UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Escuela de Ingeniería

Maestría en Seguridad Informática

Metodología Escolar en Seguridad de la Identidad Digital para Prevenir el Engaño Pederasta, el Acoso Virtual y el Acoso Sexual Digital

T E S I S

QUE PARA OBTENER EL TITULO DE MAESTRO EN SEGURIDAD INFORMATICA

P R E S E N T A

CHRISTIAN CÉSAR GÁLVEZ CARBAJAL

Ciudad de Lima 2020

Resumen

Esta investigación aportará una metodología que sirva al entorno escolar como instructivo a realizar para agregar seguridad a su identidad digital para prevenir el engaño pederasta, el acoso virtual y el acoso sexual digital.

La metodología propuesta cuenta con tres unidades consecutivas, las cuales se aplican incrementalmente según se va superando los ciclos de estudio, según los niveles académicos, en la educación básica regular.

La metodología propuesta espera aportar el conocimiento necesario para que los escolares puedan saber la importancia de la identidad digital y como protegerla, así como también puedan saber sobre los tres delitos cibernéticos a los que están expuestos y cómo prevenirlos técnicamente.

La metodología propuesta espera como resultado formar jóvenes con cultura digital en la seguridad de su identidad digital, para que puedan afrontar e interactuar de manera responsable en una sociedad digital que conforme pasa el tiempo, es envuelta más y más por la tecnología.

Palabras Clave: Engaño Pederasta, Acoso Virtual, Acoso Sexual Digital, Identidad Digital, Red Social, Seguridad Cibernética

Abstract

This research will provide a methodology that serves the school environment as instructive to be carried out to add security to their digital identity to prevent pedophile deception, virtual harassment and digital sexual harassment.

The proposed methodology has three consecutive units, which are applied incrementally as the cycles of study are passed, according to the academic levels, in regular basic education.

The proposed methodology hopes to provide the necessary knowledge so that schoolchildren can know the importance of digital identity and how to protect it, as well as know about the three cyber crimes to which they are exposed and how to prevent them technically.

As a result, the proposed methodology hopes to train young people with digital culture in the security of their digital identity, so that they can face and interact responsibly in a digital society that as time passes, is more and more enveloped by technology.

Keywords: Grooming, Ciberbullying, Sexting, Digital Identity, Social Media, Cybersecurity

Maestría en Seguridad Informática

Tabla de Contenido

1 Introducción

La Internet a pesar de sus ventajas y de ser parte de la enseñanza en los sistemas educativos, está ocasionando un cambio brusco en los modos de vida, las costumbres y la forma de interrelacionarse de los escolares. Pero no todos los internautas utilizan con buenas intenciones esta maravillosa herramienta de comunicación, hay quienes la emplean para agredir o abusar de otros internautas indefensos que no cuentan con el conocimiento básico para prevenir las malas intenciones cibernéticas, como lo son los escolares; estas malas intenciones son conocidas como delitos informáticos, en el cual un usuario emplea una serie de conductas para atacar al escolar, con el propósito de humillarlo, difamarlo, chantajearlo o abusar físicamente de él.

Para esta investigación se realizó un análisis de los delitos cibernéticos dirigidos a los jóvenes, que circulan actualmente por la Internet, concluyendo que, en base a la media de edad de las víctimas, existen tres principales delitos cibernéticos a los que están expuestos los escolares, los cuales son: *el engaño pederasta, el acoso virtual y el acoso sexual digital*. Este análisis también nos hace observar que la principal razón por la que el escolar se vuelve víctima, es por la falta de conocimiento sobre la protección a su identidad digital, y eso es debido a la falta de conocimiento en temas relacionados con seguridad para el uso responsable del internet, como es el desconocimiento de la existencia de los delitos cibernéticos, desconocimiento del concepto de identidad digital y la importancia en nuestra vida digital, desconocimiento del concepto de cultura digital y uso responsable del internet, y finalmente el desconocimiento técnico básico de seguridad tecnológica en su identidad digital.

Esta investigación propondrá una metodología que ayudará al escolar a mitigar los riesgos de los tres delitos cibernéticos a los que están expuestos. Logrando el escolar poder prevenir técnicamente estos delitos cibernéticos, pudiendo

identificar un intento del delito, reportarlo, escalarlo y eliminarlo, tanto administrativa y legalmente, como también tecnológicamente hablando.

1.1 Antecedentes

Revista UNIR (2020) publicó que el método KiVa es eficaz para combatir los acosos cibernéticos en etapa escolar. Para Finlandia la educación y el bienestar escolar es una prioridad nacional. Por eso se ha desarrollado un innovador método para combatir y prevenir el acoso. KiVa (chulo, guay) es el acrónimo de "Kiusaamista vastaan" (contra el acoso escolar) que se denominan el exitoso programa anti-bullying finlandés originado en la universidad de Turku. El 90% de las escuelas finlandesas ya emplean este método. El programa se inició en el 2007, y hoy en día ya no sólo se aplica en Finlandia, sino que también se ha empezado aplicar en diferentes países como Suecia, Estonia, Bélgica, España, Reino Unido, Nueva Zelanda y se ha evaluado también en otros como Francia e Italia. De esta manera se está pudiendo comprobar el éxito fuera de Finlandia. Los centros que optan por el método cuentan con un equipo de profesores formados con el programa, que actúan de manera diferente que hasta hoy se venía haciendo, cuando se produce el acoso. En la región de Sur América, es Chile quien se encuentran en proceso de implementar la solución finlandesa, mientras que Colombia y Argentina se encuentran en etapa inicial de validación del método a su realidad local.

Lo que pretende la metodología de KiVa es que los estudiantes no apoyen al acosador y que reporten el acoso (incluyendo los acosos que no están dirigidos para él) en lugar de quedarse callados, si no que los estudiantes apoyen a la víctima y se comunique el acoso. Muchos de los niños hoy en día se callan o incluso apoyan al acosador. Sin embargo, lo que realmente funciona en KiVa es precisamente lo contrario. Que el acosador no reciba ningún tipo de apoyo, sino más bien que la víctima encuentre que los demás están de su parte. y por supuesto que lo comuniquen a los profesores. KiVa está perfectamente testado bajo rigurosos estudios científicos, a diferencia de muchos otros métodos que

hay en el mercado. Los efectos del método KiVa han sido evaluados en numerosos estudios.

El programa KiVa consta de lecciones y trabajos realizados durante el curso. Dependiendo del grado de estudios, será la clase impartida. En la clase se habla de cómo respetar a los demás, de cómo trabajar en grupos. Además, se complementa con un videojuego a través de una plataforma virtual que puede ser utilizado también desde casa. Lo más importante es que los alumnos comprendan la importancia de evitar y detener el acoso escolar. De esta manera los alumnos en vez de apoyar al acosador, apoyarían a la víctima, así transmiten que no están de acuerdo con esas acciones. Otros métodos se centran solamente en la víctima y el acosador, sin embargo, el programa hace hincapié en involucrar e instruir a todos los compañeros, porque en el grupo están los observadores, los que se ríen, los que se callan, etc. Porque el acoso es un fenómeno de grupo. El programa tiene tres unidades, la primera que es para edades de 6 a 9 años, la segunda de 10 a 12 años y la tercera, solamente disponible para Finlandia está diseñada para después de la enseñanza secundaria o media.

El programa incluye una extensión de material para profesores, estudiantes y padres. Está disponible en varios idiomas. Realmente el programa no está indicado para un año, si no que debería ser permanentemente parte del programa "anti acoso" de la escuela.

Parte de la propuesta de esta investigación se basa en lo que pretende KiVa con que los compañeros del escolar acosado no se queden como observadores sin hacer nada, que no se queden callados, sino que reporten y denuncien al acosador. Esta investigación pretende hacer lo mismo, pero a nivel técnico, es decir, que usando las herramientas, opciones y funcionalidades que en la actualidad incluyen las redes sociales, reporten, denuncien y bloqueen al internauta acosador.

1.2 Objetivos

1.2.1 Objetivo General

Analizar los delitos cibernéticos que actualmente circulan por internet e identificar aquellos que están dirigidos para los escolares para establecer una metodología que le sirva al escolar como guía de mejores prácticas que debe realizar para agregar seguridad a su identidad digital con el fin de prevenir los tres delitos cibernéticos a los que están expuestos, los cuales son: el engaño pederasta, el acoso virtual y el acoso sexual digital, proponiendo una metodología orientada al sector de educación escolar, alineada a la seguridad de la identidad digital para mitigar los riesgos relacionados con los tres delitos cibernéticos a los que están expuestos los escolares.

1.2.2 Objetivos Específicos

- Tener conocimiento de la identidad digital y la importancia de agregarle seguridad a ella, para una interacción adecuada en la vida digital, a través de las distintas plataformas digitales, para que finalmente pueda trasmitir ese conocimiento.
- Acoplarse a la sociedad digital de manera segura, aplicando las mejores prácticas en seguridad tecnológica, para interactuar digitalmente de forma responsable en las plataformas digitales y navegar de forma segura a través de la Internet, tanto para propósitos académicos como para temas no académicos.
- Ser consciente de los delitos cibernéticos y de los riesgos a los que se exponen si no sigue la guía descrita en la metodología de esta investigación, para que finalmente mejore la concientización, la comunicación y el aprendizaje del escolar.
- Podrá identificar, desde un principio, un intento de los tres delitos cibernéticos, ya sea que el ataque esté dirigido hacia él o que el ataque esté dirigido hacia algún tercero (por ejemplo, hacia algunos de sus compañeros del colegio), para que finalmente sepa activar los controles

tecnológicos para prevenir, reportar y denunciar al atacante y su delito cibernético cometido.

1.3 Límites y Alcances

Esta investigación abarcará los tres principales delitos cibernéticos que están dirigidos hacia los jóvenes, ya que la edad media de las víctimas, que es entre los 8 años de edad y los 16 años de edad, recae en los escolares, y propone una metodología que agregará seguridad a la identidad digital del escolar para prevenir los tres delitos cibernéticos los cuales son:

- El Engaño Pederasta ("grooming" "online grooming" en inglés): Psicología Velázquez (2016) dice que la media de edad de la víctima ronda entre los 8 y los 12 años (edades en las que se producen un tercio de todas las agresiones sexuales).

  (para mayor información sobre este delito ver: Apéndice A - Glosario de Términos)
- El Acoso Virtual ("cyberbullying" en inglés): Ana Aznar (2017) dice que la edad, tanto de los agresores como de las víctimas, se comprende entre los 11 y los 16 años, en plena etapa donde los niños están formándose como personas.

  (para mayor información sobre este delito ver: Apéndice A - Glosario de Términos)
- EL Acoso Sexual Digital ("sexting" en inglés): Lidia Dóniga Alonso (2018) dice que la edad media de la víctima está entre los 13 y los 16 años (el sexting secundario se practica con más frecuencia conforme aumenta la edad del niño).

  (para mayor información sobre este delito ver: Apéndice A - Glosario de Términos)

Esta investigación está analizada dentro de los límites del territorio peruano, país ubicado en la región de sur américa.

