralización de datos y de procesos, y la gestión integral de datos. No cuenta con una certificación por parte de la ISO 27001 pero si cuenta con una plataforma estable que cuenta con app para dispositivos móviles.
Google forms	Esta herramienta es una de las más utilizadas y seguras que existen, su función principal es la realización de cuestionarios, cuenta con dos opciones, la primera es que se puede crear el cuestionario y no requiere registro con correo electrónico, pero es mucho más viable pedir correo electrónico para poder saber desde donde se remite la respuesta, es controlada por Google y es segura tanto para el estudiante como	Se considera que la aplicación tiene un nivel de seguridad alto, ya que se encuentra administrada por una plataforma confiable y sus datos quedan almacenados de manera correcta.	Como ventaja podemos encontrar la pluralidad de la plataforma, la encuesta se puede configurar como publica y cualquier persona puede acceder a la misma.	Su única desventaja es que es administrada por Gmail, un dominio público y gratuito, donde no se tiene un control establecido y cualquier persona podría suplantar la identidad de un estudiante.	En la plataforma Google forms se evidencia que la norma ISO 27017 hace un gran aporte a nivel de controles tanto para proveedores como clientes. Esta norma ayuda a que los datos compartidos en la aplicación sean transmitidos de manera segura el cual está respaldado por un sistema de gestión por certificados de confianza.

	para el docente.				
Forms office 365	Si la institución educativa cuenta con esta herramienta, que se tenga una licencia, tiene demasiados beneficios a nivel educativo, uno de ellos es esta herramienta, la cual, si se puede tener un dominio propio y se le puede asignar uno a cada estudiante, y esta plataforma si	Se considera que tiene un nivel alto en seguridad, es administrada por Outlook 365 y tiene políticas de privacidad en la información suministrada por los estudiantes	Permite privatizar pruebas y exámenes, donde solo el estudiante es dueño de su usuario y contraseña; donde toda la información que se comparte por este medio es utilizada para fines educativos.	Se debe contar con licenciamiento de office 365 para poder contar con toda la suite de herramientas	Esta plataforma garantiza un nivel de seguridad alto, gracias al aporte que hace la norma ISO 27001 y en la ISO 27018, que trata de la protección de la información almacenada en la nube, en este caso, forms maneja formularios que sus resultados se guardan de manera correcta y adecuada.
Kahoot	Es una herramienta que es utilizada de manera online, es una herramienta bastante interactiva ya que funciona en tiempo real; y consiste que el docente plantee un grupo de preguntas con 4 opciones de respuesta, el docente comparte un link en el que solo el estudiante debe poner su nombre e ingresar a realizar la prueba, es una herramienta bastante sencilla pero bastante práctica.	Tiene un nivel de seguridad alto, ya que se trabaja de manera online y no tiene riesgos de filtración de información sensible, solo se pide un nombre de usuario.	Como ventaja tiene la interacción en tiempo real de la aplicación entre los estudiantes y el docente	Como desventaja se considera que se debe tener una conexión a internet estable para que este ejercicio no tenga fallos	Esta aplicación web, su modo de operación es de manera sincrónica al navegador web, realmente para su funcionamiento no requiere alguna certificación o norma, ya que en su uso solo requiere un nombre de usuario y las preguntas que se hacen a través de la web se realizan al instante y no requieren de datos personales para poder utilizarla.

Fuente: Propia – Basado en el análisis de las plataformas de evaluación

- **Plataformas de gestión de tareas**

Se entrará a identificar las plataformas de gestión de tareas más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de esta:

Tabla 4: Plataforma de gestión de tareas

Nombre aplicación	Resumen	Nivel de seguridad	Ventajas	Desventajas	Norma y lineamientos
Mahara	Es una plataforma en la cual se puede dar un seguimiento a toda la actividad realizada por el estudiante y a su vez, se puede gestionar y administrar todas las herramientas en ella	Se considera que es una herramienta con un nivel de seguridad aceptable, ofrece toda la información en un solo sitio o plataforma	Como ventaja es la adecuación de un espacio web, para el trabajo de todas las competencias planteadas en este trabajo	Como desventaja se puede evidenciar,	Esta plataforma contiene varias certificaciones que dan garantía de la seguridad y confiabilidad que puede tener la misma, esta alineado con el certificado ISO 27001:2013 pero hasta la fecha no ha sido certificado formalmente. Como conclusión se tiene una plataforma segura, capaz de administrar y manejar la información de manera adecuada.
Ilias	Es un software de código abierto que tiene herramientas como la planificación de evaluaciones, asignaciones de tareas y permite la comunicación entre el estudiante y docentes.	Se considera que tiene un nivel de seguridad en riesgo, ya que es un software con código abierto, pero a su vez significa que se puede modificar o alterar su código.	Como ventaja se puede evidenciar que al ser una plataforma con código abierto se puede organizar de acuerdo con la necesidad de la institución educativa	Como desventaja se evidencia que, al ser de código abierto, se tiene como valor negativo que se puede añadir códigos maliciosos al software y a su vez ocasionar problemas de seguridad	No se encuentra registrado si la herramienta cuenta con certificación en norma ISO 27001.
Teachstars	Es una plataforma que permite crear cursos en línea, en el cual se puede subir material, programar actividades y	Es una plataforma que tiene un buen nivel de seguridad, se evidencia que la	Permite conectarse desde dispositivos móviles para su fácil acceso	Como desventajas se encuentra que para acceder a todo el contenido se	Es una plataforma educativa que ofrece servicio de cursos y actividades

	exámenes.	información suministrada por la plataforma esta consignada en un lugar seguro.	y administración	debe pagar una membresía para acceder al mismo.	académicas a usuarios, no se encuentra referencia de si tiene una certificación en la norma ISO 27001, pero toda su operación es de manera virtual, así que contiene una seguridad aceptable para operar en la web.
Rubistars	Es una herramienta gratuita que es de gran ayuda para docentes y educadores, ya que permite crear rubricas de evaluación, las cuales se utilizan para plasmar actividades, que criterios de evaluación se van a calificar y toda la documentación que el estudiante necesitará para realizar la misma.	Se considera que tiene un alto nivel de seguridad ya que no pide datos personales para ingresar a trabajar en el portal	Como ventajas se tiene que se puede trabajar de manera online, no pide registros previos para poder trabajar en la web.	Como desventaja se evidencia que, si no se tiene un previo registro, no permite almacenar y seguir trabajando desde otro equipo a través de la nube.	Es una aplicación que permite crear contenido a través de rubricas, dentro lo que se encuentra en la web, no existe una certificación oficial con la norma ISO 27001, pero si opera con normalidad y permite compartir diseños de rubricas de otras personas y crear contenido propio de rubricas.
Rubrix	Es una aplicación que, si requiere estar instalada en el computador, es utilizada por educadores y sirve para realizar planeaciones y rubricas de evaluación a estudiantes.	Se considera que tiene un nivel medio en el marco de descarga e instalación, ya que requiere dar permisos de administración en la ejecución del programa	Permite trabajar de manera óptima y tiene muchas funciones que ayudan a tener un buen manejo de recursos de rubricas	Hay riesgo de que el cliente instale la aplicación de manera indebida y lo pueda descargar de la web de una tercera persona.	No se encuentra registrado si la herramienta cuenta con certificación en norma ISO 27001.

Fuente: Propia – Basado en el análisis a estas plataformas de gestión de tareas

- **Plataformas de creación de ambientes virtuales**

Se entrará a identificar las plataformas de ambientes virtuales más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de esta:

Tabla 5. Plataformas de ambientes virtuales

Nombre aplicación	Resumen	Nivel de seguridad	Ventajas	Desventajas	Norma y lineamientos
Rcampus	Es una plataforma que permite gestionar los cursos, tareas y planilla de calificaciones de los estudiantes.	Posee un nivel de seguridad alto, en la investigación realizada no se ve que tenga problemas con la seguridad o manejo de la información	Es una plataforma gratuita diseñada para la administración del personal académico de una institución.	Como desventaja solo se puede evidenciar que no cuenta con un módulo de comunicación entre el docente y el estudiante.	Está fundamentada en la norma ISO 27017 que trata acerca de los servicios cloud, en este caso esta plataforma educativa, tiene varios métodos de implementación, pero toda su información se aloja en la nube, por esto es importante certificar la norma ISO 27017 que ayuda a gestionar de manera correcta y segura los servicios prestados a clientes finales.
Sakai	Es una herramienta versátil que permite la comunicación a través de fotos, mensajería	Tiene un nivel de seguridad medio, ya que terceras personas pueden entrar a colaborar en el proyecto del software y eso no permite que haya una	Permite la retroalimentación entre el docente y el estudiante de acuerdo con las actividades vistas.	Implementa otros proyectos desarrollados por otras empresas o personas independientes.	No se evidencia que estén certificados por algún ente como la norma ISO 27001, pero con los servicios que ofrece puede optar a estar categorizada en

		cronología en la realización del software			la norma 27018, basado en la protección de la información y el manejo de datos confidenciales.
Atutor	Es un sistema de código abierto web, pueden llevar a cabo clases online y permite enviar mensajería a los estudiantes.	Posee un nivel de seguridad medio, inclinado a delicado por la cuestión de que es un software de código abierto y esto puede ocasionar problemas de seguridad en implantación de código malicioso.	Permite realizar evaluaciones en línea y cuenta con una herramienta que se encarga de dar autoría a los documentos subidos a este ambiente virtual	Es un software de código abierto que ofrece accesibilidad y adaptabilidad, pero a su vez es una desventaja por los problemas que se pueden originar con el código abierto	Su última versión estable fue del año 2013, contiene licencia GPL y es open source, es diseñada en php y MySQL, pero no se encuentra registro si tiene alguna certificación en norma ISO.
Google classroom	Es una herramienta bastante interesante ya que tiene varios roles en el sistema, trabaja bajo la plataforma de Gmail y acepta usuarios registrados como invitados. Existen varios roles dentro de la plataforma y cada rol tiene sus funcionalidades, la cual permite crear y diversificar muchos contenidos dentro del programa.	Es una herramienta que tiene un nivel de seguridad alto ya que maneja los distintos roles del sistema, los cuales hacen que sus políticas sean más eficientes	Permite enviar comentarios en tiempo real y se puede invitar a otros docentes y padres de familia para que estén pendientes de próximas actividades que van a ver en la asignatura.	Se debe registrar usuario por usuario a la plataforma Gmail, para poder tener un acceso más controlado, se debe adquirir un dominio con Gmail, buscando que sea más controlada la administración de este.	En la plataforma Google classroom se evidencia que la norma ISO 27017 hace un gran aporte a nivel de controles tanto para proveedores como clientes. Esta norma ayuda a que los datos compartidos en la aplicación sean transmitidos de manera segura el cual está respaldado por un sistema de gestión por certificados de confianza.

Fuente: Propia – Basado en el análisis a estas plataformas de ambientes virtuales

- **Plataformas de gestión de archivos**

Se entrará a identificar las plataformas de gestión de archivos más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de esta:

Tabla 6: Plataforma de gestión de archivos

Nombre aplicación	**Resumen**	**Nivel de seguridad**	**Ventajas**	**Desventajas**	**Norma y lineamientos**
OneDrive	Es un servicio en la nube que ofrece un excepcional servicio a la hora de gestionar y guardar archivos personales del personal académico y estudiantes.	Tiene parámetrosde seguridad bastante altos, con los cuales se garantiza la confidencialidad y autenticidad de la información.	Como ventajas se tiene que es un servicio autentico, seguro y en línea, el cual garantiza que la información este online y offline.	No se evidencia una desventaja como tal, solo se evidencia que, si hay una suplantación de identidad, la tercera persona puede acceder a todos sus archivos.	Cuenta con certificación en la norma ISO 27001 y se encuentra específicamente en la ISO 27040, que es una guía que ayuda a proteger y salvaguardar la información en sistemas de almacenamiento masivo. También se apoya de la norma ISO 27017 que trata de la protección de la información en los servicios cloud.
Claroline	Es un software que permite administrar y crear contenido educativo el cual se presta para tener espacios colaborativos o privados, permite administrar cursos y subir documentación como tareas, trabajos y actividades. Es una plataforma en la cual se evidencia una interfaz usable, permite cargar documentos y archivos en cualquier formato.	Se muestra con nivel de seguridad media, ya que como es a código abierto, cualquier persona puede acceder a la misma y puede modificar su código fuente	Permite enviar cualquier tipo de formatos de archivos que se requieran dar a conocer, desde archivos de sonido, hasta archivos de video	Es una plataforma que se puede utilizar de manera óptima, pero no para enviar información por la misma, ya que la autoría de los documentos enviados por los estudiantes puede ser utilizados por terceras personas	Es una plataforma netamente educativa que es open source, es implementada por miles de instituciones educativas y posee valores agregados como la flexibilidad y robustez. Esta plataforma no cuenta con una certificación oficial en la ISO 27001, pero en su última versión proporcionaron estabilidad a largo plazo.
Google drive	Es un servicio en la nube que ofrece un	Tiene parámetros de	Como ventajas se tiene que	No se evidencia una desventaja	Cuenta con certificación en la

	excepcional servicio a la hora de gestionar y guardar archivos personales del personal académico y estudiantes.	seguridad bastante altos, con los cuales se garantiza la confidencialidad y autenticidad de la información.	es un servicio autentico, seguro y en línea, el cual garantiza que la información este online y offline.	como tal, solo se evidencia que, si hay una suplantación de identidad, la tercera persona puede acceder a todos sus archivos.	norma ISO 27001 y se encuentra específicamente en la ISO 27040, que es una guía que ayuda a proteger y salvaguardar la información en sistemas de almacenamiento masivo. También se apoya de la norma ISO 27017 que trata de la protección de la información en los servicios cloud.
Xmind	Es un programa que se utiliza para crear mapas conceptuales, organizar ideas, mapas mentales, diagramas de pez, diagramas de árbol y se puede trabajar de manera colaborativa con más personas. Admite tópicos, relaciones, etiquetas, notas, etc. Es una aplicación segura, no requiere datos personales y es creado para fines educativos.	Es una plataforma segura, no comprende ningún tipo de registro de información.	Como ventajas se obtiene la pluralización de distintos mapas, diagramas y permite trabajar de manera colaborativa y online.	Como desventajas es que se debe tener conexión a internet para poder trabajar con los mismos.	Es una plataforma educativa online que tiene como función la creación de mapas mentales online y permite compartir estos mapas con otros usuarios. No contiene ningún tipo de norma o certificación en la norma ISO.

Fuente: Propia – Basado en el análisis a estas plataformas de gestión de archivos

- **Plataformas de interacción**

Se entrará a identificar las plataformas de gestión de interacción más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de esta:

Tabla 7. Plataformas de interacción

Nombre aplicación	Resumen	Nivel de seguridad	Ventajas	Desventajas	Norma y lineamientos
Docebo	Es una plataforma que tiene varias funcionalidades, puede crear actividades e incentiva a la	Se evidencia que tiene un nivel de seguridad aceptable, los	Cuenta con una gran ventaja y es que contiene inteligencia	La única desventaja que se evidencia es que, al ser como una red social,	No se encuentra registrado si la herramienta cuenta con certificación en

	participación grupal e individual de los estudiantes	datos suministrados en la plataforma no se contemplan que sean compartidos con terceras personas	artificial, capaz de dar respuestas instantáneas a los estudiantes y a su vez hacer un seguimiento constante a los mismos.	se debe tener mucho cuidado con la información que se proporciona en esta plataforma	norma ISO 27001.
SocialGo	Es una plataforma que permite crear un perfil educativo para la red social, se pueden publicar fotos, videos y permite comunicarse con otras personas a través de mensajes públicos o privados.	Se evidencia que es una plataforma segura, pero a su vez es muy insegura, ya que se deben suministrar datos privados de los estudiantes y eso es un gran problema a nivel de seguridad.	Como ventaja se evidencia la interacción entre los estudiantes basados en una red social educativa y todo lo integrado está basado en el ámbito de educación.	La única desventaja que se evidencia es que, al ser como una red social, se debe tener mucho cuidado con la información que se proporciona en esta plataforma	No se encuentra registrado si la herramienta cuenta con certificación en norma ISO 27001.
Eduteka	Es un portal educativo que está enfocado a la educación básica primaria y media, contiene disciplinas como juegos, videos, entre otros.	Se evidencia que es una plataforma segura, pero a su vez es muy insegura, ya que se deben suministrar datos privados de los estudiantes y eso es un gran problema a nivel de seguridad.	Como ventaja se evidencia la interacción entre los estudiantes basados en una red social educativa y todo lo integrado está basado en el ámbito de educación	La única desventaja que se evidencia es que, al ser como una red social, se debe tener mucho cuidado con la información que se proporciona en esta plataforma	Es un portal web que ayuda al personal docente a planificar y crear clases de manera didáctica y ágil, no cuenta con ninguna certificación que garantice la seguridad de la información o datos tratados.

Fuente: Propia – Basado en el análisis a estas herramientas de interacción

- **Plataformas LMS**

Se entrará a identificar las plataformas de gestión LMS más usadas durante el periodo de la virtualidad, se hará un análisis al nivel de seguridad, las ventajas y desventajas de esta:

Tabla 8. Plataformas LMS

Nombre aplicación	**Resumen**	**Nivel de seguridad**	**Ventajas**	**Desventajas**	**Norma y lineamientos**
Moodle	Moodle es el aula	Es una	Tiene muchas	Como	Es una de las

	virtual que permite conectar a muchos usuarios dentro de la plataforma. Permite crear clases, foros, muros, evaluaciones, tareas y demás actividades propicias para el ámbito estudiantil. Aparte de ello permite la administración de usuarios y permite subir archivos a la plataforma.	plataforma 100% segura y utilizable	ventajas como la administración y manejo de la plataforma, y la gestión de usuarios	desventajas se dificulta al inicio su configuración inicial para matricular y parametrizar usuarios	principales plataformas LMS, está certificado en estándares como LTI (Learning tool interoperability) y esta se encarga básicamente de lograr una integración entre aplicaciones para el aprendizaje. No se refleja una certificación en norma ISO 27001.
Blackboard	Este software permite diseñar y planificar cursos de acuerdo con la necesidad del usuario. Tiene varias herramientas de seguimiento a los usuarios y permite revisar el rendimiento y avance de cada estudiante, es usada en el ámbito laboral y ámbito educativo.	Se encuentra en un nivel alto de seguridad, tiene un sistema robusto el cual permite la administración y configuración de la información de los usuarios	Como ventaja se encuentra la reglamentación respecto a la autoría de los documentos subidos a la plataforma, no pasan a ser parte de la empresa, sino que son propiedad del propio autor	Como desventaja se encuentra que no maneja la pluralidad de idiomas y solo está disponible en inglés.	Es una plataforma educativa LMS que está certificado por la norma ISO 27001, es una plataforma educativa, que tiene variedad de idiomas y de usabilidad en diferentes entornos, esta aplicación está orientada a la norma 27034, que busca tener parámetros necesarios para proteger la información suministrada dentro de la plataforma educativa.
Edmodo	Es catalogada como una red social virtual que tiene muchas funciones que permite a los docentes, administrar clases, tareas, contenidos, recursos, comunicarse con padres y alumnos. Sintetizar información, mapas conceptuales y fichas de refuerzo:	Tiene un nivel de seguridad medio, ya que exige que el personal docente y estudiantil se registren en una plataforma que no está siendo administrada por la institución educativa	Permite conceptualizar mapas mentales y conceptuales y a su vez trae consigo fichas de refuerzo para el manejo de estas.	Posee una plataforma de comunicación con padres de familia, buscando una comunicación entre las mismas, pero se han tenido problemas con esta comunicación	La plataforma educativa cuenta con varios soportes de varios estándares que ayudan a que la normatividad se lleve a cabo de la mejor manera, buscando que la privacidad y autenticidad de la información sea

					salvaguardada de la mejor manera. No hay algún estándar de la norma ISO 27001 que abarque esta aplicación web, pero se evidencia que es una plataforma usable e innovadora.
Neo LMS	Permite administrar clases, evaluar a estudiantes, realizar seguimiento a cada uno de ellos y se encuentra en diversos idiomas.	Se evidencia que tiene un buen nivel de seguridad en los archivos que se almacenan allí, además de ello se pudo evidenciar la confidencialidad e integridad de los datos proporcionados	Como ventaja se puede dar seguimiento personalizado a cada alumno, respecto a la evolución de su proceso académico. Cuenta con variedad de idiomas.	Como desventaja, solo permite alojar hasta 400 alumnos.	Es una plataforma educativa que cumple con funciones de creación de contenido, administrar actividades y ayudar a que la educación pueda realizarse desde cualquier parte. No cuenta con un estándar aprobado por ISO, pero si cuenta con otro tipo de políticas y manuales que ayudan a garantizar la privacidad de la información.

Fuente: Propia – Basado en el análisis a estas plataformas LMS.

7 GRADO DE APROPIACIÓN Y SEGURIDAD SOBRE EL USO DE AMBIENTES VIRTUALES POR PARTE DEL PERSONAL ACADÉMICO, MEDIANTE LA CONSULTA Y COMPARACIÓN DE INFORMES ASOCIADOS QUE PERMITAN ESTABLECER EL GRADO DE CONOCIMIENTO Y MANEJO SEGURO DE LAS HERRAMIENTAS DIGITALES.

En el proceso que se vivió durante la pandemia, se observó la necesidad de construir mecanismos evaluativos capaces de cuestionar el uso de los ambientes virtuales, ya que anteriormente se tenían modelos de evaluación tradicionales y al evaluar ya en entornos virtuales, se debía de revisar bajo que fundamentos pedagógicos se sustenta una evaluación virtual, si realmente el estudiante podía obtener aprendizaje oportuno y también se busca cuestionar si las evaluaciones de los estudiantes a los docentes son buenas hasta qué punto o si son por lo contrario algo que no lleva a algún fin educativo.

Dentro de la educación virtual, se conoce a la evaluación como un proceso el cual debe transmitir enseñanza y aprendizaje, donde el estudiante pueda reconocer sus fortalezas y debilidades en un tema en especial, a través de parámetros establecidos de estudio y aprendizaje. Bajo esta premisa de la evaluación a implementar, el docente entra a rediseñar su método de enseñanza. La evaluación se realiza en diferentes momentos y situaciones en las cuales transcurre un año académico natural, ya sea que esta parametrizado de manera semestral, trimestral o anual.

Para tener claro los principios de evaluación que se llevaron a cabo durante la pandemia se debe tener en cuenta, cuatro principios fundamentales: Confiabilidad, autenticidad, validez y objetividad.

Confiabilidad: A la hora de plantear criterios de evaluación, se debe reflejar a través de una evaluación, que el estudiante pueda mostrar que lo aprendido se vea reflejado en ello. A través de los ambientes virtuales, el estudiante reconoce a través de sus actividades y foros el conocimiento adquirido.

Autenticidad: Los recursos que se deben utilizar a través de los entornos virtuales, deben facilitar que se puedan desarrollar de manera adecuada y que pueda ser un entorno propicio para que la evaluación se desarrolle satisfactoriamente.

Validez: Se debe garantizar que cual sea el instrumento que se vaya a utilizar, pueda permitir medir los indicadores académicos, para poder encontrar fundamentación y organización en la evaluación.

Objetividad: Se debe evitar que el instrumento que se vaya a utilizar para realizar la evaluación no tenga preferencias ni favoritismo con ningún estudiante y que este instrumento tenga claro los criterios de evaluación.

Dentro de los escenarios de los ambientes virtuales que se desarrollaron durante la pandemia, existen las plataformas e-learning, capaces de dar diferentes tipos de estrategias, capaces de proporcionar desde desarrollo de contenidos hasta diferentes tipos de actividades capaces de construir evaluaciones objetivas a los estudiantes.

Las nuevas modalidades desarrolladas a través de las plataformas e-learning ofrecen diversidad de herramientas y permiten al docente contar con un gran abanico de posibilidades académicas, capaces de proporcionar construcción al aprendizaje y a su evaluación. Para ello se debe contar con herramientas flexibles que permitan realizar una planificación minuciosa a una formación online.

En la capacidad de relación aprendizaje-evaluación se han originado varios tipos de evaluación, teniendo en cuenta el enfoque y el marco que se desea usar:

Dentro del proceso de evaluación de los entornos virtuales, se debe tener en cuenta las evaluaciones diagnosticas, la formativa a donde se quiere orientar el tipo de evaluación y la sumativa.

Las evaluaciones diagnosticas ayudan a identificar en qué nivel se encuentra el alumno, sirve como punto de referencia para conocer desde donde se debe planear las clases y actividades a realizar.
La formativa se realiza a lo largo que se dicta la materia o curso, y tiene como objetivo ayudar al estudiante en todo su proceso formativo educativo, donde se pueda evidenciar sus debilidades y fortalezas.

La sumativa se desarrolla al final del curso para ya determinar el aprendizaje adquirido y la posterior certificación.

Dentro del proceso evaluativo que lleva a cabo los docentes a los estudiantes, se tienen en cuenta varios factores a la hora de implementar un sistema de evaluación o un sistema de planeación académico; uno de estos factores es la retroalimentación, el cual

cada estudiante tiene como derecho recibir, ya que este contribuye al aprendizaje de estos y a su vez puede diagnosticar errores y corregirlos posteriormente. Para esto es importante que el docente centre sus esfuerzos en facilitar estrategias a los estudiantes para que ellos hagan autocritica y encuentren sus habilidades, aparte de eso es importante que, en una relación conjunta con los estudiantes, se planteen criterios de evaluación y de acreditación para que se puedan fortalecer los aspectos del desarrollo y fortalezas de los estudiantes y a su vez se generan preguntas interesantes que pueden ser llevadas a la reflexión.

A través de distintas actividades se pueden incluir prácticas de retroalimentación, como, por ejemplo, los foros, las wikis, los mensajes con comentarios, los cuales se comparten a través de documentos como Google drive, las sesiones de chat y correo electrónico, etc.

Dentro de la evaluación de aprendizaje en los entornos virtuales, se identificaron 4 factores importantes, los cuales se deben implementar para que el aprendizaje dado a los estudiantes tenga coherencia de estructura como un elemento facilitador entre el docente y el estudiante.
La interactividad es un factor determinante en los entornos virtuales, el cual se debe llevar a cabo de manera constante y con el mayor acompañamiento posible; se puede llevar a cabo a través de diferentes herramientas virtuales y de manera sincrónica y asincrónica.

A su vez el dialogo debe estar acompañado de una buena comunicación estudiante-docente, que ayude a retroalimentar todos estos procesos de enseñanza impartidos a los estudiantes.

A continuación, se explicarán algunas herramientas adaptadas a la enseñanza virtual, capaces de impartir ayudas a la hora de implementar una retroalimentación efectiva a los estudiantes:

Mapas conceptuales: Se emplea de una manera fuerte en los procesos de aprendizaje Online, pero es importante tener en cuenta ya que el estudiante debe conocer el alcance de este y los objetivos que se pueden alcanzar a la hora de analizar este producto.

Preguntas intercaladas: Se realiza a través de una clase en la enseñanza tradicional, es un plan que ya está planteado desde un comienzo, es decir, en el momento que se estructura el plan académico, ya se encuentra ideado para realizar.

E-portafolios: Es un sitio en la web, donde se recopilan trabajos y evidencias, el cual tiene como propósito medir los aspectos más favorables y desfavorables; ayuda a que el estudiante tome conciencia de todas sus falencias y fortalezas que se presentaron en la actividad. A través de este portafolio puede el estudiante revisar su aprendizaje y a su vez puede evaluar a sus compañeros a través de la heteroevaluación y la coevaluación.

Rubricas: A través de las rubricas, se puede facilitar la comprensión de todas las actividades macros a desarrollarse, además de ello se contemplan diferentes competencias y habilidades. Ayuda a que el docente pueda especificar qué actividades y cuánto puntaje se dará a cada actividad y qué cantidad de logros se alcanzan a realizar esa actividad.

Foros: A través de los foros, se establece un canal de comunicación bastante interesante, capaz de que el estudiante pueda construir el conocimiento a partir de la retroalimentación del docente y los aportes que los compañeros del grupo puedan realizar. Para el docente significa que debe monitorear de manera constante y seguida todo el proceso que se lleva a cabo dentro del mismo. Estos foros ayudan a ordenar ideas, a analizar las opiniones y reflexionar acerca de cada comentario de cada persona.

7.1 Análisis grado de apropiación y seguridad sobre el uso de ambientes virtuales por parte del personal académico

Para evaluar todo el proceso de aprendizaje a través de entornos educativos, se tomaron 2 informes enfocados al manejo de recursos en diversos ambientes virtuales son necesarios para que exista una interacción entre estudiantes y docentes.

Se efectúa un análisis sobre los resultados de dos estudios asociados al grado de apropiación y seguridad sobre el uso de ambientes virtuales, con el objetivo de conocer el pensamiento reflexivo y lógico del personal académico sobre las diferentes habilidades, experiencias y dificultades experimentadas durante el proceso de virtualización durante el COVID 19 y cómo esto incidió en los procesos de aprendizaje tradicionales.