El ministerio de educación de la república del Perú (2010) establece que, en la etapa de educación básica, en la modalidad de educación básica regular, se cuenta con tres niveles de educación:

- **Educación Inicial**: Constituye el primer nivel y atiende el desarrollo integral de los niños menores de seis años, dividido en dos ciclos:
  - ***Ciclo I*:** De 0 a 2 años.
  - ***Ciclo II*:** De 3 a 5 años.
- **Educación Primaria**: Tiene como finalidad educar integralmente a los niños, tanto en el despliegue de sus potencialidades como en la adquisición y desarrollo de conocimientos. Se realiza a través de seis grados, y tienen una duración de seis años, divido en tres ciclos:
  - ***Ciclo III*:** 1er grado y 2do grado (referencial, de 6 y 7 años)
  - ***Ciclo IV*:** 3er grado y 4to grado (referencial, de 8 y 9 años)
  - ***Ciclo V*:** 5to grado y 6to grado (referencial, de 10 y 11 años)
- **Educación Secundaria**: Ofrece a los estudiantes una formación científica, humanista y técnica, afianzando su identidad personal y social. Tiene una duración de cinco años, divido en dos ciclos:
  - **Ciclo VI**: 1er año y 2do año (referencial, de 12 y 13 años)
  - **Ciclo VII**: 3er año, 4to año y 5to año (referencial, de 14, 15 y 16 años)

La metodología propuesta será direccionada por grado y escalonada ascendentemente, por delito cibernético, según la media de edad y en base a los niveles de educación básica regular, los cuales comprenderán desde el ciclo IV del nivel de primaria, hasta el ciclo VII del nivel de secundaria.

1.4 Justificación

Cepal (2016) dice que la nueva era digital dejó atrás viejas y nocivas prácticas, para transformarlo todo. Los recursos que en el pasado estaban celosamente guardados, hoy son compartidos por las instituciones y entidades públicas, que han debido transparentar sus acciones. Es la nueva forma incorporar el

uso de las tecnologías de la información y la comunicación en todo lo que nos rodea.

Los escolares desde que ingresan al colegió interactúan con a la nueva era digital principalmente en dos temas, lo usan en temas relacionados con el colegio como también en temas que no lo están. La actual pandemia que está afrontando el mundo del Covid19 ha hecho que los escolares intensifiquen el uso de ambos temas. La Organización Mundial de la Salud (2020) dice que el COVID-19 (no es un acrónimo, sino un nombre científico establecido para el virus) es la enfermedad infecciosa causada por el coronavirus que se ha descubierto más recientemente. Tanto este nuevo virus como la enfermedad que provoca eran desconocidos antes de que estallara el brote en Wuhan (China) en diciembre de 2019. Actualmente la COVID-19 es una pandemia que afecta a muchos países de todo el mundo. Los coronavirus son una extensa familia de virus que pueden causar enfermedades tanto en animales como en humanos. En los humanos, se sabe que varios coronavirus causan infecciones respiratorias que pueden ir desde el resfriado común hasta enfermedades más graves como el síndrome respiratorio de Oriente Medio (MERS) y el síndrome respiratorio agudo severo (SRAS).

A raíz de la pandemia del COVID-19 se ha impulsado el uso de las plataformas digitales como medios de educación a distancia y virtual en los colegios. Recordemos que los colegios usan la tecnología a menor escala como parte de la enseñanza técnica, por ejemplo, la enseñanza de la mecanografía, de la computadora o de la hoja de cálculo, pero no la aplicaban como herramientas para una educación hibrida presencial-virtual, sin embargo, la pandemia del COVID-19 ha obligado a los colegios a que usen las plataformas digitales como medio y soporte en el cual el colegio se tiene que montar para enseñar a sus alumnos. Valentina Giraldo (2020) dice que las plataformas digitales son soluciones online que posibilitan la ejecución de diversas tareas en un mismo lugar a través de internet, es decir, son espacios en Internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para

satisfacer distintas necesidades. Cada una cuenta con funciones diferentes que ayudan a los usuarios a resolver distintos tipos de problemas de manera automatizada, usando menos recursos.

Los colegios comenzaron a usar herramientas de videollamadas para las clases virtuales, herramientas de redes sociales para los grupos de trabajo, herramientas de mensajería instantánea "chat" para consultas grupales o directas, y herramientas de correo electrónico para las comunicaciones formales como entregas de trabajos. Justo Zaragoza (2020) dice que de los 6,700 colegios privados en Lima-Perú, son 5,000 los que no cuentan con una herramienta tecnológica de educación a distancia, los cuales representan el 74.63%, mientras que 1,700 si cuenta con tecnología, los cuales representan el 25.37%. Este 74.63% se ve obligado a usar alternativas como, por ejemplo, aplicaciones informáticas para comunicación como el Zoom para las clases virtual, el Whatsapp para las comunicaciones informales, el Gmail para los correos electrónicos de comunicación formal, entre otros.

Entonces, para que el escolar pueda acceder a las plataformas digitales, tienen que crearse una cuenta o credenciales en dicha plataforma, es decir, crear un usuario y contraseña para que pueda acceder y usar la plataforma digital. Esta acción ha conllevado a los escolares a tener una identidad digital desde muy temprana edad en el mundo cibernético, creciendo exponencialmente el uso del Internet en los escolares sin haber tenido una adecuada educación en el uso responsable de las plataformas digitales, del internet y principalmente en la seguridad en su identidad digital (Diego Suárez Bosleman, 2019). Una desventaja en iniciarse a temprana edad en el uso de la Internet es la falta de orientación sobre el uso responsable del internet, y sin tener una correcta educación en el colegio sobre el uso seguro de su identidad digital, el escolar queda prácticamente solo para afrentarse contra todos los delincuentes cibernéticos que circulan diariamente por la internet, poniendo en riesgo la identidad digital y posiblemente también la integridad física del escolar, volviéndolo una potencial víctima, que por desconocimiento de la

delincuencia cibernética o por desinformación de como mitigar esos riesgos cibernéticos, se vuelve una presa fácil para:

- *El Engaño Pederasta*, también conocido como abuso sexual en línea (“grooming” “online grooming” en inglés), es una práctica de acoso y abuso sexual del adulto contra niñas, niños, jóvenes y adolescentes, donde el adulto se gana la confianza poco a poco de la víctima, inclusive haciéndose pasar como alguien de la misma edad de la víctima, para finalmente involucrarse en una actividad sexual (Nasheli Escobar, 2015).
- *El Acoso Virtual*, también conocido como acoso cibernético o acoso electrónico (“cyberbullying” en inglés), es la intención de acosar psicológicamente a terceros, entre iguales como niños, jóvenes o adolescentes, es decir, el agresor y la víctima del acoso tendrán relativamente la misma edad y compartirán un contexto social. No incluye acoso o abuso sexual ni intervienen personas adultas en el acoso (Megan Moreno, 2018).
- *EL Acoso Sexual Digital* (“sexting” en inglés), es la actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, ya sea utilizando aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación. Habitualmente se suele realizar de manera íntima, entre dos personas, aunque pueda llegar a manos de muchos otros usuarios si no se respeta esa intimidad, lo que por desgracia es bastante habitual. De ahí su mala fama, a pesar de ser una de las prácticas más comunes en la actualidad para 'subir grados' tras conocer a alguien en una aplicación de cómputo móvil “app” de contactos, por ejemplo, o bien para 'calentarse' en pareja y mantener relaciones sexuales cuando la distancia lo impide o, simplemente, por placer o para escapar de la rutina. (Ana Sierra, 2018).

(para mayor detalle de los delitos mencionados ver: Apéndice A - Glosario de Términos)

Loraine Bosch Taquechel (2019) dice que el peligro de navegar en internet se puede prevenir o mitigar con una buena cultura digital en donde se promueva la seguridad en la identidad digital para contrarrestar los ataques de delitos cibernéticos desde las bases escolares de la sociedad.

1.5 Metodología

Esta investigación propone una metodología orientado para la educación básica regular dentro de los niveles de los grados académicos del sistema escolar, la cual será estructurada y secuencial de manera ascendente, según el nivel de educación que se vaya superando, con el fin de que todas las piezas de la metodología se vayan acoplando según las edades de los escolares.

La metodología propone una guía robusta, pero a la vez sencilla para el entendimiento y aplicabilidad en los escolares, el nivel de complejidad irá desarrollándose de menor a mayor conforme el escolar vaya superando los grados académicos, encajando de esta forma, el desarrollo intelectual del escolar académicamente hablando versus el avance de la metodología tecnológicamente hablando, según como se muestra en los siguientes diagramas de cuadrantes, Diagrama 1 “Engranaje metodológico Primaria” y Diagrama 2 “Engranaje metodológico Secundaria”:

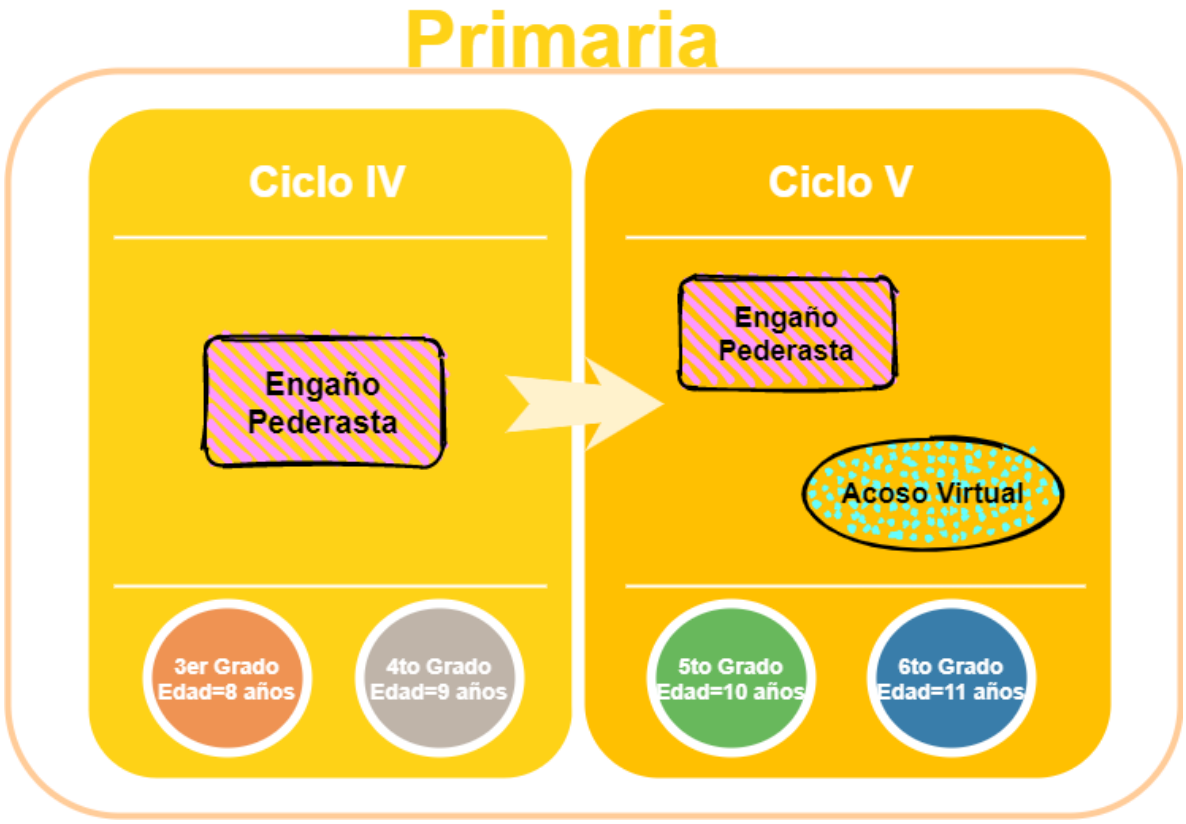

Diagrama 1: “Engranaje metodológico Primaria”

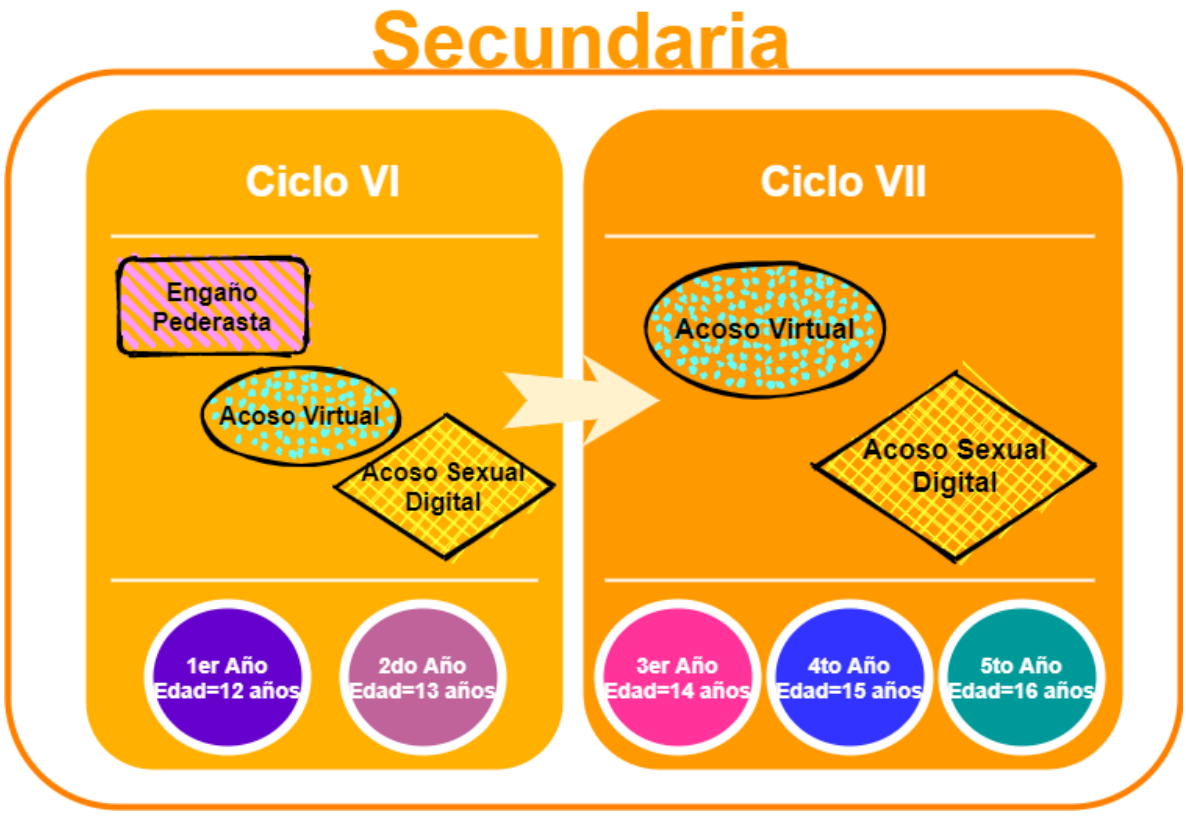

Diagrama 2: "Engranaje metodológico Secundaria"

La metodología propuesta está dividida en tres unidades secuenciales en orden ascendente, estratégicamente segmentadas con base a la media de edad en que se comenten los delitos cibernéticos por nivel educativo, según como se muestra en la siguiente tabla 1 "Delitos cibernéticos en los niveles educativos":

Unidad	Nivel Educativo	Delito Cibernético
Unidad 1	- Ciclo IV de Primaria.	- Engaño Pederasta.
Unidad 2	- Ciclo V de Primaria. - Ciclo VI de Secundaria.	- Engaño Pederasta. - Acoso Virtual. - Acoso Sexual Digital.
Unidad 3	- Ciclo VII de Secundaria.	- Acoso Virtual. - Acoso Sexual Digital.

Tabla 1: "Delitos cibernéticos en los niveles educativos"

Se aplicará en las clases de los niveles educativos de cada uno de las tres unidades, para que el escolar se nutra de conocimiento sobre la seguridad y los delitos cibernéticos, y le sirva como herramienta para evitar, detener y/o alertar sobre el engaño pederasta, acoso virtual y acoso sexual digital. Con esto se espera que el escolar, en lugar de caer silenciosamente en el ciberdelito o alentar al ciberdelincuente, los escolares comiencen a prevenir y/o apoyar a los compañeros víctimas, transmitiendo el mensaje de que no aprueban dichos delitos.

Mitigar los delitos cibernéticos escolares es posible cuando se desarrolla un sentido compartido de responsabilidad, se cambian las normas del grupo, y se inculquen como parte del día a día.

Unidad 1:

- Selección de la plataforma digital: Se debe escoger una plataforma digital oficial y con respaldo o reconocimiento en la industria tecnológica, en base a sus términos y condiciones, la cual garantice que la información personal registrada sea usada bajo marco regulatorios. También, como parte de la selección, se debe tener en cuenta que la plataforma digital a escoger tenga integración de inicio se sesión con las principales redes sociales con las que deseamos interactuar.

  Se sugieren las siguientes plataformas: Google (gmail), Microsoft (outlook), Apple (iCloud Mail), Yahoo! (yahoogmail).
- Creación de cuenta de usuario: Se debe tener una sola cuenta de usuario en una plataforma digital, en el caso que se quiera cambiar de plataforma digital, se debe dar de baja a la cuenta de usuario actual antes de crear la nueva cuenta de usuario. Las aplicaciones o redes sociales con las que interactuaremos deben tener integración con la plataforma digital donde hemos creado la cuenta, esto es para no tener que crear cuentas de usuario en cada aplicación social, sino que re-utilizaremos la cuenta de usuario

única para iniciar sesión con la misma contraseña en todas las redes sociales donde interactuaremos.

La cuenta de usuario única nos dará mayor ventaja al momento de proteger la identidad digital, ya que es más sencillo mitigar una sola cuenta a tener que hacerlo con más de una.

Las aplicaciones o redes sociales a interactuar deben ser sitios oficiales y reguladas, que garanticen la privacidad de la información y que cuenten con las funcionalidades mínimas necesarias para una interacción privada, mínimo debe cumplir las siguientes funciones:

agregar, eliminar, bloquear, denunciar y hacer público a un usuario malintencionado.

- Respaldo de Información: Se debe elegir la red social que tenga integración con funcionalidad de respaldo de información con la plataforma digital en donde se ha creado la cuenta de usuario del escolar. Las plataformas digitales sugeridas incluyen espacio en la nube donde se puedan reguardar información. Cabe mencionar que la información debe ser apta de acuerdo a la edad y funciones del usuario.
- Establecer Identidad Digital: Se debe registrar la información mínima personal, previa aprobación de los padres y/o tutor, se debe establecer el perfil como privado, y se debe relacionar a la identidad de los padres, de manera que la actividad de la identidad digital del escolar sea visible para los padres.
- Establecer Privacidad: Se deben activar todos los parámetros de privacidad que ofrezca la plataforma digital, de manera que solo tu entorno conocido y que tú has aceptado previamente, sean los único en que pueda conocer a detalle tu identidad y actividad digital, esto con el fin de prevenir que potenciales delincuentes cibernéticos obtengan información para cometer sus delitos y acosos.
- Establecer Amistades Digitales: Se debe agregar contactos a la red digital del escolar, solo de las personas que presencialmente conozca, se recomiendo que en esta unidad que los contactos digitales de la red social

del escolar sean sus familiares y amigos o compañeros del colegio, nada más.

- Media de Contactos: En esta unidad la cantidad promedio de contactos que debe tener el escolar debe ser de 50.
- Perfil Privado: Se debe siempre mantener el perfil, la información y la actividad de la identidad digital como restringida y/o privada, para que ningún usuario externo y extraño a nuestra red de contactos pueda curiosear y explorar en nuestra información, con el fin de prevenir que el pederasta obtenga información del escolar a través de la identidad digital del escolar.
- Palabras Peligrosas: Activar alertas sobre palabras comunes que usan los pederastas como modus operandis para engañar al escolar. Estas alertas deben ser configuradas para que se disparen hacia el correo electrónico de los padres y del tutor del escolar.
- Establecer Respaldo de Conversaciones: Se debe activar el respaldo automático de todas las conversaciones para que se guarden en la nube asociada a la cuenta de usuario de la plataforma digital del escolar. Esto con el fin de tener las evidencias del modus operandis del pederasta.
- Instalar y Desinstalar: Se le debe enseñar al escolar que es una software o aplicación o app, y como instalarlos y/o desinstalarlos.
- Desactivar Cámara Web: Si el escolar usa una PC de escritorio no se debe instalar una cámara web, en el caso que use una laptop o tablet o Smartphone, se debe desinstalar y desactivar la aplicación de gestiona la cámara web en el respectivo dispositivo. Esto con el fin de prevenir que un potencial delincuente cibernético tome el control de la cámara web para capturar imágenes sin consentimiento que podría usar como parte del acoso.
- Bloqueo de Intrusos: Al recibir las alertas de las palabras peligrosas o al detectar algún comportamiento extraño en el contenido o imágenes o publicaciones que le envían al escolar, se deberá bloquear al usuario, eliminarlo de la red de contactos digitales del escolar, denunciarlo en la red social, hacer público al usuario e información que se tenga del

pederasta con el propósito que todos los contactos de mi red se enteren del caso y hagan lo propio con ese usuario pederasta en su red (en el caso que también tenga a dicho usuario pederasta como contacto u otro usuario con comportamiento similares), y reportar el caso con sus padres y tutor, para que estos realicen los procedimientos legales respectivos.