Luego de ello, se procedió a identificar las estrategias o los entornos de ambientes virtuales y a través de ello poder identificar el grado de apropiación de las herramientas digitales, aplicados a la modalidad virtual.

En el análisis de informes, se evidencia al personal académico acerca de que factores fueron obstáculos a la hora de impartir conocimiento de manera virtual, se encontraron dos premisas muy marcadas: La primera es que algunos estudiantes no contaban con accesibilidad o con los dispositivos necesarios para poder conectarse a la plataforma de manera virtual y el poco acompañamiento que recibían por parte de los acudientes, esto conllevaba a la mala administración de los ambientes virtuales.
Como valores agregados o valores positivos de los ambientes virtuales se encontró gran acogida en el manejo del tiempo, se podía realizar en cualquier momento del día, también se rescata que se puede encontrar bastante material en la web, los diferentes medios de comunicación con los cuales los docentes se podían comunicar con los estudiantes.

En el análisis que se efectúa, se observa en la evaluación de los aprendizajes en ambientes virtuales, existen aspectos importantes a aclarar, como lo es la devolución o retroalimentación de los docentes a los estudiantes, esto favorece en gran manera el aprendizaje de los estudiantes y construye en ellos una autocrítica de este.

Dentro de los ambientes virtuales proporcionados para la interacción entre el docente y el estudiante, se evidencia que los foros son una herramienta que ayuda mucho a la retroalimentación y al aprendizaje en conjunto a los estudiantes. A su vez al personal docente ayuda para que los estudiantes realicen sus consultas y a su vez se dé la retroalimentación respectiva con sus observaciones. Dentro de la evaluación presentada por el personal académico, se observa que los docentes manifiestan que es primordial que los canales de interacción y de comunicación, sean lo más ágil, efectivo y seguro posible. El personal académico manifiesta en su mayoría que costó adaptarse a los ambientes virtuales de comunicación, ya que no contaban con una preparación y con una asesoría dada con anterioridad, pero a medida que iba avanzando la educación a distancia, fueron afianzando conocimientos y manifiestan la diversidad de plataformas con las cuales podían desempeñar su trabajo.

Otro punto importante por resaltar en este grado de apropiación por el personal académico a los ambientes virtuales se evidencia a través de este estudio asociado, los diferentes tipos de enseñanza y estrategias implementados por el personal académico, entre los más destacados se encuentran:

- Trabajos colaborativos de manera virtual, pero con el acompañamiento del personal académico.
- Actividades que fomenten la interacción docente-estudiante y se incluyan los aspectos teórico-practico
- Elaboración de distintos tipos de materiales asociados a la enseñanza de los estudiantes (guías, talleres, trabajos, investigaciones)
- La implementación de distintos ambientes virtuales que ayudan a que el proceso de enseñanza sea viable y optimo a su vez, como: foros, librerías online, las wikis, las videoconferencias, la planeación de las actividades y el seguimiento a las mallas curriculares.
- La interacción entre los docentes y estudiantes, mediante los diferentes ambientes virtuales implementados para las videoconferencias (Microsoft teams, Skype, Google meet, etc.), así mismo tener la posibilidad de grabar los encuentros sincrónicos, para que el estudiante pueda ingresar a la grabación y ver la grabación en el momento que lo pueda hacer.
- Revisión a los contenidos planteados en la malla curricular y en los planes propuestos con anterioridad; analizando si se cumplieron los objetivos de enseñanza de aprendizaje.

Gran parte del personal académico manifiestan a través de este análisis, que los instrumentos de evaluación implementados ayudan a diversificar el ritmo del aprendizaje, el aprendizaje colaborativo y la regulación de todos los procesos de aprendizajes en ambientes virtuales. Así mismo intensifica la retroalimentación, tanto individual como grupal.

En este análisis realizado se puede inferir que valoran en gran manera la variedad de ambientes virtuales disponibles para impartir su conocimiento; ya que el docente es quien se encarga de impartir su conocimiento, de dar respuesta a las inquietudes y plantear debates acerca de temas de interés. También se evidencia que existían diversos ambientes virtuales evaluativos, ideales para cuestionar si el estudiante obtuvo las competencias impartidas en el curso. Finalmente, el personal académico hace referencia a que el ambiente virtual de comunicación para videoconferencias, Microsoft Teams, tuvo gran acogida entre ellos, se hizo referencia a esta plataforma como la más completa, a nivel de seguridad, a nivel de prestación de servicios y de la manera como se podía configurar las clases para tener mayor control sobre las mismas.

7.2 Manejo de contenidos virtuales y material disponible en la web para uso académico

Bajo este análisis, se evidencia varios puntos de vista, como por ejemplo de acuerdo con el rol o carga académica que desempeñen se puede dificultar o se puede garantizar encontrar información suficiente para dar a conocer los distintos contenidos virtuales que están en la web. También se analiza que hay docentes que no tienen el manejo o la experiencia en herramientas virtuales y esto hace que se dificulte la enseñanza hacia los estudiantes.

7.3 Valoración de la seguridad de los ambientes virtuales, con respecto a la confidencialidad de la información

En el análisis de estudio se muestra gran seguridad en la confidencialidad de la información, ya que si una institución educativa utiliza estas herramientas es porque se consideran seguras, pero también influye en que el padre de familia juega un papel importante en la supervisión de estos medios.

Dentro de las ventajas que se pueden encontrar en la educación a distancia, se puede evidenciar que en el análisis de estudio cuentan con ventaja, la disponibilidad del material en la web, así mismo se ve como ventaja que los estudiantes pueden acceder a las grabaciones de manera ilimitada, esto sirve por si no se pudo conectar a la hora indicada por un problema en la red o con el equipo, permite que el estudiante pueda ver su clase sin problema y no perder una explicación.

Para las desventajas que se encontraron en la educación de manera virtual o a distancia, se observa que la mayor intensidad laboral es un factor importante y relevante, el cual manifiestan que en la virtualidad, se les duplicó el trabajo y no tenían tiempo de cumplir con todas sus actividades a cabalidad.

En algunos casos no se podían comunicar con los estudiantes, ya sea por los horarios en los cuales se comunicaban o por el tipo de dispositivo que manejaba el estudiante.
Bajo las herramientas que más facilitaron el proceso de enseñanza hacia los estudiantes, se encuentra con gran ventaja que las videoconferencias fue el recurso que más se utilizó durante este periodo y ayudó a los estudiantes a aumentar su proceso de aprendizaje.

7.4 Evaluación de los ambientes virtuales respecto a la seguridad y manejo seguro de las herramientas virtuales

Bajo los ambientes virtuales, el análisis al informe detallado muestra que el personal académico manifiesta que inicialmente se sentían inseguros, ya que no conocían las plataformas ni su funcionamiento en general, pero luego ya conociendo mas a fondo, se concluye que ya es seguro y fiable.

7.5 Herramientas e instrumentos utilizados para la evaluación de aprendizajes

Dentro del análisis de informes que se conoce por parte del personal académico, se muestra con gran fuerza que herramientas como Microsoft Teams, es una de las plataformas más seguras y confiables que hay en el mercado, también se habló de Kahoot como una herramienta de interacción entre estudiantes y docentes; también se habló de la herramienta Moodle, la consideran indispensable como instrumento para evaluar el conocimiento de los estudiantes y a su vez realizar la respectiva retroalimentación.

7.6 Se analiza si las herramientas virtuales pueden aportar a el proceso de aprendizaje de la educacion presencial

En el análisis a los informes mostrados por el personal académico, se reflejan varios puntos de vista: el personal académico preescolar, manifiesta que no se pueden obtener los mismos resultados académicos, entre lo presencial y lo virtual, manifiestan a través de la encuesta que cuando los estudiantes ven clases a través de estos medios, se quedan vacíos, los cuales deben ser suplementados por otras personas. Para la educación de básica primaria y secundaria, piensan que los objetivos si se cumplen, la única cuestión que ponen en duda son los procesos evaluativos, si realmente el estudiante puede aprender y si los exámenes se realizan de manera consciente, para la educación pregrado si manifiestan que se pueden suplir ambos procesos sin afectar su calidad educativa.

7.7 Manejo de las planeaciones y estrategias, basado en los entornos de aprendizaje actuales.

El personal académico en este análisis de informes tiene una opinión centralizada y es que opinan que, si se cambian las planeaciones académicas ya planificadas con anterioridad, es muy viable que se deba cambiar de estrategias y de ambientes virtuales, ya que se debe tener en cuenta que se debe implementar la mejor alternativa, buscando que el estudiante pueda adquirir sus conocimientos de manera efectiva y pueda tener una total interacción con sus otros compañeros.

7.8 Perspectiva de los docentes de acuerdo con el grado de apropiación en los ambientes virtuales.

En el análisis que se realiza a este informe se encuentra algo dividido, pero se resalta dos valores importantes, la primera es que el personal académico, opina que al comienzo el adaptarse a estos ambientes, se complicó bastante, ya que algunos no conocían las herramientas proporcionadas y aparte de ello no se contaban con una capacitación previa.
El segundo factor es que algunas personas del personal académico consideran que fue fácil la adaptación ya que conocían algunos ambientes virtuales, los cuales ayudan a que las plataformas se manejaran de manera más práctica.

7.9 Proceso de formación virtual a través de entornos virtuales

Se evidencia en el análisis a el informe, que la experiencia fue buena, ya que se aprendió en gran manera todo lo relacionado con entornos virtuales y a algunos de ellos ayudo a enriquecer su proceso pedagógico. Dificultó algo en que no se tenía inicialmente, personal que capacitara el funcionamiento de las plataformas.

7.10 Manejo de criterios de evaluación realizados de manera virtual

En el análisis efectuado, se evidencia que los métodos pedagógicos para llegar al aprendizaje son buenos y adecuados, pero cuando se habla de los criterios de evaluación se piensa que no se suple los criterios de evaluación presenciales.

7.11 Instrumentos de evaluación más utilizados en las formaciones virtuales

Los instrumentos de evaluación que más se usaron en las formaciones virtuales según el análisis realizado, se destaca a Microsoft Teams, Kahoot, Canva y formularios de Google.
Se muestra con bastante fuerza entre el análisis, que la plataforma Moodle, fue factor importante y diferencial a la hora de realizar evaluaciones.

7.12 Características y funciones de los ambientes virtuales más utilizados

Entre el análisis y el estudio asociado a los ambientes virtuales, se especificaron dos ambientes virtuales más comunes, uno es Moodle, se dice que es un ambiente virtual, seguro y confiable, en la cual se podía planificar y estructurar un curso, de manera tal que el docente pueda configurar el sistema de manera óptima. Aparte de ello hablan de ambientes virtuales interactivos como Kahoot, que permite la interacción entre varios estudiantes y lo más importante que se puede llevar a cabo en tiempo real.

7.13 Aspectos positivos y negativos de la usabilidad de los ambientes virtuales

Como aspectos positivos de la usabilidad de los ambientes virtuales, se encuentra dentro del análisis, que las plataformas utilizadas contaban con soporte necesario, con manuales en línea, videotutoriales y demás información que ayudara a que el ambiente virtual pueda ser llevado de la mejor manera. Como desventaja o parte negativa, se evidencia en el análisis que no tenían las competencias necesarias para afrontar una educación a distancia, pero a través del tiempo se pudieron dar cuenta que los ambientes virtuales son bastante interactivos y usables.

7.14 Manejo de ambientes virtuales y su participación en mallas curriculares y planeaciones

Los ambientes virtuales que se tienen se muestran que tiene todas las herramientas capaces de dar desarrollo a estas planeaciones previamente diseñadas.
En el caso de otro tipo de formación académica, se evidencia en el análisis a los estudios asociados que los contenidos de las mallas curriculares no iban acorde con lo que se encontraba en los ambientes virtuales.

7.15 Manejo de información de los instrumentos de evaluación basado en procesos de enseñanza

Dentro de la recopilación de los estudios asociados a los instrumentos de evaluación, se encuentra que la información recogida, sirve como insumo para ver falencias o actitudes positivas que puedan proyectarse en los estudiantes, pero aparte de ellos una pequeña mayoría opina que los instrumentos de evaluación se deben llevar a cabo de manera presencial, garantizando la transparencia de los datos suministrados, sin pensar en el plagio que los estudiantes pueden cometer desde casa.

7.16 Retroalimentación de los instrumentos de evaluación en favor de los procesos de enseñanza virtual

El análisis arrojado, opina que si favorece la retroalimentación a los estudiantes ya que permite observar de manera unificada y manera grupal las falencias y los valores positivos que el instrumento de evaluación proporcione.

Análisis basado en el desarrollo de habilitades digitales del personal académico en la docencia universitaria.[49]

Para este análisis se entraron a analizar diferentes puntos de vista, dados dentro de la Universidad de Antioquia en la facultad de Ciencias Agrarias.
Se efectuaron variables de tipo cualitativo asociados a temas de interés, basado en la herramienta Moodle, en el uso de aplicativos en la docencia y necesidades de formación y capacitación.

Dentro de las respuestas obtenidas en este análisis, se encuentra que el personal docente cuenta con un bajo nivel de manejo de la plataforma Moodle. Los docentes jóvenes tienen mayor dominio en la plataforma virtual. El personal masculino tiende a utilizar las redes sociales para realizar procesos de enseñanza. El personal femenino manifiesta que carecen de apoyo técnico y capacitación. El personal masculino tiene mayor conocimiento en la herramienta Moodle.

Se evidencia que el personal docente que esta entre 31 y 50 años tiende a utilizar más los motores de búsqueda y el personal docente de 20 a 30 años tiende a utilizar la plataforma Moodle.

Imagen 1. Herramientas informáticas utilizadas en la docencia

Herramienta	Porcentaje										
	Total	Género		Valor *p*	Edad			Valor *p*	Tipo de contrato		Valor *p*
		M	F		21 a 30	31 a 50	51 a 75		Planta	Cátedra	
Blogs	15.4	12.8	19.3	0.4906	11.1	13.9	23.0	0.6862	10.2	23.1	0.165
Correo electrónico	92.3	89.7	96.1	0.3498	100	90.7	92.3	0.6469	92.3	92.3	0.999
Motores de búsqueda	72.3	76.9	65.4	0.3160	66.7	79.1	53.9	0.0461	71.8	73.1	0.911
Redes sociales	29.2	38.4	15.4	0.0451	22.2	32.6	23.1	0.7212	28.2	30.8	0.827
You tube	1.5	0.0	3.9	0.2232	0.0	2.3	0.0	0.7797	0.0	3.9	0.223
AVA (Moodle)	10.7	7.7	15.4	0.3347	22.2	6.9	15.4	0.0307	12.8	7.7	0.521

Fuente: Propia – Basado en el análisis de las plataformas de evaluación

Otro dato para tener en cuenta es que el personal docente con un 13.8% participo en el curso de evaluación integral del aprendizaje y tan solo el 6.2% participo en la formación

[49] Rodríguez, H., Restrepo, L.F. Aránzazu, D. (2016) Desarrollo de habilidades digitales docentes para implementar ambientes virtuales de aprendizaje en la docencia universitaria. Sophia 12 (2):261-270.

de aprendizaje colaborativo. En la formación de modelo didáctico operativo, se cuenta con un 6.2% y el 78.5% manifiesta no haber participado en ningún curso de formación.

Imagen 2. Participación docente en cursos de formación permanentes del Programa de integración de tecnologías a la docencia

Tipo de programa	Total	Valor de p		
	%	Géneros	Edad	Tipo de contrato
Moodle básico para docentes	46.8	0.2302	0.1453	0.0873
Taller de Moodle avanzado	3.0	0.2476	0.1234	0.0873
Formación de tutores virtuales	6.0	0.5347	0.7170	0.5347
Ambientes virtuales de aprendizaje	10.6	0.8727	0.5073	0.0762
Tratamiento de imágenes digitales	4.6	0.8129	0.4869	0.8129
Taller de medios (audio y video)	4.6	0.3421	0.4497	0.8129
Taller de herramientas de autor	4.6	0.8129	0.1155	0.8129
Taller de herramientas web 2.0	6.1	0.5347	0.7177	0.5347

Fuente: Propia – Basado en el análisis de las plataformas de evaluación

En la imagen 3 se analiza la habilidad del personal docente respecto al uso de la plataforma Moodle, se muestra que hay un nivel aceptado sobre el manejo de la herramienta, en la cuestión de manejo de herramientas y vínculos a páginas web, además de ello muestran un nivel de adaptación favorable respecto al manejo de cuestionarios y la realización de banco de preguntas.
En relación con la elaboración de tareas, recepción de talleres, foros y actividades similares se evidencia que los conocimientos adquiridos son nulos.

Imagen 3. Habilidades docentes en el uso de Moodle

Géneros*

Herramienta	Habilidad (%)										Valor de p
	1		2		3		4		5		
	M	F	M	F	M	F	M	F	M	F	
Foro	25.6	11.5	17.8	11.5	28.2	34.6	20.5	38.8	7.9	3.6	0.146
Recursos para actividades	23.0	11.5	25.6	19.2	28.2	30.7	15.3	26.9	7.9	11.7	0.118
Recursos para información	5.1	0.0	23.1	7.7	28.2	34.6	30.7	42.3	12.9	15.4	0.104
Tareas	25.6	19.2	23.0	7.7	23.0	26.9	12.8	30.7	15.6	15.5	0.191
Cuestionarios	18.0	15.3	28.2	7.7	20.5	26.9	15.4	30.7	17.9	19.4	0.201
Lecciones	38.5	30.7	23.1	15.4	28.2	26.9	5.1	19.2	5.1	7.8	0.179

Edad**

Herramienta	Habilidad (%)														Valor de p
	1			2			3			4			5		
	J	A	M	J	A	M	J	A	M	J	A	J	A	M	
Foro	33	16	23	0	21	8	44	26	38	23	33	0	4	16	0.743
Recursos para actividades	33	14	23	22	26	15	22	30	31	11	23	12	7	16	0.677
Recursos para información	0	2	8	11	21	8	11	28	51	55	37	24	12	18	0.291
Tareas	33	19	31	11	19	14	11	28	23	22	21	23	13	17	0.866
Cuestionarios	22	12	31	44	19	8	11	28	15	11	23	12	18	23	0.334
Lecciones	55	32	31	22	21	15	11	33	23	12	9	0	5	16	0.237

Tipo de contrato***

Herramienta	Habilidad (%)														Valor de p
	1			2			3			4			5		
	P	O	C	P	O	C	P	O	C	P	O	P	O	C	
Foro	20	15	19	10	20	23	33	15	27	30	35	7	15	8	0.682
Recursos para actividades	18	20	19	18	20	31	35	30	19	26	20	3	10	19	0.902
Recursos para información	5	5	0	13	20	23	36	30	23	33	30	13	15	16	0.692
Tareas	23	25	23	23	25	8	26	35	23	23	10	5	5	31	0.091
Cuestionarios	18	20	15	18	30	23	31	25	12	21	15	12	10	27	0.376
Lecciones	31	40	42	26	20	12	31	30	23	12	7	0	3	15	0.599

Fuente: Basado en el documento - Desarrollo de habilidades digitales docentes para implementar ambientes virtuales de aprendizaje en la docencia universitaria

En relación con el uso de la plataforma Moodle, se evidencia que el 72.3% de los docentes no tienen ningún curso montado en la plataforma y se manifiesta que es por falta de capacitación, donde se muestra que el personal femenino es quien se ve más afectado a la hora de elaborar contenidos. Además, el personal joven es quien más se muestra más capacitado y afianzado en el manejo de la herramienta. El personal adulto manifiesta que la falta de apoyo técnico dificulta el montaje de herramientas en la plataforma.

Imagen 4. Razones de los docentes que no tienen su curso en Moodle

Herramienta	Porcentaje										
	Género		Valor de p	Edad			Valor de *p*	Tipo de contrato			Valor de *p*
	M	F		21-30	31-50	51-75		Planta	Ocas.	Cátedra	
Falta de capacitación	25.6	26.9	0.912	44.4	23.2	23.0	0.041	20.05	35.5	34.6	0.412
Falta de confianza en el manejo de Moodle	15.3	7.7	0.362	22.2	9.3	15.3	0.536	10.2	15.6	15.6	0.734
Desconocimiento de las herramientas de Moodle	12.8	19.2	0.496	44.4	9.3	15.3	0.028	5.1	31.2	30.8	0.034
Falta de apoyo técnico para elaborar contenido	12.8	30.7	0.043	22.2	16.2	30.8	0.523	23.1	15.8	15.4	0.326
Falta de apoyo técnico para montar materiales en la plataforma	12.8	19.2	0.496	22.2	6.9	38.4	0.012	17.9	12.3	11.5	0.287
Falta de asesoría sobre utilidad de Moodle en la docencia	12.8	7.7	0.521	22.2	9.3	7.7	0.492	7.9	15.7	15.4	0.084
Falta de tiempo para recibir capacitación y elaborar contenidos	12.8	19.2	0.495	0.0	20.9	7.7	0.206	17.9	12.8	11.5	0.0519

Fuente: Basado en el documento - Desarrollo de habilidades digitales docentes para implementar ambientes virtuales de aprendizaje en la docencia universitaria

En la imagen 5 se evidencia que en los servicios básicos de apoyo requeridos por los docentes para el montaje de cursos en la plataforma Moodle, seguido de falta de asesoría para subir y documentar presentaciones. El personal de planta manifiesta a través de la encuesta que no requiere asesoría en el diseño del curso en el manejo de la plataforma Moodle.

Imagen 5. Servicios básicos de apoyo requeridos por los docentes para el montaje de cursos en Moodle

Servicio	Porcentaje										
	Género		Valor de p	Edad			Valor de p	Tipo de contrato			Valor de p
	M	F		21-30	31-50	51-75		Planta	Ocas.	Cátedra	
Capacitación en manejo general de Moodle	56.4	57.6	0.91	77.7	53.5	53.8	0.40	53.8	32.5	61.5	0.42
Capacitación específica en uso de herramientas	46.1	51.4	0.24	44.4	53.5	52.8	0.88	48.7	57.6	57.6	0.54
Asesoría para realizar el diseño instruccional del curso	51.2	53.8	0.82	66.6	46.5	61.5	0.42	41.1	70.9	69.2	0.04
Asesoría para el desarrollo de contenidos de texto y diapositivas	41.1	30.7	0.44	33.3	36.5	53.8	0.37	30.7	45.2	46.1	0.38
Apoyo para ajuste de contenidos a normas sobre derechos de autor	69.2	42.3	0.03	55.5	60.4	61.5	0.90	56.1	63.2	61.5	0.48
Apoyo para el montaje de recursos a Moodle	64.1	46.1	0.15	66.6	55.8	53.8	0.81	53.8	61.5	61.5	0.462

Fuente: Basado en el documento - Desarrollo de habilidades digitales docentes para implementar ambientes virtuales de aprendizaje en la docencia universitaria

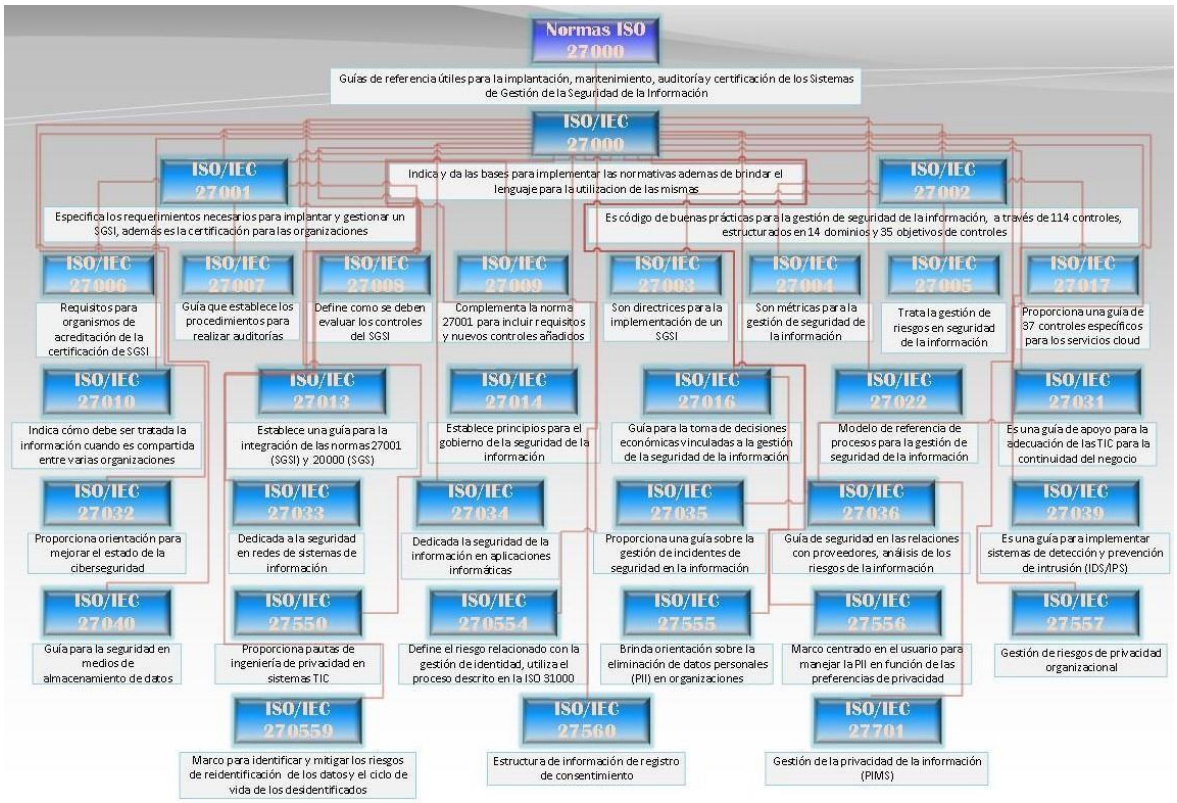
8 DESARROLLO DE ESTRATEGIAS, MODELOS Y RECOMENDACIONES PARA LOGRAR AMBIENTES Y ENTORNOS EDUCATIVOS DIGITALES SEGUROS TENIENDO COMO REFERENCIA LAS ISO 27000

Para la introducción de este nuevo capítulo, se va a determinar el alcance y la forma en la que se va desarrollar el capítulo, siendo claros la norma ISO 27000 es un conjunto de normas bastante grande, que puede ser utilizada para mejorar la seguridad de diferentes formas pues en ella habla sobre distintos peligros informáticos y de información, pero cabe resaltar que no todas las normas se deben ni pueden implementar pues algunas normas son específicas de un campo de trabajo, además se habla de la implementación de un SGSI sistema de gestión de seguridad de la información, la cual puede ayudar realmente a implementar un sistema seguro y a su correcta gestión, lo cual hace parte de las estrategias y recomendaciones , pero no es obligación su implementación, también hay que aclarar que en este apartado no se tratará detalladamente las herramientas usadas, pues ya se habló de ellas en capítulos pasados, por lo tanto este capítulo se enfocará en lo recomendado por la normas, enfocándose en el campo educativo, lo que significa que será una explicación o guía como la norma lo explica, de cómo lograr entornos y ambientes seguros utilizando la normativa sugerida en la ISO 27000.

Es importante el aclarar estos aspectos porque en la misma norma nos indica una serie de caminos que se pueden recorrer para lograr dicho objetivo pero esto es solo una serie de sugerencias hasta para lograr la certificación no es necesario implementar todos sus controles, pero si dan una serie de requerimientos básicos por los cuales partir y conforme más avanzamos en el número de normas, logramos formar una estrategia lo suficientemente segura y adecuada a nuestros propios requerimientos, por lo cual es muy general y a la vez especifico, generar porque no importan las herramientas utilizadas habrá un modelo seguro que soportarlo y además unos requerimientos para su uso, también especifico porque todas las normas están diseñadas a apartados específicos y detallados de seguridad, desde la estructura de la organización hasta los datos que se transmiten y almacenan., por lo cual nos deja muy

poco sin tener en cuenta en el plan más que el seguimiento y la retroalimentación basado en el propio uso.

Imagen 6. Normas 27000 Para tener en cuenta



Fuente: Propia. Basado en la norma ISO 27000.

8.1 Desarrollo de entornos seguros

Normalmente cuando se desea implementar un plan o una estrategia de seguridad, es para ayudar a una empresa o en este caso hablando de educación a una institución educativa a desarrollar seguridad, y el primer paso sería realizar un análisis, detallar e identificar cuáles son los puntos más críticos de la organización, para enfocarse en la mejora y mitigación de los riesgos encontrados, aunque finalmente se crea una estrategia conjunta que abarque todos los aspectos relevantes e involucrados en el este objetivo, pues la norma ISO 27000, nos pide más que un estado, una serie de requisitos que se deben cumplir para considerar seguro un entorno o mejor una organización, por ejemplo la norma 27002 nos ofrece una serie de controles y dominios que permiten determinar el estado de seguridad pero solo nos indica que hay que tener en cuenta por lo tanto como minimizar el riesgo y enfrentarlo, por lo tanto la descripción de un problema así que solo quedaría seguir las recomendaciones además de tomar decisiones para cumplir con dicho requerimiento equivalente a una configuración segura, para esto tendremos en cuenta una serie de normas de la familia ISO, con esto

desarrollaremos una serie de políticas, recomendaciones y acciones a seguir para cuando se decida realizar un plan de acción general cubra todo lo relacionado con la seguridad de las organizaciones.