- Implementar Congelamiento: Se debe instalar una aplicación de control de tiempo de uso del dispositivo desde donde el escolar ingresa a sus plataformas digitales, esta aplicación tipo "congelamiento" lo que hace es bloquear el dispositivo al instante en que se supera el tiempo configurado como tope. Este tiempo no debe de iniciar durante las clases y no debe finalizar después de las 08:00 p.m., cabe mencionar que el dispositivo debe estar ubicado en un espacio cercana y a la vista de los padres y tutores.
- Adaptación de Entornos: Las aplicaciones de control, se deben adaptar a los entornos de navegación del escolar, teniendo en cuenta que, el escolar podrá usar: sus propios dispositivos, los dispositivos del hogar y los dispositivos del colegio. En ese sentido, cuando estos tipos de aplicaciones de control se desinstale del dispositivo, se llegue una notificación al correo electrónico del tutor y/o los padres.

Unidad 2:

Mantener Dispositivo Seguro: Se debe instalar y tener actualizados los programas contra software malintencionado como virus, malware, spyware, troyano, gusano, etc (no son acrónimos, son nombres establecidos para dichos conceptos; para mayor detalle de los conceptos mencionados ver: Apéndice A - Glosario de Términos). Se debe tener activo la protección en tiempo real, para evitar que algún delincuente informático ataque el dispositivo del escolar con el propósito de obtener información valiosa que le permita cometer el delito cibernético contra el escolar o que pudiera robar y/o suplantar la identidad digital del escolar.

Se debe verificar que el programa a utilizar sea de origen confiable de procedencia oficial y con respaldo garantizado, para asegurarnos no instalar algo malicioso que vulnere la privacidad y seguridad del dispositivo desde donde el escolar accede a sus aplicativos.

- Personalizar la Comunicación: Adicionalmente a que el perfil de usuario debe ser privado, se debe configurar las acciones permitidas por los contactos aceptados, en el perfil de usuario del escolar, esto con el fin de que sea el escolar quien permita que solo sus padres, tutores y amigos cercanos puedan escribirle en modo público y/o en modo privado, con el objetivo que el escolar pueda tener control de con quienes interactuar cibernéticamente y así rechazar los mensajes con contenido inapropiado, exigiendo respeto.
- Control Parental: Instala herramientas de control parental para restringir el acceso de otros usuarios del mismo dispositivo a la información delicada del escolar. También se debe restringir a el acceso a sitios web inapropiados para el escolar.
- Aplicación de Control del Dispositivo: Se debe instalar aplicaciones de control en el dispositivo según tiempo de uso, eso quiere decir que, a mayor tiempo que el escolar use el dispositivo mayor números de controles debe tener el dispositivo, para una mayor supervisión de lo que está sucediendo en el dispositivo. Según como se muestra en el siguiente diagrama 3 “Control del Dispositivo vs Tiempo de Uso”:

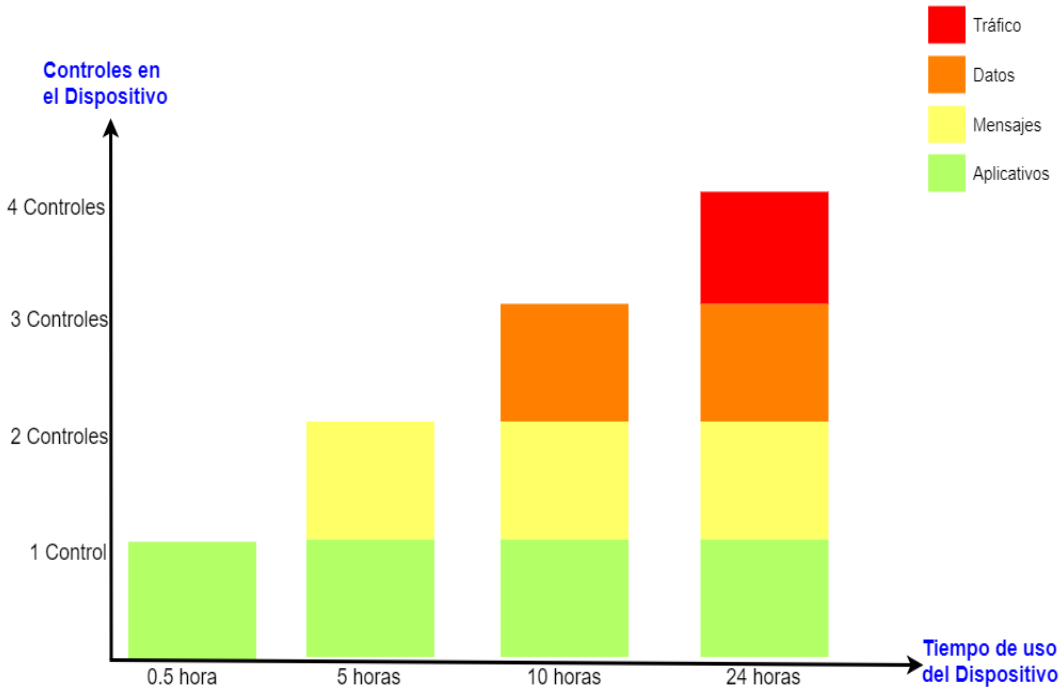

Diagrama 3: "Control del Dispositivo vs Tiempo de Uso"

- Imágenes Propias: El escolar no debe subir fotos ni videos donde él aparece, sin antes solicitar autorización y aprobación de sus padres, para ello se deberá activar la aprobación de etiquetado y el escolar, toda foto o video que suba, deberá etiquetar a sus padres, de manera que a estos les llegará la notificación solicitando si deseas aparecer en dicha etiqueta, esto servirá como alerta para que los padres acepten la publicación de la imagen o indiquen al escolar que elimine la imagen.
- Imágenes Terceros: Adicional a activar todas las opciones de privacidad en la red social, y tener el perfil del escolar en modo privado, no se debe subir fotos o videos en donde aparezcan otros compañeros sin la autorización de los padres de sus compañeros escolares, para ello se deberá activar la aprobación de etiquetado y el escolar, toda foto o video que suba, deberá etiquetar a sus padres y a los padres de sus compañeros escolares, de manera que a todos los padres involucrados

les llegará la notificación solicitando si deseas aparecer en dicha etiqueta, esto servirá como alerta para que los padres acepten la publicación de la imagen o indiquen al escolar que elimine la imagen.

- Información Terceros: No se debe comentar en la sección pública la información privada y/o personal de los compañeros escolares. De encontrar que en otras cuentas digitales están publicando la información privada ajena a ellos, se debe capturar la pantalla y guardar la imagen como evidencia, luego se debe denunciar el caso en la red social con el fin de que esta revise el caso y desactive la cuenta de los usuarios involucrados, finalmente se debe reportar el caso a los padres y tutor del escolar para que ellos analicen el caso y escalen a las autoridades en el caso que se esté infringiendo algún marco legal, como la ley de protección de datos personales.
- Contraseña Segura: Debemos seguir los siguientes pasos para establecer la contraseña con un mayor grado de seguridad,
    - La contraseña debe tener una longitud mínima de 15 caracteres.
    - La contraseña debe contener combinaciones alfanuméricas, incluyendo mayúsculas, minúsculas, símbolo y caracteres extraños.
    - Se debe evitar incluir palabras comunes y de diccionario, porque hacen más vulnerable la contraseña.
    - A las preguntas planteadas en el proceso de recuperación de contraseñas se debe evitar dar información personal conocida por muchas personas.
    - Se debe evitar el uso de contraseñas que hagan referencia a datos fácilmente deducibles como son las fechas de cumpleaños, aniversarios, etc.
    - Se debe evitar el uso de contramedidas forzadas y ampliamente utilizadas como cambiar algunas letras por números similares. El hecho de utilizar simbología similar hace las contraseñas más vulnerables.

    - Se debe cambiar la contraseñe entre 15 y 60 días, se sugiere 45 días, este valor debe estar establecido como tiempo de expiración de la contraseña.

- Navegación Segura: Se debe instalar programas de navegación segura que alerten al escolar sobre sitios sospechosas o links malintencionados, con el fin de contrarrestar que un delincuente informático robe la información privada o robe la identidad digital del escolar. El programa también registrará todos los sitios web con los que interactúa el escolar, con el fin de que los padres puedan obtener un reporte para el seguimiento de la actividad digital del escolar.
- Incremento de Media de Contactos: En esta unidad la cantidad promedio de contactos que debe tener el escolar debe ser de 70.
- Autoprotección: Es deber del escolar entender las opciones de configuraciones de la red social que usa, y tener siempre presente que el mismo deberá utilizarlas de la manera adecuada para aumentar el grado de seguridad, para que tenga claro que la protección en el espacio cibernético empieza por uno mismo. Por ello, es importante que el escolar diferencie entre la información que deben y no deben aportar, que mantengan a salvo su intimidad, manteniendo solo a los contactos que conocen físicamente. El escolar debe comprender que a cuanta más información personal proporcionen a sus contactos, más vulnerable se vuelve.

  Es importante que el escolar entiendo que actuar en la vida virtual dentro de las redes sociales debe ser igual que como lo harían en la vida real, de este modo, podrán comprender que, al igual que no se debe hablar con un desconocido por la calle, tampoco deberán hacerlo a través de internet.
- Frenar Acoso: Ante las primeras manifestaciones de acoso virtual el escolar debe compartir, las publicaciones donde lo acosan, con sus padres, con el tutor o autoridad estudiantil, con los padres del acosador y debe denunciar el caso en la red social, con el fin de cada actor mencionado tome cartas en el asunto y actúa pertinentemente según

normas estudiantiles o legislación vigente. El objetivo de utilizar la misma red social para compartir, mencionar y etiquetar a las autoridades estudiantiles y a los padres de los acosadores, es para que se vean obligados a actuar, ya que se tendrá la evidencia que el escolar victima realizo el escalamiento respectivo.

El escolar debe guardar las pruebas necesarias (fotos, comentarios, mensajes privados), en ningún caso el escolar victima debe responder a los insultos o actos provocadores, puesto que esto conlleva el agravamiento del problema (el agresor estará satisfecho por haberlo provocado y no percibirá ningún castigo). Desde casa, es importante mostrarle una actitud abierta y comprensiva, que facilite la comunicación entre los distintos miembros de la familia.

Este punto aplica tanto para la escolar víctima como también para los compañeros del escolar victima que no son parte de los acosadores, con el objetivo que, si una escolar víctima de actitud pasiva no reporte el acoso, cualquier otro compañero lo podrá hacer, y así acortar el espacio de acción de los escolares acosadores.

- Notificaciones Padres: Los padres debe pertenecer a la red de contactos de sus hijos, y debe activar todas las notificaciones del contacto de su hijo, con el fin de que toda actividad digital, ya sea que el hijo sea quien publique o a él lo mencionen/etiqueten, pueda ser visualizada por sus padres, con el objetivo de que los padres se enteren del acoso de primera mano, y no esperar hasta que el hijo se los cuente para que puedan tomar acción.
- Denegación de Sitios Bullying: El padre del escolar deberá agregar a la herramienta de control parental los sitios web, que son ajenos a las redes sociales pero que son usados para agregar contenido que fomente el acoso virtual, con el fin de bloquear el acceso a dichos sitios web en los dispositivos utilizados por el escolar, para que este no tenga acceso a dicho sitios donde le están haciendo el acoso virtual.