La ISO es un estándar de normas y la ISO 27000 define las normas relacionadas con sistemas de gestión de seguridad de la información, tanto la norma 27001 como la 27002 se utilizan para la implementación de los SGSI describen una serie de controles que no son necesariamente obligación implementar en su totalidad pero como la norma ISO 27001 es certificable indica que a pesar de no ser necesario implementar todos se debe justificar el no uso de aquellas que no serán implementadas, para tener dar seguridad comprobada se recomienda certificarse pero no es lo que se busca en esta ocasión específicamente, para conseguir esto hay auditorias que dan constancia sobre los controles de seguridad implementados su estado y así conseguir la certificación.

comenzando la norma 27001 la compone 10 puntos a desarrollar y las 10 fases para su implementación.

Tabla 9. Norma 27001 Puntos

NOMBRE	DESCRIPCIÓN
1. Alcance y campo de aplicación	Indica la aplicabilidad de la norma y de cómo usarla, teniendo en cuenta el estado actual.
2. Referencias normativas ISO 27000	Hace referencia a la norma ISO 27000, generando una visión general de los SGSI y la metodología PHVA.
3. Términos y Definiciones	Ofrece una descripción y definición referente al vocabulario utilizado e incluido en el documento de la ISO 27000.
4. Contexto de la organización	En la organización se debe de controlar todos los procesos internos y externos para tener en cuenta la influencia de los resultados en la seguridad, como también entender las necesidades, su alcance, los límites y la capacidad.
5. Liderazgo	Los directivos de la organización deben ser los encargados de llevar y gestionar el SGSI, asegurando el cumplimiento de las normativas, velando porque la disponibilidad de los recursos, realizando la documentación correspondiente y cumpliendo con los objetivos contemplados, realizando las correspondientes asignaciones y responsabilidades, además de promover el mejoramiento continuo.
6. Planificación	Se deben de definir en la organización, la acciones a tomar para mitigar o tratar los diferentes y posibles riesgos, con el uso de metodologías para la clasificación, el análisis y la valoración de estos, creando controles de seguridad basado en los criterios de seguridad, para así mitigar los riesgos en los procesos, definiendo los objetivos de seguridad y los planes para conseguirlo.
7. Soporte	Para dar soporte y seguimiento, la organización debe asegurar los recursos garantizando su funcionalidad, asignando las responsabilidades de cada persona y sus labores, también debe aplicar las políticas y concientizar sobre ellas, fomentando siempre la mejora continua, además de administrar y gestionar la cuestión documental de la información de la organización.
8. Operación	Se debe hacer una planeación de los procesos y actividades, además de dejar documentado todo por parte de la organización, incluyendo análisis de

	riesgos y planes de mitigación o respuesta.
9. Evaluación del desempeño	Se debe encargar la organización de realizar evaluaciones de desempeño para garantizar la eficiencia de la seguridad de la información y la eficiencia de las intervenciones y mejoras del SGSI por medio de auditorías programadas por parte de las directivas.
10. Mejora	Se deben crear planes de acción tanto preventivas como correctivas en donde la organización responda de manera oportuna y eficiente ante las no conformidades y garantice las acciones de mejora continua.

Fuente: Propia. Basado en la norma ISO 27001

Tabla 10. Norma 27001 Fases

FASE	DESCRIPCION
Fase 1 Auditoria inicial ISO 27001 gap analysis	Consiste en realizar un análisis de deficiencias la cual se puede considerar una auditoria inicial del estado actual de los controles o requisitos de la norma
Fase 2 Análisis del contexto de la organización y determinación del alcance	En esta fase se establece el contexto del SGSI en cumplimiento con la norma, alineándolo con las necesidades y requerimiento s de la organización.
Fase 3 Elaboración de la política. objetivos del SGSI	Se debe crear una política de seguridad que cumpla como requisito de la norma, considerando los objetivos de la organización. Además de implementar un objetivo general que genere iniciativas que conduzcan al cumplimiento del SGSI.
Fase 4 Planificación del SGSI	En esta fase de planifican las actividades necesarias, como el inventario de activos, catálogo de amenazas, valoración de las amenazas para la seguridad de la información, análisis de riesgos, evaluación de riesgos, plan de tratamiento de riesgos y selección de controles con la declaración de aplicabilidad.
Fase 5 Documentación del SGSI	En esta fase se debe generar y construir la documentación adecuada del sistema de gestión, evidenciando todo lo realizado y considerado.
Fase 6 Implementando un SGSI	Esta es la fase de implementación en donde

	se pondrá en marcha los controles de seguridad a los procesos de la organización, previamente identificados priorizados y escogidos.
Fase 7 Comunicación y sensibilización SGSI	En esta fase se hace especial relevancia a los procesos de cultura segura, lo cual quiere decir que indica las pautas para la comunicación e interiorización de las acciones tomadas e implementadas buscando concienciar al personal involucrado.
Fase 8 Auditoría interna según ISO 27001	Como su nombre lo indica se trata de realizar auditorías internas, según la norma ISO 27001:2013 se deben programa y realizar auditorías internas para la revisión del SGSI y estar al tanto de su estado para lograr retroalimentar su implementación y crear planes de mejora.
Fase 9 Revisión por la dirección según ISO 27001	Este es otro requisito de la norma y se trata de una revisión a cargo de la dirección, en donde se evalúa el SGSI desde el punto de vista de la dirección de la organización.
Fase 10 El proceso de certificación ISO 27001	Tal como su nombre lo indica es la última fase y el momento en donde se busca la obtención de la certificación, para esto se necesita contactar con una entidad acreditada o especializada en la expedición de estos, la cual programará una o varias auditorias en donde pondrá a prueba la implementación del SGSI y su eficacia en la organización para con esto determinar si puede certificarse.

Fuente: Propia. Basado en la norma ISO 27001

Para esto como previamente se ha mencionado se realiza para una organización o entidad especifica, y se trabaja con base a su estado, se plantea e implementa una solución, la cual también será revisada para establecer su nivel y así llegar a un nivel de

madurez avanzado en cada uno de los controles escogidos, y ofrecer seguridad que es su objetivo.

A continuación, se hará un desarrollo más específico de cada una de las normas y su utilidad o importancia en el proceso de implementación de seguridad.

Norma ISO 27003
Esta norma orienta sobre los aspectos de gestión y sobre el uso del modelo (PHVA) planificar, hacer, verificar y actuar, para la adecuada implementación de la norma ISO 27k en sus organizaciones, el estándar se complementa y se basa en otras normas como la ISO27000, ISO 27001, ISO 27004, ISO 27005, ISO 31000 e ISO 27014.

Norma ISO 27004
Esta norma brinda orientación sobre la especificación, el uso de técnicas de medición y utilización de métricas para determinar la eficiencia de un SGSI e implementación de la norma ISO 27k, lo cual es muy importante para verificar su correcto uso y obtener los resultados que se desean por tanto la implementación de la norma es vital para la implementación.

Norma ISO 27005
Esta norma ofrece directrices para gestionar los riesgos de la seguridad de la información, para así hacer una correcta y satisfactoria implementación del SGSI, brindar seguridad y aplicarla enfocándola en los riesgos, todo esto ayuda a la organización a afianzar sus procesos de evaluación de riesgos y a generar más control sobre su esquema organizacional.

Norma ISO 27007
Esta norma específica las directrices para la auditoria de SGSI dirigida para las organizaciones que las realizan interna o externamente, orienta como y que se necesita al realizar una auditoría, con lo cual al implantar una SGSI y velar por su correcto funcionamiento, aplicación e implantación, la mejor manera de saberlo es con una auditoria, y teniendo en cuenta lo necesario, se puede capacitar para la realización de auditorías internas para la verificación.

Norma ISO 27008
En esta norma nos brindan un informe técnico para la evaluación de la implementación de los controles del SGSI, son directrices para auditar los controles técnicos de seguridad, esto nos sirve para mantener un control sobre los estándares

implementados y analizar el estado en el que se encuentran para así tener mejores resultados, además de más confiables.

Norma ISO 27009

Esta esta norma describe los requisitos para el uso de la norma ISO 27001 y su aplicación en sectores específicos además de explicar cómo incluir controles adicionales, sin que estos entren en conflicto con los de la norma ISO 27001, lo cual sirve para realizar una especificación al implantar los controles y ajustarlos al sector de la organización y a su sector de ser necesario.

Norma ISO 27010

En esta norma se dan las directrices para implementar la gestión de la seguridad de la información para comunicaciones intersectoriales e interorganizacionales, que corresponde a implementación, mantenimiento, mejoras y protección en el intercambio de información, y como en algunas situaciones se tiene acuerdos con entidades externas con las cuales se intercambia o comparte información es importante aplicarla.

Norma ISO 27013

Esta norma brinda una guía en la implementación integrada de la ISO 27001 y la 20000-1, para organizaciones que quieran alinear un sistema integrado de gestión de servicios de TI y seguridad de la información, para una organización que desea implementar estándares para la seguridad, es importante apoyarse en otras normas que consoliden una buena gestión y como estas se pueden alinear gracias a la orientación brindada por esta norma es muy factible y de utilidad su uso.

Norma ISO 27014

En esta norma nos brindan apoyo y guía en el desarrollo y uso de la gobernanza de la seguridad de la información (SIG), con el fin de dirigir y controlar los procesos del sistema de gestión de seguridad de la información, con esto se logra eficacia en la dirección de la organización en la seguridad de la información, algo fundamental para una buena gestión y un integro progreso.

Norma ISO 27016

Esta norma nos proporciona un informe técnico sobre la economía organizacional para la protección y valoración de los aspectos financieros concernientes a la seguridad de la información, lo cual es de vital importancia en una organización pues consiente las consecuencias contextualizando las decisiones y exponiendo su resultado, tomando los requisitos competitivos de sus recursos, para una correcta utilización y distribución.

Norma ISO 27017

Esta norma define un conjunto de prácticas para controles de seguridad de la información para el uso de servicios en la nube, son especificaciones técnicas que permiten implementar un estándar que permita tanto a clientes como a proveedores gestionar la seguridad de la información, ya que se utilizan servicios y se tiene servicios activos, debemos aplicar esta norma que nos permitirá implementar controles necesarios basado en las evaluaciones de riesgos correspondientes a este servicio.

Norma ISO 27022

Esta norma nos brinda orientación para la gestión de la seguridad de la información con un modelo de referencia de procesos (MRP), así con esto se alinean las normas desde la operación de los procesos SGSI, por lo cual sirve para que la organización al implantar las normas pueda orientarlas también a la parte operativa y a sus procesos correctamente.

Norma ISO 27031

En esta norma se dan las directrices para la adecuada utilización de las TIC y así asegurar la continuidad del negocio, define los principios y conceptos del uso de las tecnologías de la información y comunicación orientadas a un apropiado uso en pro del progreso de la organización, algo muy importante para las instituciones que quieran tener un progreso en su manejo y gestión para su organización y proporcionar continuidad a sus actividades.

Norma ISO 27032

Esta norma proporciona las directrices para mejorar la ciberseguridad, tomando en cuenta la seguridad de la información, la seguridad en las redes, la seguridad en internet y la información de protección de infraestructuras criticas (IPIC), está de más explicar porque esta norma es tan importante en cualquier organización que desea implantar estándares que ayuden a mejorar su estado de seguridad de manera íntegra en su organización, pues cubre lo básico para unas prácticas seguras en el ciberespacio, preservando los pilares de la información, que son confidencialidad, integridad y disponibilidad, fundamental en cualquier espacio seguro.

Norma ISO 27033

Esta norma está dirigida a la seguridad en la gestión, operación y uso de las redes de sistemas de información, está dividida en partes, en las cuales toca temas diversos relacionados con la seguridad en redes, como conceptos y descripción, directrices para su diseño y posterior implementación, escenarios de amenazas, técnicas de diseño y control de problemas, protección de las comunicaciones, seguridad en VPN, acceso por

redes inalámbricas y directrices para la seguridad en redes virtualizadas, todo esto sirve a la implementación de seguridad en las redes sin importar el tipo y siguiendo las ultimas o actuales recomendaciones.

Norma ISO 27034

Esta norma brinda un guía sobre la seguridad de la información en aplicaciones informáticas, está dividida en partes distribuyendo la información de forma estructurada, cuenta con conceptualización, marcos normativos, procesos de gestión en la seguridad de aplicaciones, validación, estructura de datos, protocolos y controles, guía de seguridad para aplicaciones en usos específicos y marco predictivo, todo esto a las instituciones le interesa ya que cuentan con aplicativos los cuales necesitan ser gestionados y asegurados correctamente.

Norma ISO 27035

Esta norma describe un estándar para la gestión de incidentes de seguridad en la información, cubre gestión de eventos, de incidentes y de vulnerabilidades, describe en partes cada una de las fases para identificar e implementar las directrices necesarias, tener un organismo de control y respuesta de incidentes es muy importante y con esto se podrían implementar directrices muy importantes para lograrlo.

Norma ISO 27036

Esta norma proporciona orientación sobre la seguridad en las relaciones con los proveedores, ofrece información sobre la evaluación y el tratamiento de los riesgos de la información y la adquisición de bienes o servicios, por lo cual puede servir para asegurar los contratos y aclarar las obligaciones de cumplimiento y garantizar así el correcto funcionamiento de la organización sin problemas con terceros, por lo menos los relacionados por este tipo de contratación.

Norma ISO 27039

Esta norma ayuda a la selección, implementación y operación de sistemas de detección y prevención de intrusos (IDPS), provee una guía para una correcta implementación de sistemas de detección de intrusos (IDS) y de sistemas de prevención de intrusos (IPS), este tipo de sistemas son necesarios y muy importantes en las organizaciones para conservar la seguridad, con lo cual si se desea tener una buena seguridad en la organización esta norma puede contribuir.

Norma ISO 27040

Esta norma guía acerca de la seguridad en medios y técnicas de almacenamiento, detalla el cómo se puede hacer una mitigación en los riesgos de la organización al implementar un buen método de almacenamiento seguro, se necesita de un medio de almacenamiento seguro por lo cual les serviría a las instituciones implementar esta norma en su organización.

Norma ISO 27550

Esta norma ofrece ayuda a las organizaciones a integrar ingeniería de privacidad en sus procesos, se incluye la ingeniería de la privacidad en los sistemas de la organización para preservar de forma segura la información, esto ayuda a la organización a cumplir las políticas de privacidad de la información al momento de implementarlas y gestionarlas enfocándose en su correcta acción.