Unidad 3:

- Incremento de Media de Contactos: En esta unidad, sin perder el foco de no aceptar ninguna solicitud de amistad o de agregar contactos a su red digital, de personas que no conoces física y presencialmente, la cantidad promedio de contactos que debe tener el escolar debe ser de 100 porque escolar tiene que entender que la cantidad de contactos superior a dicho promedio, significaría que se está teniendo como contacto a personas que no conoce presencialmente, lo cual aumenta la vulnerabilidad de su identidad digital, y con ello aumenta el riesgo de caer y ceder ante los acosadores.
- Mantener Dispositivo Actualizado: El escolar debe mantener actualizado con los últimos parches de seguridad el sistema operativo del dispositivo, y todas las aplicaciones (software) que tiene instalado en el sistema operativo, a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.
- Utilizar Tecnologías de Seguridad: Se debe instalar las aplicaciones de antimalware, antivirus y antispam, estas representan a las aplicaciones más importantes para la protección del dispositivo ante las principales amenazas que se propagan por Internet.
- Implementar Cortafuegos: Se debe instalar y/o activar un cortafuego que bloquee las conexiones entrantes al dispositivo por parte de otros dispositivos o usuarios extraños. Los sistemas operativos actuales incluyen un cortafuego, el escolar debe activarlo estableciendo la red en la que se encuentra (privada o pública). Con ello se mitiga que el acosador pueda ingresar al dispositivo del escolar para obtener información privada valiosa, la cual podría usar para cometer el acoso.
- Verificar Acceso a Internet: El escolar debe analizar el punto desde donde está conectándose a internet, debe entender la diferencia entre conectarse a internet desde la red de su hogar o del colegio, que conectarse desde una red extraña, como lo son la WiFi pública o de acceso libre y los riesgos que estos conlleva, ya que una red pública no

tiene la protección que una red privada ofrece; por ello, para mitigar el riesgo que se genera en la identidad digital por conectarse a una WiFi Pública se debe realizar lo siguiente:

  - Utilizar una VPN, la cual establecerá la comunicación como un "túnel privado" en donde se cifra todos los datos que pasan por ahí, esto evitará que los delincuentes informáticos intercepten la información privada del escolar.
  - Establecer el cortafuego del dispositivo en modo red pública.
  - No utilizar datos sensibles, se debe tener mucho cuidado con los datos (información, imágenes, audios y videos) que usan mientras te encuentres conectado en el WiFi público, estos datos pueden ser interceptados por el acosador.
  - Desactivar el WiFi del dispositivo cuando no lo esté usando, para evitar que el dispositivo se conecte automáticamente a redes inseguras ya guardadas.
  - Borrar las redes WiFi públicas guardadas en el dispositivo luego de terminarla de usar.
  - Desactivar la funcionalidad de uso compartido del sistema operativo del dispositivo, para evitar compartir los datos del dispositivo con desconocidos que podría ser el acosador.

- Mantener Identidad Digital Privada: El escolar debe mantener su perfil digital en privado, esta acción rutinaria se realiza para prevenir que hayan puesto público el perfil digital del escolar de manera malintencionada, para ello el escolar tendrá que verificar cada fin de semana lo siguiente:
  - Que su perfil digital se encuentre establecido en modo privado
  - Que todas las opciones de privacidad de su red social se encuentren activas.
- Validar URL: Antes de ingresar a la plataforma digital, el escolar debe verificar que la estructura de la URL contenga lo siguiente:
  - El candado de seguridad, el cual contiene el certificado digital que se encargará de cifrar la comunicación dentro del sitio web.

- El protocolo seguro HTTPS, el cual garantiza que el certificado digital se está usando.
- La dirección oficial de la plataforma digital, la cual asegura que se está en el sitio web real de la plataforma digital. Según como se muestra en la siguiente figura 1 “Validación de URL oficial y segura”:

Figura 1: “Validación de URL oficial y segura”

Esto se realiza con el fin de evitar ingresar información personal y sensible en sitios web falsos controlados por el delincuente cibernético, que podría ser utilizado para el acoso.

- Reducir uso de Dispositivo Ajeno: Tratar en lo posible de no usar dispositivos compartidos o de terceros para acceder a las plataformas digitales y/o para gestionar información personal sensible. Sin embargo, solo en casos de emergencia que amerite el uso temporal del dispositivo ajeno se debe aplicar lo siguiente:
  - Cerrar sesión al termino de usar el dispositivo ajeno, para evitar que la sesión se quede abierta y sea aprovechada por la próxima persona que utilice dicho dispositivo.
  - No aceptar que el navegador web recuerde la contraseña. Los navegadores brindan la opción de guardar y recordar las contraseñas que se van ingresando. Pero como el dispositivo es ajeno, no se debe guardar nada, en su lugar se debe introducir la contraseña manualmente cada vez que utilices dicho dispositivo ajeno.

  - Nunca alejarse físicamente del dispositivo ajeno mientras tengas la sesión abierta de la plataforma digital, porque eso generaría un riesgo sobre tu identidad digital.
  - Navega en modo incógnito. Los navegadores web actuales incluyen esta opción, la cual permite navegar sin dejar tantas huellas. OJO: no hace la navegación 100% invisible, pero se navegará con un poco más de anonimato.
  - Utilizar un teclado virtual, este tipo de teclado digital permite escribir los caracteres con el mouse, a través de un teclado que aparece en la pantalla, de esta manera, los malware del tipo keyloggers que pueda tener instalado el dispositivo, no registrará las pulsaciones que se realizan a través del teclado físico.
- Evitar Ejecución de Archivos Sospechosos: No se debe abrir archivos sospechosos o de dudosa procedencia del tipo ejecutable que hayan sido enviados a la plataforma digital. El escolar debe rechazar dichos archivos y proceder a bloquear y eliminar al contacto. Esto porque el archivo podría contener un malware que robe información privada y ponga en riesgo la identidad digital del escolar, que podría ser usada por el acosador.
- Cursos técnicos: Se debe reforzar técnicamente al escolar, para que pueda tener la capacidad de entender y aplicar la metodología en esta unidad.

<u>Evaluación de la metodología propuesta:</u>

En el supuesto de que todos los pasos de la metodología se apliquen correctamente, tanto el escolar, como el tutor y los padres quedarían engranados en la concientización e importancia de aplicar, la seguridad en la identidad digital del escolar, tanto en el colegio, como en casa y en ambientes externos, siendo conscientes de los peligros físicos a los que podrían ser víctimas el escolar por caer en los delitos cibernéticos del engaño pederasta, del

acoso virtual y del acoso sexual digital, quedando demostrado que desde un primer contacto virtual, sin aplicar la metodología propuesta, se puede llegar a un daño físico, ya sea provocado por el delincuente cibernético o por el mismo escolar. Por lo tanto, en el supuesto que lo descrito se cumpla, el escolar tendría el conocimiento para prevenir los delitos, porque los dispositivos, ya sean de la escuela, del hogar o propio, estarán preparados para mitigar el riesgo al que el escolar está expuesto, y alertará al tutor y padres ante posibles ataques, también el escolar sabrá cómo actuar ante un ataque, y finalmente se generará la denuncia respectiva para que las autoridades tomen cartas en el asunto.

1.6 Organización del Documento

Este documento se ha organizado alineadamente a la metodología propuesta, distribuida de la siguiente manera:

- En la unidad 1, se abarca al delito cibernético que ataca a muy temprana edad, el cual es el engaño pederasta, relacionando dicho delito con los ciclos escolares de los niveles académicos, engranando cada instrucción de la metodología propuesta versus los grados educativos que el escolar va superando de manera satisfactoria. Finalmente se resuelven los problemas del desconocimiento de la existencia del engaño pederasta, y de la falta de conocimiento en seguridad de la identidad digital para la prevención del engaña pederasta.
- En la unidad 2, se abarca al delito cibernético del acoso virtual, relacionando dicho delito con los ciclos escolares de los niveles académicos, engranando cada instrucción de la metodología propuesta versus los grados educativos que el escolar va superando de manera satisfactoria. Finalmente se resuelven los problemas del desconocimiento que el acoso virtual sea un delito legislado, y de la falta de conocimiento en seguridad de la identidad digital para la prevención del acoso virtual.
- En la unidad 3, se abarca al delito cibernético del acoso sexual digital, relacionando dicho delito con los ciclos escolares de los niveles académicos, engranando cada instrucción de la metodología propuesta

versus los grados educativos que el escolar va superando de manera satisfactoria. Finalmente se resuelven los problemas del desconocimiento que el acoso sexual digital sea un chantaje catalogado como delito vigente en la legislación, y de la falta de conocimiento en seguridad de la identidad digital para la prevención del acoso sexual digital.

2 Marco Teórico

2.1 Identidad Digital

2.1.1 Los Inicios

El avance tecnológico ha hecho que nuestras vidas y nuestro día a día se mescle con la tecnología, de hecho, habría que integrar dicha tecnología en los procesos de formación de los escolares, en cuanto a formación de personalidad, formación de identidad digital, formación en uso de la tecnología y en formación de seguridad en la identidad digital. El concepto de la identidad digital ha sido un tema constante desde la creación de la Internet, éste necesita dar respuesta a las dos interrogantes de ¿quién soy? ¿realmente soy quien digo ser?, algo que cuya respuesta no resulta nada fácil y más aun teniendo en cuenta que cada momento clave e importante que sucede en Internet se necesita dar veracidad de que la identidad digital sea real, que hacen que la búsqueda de esa identidad y el proceso de formación de la misma sea única en cada momento y único a su vez en cada escolar.

Hablando de lo único, el término identidad está compuesto de dos palabras de origen latino: por un lado, tenemos la palabra "ídem", que significa, igual y por otro lado tenemos la palabra "entitas" que significa entidad, o lo que es lo mismo, ser. Bajo esta premisa la palabra entidad, no sería más que la esencia de algo, haciendo referencia a la unidad y al entero que significa uno, o completo. Siguiendo esta analogía, idéntico significaría igual a uno, a lo entero. Entonces, podemos empezar indicando que el ser humano es único, esto es cierto ya que cada persona cuenta con su propia personalidad, sus propios valores, en el estricto sentido que todos somos diferentes. Por ello, el término identidad es cómo podemos observar un término con doble significado, ya que por un lado hace referencia a lo único, a las características que nos hacen percibir que una persona es única; y por otro lado y a la vez contrapuesto, hace referencia a lo diferente, a las características que poseen las personas que nos hacen percibir que son lo mismo que otras. Por lo tanto,

dada la complejidad del ser humano, podemos decir que lo que denominamos como entero no puede llegar a ser tal cosa sin lo otro, es decir, sin lo diferente. Es decir, aquello que permite la unidad al ser humano es justamente lo otro, lo diferente, lo separado, lo distante. En un sentido hegeliano somos lo que somos y lo que no somos a la vez, puesto que las cosas en un sentido puramente conceptual, pueden ser a la vez ellas mismas y sus contrarias, siendo la contradicción el elemento que completa y da validez a la realidad.

PIFARRÉ, L. (1989) dice que Hegel no elige entre dos cosas, sino que asume a ambas mediante el recíproco pasar de la una a la otra en que consiste la tesis (afirmación del ser), la antítesis (negación del ser), uniéndose sintéticamente para originar la concreción de una tercera cosa, que expresa la verdad completa, derivada de la parcialidad unilateral de la tesis y la antítesis.

Referente a la era 2.0, Íñiguez (2001) dice que la identidad es, por encima de todo, un dilema. Un dilema entre la singularidad de uno/a mismo/a y la similitud con nuestros congéneres, entre la especificidad de la propia persona y la semejanza con los/as otros, entre las peculiaridades de nuestra forma de ser o sentir y la homogeneidad del comportamiento, entre lo uno y lo múltiple.

El proceso de formación de la identidad, se realiza en el colegio, no es un concepto que sólo afecte al escolar, sino que como ser que está inmerso en una sociedad está rodeado, influenciado, atraído, desencantado, y por eso, el proceso de formación de la identidad digital personal tiene que ver con lo individual, pero también con todo lo que le rodea. Es por esto que la identidad personal no es sólo individual sino también social. En la era 2.0, la cual es la que actualmente vivimos, se agrava la validez de la identidad digital por la aparición, desarrollo y utilización de las tecnologías como parte de nuestras vidas, especialmente las que tienen que ver con la información, comunicación y la Internet, es por esto que el proceso de formación de la identidad digital incluye el aspecto individual y el aspecto social en su concepción más tradicional o físico, el aspecto digital o cómo la digitalización y los grupos

digitales o virtuales tienen un papel importante, y que no debemos dejar de lado, en el proceso de formación de la identidad del ser humano.

Hernando (2002) dice que la identidad implica una relación con la realidad, la puesta en activo de una determinada forma de estar en el mundo que haga posible la supervivencia efectiva de los seres humanos. Por eso se transforma constantemente, dependiendo de las condiciones de supervivencia, de los riesgos que cada grupo humano haya de afrontar.

Mercado y Hernández (2010) dicen que el término identidad se incorporó al campo de las ciencias sociales a partir de las obras del psicoanalista austriaco Erick Erickson, quien a mediados del siglo XX empleó el término ego-identidad en sus estudios sobre los problemas que enfrentan los adolescentes y las formas en que pueden superar las crisis propias de su edad.

Finalmente, Habermas (1992) dice que la identidad social y de la identidad nacional, sin dejar de lado el tema de la identidad personal afirmando que en cuanto a esta relación entre individuo y sociedad nos indica que el individuo humano empieza pensando en términos enteramente sociales y por tanto la misma individuación sólo puede conseguirse por socialización. Bajo la misma premisa, Bauman (2007) considera que la construcción de la propia identidad implica el triple desafío, y riesgo, de confiar en uno mismo, en otros y también en la sociedad.

Estas teorías fueron las bases para orientar el tema principal de esta investigación, por lo tanto, aportaron la línea base del tema a investigar, aportaron el concepto principal para la formación del título de esta investigación, y ayudaron a identificar la raíz para prevenir los tres delitos cibernéticos mencionados en esta investigación, la cual es la identidad del escolar, la cual hay que darle seguridad para prevenirlos de los delincuentes cibernéticos acosadores.

2.1.2 La identidad en la Actualidad

Tajfel (1982) dice que desde la perspectiva de la psicología social plantea una teoría de la identidad social partiendo de la idea que sugiere que existe una relación de índole psicológico en el hecho de que una persona determinada se una o se identifique con un grupo, para ello se tiene que cumplir por un lado que el individuo sienta la pertenencia al grupo en cuestión y por otro lado que el individuo tenga consciente que por el mero hecho de pertenecer a un determinado grupo, va a tener una calificación bien positiva o bien negativa. Bajo la misma perspectiva, Turner (1990) dice que el grupo psicológico como aquel que es significativo para los individuos que lo forman, psicológicamente hablando, al que se remiten de modo subjetivo a la hora de establecer comparaciones sociales, así como para la adquisición de valores y normas y al que aceptan pertenecer a título personal y que además influye de forma determinante sobre sus actitudes y comportamiento.

En la teoría de la identidad social planteada por Tajfel y Turner se pondría foco a los siguientes componentes:

- Categorización: consiste en establecer categorías de todos aquellos grupos e individuos que nos rodean e incluso a nosotros mismos. Etiquetamos a los demás individuos y grupos.
- Identificación: consiste en crear una asociación con determinados grupos (aquellos grupos con los que nos sentimos cercanos, que pueden ser varios grupos y de muy diversa naturaleza), con el objetivo de reafirmarnos.
- Comparación: consiste en realizar comparaciones de nuestros grupos con el resto, pero siempre con un grado de positividad hacia los nuestros.
- Distinción psicosocial: consiste en que seamos y nos consideren distintos de los demás grupos, además esa distinción tendría que ser positiva.

Por ello, Turner (1990) dice que es posible analizar el comportamiento social humano desde un punto de vista estructural, desde el punto de vista de los procesos y de las leyes que se dan en el nivel de las relaciones sociales, sin

tener por qué necesariamente hacer referencia a las características psicológicas individuales de cada sujeto que forma parte del grupo. Así, McDougall (1921) en Turner (1990) analiza el tema de las masas sociales y afirma que una masa no tiene por qué necesariamente ser reflejo de los componentes que la forman, pudiendo llegar a ser mejores que sus miembros individuales, pero también peores, de forma que a mayor organización del grupo más compleja sería su psicología a modo grupal y más desarrollada estaría su mente colectiva. A modo de síntesis la pertenencia social consistiría en la inclusión de la personalidad individual en una comunidad o grupo hacia la cual se experimenta un sentimiento de lealtad y para esto debe cumplirse que el individuo asuma e interiorice aquellas ideas, bien de forma total o bien de forma parcial, que caracterizan a dicho grupo y generalmente el individuo asume un rol dentro de ese grupo. Siguiendo con esto se puede deducir que el estatus de pertenencia tiene que ver fundamentalmente con la dimensión simbólico-cultural de las relaciones e interacciones sociales.

Este punto aportó a esta investigación, el poder entender, como en la actualidad para los escolares, el mundo gira en relación a su identidad social, la cual se forma directamente proporcional entre su identidad física versus su identidad digital, y que la interacción de estas finalmente les da una identidad en la sociedad, y que en etapa escolar y sin un guía de como agregar seguridad a su identidad, vuelven al escolar en punto de atención y carnada para los delincuentes cibernéticos, aprovechándose estos últimos del desconocimiento del escolar en seguridad para su identidad digital, para que pueda cometan sus ataques.

2.1.3 Análisis de la Identidad 2.0

En la era que actualmente vivimos, la era 2.0 donde la tecnología impera y nos rodea, y que forma parte de nuestra vida diaria. La tecnología avanza a gran rapidez y esta nos empuja a avanzar en. El avance de la Internet nos abre nuevas puertas a la hora de comunicarnos, a la hora de estudiar y a la hora de relacionarnos con las demás personas.

La Internet ha evolucionado masiva y rápidamente a gran escala, de este mensaje partimos cuando analizamos el concepto identidad digital, ya que la identidad digital no es sólo aquello que aparece acerca de nosotros al realizar una búsqueda en un portal de Internet, en una plataforma digital o en las redes sociales, como a veces se resume, sino que también es el comportamiento o la idea que se transmite de uno mismo a través de Internet. Cabe mencionar que dicha transmisión no responde siempre a la información que uno mismo introduce en la Red, sino que se amplía a aquella información que otras personas introducen en la Red y que versa sobre nosotros. Bajo esta premisa, Giones y Serrat i Brustenga (2010) dicen que una parte de su trabajo al análisis del engaño en la Red, planteando que la gestión de la identidad digital es algo que nos compete a cada uno de nosotros y dicha gestión se aprende y lleva asociada consigo la adquisición de una serie de habilidades que hay que trabajar constantemente y que se pueden aprender.

Freire (2009) propone una serie de retos y problemas a la hora de gestionar nuestras identidades digitales, poniendo énfasis en las que abordan el tema de las suplantaciones de identidad, tan frecuentes en el mundo virtual precisamente por esa aparente invisibilidad que se asume de forma equivocada de la Red. Igualmente propone el término de identidades híbridas como aquellas que surgen de la interrelación de todos aquellos círculos sociales digitales y no digitales que lo rodean y de los que toman prestados ciertos atributos de cada uno de ellos, según les interese y según sea el grado de identificación de dichos círculos con el propósito de incorporarlos a la formación de la propia y particular identidad.

Moscovici, Mugny y Pérez (1991) dicen que los criterios de pertenencia a las categorías son, con frecuencia, múltiples, es decir, que no funcionan necesariamente por inclusiones o exclusiones tajantes, y que hay grados y niveles jerarquizados de pertenencia a las categorías. Podría decirse que esta pluralidad de pertenencias no sólo no anula la identidad personal, sino que

hoy en día es la que la define y da consistencia a la propia identidad personal. Cuanto más amplios son los círculos sociales de los que un individuo es miembro y se siente identificado y reconocido como tal, más se reforzaría la propia identidad personal. Ante esta variedad de círculos sociales, culturas diferentes, y esta pluralidad de pertenencias que caracteriza la era 2.0 podríamos hablar de identidades híbridas y culturas híbridas, en el sentido de que seguimos contando con nuestra propia identidad tanto individual como social, donde parece obvio incluir la digital como extensión de la identidad física. Lo que ocurre es que esa identidad se ha visto enfrentada, mejorada, complementada y renovada, con características tomadas de esos diferentes círculos culturales con los que nos identificamos.

Bartolomé (2002) dice que a la vez que estamos inmersos en un proceso de globalización de la sociedad a todos los niveles, también estamos asistiendo a un resurgir de nuevas identidades, como las culturales y que precisamente los medios de comunicación y las nuevas tecnologías de la información nos facilitan la tarea, ya que permite a las personas de diversas partes del mundo ponerse en contacto en tiempo real. También señalan que una de las consecuencias de esta globalización social es lo que se denomina homogeneización cultural, es decir, se está unificando en cierto modo la visión del mundo y la aceptación e incorporación tanto de valores como de actitudes en todos los lugares del planeta y eso es lo que hace en parte que surjan esas nuevas identidades, para reafirmar la propia identidad. En relación con este tema de la globalización y cómo afecta la misma al proceso de formación de la identidad en la era en la que vivimos actualmente. Mercado y Hernández (2010) sostienen que a consecuencia del proceso de globalización a nivel mundial y en todos los ámbitos se han generado nuevas identidades como resultado de la apertura de fronteras, y la reivindicación de la propia identidad, por parte de ciertos grupos que se resisten a abandonar su cultura. Molina (2011) dice que analizando la realidad comunicativa y que se enmarca en una comunidad de comunicación como es la actual el proceso de formación y adquisición de la identidad tendría dos aspectos complementarios, por un

lado, el aspecto de universalización y por otro lado el aspecto de particularización. Mercado y Hernández (2010) dicen que, si bien es cierto que la globalización y debido principalmente a la apertura de las fronteras físicas ha permitido generar nuevas identidades, también es cierto que ha provocado una reivindicación de lo propio por parte de algunos grupos en respuesta a esa apertura sin límites.