Norma ISO 27554

En esta norma se definen los riesgos de la gestión de identidad aplicada a las directrices de gestión de riesgos ISO 31000, por lo cual puede ayudar a implementar y gestionar directrices que ayuden a la identificación de riesgos en la gestión de identidad que puede referirse a la información tanto de los estudiantes como de los empleados (administradores, directivos o docentes) y su exposición.

Norma ISO 27555

Esta norma ofrece directrices sobre la eliminación de información de identificación personal, desarrolla y establece políticas y procesos para la correcta eliminación de PII dirigida a organizaciones, al manejar datos personales e información privada de clientes y proveedores, la organización está obligada a garantizar su confidencialidad y, por lo tanto, la eliminación de estos datos de manera eficiente, con lo cual se puede dar gran uso a esta norma.

Norma ISO 27556

Esta norma establece un marco centrado en el usuario para el manejo de información de identificación personal (PII) basado en preferencias de privacidad, para la implementación de sistemas y mecanismos de control de privacidad, es necesario garantizar el buen manejo de la información personal, por lo tanto al querer un sistema seguro, privado y que resguarde los datos personales de forma eficaz y ya que se maneja este tipo de información, es necesario esta norma para su implementación en la organización.

Norma ISO 27557

Esta norma orienta sobre la gestión de riesgos de privacidad en la organización, guía sobre los riesgos relacionados con el procesamiento de información de alto riesgo como la personal, por lo cual al manejar información personal se necesita implementar este tipo de normas que garanticen una buena gestión de seguridad para cuidar la privacidad.

Norma ISO 27559

En esta norma se proporciona un marco para la identificación y mitigación de los riesgos de la privacidad relacionados con la desidentificación y la identificación permanente, ofrece ayuda en la protección de la información personal y la reutilización de los datos, todo esto puede ayudar a la organización a mantener la seguridad.

Norma ISO 27560

Esta norma estructura la información de registro de consentimiento, consiste en especificar como se debe tratar la información personal registrando el consentimiento de su trato y así respetar el procesamiento de datos privados autorizados, en organizaciones que tengan un intercambio de información personal se necesita un sistema de consentimiento para su correcto trato con las organizaciones aliadas, sin romper el contrato de privacidad.

Norma ISO 27701

Esta norma es una extensión de la ISO 27001 e ISO 27002 en donde especifica lo relacionado con PII y las PIMS, con lo cual se podría describir más como un documento enfocado en establecer, implementar, mantener y mejorar los sistemas de gestión de información de privacidad (PIMS) dentro de la organización, orienta sobre los controladores y procesadores de Información de identificación personal (PII).

8.2 Definición de Políticas, Controles de Seguridad de la Información y Estrategia Final

Tomando todo lo aprendido se pueden utilizar los recursos para crear una estrategia en donde se ponga en práctica todos los detalles y estancias involucradas en la seguridad, para estos en general, se crea un plan de gestión e implementación de seguridad que lo cubra, en el cual se deben especificar políticas a implementar, personal para revisar o auditar el proceso y su gestión, involucrar a los directivos para manejar políticas en

conjunto y que se alineen para los intereses de la organización, revisión constante de la estructura, y muy importante revisar las políticas ajenas o exteriores de empresas con las que se tenga un contacto, al hablar de ambientes online, a menos que se creen especificados para cada institución, se tiene que tener en cuenta las empresas contratadas de las cuales utilizamos sus servicios, teniendo en claro sus términos y condiciones de uso y que no afecte a las políticas objetivos e intención de la organización en cuanto al tema de seguridad e integridad.

Es tan importante la implementación de un sistema seguro de la organización si se van a utilizar recursos externos está claro, pero también cabe la posibilidad de que alguna institución quiera desarrollar su propio entorno virtual, lo cual ocurre, en este caso sería de mucha más importancia, pero no le resta importancia el utilizar la de un tercero, primero se tiene que encontrar seguridad en su entorno local y luego buscarlo en el online, generalmente las empresas que ofrecen sus servicios tienen una estructura muy segura y hasta certificada pero es importante conocerlo y tenerlo claro, alinear todo para que sea un enlace seguro y se pueda ofrecer un servicio de calidad en donde ninguno sea el causante y minimizar el riesgo al que se expone el usuario.

Ahora sin más preámbulo ni más contexto trasladaremos todo lo concebido por la norma 27k, en una serie de reglas o recomendaciones en donde se pondrá todo en práctica y se creara una estructura de seguridad que realmente pueda contener o minimizar al máximo las amenazas en las instituciones o por lo menos tengan la posibilidad de mitigarla cuando surja, además de tener una gestión y administración ordenada y pulcra sobre la cual trabajar, por lo tanto como se venía explicando esta estrategia abarca desde la parte de estructura física hasta la utilización de software de forma segura.

8.2.1 Políticas de Seguridad de la Información

Política de Contraseña segura

Para las contraseñas una vez asignado un usuario el encargado o responsable de dicho usuario debe cambiar dicha contraseña de forma segura luego del primer ingreso, además de seguir las siguientes recomendaciones para evitar que personas no autorizadas tengan acceso:

- Las contraseñas no deben ser intuitivas por lo tanto no debe contener datos personales.
- Las contraseñas deben contar con un mínimo de longitud de ocho caracteres, compuesta por números, letras minúsculas y mayúsculas y caracteres especiales contenida en ella.

- la contraseña y el nombre de usuario debe ser diferente y cumplir con los requisitos correspondientes.
- El usuario debe ser asignado y aprobado por el departamento de TI.
- Tanto la contraseña como el nombre de usuario debe ser único, privado e intransferible, además no se debe tener escrita por lo menos en los lugares de trabajo.
- Se debe cambiar la contraseña cada 3 meses o aproximadamente 60 días o en el caso de ver que se encuentra comprometida su privacidad de algún modo.
- NO reutilizar las contraseñas utilizadas con antelación.

Política de Uso de Controles Criptográficos

Se deben usar controles criptográficos en algunos casos, como en:

- La implementación de seguridad de claves de acceso como: sistemas, datos y servicios.
- La Utilización de medios de almacenamiento externo y transmisión de información restringida, y usada en entornos externos de la organización.

Política de Seguridad con Sistemas Físicos

Los empleados deben ser responsables de cuidar y proteger tanto los activos físicos como de la información de la organización, en especial los asignados a su nombre, teniendo en cuenta recomendaciones como:

- NO dejar el puesto de trabajo, ni dispositivos desatendidos, olvidados o descuidados en sus labores diarias.
- Mantener la seguridad proporcionada por la organización, asegurando la ubicación asignada de cada activo y su integridad.
- Al retirarse o acabar su día laboral asegurarse de apagar todos los dispositivos utilizados de forma correcta.
- De ser el caso de contar con un espacio asignado, velar por su seguridad y mantener cerrado el puesto de trabajo.
- Se deben de asegurar los activos destinados para el almacenamiento de información física, mantener los accesos limitados y el espacio cerrado y apartado del personal no autorizado.
- Se debe capacitar al personal para que reconozcan las acciones consideradas no aprobadas o riesgosas tanto para él como para la organización, su información, su infraestructura o activos y evitar realizarlas.

- Se debe contar con un permiso por parte del área de TI para mover o cambiar de lugar activos de la organización, para verificar las condiciones del traslado y así evitar posibles daños y/o perdidas de algún tipo.
- Se deben de abstener de utilizar equipos considerados en peligro o riesgo de alguna infección o software malicioso y comunicar de inmediato al departamento asignado para tratar con estos temas.
- Solo los encargados y asignados por parte del departamento de TI de la organización tienen permisos para desarmar, revisar, manipular extraer, reparar, destapar o cambiar partes a equipos de la organización.
- La mala utilización de los activos de la organización está prohibida, así como golpear, dañar o usar equipos no asignados con antelación y pertenecientes a otra persona.

Política de Uso de Software Legal

La utilización de software debe estar administrada y solo se podrán utilizar aplicaciones legales adquiridas o con una licencia vigente, además de previamente aprobado por la organización. Solo se puede duplicar el aplicativo si es que está sujeto a los términos y condiciones de uso en la licencia, para la instalación de software se debe tener una aprobación con antelación y permisos del área encargada de TI, la cual asegurar el uso y su alineación con los objetivos de la organización. Por lo tanto, el usuario del aplicativo debe:

- Abstenerse de hacer uso indebido del aplicativo ya sea distribuyéndolo, creando copias, haciendo negocio con este o enajenar sin previa autorización del creador.
- Incentivar a los usuarios al uso de un software no permitido, sin licencia o no autorizado por la organización.
- NO permitir realizar copias de los programas utilizados.
- Se debe tener autorización con antelación para ejecutar 2 aplicativos simultáneamente si no se cuenta con el permiso abstenerse de hacerlo.
- El uso de programas o hardware de monitoreo o administración de procesos y actividades está restringido a únicamente el área de TI y se debe tener autorización.
- Todas las aplicaciones que se pueden usar deben estar aprobadas con anterioridad por el departamento de TI.
- Los servicios o aplicativos de comunicación deben ser autorizadas y avaladas por los encargados del departamento de TI.
- El uso de herramientas que permitan el control remoto debe estar restringido para uso exclusivo de personal autorizado.

- Se debe de abstenerse de usar tanto hardware o software que puedan evitar los controles o vulnerar de algún modo los controles de la organización.
- El parcheo o mod de aplicativos o paquetes de software no está autorizado.

Política de Derechos de Autor

Se debe velar por respetar los derechos de autor tanto de las obras escritas, documentos, entre otros, como en los softwares utilizados. Teniendo en cuenta los siguientes lineamientos:

- El uso de software está restringido y solo está autorizado el uso de licenciados o libres.
- La referenciación debe ser un requisito para la realización de documentación.
- La creación de copias no autorizadas ya sean parciales o totales de artículos, documentos y demás archivos creados por terceros, deben cumplir con las leyes de derecho de autor al usarse o se debe abstener de utilizarlos.
- El uso de la información propiedad de la organización debe ser de uso exclusivo de esta no puede utilizarse de ningún modo esta información de modo personal o sin autorización de esta, y los usuarios que manejen información se deben de limitar a usarla para lo que fue asignado únicamente.

Política de Uso de Internet

El uso del servicio de internet y todas las herramientas utilizadas mediante este servicio deben ser correctamente utilizadas y de forma segura, haciendo que sea eficiente y no provoque baches de seguridad. a continuación, se describen lineamientos para ayudar a cumplir con esto:

- El uso de software o herramientas de hacking están prohibidas.
- La utilización de la información debe ser de único acceso y no se deben publicar en internet ningún tipo de información o documentación.
- Se prohíbe el uso o publicación de material considerado inapropiado, ofensivo, denigrante, y/o irrespetuoso.
- Se prohíbe utilizar aplicativos o herramientas que permitan saltase los controles de internet establecidos.
- Para el uso pleno del servicio se debe usar con responsabilidad social y corporativa además de la cultura segura y velar por la protección de la integridad de la red de la organización.

Política de Uso de Correo Electrónico

Las siguientes son los lineamientos que se deben tener en cuenta al hacer uso de los correos electrónicos:

- Las cuentas asignadas por el personal encargado deben ser exclusivamente para labores del cargo asignado, y no está autorizado la comunicación con cuentas que no sean del dominio de la organización.
- El uso de correo electrónico para él envió de spam o información no relevante debe estar prohibido.
- El uso indebido del correo electrónico como la distribución o consumo de material considerado inapropiado o no aprobado por la organización debe ser prohibido.
- El envío de correos masivos debe ser prohibido.
- Cualquier uso considerado como molesto o indebido no se debe permitir para mantener la cordialidad entre los usuarios.
- Para responder a un correo se debe validar con antelación el historial del remitente para asegurarse que no está siendo expuesto a un desconocido.
- El correo electrónico no debe usarse como servicio de chat o mensajería instantánea.
- Según la ley colombiana un correo electrónico puede valerse como prueba tal como lo hacen los documentos impresos.

Política de escritorio y pantalla limpia

Se debe instruir a los usuarios a no dejar ningún tipo de información sensible, dispositivo de almacenamiento, documento o aplicativo, descuidado o al alcance de otro usuario o desconocido, exponiéndolos, por lo tanto, se debe mantener controlado y bloqueado los equipos que se usan además de mantener un ambiente ordenado y seguro, restringido y delimitado.

ESTRUCTURA

Para la estructura se tiene que definir el concepto, el cual se refiere a la estructura en donde este montada la infraestructura, sus componentes y toda la organización, en este caso nos referimos a la ubicación y el lugar que toma la institución educativa, aunque dicha institución sea más de contenido virtual de igual modo se debe tener él cuenta el lugar físico.

Condiciones del lugar

para empezar, se debe tener todos los datos del lugar, en qué sector se encuentra, ciudad y país, para tener en cuenta todas las leyes que le apliquen en dicho lugar, también el diámetro que ocupa las instalaciones, el acceso a la ubicación y todo lo que sea relevante de la edificación en sí.

Riesgo y peligros inminentes

Para esta parte es muy importante tener en cuenta que dependiendo la estructura y la ubicación se pueden generar diversos peligros o riesgos, que se realiza analizando y estudiando la zona y el lugar, en donde se tiene en cuenta aspectos como las condiciones meteorológicas el terreno la incidencia de desastre naturales y de delitos, ataques o criminología.

Restricciones

Se tiene que delimitar el área y restringir su paso, para evitar a personas no autorizadas, y se debe monitorear el lugar en caso de algún incidente, por lo tanto, se requiere personal de vigilancia que proteja la estructura y de ser posibles un conjunto cerrado de cámaras para evitar algún tipo de afección además de generar un mayor control de la situación y un registro constante de las actividades.

INFRAESTRUCTURA

Para entender el concepto infraestructura, como su nombre lo indica nos referimos a la estructura interna que conforma a una organización, en este caso toda la infraestructura TI de la institución educativa.

Activos

La gestión de activos es algo muy importante aclarar que nos vamos a referir a dos clases de activos de información y los activos físicos.

Para esto se tiene que hacer una clasificación de los activos, no solo definiendo su tipo sino también su nivel de importancia además de realizar una estimación de riesgos y de priorización en el cual se tenga en cuenta todos los aspectos referentes al activo para su correcta utilización y gestión.

Redes

Para la infraestructura de red se debe tener un claro mapeado o una señalización de la ubicación de todos los equipos pertenecientes en la red, además de realizar un seguimiento o una auditoria en cuyo caso servirá para ver el estado de dicha infraestructura y sus componentes, con esto ofrecer no solo seguridad, sino que también soporta la disponibilidad y el estado de utilidad de los activos.

Área TI configuración y gestión

Es fundamental para los encargados del área TI llevar a cabo o conocer todos y cada uno de los procesos de seguridad, configuración y gestión de los activos de TI, de la infraestructura y estructura en la cual se trabaja, en este caso con los activos ya

clasificados se tiene que ofrecer una seguridad y disponibilidad al usar estos, la red debe estar gestionada y configurada para que funcione sin perdidas ni caídas, y la estructura debe ofrecer resguardo y cabida a todo lo que conforma a la organización.

USUARIOS

Para el control de usuarios también se definen dentro a los usuarios dentro y fuera de la institución haciendo que cada persona que ingrese o que se relacione con la entidad de alguna manera este incluido.

Capacitaciones y responsabilidades

Para comenzar se debe declarar políticas y medidas de seguridad además de control y gestión de los accesos, de los activos, y todo esto quien lo tiene que implementar o tener en cuenta en sus quehaceres diarios son el personal, por lo cual es fundamental crear concienciación, capacitar a todos los usuarios y concientizar sobre su responsabilidad en estos asuntos y para con sus deberes con la institución.

Personal

Las políticas para el personal varían dependiendo del cargo, pero cada uno debe tener claro su rol a desempeñar en la organización, los encargados de igual modo deben de verificar que cada persona desenvuelva su rol de forma correcta, y además tiene claro las restricciones y limitaciones dentro de su rol, para así garantizar la seguridad que ofrece el personal encargado.

SERVICIOS

Con servicios, se refiere a los diferentes servicios a los cuales no solo la institución utiliza sino también a los servicios con los que su personal cuenta o usa.

Proveedores

Para servicios con terceros o acuerdos de servicio con proveedores, se debe tener en cuenta que nivel de seguridad manejan y ofrecen para que con esto se pueda ajustar y alinear con los intereses de la organización y su estructura de seguridad.

Puntos de conexión

Se debe garantizar la seguridad en los puntos de conexión y en la configuración, tanto internos como de externos, para esto la gestión de los encargados de la parte de TI es fundamental, se tiene que poner en contacto con el personal externo para establecer

una conexión segura, y configurar todos los dispositivos de forma correcta y segura dentro de las instalaciones.

Políticas de uso
Se debe asegurar el uso correcto de los activos, de los espacios, y de cada recurso utilizado por la organización, para evitar algún mal funcionamiento o la exposición de alguna vulnerabilidad, esto se debe especificar para cada uno de los activos o ubicación, además de tener en cuenta la estructura interna o roles de usuario.

Política de desarrollo seguro
Para las instituciones que creen su propia plataforma de aprendizaje o tengan una interfaz propia desarrollada, o en desarrollo se deben establecer normas y políticas básicas de seguridad para el desarrollo del proyecto de forma seguro, ofreciendo integridad y confidencialidad al desarrollo.

Ambiente de desarrollo seguro
Es muy importante también asegurar que se tendrá un ambiente bien equipado, tranquilo y seguro en donde se puedan desarrollar los proyectos con satisfacción.

Desarrollo contratado externamente
Para los desarrollos contratados se necesita tener la información del desarrollador y las especificaciones técnicas del desarrollo que se quiere o se está llevando a cabo para que cumpla con las políticas y normativa implantada por la organización.

Tratamiento de información
Para garantizar el correcto uso de la información se debe tener en cuenta aspectos como su uso correcto, su adecuado almacenamiento y una correcta clasificación de la información, teniendo en cuenta aspectos como su prioridad, su nivel de privacidad y confidencialidad.

Datos y reutilización de datos
Se refiere también a la trata de los datos según su clasificación, pero también existen los derechos de autor y los datos confidenciales, por lo cual se deben defender de un mal uso garantizando su integridad y restringiendo su disponibilidad, todo esto para lograr un correcto uso de los datos y su correcta utilización para los fines que especifique o requiera la organización.

Verificación de seguridad con terceros

Se refiere a mantener la seguridad con personas que se relacionen con la organización, pero no pertenezcan directamente a ella, así que cualquier persona o entidad con la que la organización tenga algún contacto debe cumplir con las especificaciones de seguridad que maneja la institución, aunque este o sea ajena a esta.

Verificación de seguridad de las apps

Para asegurar la seguridad en la organización al usar una aplicación se debe tener en cuenta, la seguridad que ofrece o tenga esta y su empresa desarrolladora, para esto se debe realizar un análisis de seguridad, para que se ajuste a la implementada en la organización, y así con esto darle un buen uso sin generar riesgos, por su uso.

Apps de pago

Se debe de tener clara la situación en cuanto a seguridad de la información tanto de la compañía propietaria como de la aplicación, para así alinearla al modelo de seguridad implementado y no crear baches de seguridad por tener políticas incompatibles o inexistentes que generen vulnerabilidad y resulte en una amenaza para la organización. Además de esto se tiene que contemplar los costos para un correcto uso de los recursos de presupuesto, también tener clara las razones del porque se utiliza una de pago y no una free, (para esto se creó un apartado sobre las aplicaciones más usadas y recomendadas después de un estudio en los capítulos anteriores), cuál será su utilidad y condiciones de uso.

Configuración adecuada de cada app

Como ya se infirió anteriormente el uso adecuado de los activos, de las instalaciones y de las aplicaciones es muy importante de eso se trata la seguridad, de hacer un uso adecuado minimizando los peligros y amenazas, pues para el uso correcto de la aplicaciones se debe gestionar su implementación, se deben restringir la instalación y utilización de estas, y se deben configurar de forma segura y que se alinee a la seguridad de la organización además de capacitar al personal que la usa para un adecuado uso.

Teletrabajo

Para las actividades de teletrabajo se deben definir las normas y políticas de uso correcto, se debe capacitar a las personas que utilizan este método y se debe crear una conexión segura con ayuda del usuario para configurar de tal forma la conexión que sin importar en donde se encuentre este igual de seguro que en la misma institución.

9 CONCLUSIONES

- Se ha podido observar en este trabajo como el desarrollo de las tecnologías es tan importante y vital para resolución de problemas que enfrenta la sociedad e influye de manera considerable en las decisiones actuales de tal manera que se le responsabiliza un tema tan vital para la humanidad como la educación.
- Se ha descrito que la educación virtual se trata más de dar una clase a distancia, y mandar los deberes de forma virtual, es la integración de todos los métodos de enseñanza y virtualizarlos de tal forma la formación educativa es integra y de calidad además de la utilización de sistemas de gestión que ayudan también a las instituciones a llevar sus procesos a niveles de gestión superiores e interrelacionados para sacar el mayor beneficio posible.
- Las herramientas que se pueden utilizar en la educación virtual son muy variadas y tienen características que las diferencian, pero todas sirven para un propósito en común que es para ayudar al proceso educativo y servir como apoyo al proceso de enseñanza y como medio de aprendizaje que facilite y contribuya en su proceso a los estudiantes.
- Es importante que en las instituciones educativas puedan garantizar a sus estudiantes, padres de familia y empleados que la información suministrada se encuentre en un lugar seguro; que se manejen las buenas prácticas de seguridad y manejo de la información.

- La norma ISO 27000 permitió ayudar a analizar los aspectos más relevantes para tener en cuenta en la segregación de funciones y gestión de actividades, mediante la seguridad de la información y el procesamiento de datos que se lleve a cabo de manera adecuada.
- Las buenas prácticas, la gestión documental y de seguridad informática, son parte importante a la hora de ayudar a que toda la información manejada en la institución educativa sea asegurada de manera correcta, llevando a cabo protocolos de seguridad y de respuesta inmediata a las vulnerabilidades que se puedan presentar como se explicó en el documento.
- Como se pudo observar, a medida que avanza la tecnología, los ataques a la información se están volviendo más frecuentes, así que es importante conocer las debilidades y fortalezas de todos los estándares, normas y protocolos vigentes, capaces de solventar este tipo de ataques.
- La seguridad de la información es de vital importancia, en este documento se recolecto y analizo el estado de la educación con respecto a el uso de herramientas, aplicativos, y con la ayuda de la norma ISO 27000 se propuso una serie de recomendaciones enfocadas al sector educativo, en la formación de estrategias que cubran las necesidades que las instituciones educativas necesitan para la implementación de un sistema seguro en su organización, lo cual es un requisito para garantizar la seguridad de sus usuarios y miembros.

10 RECOMENDACIONES

Para las instituciones educativas como para cualquier organización se aconseja siempre revisar las normativas y metodologías para la gestión de seguridad de la información y la informática, así pueden implementar políticas y planes de seguridad actuales y normalizados que pueden traerle grandes beneficios aparte del que buscan que es el de la seguridad.

Las herramientas son muchas y pueden variar, pero algo que se recomienda son utilizar las herramientas que integran diversas funciones, que ofrecen en una sola la posibilidad de realizar diversas tareas e integrarlas automáticamente y sin problemas de compatibilidad o inconvenientes que compliquen los procesos, en el documento se da algunas sugerencias que pueden ser adoptadas con mayor detalle.

Se debe tener en cuenta el tipo de herramientas que se manejan, la privacidad que maneja cada una de ellas, la compatibilidad con los diferentes sistemas operativos y dispositivos; dentro de las funciones de cada herramienta, buscar que exista una coherencia y una cohesión en las aplicaciones a utilizar y lo más importante que se respete la integridad de los datos , la información personal de los estudiantes, para así cumplir con las diferentes leyes en Colombia acerca de la protección y buen manejo de los datos de los estudiantes.

La norma ISO 27000 permite a través de sus estándares conocer las debilidades y fortalezas que pueda tener una institución educativa y a su vez permite asegurar toda la información de todas las áreas y aplicaciones que se utilizan en la misma. Se

recomienda a las instituciones educativas y a los encargados de la parte de tecnología, documentar e implementar diferentes técnicas de penetración para asegurar la información de los estudiantes.

11 BIBLIOGRAFÍA Y REFERENCIAS

REFERENCIAS

Adictos al trabajo. Introducción a OWASP. [En línea] 2016. Disponible en: https://www.adictosaltrabajo.com/2016/03/07/introduccion-a-owasp/

Arte y Animación. Conoce las 7 mejores herramientas “gratis” para clases y reuniones virtuales 2021. [En línea] 2021. Disponible en: https://arteyanimacion.com/herramientas-clases-y-reuniones-virtuales/

BIBDIGITAL. Utilización de Hacking ético para diagnosticar, analizar y mejorar la seguridad informática. [En línea] 2007. Disponible en: http://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD1053.pdf

Características. Educación a distancia. [En línea] 2021. Disponible en: https://www.caracteristicas.co/educacion-a-distancia/

CCIT. Hasta 5.000 millones de pesos pierde una empresa por cada ataque cibernético. [En línea] 2019. Disponible en: https://www.ccit.org.co/noticias/hasta-5-000-millones-de-pesos-pierde-una-empresa-por-cada-ataque-cibernetico/

CCIT. Tendencias del Cibercrimen en Colombia 2019-2020. [En línea] 2019. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Computerworld. El sector educativo, acosado por los ciberataques en 2021. [En línea] 2021. Disponible en: https://cso.computerworld.es/cibercrimen/el-sector-educativo-acosado-por-los-ciberataques-en-2021

Cerebriti. cerebriti. [En línea] 2022. Disponible en: www.cerebriti.com

Ecured. Tipos de virus. [En línea] 2020. Disponible en: https://www.ecured.cu/EcuRed:Enciclopedia_cubana

EDTECH. 10 herramientas gratuitas para dinamizar tus clases virtuales. [En línea] 2021. Disponible en: https://pupitres.net/blog/10-herramientas-gratuitas-para-dinamizar-tus-clases%02virtuales

EDTECH. 5 herramientas gratuitas para dinamizar tus clases virtuales. [En línea] 2021. Disponible en: https://pupitres.net/blog/5-herramientas-gratuitas-para-dinamizar-tus-clases%02virtuales

Educación 3.0. 15 bibliotecas on line para docentes. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/bibliotecas-on-line-docentes/

Educación 3.0. 30 herramientas para la comunicación entre familias, alumnos y centro. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-comunicacion-familias-centros/

Educación 3.0. Herramientas colaborativas para el aula. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-colaborativas-aula/

Educación 3.0. Herramientas educativas para organizar, crear y gestionar la labor docente. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/herramientas-educativas-docentes-ahorrar-tiempo/

Educación 3.0. Plataformas gratuitas para aprender a través de videoconferencias. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/plataformas-de-videoconferencia/

Educacion 3-0. Formas gratuitas para aprender a través de videoconferencias. [En línea] 2021. Disponible en: https://www.educaciontrespuntocero.com/recursos/plataformas-de-videoconferencia/

Evirtualplus. WhatsApp como herramienta educativa. [En línea] 2017. Disponible en: https://www.evirtualplus.com/whatsapp-como-herramienta-educativa/

GCFGlobal. El Futuro de la Educación y el papel de GCFGlobal. [En línea] 2021. Disponible en: https://edu.gcfglobal.org/es/educacion-virtual/el-futuro-de-la-educacion-y-el-papel-de-gcfglobal/1/

HUBSPOT. Los mejores 30 programas para videoconferencias en 2022. [En línea] 2021. Disponible en: https://blog.hubspot.es/sales/programas-videoconferencias

HUBSPOT. Los mejores programas para videoconferencia. [En línea] 2021. Disponible en: https://blog.hubspot.es/sales/programas-videoconferencias

IADB. Los Sistemas de Información y Gestión Educativa (SIGED) de América Latina y el Caribe: la ruta hacia la transformación digital de la gestión educativa. [En línea] 2021. Disponible en: https://publications.iadb.org/publications/spanish/document/Los-Sistemas-de-Informacion-y-Gestion-Educativa-SIGED-de-America-Latina-y-el-Caribe-la-ruta-hacia-la-transformacion-digital-de-la-gestion-educativa.pdf

Kaspersky. Ingeniería social: definición. [En línea] 2021. Disponible en: https://latam.kaspersky.com/

MinEdu. La educacion virtual. [En línea] 2017. Disponible en: https://www.mineducacion.gov.co/1780/w3-article-196492.html?_noredirect=1

Sabnis, S., Verbruggen, M., Hickey, J. and McBride, A. J. (2012), Intrinsically Secure Next-Generation Networks. Bell Labs Tech. J., 17: 17–36. doi: 10.1002/bltj.21556. Disponible en: https://revista.seguridad.unam.mx/numero-20/seguridad-inform%C3%A1tica-en-entornos-virtuales

Rodríguez, H., Restrepo, L.F., Aránzazu, D. (2016) Desarrollo de habilidades digitales docentes para implementar ambientes virtuales de aprendizaje en la docencia universitaria. Sophia 12 (2):261-270.

SOPHOS. Sophos State of Ransomware in Education 2021. [En línea] 2021. Disponible en: https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/?msclkid=d137c220c7ef11ec84a62436ee0fc7c7

Tecnológico Monterrey. Educación en tiempos de pandemia: COVID-19 y equidad en el aprendizaje. [En línea] 2020. Disponible en: https://observatorio.tec.mx/edu-news/educacion-en-tiempos-de-pandemia-covid19

UDLA. Instituciones educativas en riesgo informático. [En línea] 2021. Disponible en: https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/?msclkid=5d356becc7e411ec8932597cb1a42872

BIBLIOGRAFÍA

ADOMAITY GALEANO TORRES. UNA MIRADA AL CAMBIO DE LA EDUCACIÓN COLOMBIANA EN TIEMPOS DE PANDEMIA. (2020). https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/3753/Monografia%20-Adomaity%20Galeano.pdf?sequence=1&isAllowed=y

Alan Jafeth Mena Mosquera. Estado actual de la auditoria de seguridad en los sistemas de información de educación superior. (2021). https://dspace.tdea.edu.co/bitstream/handle/tdea/1391/Informe%20Auditoria%20seguridad.pdf?sequence=1&isAllowed=y

ASCUN. VIRTUALIDAD, UN ANTÍDOTO DE LA EDUCACIÓN EN TIEMPOS DE CORONAVIRUS. (2021). https://www.ascun.org.co/noticias/detalle/virtualidad-un-antidoto-de-la-educacion-en-tiempos-de-coronavirus-273

Asociación de Usuarios Sanitas. ASÍ ES LA EDUCACIÓN VIRTUAL EN EPOCAS DE COVID. (2020). http://asociacionusuariossanitas.com/asi-es-la-educacion-virtual-en-epocas-de-covid/

Auditoria2017. Hacking Ético. Corporación Unificada Nacional de Educación Superior, s.f. [Citado 26-mayo-2018]. https://auditoria2017.wordpress.com/hacking-etico/.

BARBERA, E. (2006). Aportaciones de la Tecnología a la e-Evaluación. RED. Revista de Educación a Distancia. Recuperado el 20 de agosto de 2016 de http://www.um.es/ead/red/M6/barbera.pdf

Biblia del programador. Hacking etico101: Como hacer profesionalmente en 21 días o menos. (2017). https://www.bibliadelprogramador.com/2017/06/hacking-etico-101-como-hackear.html.

BID. Ciberseguridad en tiempos de pandemia. (2020). https://blogs.iadb.org/energia/es/ciberseguridad-en-tiempos-de-pandemia/

Bupasalud. COVID19 Coronavirus. (2020). https://www.bupasalud.com.co/salud/coronavirus

Bortnik, S. (s.f.). Revista de Universidad Nacional Autónoma de México. (2021). https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Braulio Fernando Ortiz. ¿Hacking Ético para detectar fallas en la seguridad informática en la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGCI), basado en la Norma ISO/IEC 27001:2005.

Caluña, A. A. Repositorio ESPOCH. (2011). http://dspace.espoch.edu.ec/bitstream/123456789/1726/1/98T00005.pdf

Byte. Nuevos desafíos de ciberseguridad en tiempos de pandemia. (2020). https://revistabyte.es/noticias/desafios-de-ciberseguridad/

CAF. Ciberseguridad energética en tiempos de pandemia. (2020). https://www.caf.com/es/conocimiento/visiones/2020/04/ciberseguridad-energetica-en-tiempos-de-pandemia/

Colaboradores Enter.co. El hacking Ético y su importancia para las empresas. Enter.co, 2014. [Citado 25-mayo-2018]. http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

CEGEP. Educación virtual: origen, ventajas y retos. (2021). https://cegepperu.edu.pe/2021/01/31/educacion-virtual-origen-ventajas-y-retos/

CEIPA. Educación virtual en tiempos de COVID-19. (2021). https://ceipa.edu.co/blog/acerca-de-ceipa/educacion-virtual-en-tiempos-de-covid-19

CENGAGE 27 plataformas virtuales educativas gratuitas (2020) https://latam.cengage.com/27-plataformas-virtuales-educativas-gratuitas/

CodeJobs. Seguridad informática es una vulnerabilidad. (2012). https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Digiware. Ciberseguridad en la educación: conozca los nuevos retos cibernéticos del sector educativo. (2021). https://www.digiware.net/post/ciberseguridad-en-la-educaci%C3%B3n-conozca-los-nuevos-retos-cibern%C3%A9ticos-del-sector-educativo

El Espectador. Tres retos de la educación virtual en Colombia. Flavia Morlachetti. (2021). https://www.elespectador.com/especiales/tres-retos-de-la-educacion-virtual-en-colombia/

El espectador-1. Los desafíos de la ciberseguridad en tiempos de pandemia. (2021). https://www.elespectador.com/contenido-patrocinado/los-desafios-de-la-ciberseguridad-en-tiempos-de-pandemia-article/

ElPais.com.co. La pandemia 'virtualizó' la educación: lo bueno y lo malo de esta modalidad. (2021). https://www.elpais.com.co/educacion/la-pandemia-virtualizo-la-lo-bueno-y-lo-malo-de-esta-modalidad.html

El tiempo. La educación virtual en Colombia, entre retos, ventajas y desventajas. FRANCISCO CAJIAO. (2020). https://www.eltiempo.com/vida/educacion/como-esta-la-educacion-virtual-en-colombia-530024

Emma Näslund, Alejandro Pareja. ¿Qué es un sistema de información para la gestión de la educación (EMIS) y para qué sirve? (2015). https://blogs.iadb.org/administracion-publica/es/que-es-un-sistema-de-gestion-educativo-y-para-que-sirve/

Eserp. LA CIBERSEGURIDAD PARA LAS EMPRESAS EN TIEMPOS DE COVID-19. (2021). https://es.eserp.com/articulos/ciberseguridad-empresas/?_adin=02021864894

Gov.co. Conoce las medidas y protocolos del gobierno nacional. (2020). https://coronaviruscolombia.gov.co/Covid19/index.html

Ethical Hack. Pruebas de penetración. (28 de mayo de 2017). http://ehack.info/tipos-de-pruebas-de-penetracion/

IESALC. COVID-19 y educación superior: De los efectos inmediatos al día después. (2020). https://www.iesalc.unesco.org/wp-content/uploads/2020/04/COVID-19-070420-ES-2-1.pdf

IESALC. PENSANDO EDUCACIÓN VIRTUAL: IMPACTO DEL COVID-19 EN LA EDUCACIÓN EN COLOMBIA, LA REGIÓN Y EL MUNDO. (2020). https://www.iesalc.unesco.org/2020/04/20/webinar-pensando-educacion-virtual-impacto-del-covid-19-en-la-educacion-en-colombia-la-region-y-el-mundo/

Incibe. Prevenir la fuga de información en el sector educativo. (2017). https://www.incibe.es/protege-tu-empresa/blog/prevenir-fuga-informacion-el-sector-educativo

InGenio. Educación en ciberseguridad: Nuevos retos para educadores. (2021). https://ingenio.edu.pe/blog/educacion-en-ciberseguridad-nuevos-retos-para-educadores/

INTEF. Seguridad del menor en internet. (2021). https://intef.es/tecnologia-educativa/seguridad-del-menor-en-internet/

Inter empresas. Ciberseguridad, más prioritaria que nunca en tiempos de pandemia. (2020). https://www.interempresas.net/TIC/Articulos/320475-Ciberseguridad-mas-prioritaria-que-nunca-en-tiempos-de-pandemia.html

IsoTools. Tips de Seguridad de la Información para instituciones educativas. (2019). https://www.isotools.org/2019/09/03/tips-de-seguridad-de-la-informacion-para-instituciones-educativas/

ITsitio. Ciberseguridad en tiempos de pandemia. (2020). https://www.itsitio.com/co/ciberseguridad-en-tiempos-de-pandemia/

Jayanthi Manikandan. Who is an Ethical Hacking? Simplilearn. [Citado 1-noviembre-2018]. https://www.simplilearn.com/roles-of-ethical-hacker-article.

Jenny Rozo, Omar Suarez. GESTION DE SEGURIDAD DE LA INFORMACION EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA. (2016). https://alejandria.poligran.edu.co/bitstream/handle/10823/659/Rozo%20Suarez%20Proyecto%20trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Legalitas. La usurpación de identidad. LEGALITAS, 2015. [Citado 1-noviembre-2018]. https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad

Magisnet. Los seis riesgos de internet para los centros educativos. (2019). https://www.magisnet.com/2019/11/los-seis-riesgos-de-internet-para-los-centros-educativos/

Maggio, S. Actividades de monitoreo de seguridad interna y externa. Techlandia, s.f. [Citado 25-mayo-2018]. https://techlandia.com/actividades-monitoreo-seguridad-interna-externa-info_194844/.

MENDAÑO, Luis. Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de estado. Quito, 2016. 246p. Trabajo de Grado (Ingeniero en Electrónica y Telecomunicaciones).

Miguel Bragado. PLAN ESTRATÉGICO EDUCATIVO DE SEGURIDAD Y PRIVACIDAD EN LA RED PARA ALUMNOS Y DOCENTES EN LOS CENTROS DE ENSEÑANZA. (2014). https://upcommons.upc.edu/bitstream/handle/2117/78923/95737_mem%C3%B2ria.pdf?sequence=1&isAllowed=y

MinEdu. Sistemas de información para mejorar la gestión. (2021). https://www.mineducacion.gov.co/1621/article-87646.html

Min. Educación. Columna / Educación en tiempos de pandemia y equidad de los aprendizajes. (2020). https://www.mineducacion.gov.co/1759/w3-article-401621.html?_noredirect=1

Min. Educación. Educación virtual o educación en línea. (2017). https://www.mineducacion.gov.co/1759/w3-article-196492.html?_noredirect=1

Movistar. El sector educativo también sufre los efectos de la ciberseguridad. (2021). https://destinonegocio.com/mx/gestion-mx/sector-educativo-tambien-sufre-los-efectos-de-la-ciberseguridad/

Munevar John. ¡Los Niños del Sexo! Pornografía Infantil en Internet. Semana. (2002). https://www.semana.com/vida-moderna/articulo/los-ninos-del-sexo-pornografia-infantil-internet/50667-3

Murillo Garzón Yeimy Camila. Delitos Informáticos y Entorno Jurídico Vigente en Colombia. cameleo, SF. [Citado 1-noviembre-2018]. http://www.it-docs.net/ddata/863.pdf

Neurona. Ciberseguridad en tiempos de pandemia. (2021). https://neurona-ba.com/ciberseguridad-en-tiempos-de-pandemia/

Nohora Malagón, Omaira Figueroa. PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA INSTITUCIÓN EDUCATIVA DE EDUCACIÓN BÁSICA Y MEDIA DELDEPARTAMENTO DE BOYACÁ, BASADAS EN LA NORMA ISO 27001:2013. (2016). https://repository.unad.edu.co/bitstream/handle/10596/11881/24167182.pdf?sequence=1&isAllowed=y

Observatorio. Educación en tiempos de pandemia: COVID-19 y equidad en el aprendizaje. (2020). https://observatorio.tec.mx/edu-news/educacion-en-tiempos-de-pandemia-covid19

OWASP. Top10-2017. [Citado 1-noviembre-2018]. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Ortega, B. M. Auditoria de sistemas de información. Gestiopolis. [Citado 25-mayo-2018]. Disponible en Internet: https://www.gestiopolis.com/auditoria-de-sistemas-de-informacion/

Pacto Global. La Ciberseguridad en tiempos de Covid-19: una perspectiva multi-actor en Colombia. (2021). https://www.pactoglobal-colombia.org/news/la-ciberseguridad-en-tiempos-de-covid-19-una-perspectiva-multi-actor-en-colombia.html

Revista Empresarial. La Educación Virtual: Retos y Desafíos en Colombia. Gisele Eugenia Becerra P. (2017). https://revistaempresarial.com/educacion/virtual/la-educacion-virtual-retos-desafios-colombia/

Real instituto el cano. Ciberseguridad en tiempos de pandemia: repaso a la COVID-19. (2020). REALCANO

SocialeTic. ¿Qué es el hacking ético y para qué sirve? SocialeTic. (s.f.). [Citado 25-mayo-2018]. https://www.socialetic.com/que-es-el-hacking-etico-y-para-que-sirve.html

SciELO. EDUCACIÓN VIRTUAL O VIRTUALIDAD DE LA EDUCACIÓN (2020). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-72382012000200007

SoluzioniTechnology. CÓMO PROTEGER LA SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES EDUCATIVAS. (2021). https://soluzionitechnology.com/como-proteger-la-seguridad-de-la-informacion-en-las-instituciones-educativas/

TelefonicaTech. Ciberseguridad en tiempos de pandemia. (2021). https://empresas.blogthinkbig.com/ciberseguridad-tiempos-pandemia-afectado-confinamiento-seguridad-digital/

Thomson Reuters. Ciberseguridad en tiempos de pandemia: Medidas y precauciones. (2020). https://www.thomsonreutersmexico.com/es-mx/soluciones-fiscales/blog-fiscal/ciberseguridad-em-tiempos-de-pandemia

Tus Abogados y Contadores. Acciones que son consideradas un delito informático en Colombia. (2018). https://tusabogadosycontadores.co/blog/acciones-que-son-consideradas-un-delito-informatico-en-colombia/

U. Javeriana. Educación virtual: realidad o ficción en tiempos de pandemia. Rennier Estefan Ligarretto (2020). https://www.javeriana.edu.co/pesquisa/educacion-virtual-realidad-o-ficcion-en-tiempos-de-pandemia/

U. libre de Cúcuta. LA EDUCACIÓN VIRTUAL EN TIEMPOS DE PANDEMIA. Sindy Gutiérrez, César Díaz. (2021). http://www.unilibrecucuta.edu.co/ojs/index.php/gestionyd/article/view/523

UNESCO. COVID-19 y educación superior: de los efectos inmediatos al día después; análisis de impactos, respuestas políticas y recomendaciones. (2020). https://unesdoc.unesco.org/ark:/48223/pf0000375125

Uniandinos. La Ciberseguridad en tiempos de pandemia: sigue estas recomendaciones. (2021). https://www.uniandinos.org.co/enterate/ciberseguridad-tiempos-pandemia-riesgos-recomendaciones-uniandinos

UNICEF. Educación en tiempos de COVID-19. (2021). https://www.unicef.org/mexico/educaci%C3%B3n-en-tiempos-de-covid-19

Victor S. Manzhirova. Los ocho delitos informáticos más comunes. Tu Experto.com, 2015. [Citado 1-noviembre-2018]. https://www.tuexperto.com/2015/09/12/los-ocho-delitos-informaticos-mas-comunes/

Wikipedia. Educación en línea. (2021). https://es.wikipedia.org/wiki/Educaci%C3%B3n_en_l%C3%ADnea#Desarrollo