Apreciamos diversos efectos sociales que tiene que ver con la forma en que los individuos se vinculan o identifican con el grupo al que pertenecen. Tradicionalmente esa identidad colectiva y grupal se hacía en referencia principalmente al grupo cercano con lo que supone la aceptación, interiorización y transmisión de los rasgos culturales de ese determinado grupo social. Una identidad digital tiene contactos y se vinculan muchos grupos muy diversos, la construcción del sentido de pertenencia se dificulta en el sentido de que debido precisamente a esa variedad de grupos con los que se siente identificado el individuo y debido a las numerosas ocasiones de contacto e interacciones se van seleccionando aquellas ideas, valores, actitudes o acciones que le van interesando al sujeto en respuesta a sus propios intereses, por lo que esta identidad colectiva o forma en que se identifican con los grupos se convierte no en algo estático sino en una construcción subjetiva y cambiante.

Este punto aportó a esta investigación el poder identificar las plataformas digitales como principal foco de riesgo sobre los tres delitos cibernéticos a los que están expuestos los escolares. Nos dio a entender que la identidad 2.0 es la identidad que en la actualidad todos los escolares viven, la cual es la identidad propia del escolar como ser humano y como ser cibernético al mismo tiempo, ya que los escolares viven sumergidos en la internet, digitalizando o publicando todo su día a día en las plataformas digitales, como la red social, y sin una metodología con la que el escolar pueda guiarse, estos convierten su día a día físico en día a día digital a diestra y siniestra exponiéndose ellos mismo a los delincuentes cibernéticos. Es por ello que esta

investigación se centra en agregar seguridad a la identidad digital del escolar para que se proteja de internautas malintencionados.

Por lo tanto, en el supuesto de que todo delincuente cibernético quiera abusar de un escolar comenzando por atacar a su identidad digital, esta metodología propuesta está dirigida para contrarrestar al delincuente cibernético agregándole capas de seguridad a su identidad digital o identidad 2.0.

3 Inclusión del Alumno en la Comunidad Digital Escolar

La inclusión del escolar a la comunidad digital del colegio debe ser parte de la malla curricular, sin discriminación, ya sea de género, etnia, religión, clase social, condiciones físicas y psicológicas, etc.

La inclusión debe iniciar en el ciclo IV, del 3er grado de primaria, junto con la metodología propuesta (que también inicia en dicho grado).

La comunidad digital estudiantil, la cual es creada y administrada por el colegio, servirá como laboratorios para que los escolares puedan practicar la metodología.

La inclusión del escolar a la comunidad digital del colegio prevé la integración y unión de los estudiantes para la lucha contra el engaño pederasta, el acoso virtual y el acoso sexual digital.

Los colegios deben estar preparadas para proporcionar la comunidad digital para el uso de los escolares, ya sea en infraestructura propio o en infraestructura alquilada. También debe proporcionar la formación de profesionales de la enseñanza para la gestión, control, seguimiento, monitoreo y supervisión de la comunidad digital.

3.1 Cultura de la Seguridad

Los colegios deben ver a internet como un escenario real, donde se viven situaciones reales, deben entender que los escolares están expuestos a riegos similares en la calle que, en internet, por ejemplo, así como en la calle no se debe hablar con ningún desconocido, la misma lógica se debe aplicar en internet.

Tanto el colegio como el escolar deben procurar tener cuidado y evitar

situaciones de riesgo, como, por ejemplo, la pérdida de información personal y/o confidencial al dañarse o extraviarse el dispositivo, el acceso de otras personas a las cuentas en redes sociales, entre otras.

Los colegios deben promover la generación de conocimiento, la cultura digital y la capacitación en temas de seguridad digital, brindando iniciativas para el uso de herramientas y prácticas para proteger la información, contraseñas y datos personales que se utilizan a través de computadores, celulares o tabletas.

La cultura en seguridad digital envolverá a toda la comunidad digital escolar con el conocimiento de herramientas para evitar riesgos y ataques, para que el escolar pueda entablar comunicación segura por computadoras, celulares y tabletas, y mejorar el contacto digital seguro dentro de la comunidad digital escolar, a fin de preparase para una buena interacción en la sociedad digital.

El escolar al estar sumergido en una cultura en seguridad digital tendrá siempre presente la importancia de prevenir los riesgos digitales y los delitos cibernéticos a que estos conlleva. Ya que es importante tener hábitos para la protección de la identidad digital. Se deben realizar charlas semanal o mensualmente sobre la cultura digital, identidad digital y su seguridad.

3.1.1 Supuesto de Éxito

En el supuesto que el colegio tenga implementada una comunidad digital orientada a temas educativos de conocimiento público, esta comunidad digital servirá como laboratorio para poner en práctica, sin riesgo real, la metodología propuesta, el tutor podrá monitorear la actividad digital de los escolares con el fin de detectar posibles acosos, y podrá supervisar la identidad digital del posible acosar, víctima y compañeros observadores, con el objetivo de ajustar y corregir en el tiempo las debilidades y/o errores en seguridad digital del escolar.

Finalmente, el escolar estará preparado para detectar, prevenir,

contrarrestar, bloquear y denunciar el engaño pederasta, el acoso virtual y el acoso sexual digital. Quedando preparado para integrarse, adaptarse e interactuar en la sociedad digital, volviéndose parte de esta sociedad y de la cultura digital en seguridad.

3.1.2 Supuesto de Error

La metodología propuesta se engrana con la comunidad digital escolar y su cultura en seguridad digital, en ese sentido, si el colegio no se prepara en lo que le corresponde referente a la comunidad digital y cultura de seguridad, o la metodología no es concientizada y aplicada en su totalidad de grado en grado, aumentará el riesgo del escolar de volverse víctima del engaño pederasta, del acoso virtual o del acoso sexual digital, y de materializarse eso, le causaría daños irreparables, pudiendo costarle hasta la vida. Finalmente, el escolar no estará preparado para integrarse e interactuar, con seguridad y mitigando los riesgos, en la sociedad digital en la cual tarde o temprano ingresará por la misma presión del avance de la tecnología y de la vida o día a día cada vez más digital o cibernético.

4 Plan de Trabajo

4.1 Desarrollo de la Investigación

El plan de trabajo para el desarrollo de esta investigación se refleja en el siguiente diagrama de Gantt, Diagrama 4 “Gantt Desarrollo de Investigación”:

Actividades	Fecha Inicio	Fecha Fin	Duración Días
Levantamiento de información	18/05/2020	1/06/2020	15
Definición del título	2/06/2020	4/06/2020	2
Cronograma de desarrollo	5/06/2020	6/06/2020	1
Revisión de la literatura	6/06/2020	27/06/2020	22
Introducción	25/06/2020	1/07/2020	7
Antecedentes	1/07/2020	9/07/2020	9
Objetivo	9/07/2020	15/07/2020	7
Alcance	15/07/2020	21/07/2020	7
Justificación	19/07/2020	1/08/2020	14
Metodología	25/07/2020	18/08/2020	25
Marco Teorico	27/07/2020	15/08/2020	20
Caratula	19/08/2020	20/08/2020	1
Glosario de terminos	20/08/2020	22/08/2020	3

Fecha Inicio	43969.00
Fecha Fin	44065.00

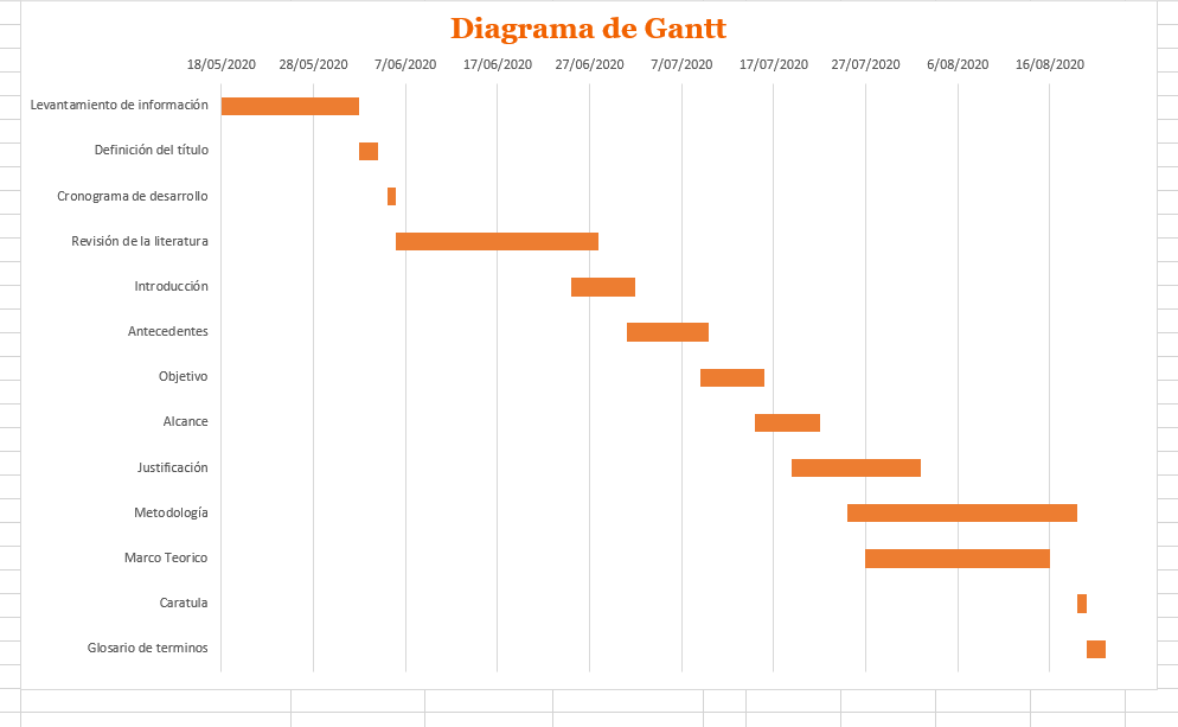

Diagrama 4 “Gantt Desarrollo de Investigación”

4.2 Implementación de la Metodología

El plan de trabajo para la implementación de la metodología propuesta en esta investigación, la fecha de inicio debe coincidir con la fecha de inicio del año escolar, en este apartado se plantea una fecha tentativa referente al año escolar en el Perú. Este cronograma se refleja en el siguiente diagrama de Gantt, Diagrama 5 “Gantt Implementación de Metodología”:

Actividades	Fecha Inicio	Fecha Fin	Duración Días
Entrega de manuales	7/03/2020	9/03/2020	2
Talleres para revisión de manuales	10/03/2020	29/03/2020	20
Capacitación de la metodología	30/03/2020	28/05/2020	60
Charlas sobre delitos cibernéticos	15/05/2020	13/06/2020	30
Charlas sobre Identidad Digital	14/06/2020	28/06/2020	15
Capacitación de seguridad en identidad digital	29/06/2020	23/07/2020	25
Capacitación en funcionalidades para la seguridad en identidad digital	24/07/2020	17/08/2020	25
Capacitación en herramientas para la seguridad en identidad digital	18/08/2020	11/09/2020	25
Evaluaciones de aprendizaje	12/09/2020	16/09/2020	5

Fecha Inicio	43897.00
Fecha Fin	44090.00

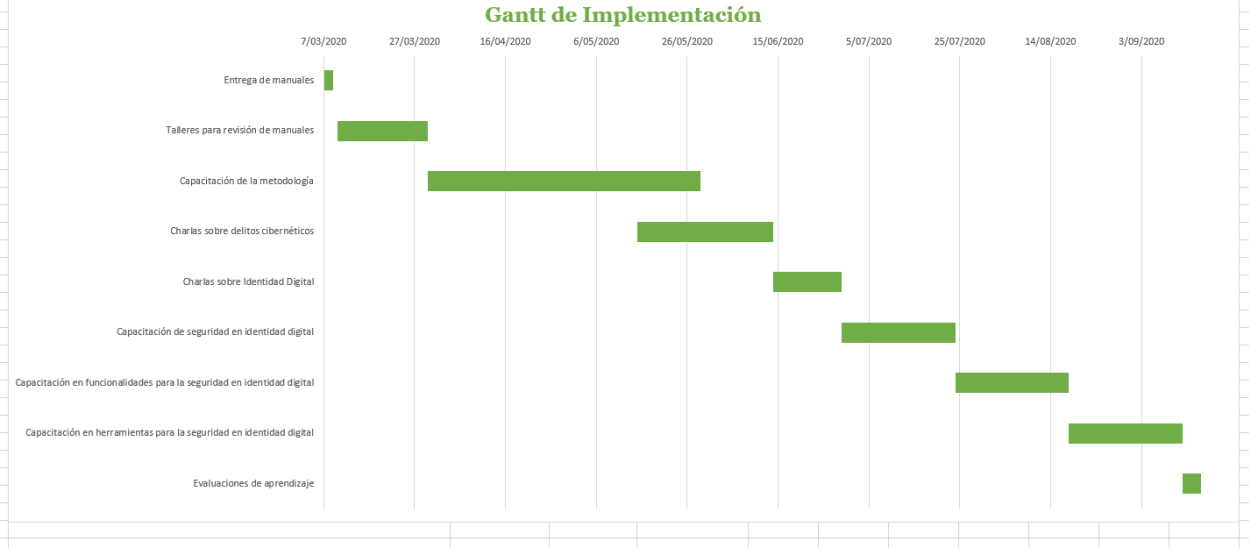

Diagrama 5 “Gantt Implementación de Metodología”

5 Conclusiones

La innovación incrustada en esta investigación se da en que esta metodología para la seguridad en la identidad digital promoverá una cultura en seguridad digital en grados escolares que sentarán las bases de las próximas generaciones, los cuales traerá consecuentemente las siguientes aportaciones principales a la sociedad digital:

- El Conocimiento de la Identidad Digital: Donde el escolar pueda usar de manera responsable su identidad digital en la internet, teniendo pleno conocimiento de los riesgos a los que estaría expuesto en la vida digital, y como mitigar estos riesgos.
- Construcción y Promoción de una Sociedad Digital Segura: Esto se da a través de la integración del ex –escolar en la sociedad, aportando a su nuevo entorno familiar, amical o laboral, una cultura digital en seguridad de la identidad digital, es decir, cuando termine el colegia y ya sea que comience a trabajar, o que forme su familia o que comience la universidad, el ex –escolar sabrá cómo usar de manera segura su identidad digital y la importancia de que dicha identidad no sea vulnerada por algún delincuente cibernético, sabrá como orientar y supervisar la identidad digital de sus hijos, y finalmente podrá compartir ese conocimiento en su nuevo entorno donde se encuentre.
- Preveención de delitos cibernéticos: Donde el escolar tendrá pleno conocimiento de los principales delitos ciberneticos, podrá identificar cuando siendo atacado por alguno de dichos delitos, y podrá enceder sus mecanismos para mitigar dichos delitos cibernéticos.
- Integración segura en la sociedad digital: El escolar estará preparado para integrarse, adaptarse e interactuar dentro de la sociedad digital, de una manera segura, reduciendo los riesgos y vulnerabilidades a las que se expondría su identidad digital.

Esta metodología propuesta espera aumentar el conocimiento sobre la seguridad en identidad digital, crear concientización sobre la exposición de

los delitos cibernéticos a los que están expuestos los escolares y que se abran nuevas investigaciones sobre los delitos cibernéticos a los que con más frecuencia están expuestos los escolares, los cuales son el engaño pederasta, el acoso virtual y el acoso sexual digital, porque esta investigación agrupa como un todo estos tres delitos cibernéticos haciendo un único frente de combate para dichos delitos, y haciendo una única pausa a seguir para prevenir dichos delitos, permitiendo que el escolar aprenda de menos a más sobre la seguridad en su identidad digital y las herramientas para protegerla, esta propuesta de aprendizaje es similar a la malla estudiantil que también enseñan de menos a más, con el objetivo de que el escolar se vaya nutriendo y aumentando su conocimiento conforme va superando los niveles escolares. Esta propuesta técnica basada en la seguridad informática, espera poder aportar a nuevas investigaciones tanto técnicas como también de otros ámbitos, como, por ejemplo, un investigador docente especialista en el sistema educativo escolar el cual este creando una metodología basada en el área de la psicología para prevenir los tres delitos mencionados, podría obtener partes técnicas de esta investigación para sumarlas a su metodología, y así sucesivamente, podrían engranarse con otras investigaciones de otras áreas de estudio, para que en una investigación final total se puedan juntar todas estas propuestas y armar un metodología de prevención, a 360 grados, sobre los tres delitos cibernéticos mencionados.

Referencias

CEPAL, N.U. (2016). La Nueva Revolución Digital. Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/38604/4/S1600780_es.pdf

Organización Mundial de la Salud - OMS, N.U. (2020). El Coronavirus que se ha descubierto más recientemente causa la enfermedad por coronavirus COVID-19. Recuperado de https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/advice-for-public/q-a-coronaviruses?gclid=CjwKCAjwrcH3BRApEiwAxjdPTcIG3iiPdJcVcXrxo5AaFw4GaeOeCOCN6FzEw-qaAohMUbTgIMRAwRoCR48QAvD_BwE

Valentina Giraldo, A.A (2020). Plataformas digitales: ¿qué son y qué tipos existen? Recuperado el 29 de mayo de 2020 de https://rockcontent.com/es/blog/plataformas-digitales/

Justo Zaragoza (2020). Director fundador del Grupo Educación al Futuro. La educación virtual en el Perú. Recuperado el 18 de abril de 2020 de https://gestion.pe/opinion/la-educacion-virtual-en-el-pais-esta-funcionando-noticia/?ref=gesr

Diego Suárez Bosleman (2019). ¿Cómo usan el Internet los escolares peruanos? Recuperado el 20 de septiembre de 2019 de https://elcomercio.pe/tecnologia/internet-escolares-peruanos-noticia-678249-noticia/?ref=ecr

Megan Moreno (2018). Investigadora principal de SMAHRT. Uso de los medios de comunicación digital en niños en edad escolar y adolescentes. Recuperado el 30 de julio de 2018 de

https://www.healthychildren.org/Spanish/family-life/Media/Paginas/cyberbullying.aspx

Nasheli Escobar (2015). Qué es el grooming y cómo podemos proteger a los niños en Internet. Recuperado el 19 de mayo de 2015 de https://hipertextual.com/2015/05/que-es-el-grooming

Ana Sierra (2018). Sexóloga. ¿Qué es el 'sexting' y por qué supone un riesgo? Recuperado el 20 de julio de 2018 de https://www.elmundo.es/vida-sana/sexo/2018/07/20/5b50b3eb468aeb2a7d8b464e.html

Loraine Bosch Taquechel (2019). Por una cultura digital que permita hacer un uso responsable y seguro de internet. Recuperado el 28 de junio de 2019 de http://www.juventudrebelde.cu/ciencia-tecnica/2019-06-28/por-una-cultura-digital-que-permita-hacer-un-uso-responsable-y-seguro-de-internet-video

Ministerio de Educación del Perú (2010). Propuesta de Metas Educativas e Indicadores al 2021. Recuperado el 01 de setiembre del 2010 de http://www.minedu.gob.pe/Publicaciones/Folleto_Metas2021_setiembre.pdf

Psicología Velázquez (2016). La Pederastia: La Mente del Abusador y Menores en Riesgo. Recuperado el 22 de febrero del 2016 de https://psicologiavelazquez.com/la-pederastia-la-mente-del-abusador-y-menores-en-riesgo/

Ana Aznar (2017). Ciberbullying: El Delito de los Menores de Edad. Recuperado el 25 de enero del 2017 de https://www.hacerfamilia.com/educacion/noticia-ciberbullying-delito-menores-edad-

20160909130113.html#:~:text=La%20edad%2C%20tanto%20de%20los,ni%C3%B1os%20est%C3%A1n%20form%C3%A1ndose%20como%20personas

Lidia Dóniga Alonso (2018). Realidad Criminológica del Sexting Secundario en Menores. Recuperado el 01 de junio del 2018 de https://gredos.usal.es/bitstream/handle/10366/139792/TG_DonigaAlonso_Realidad.pdf;jsessionid=980F50D6EB0BFF238DF05A0381700B95?sequence=1

Revista UNIR (2020). ¿Qué es el método KiVa? Consejos para aplicarlo en el aula frente al acoso escolar. Recuperado el 17 de marzo del 2020 de https://www.unir.net/educacion/revista/noticias/metodo-kiva/549204925805/

PIFARRÉ, L. (1989). El itinerario del ser: Resumen histórico. Barcelona: PPU

ÍÑIGUEZ, L. (2001). Identidad: de lo personal a lo social. Un recorrido conceptual. En CRESPO, E. (Ed.), La constitución social de la subjetividad. (págs. 209-225). Madrid: Catarata. Recuperado de http://uab.academia.edu/LupicinioI%C3%B1iguezRueda/Papers/114932/IDENTIDAD_de_lo_personal_a_lo_social._Un_recorrido_conceptual

HERNANDO, A. (2002). Arqueología de la identidad. Madrid: Ediciones Akal

HABERMAS, J. (1992). Teoría de la acción comunicativa, vol. 2. Crítica de la razón funcionalista. Madrid: Taurus.

TAJFEL, H. (1982). Social Identity and Intergroup Relations. Cambridge: Cambridge University Press

TURNER, J.C. (1990). Redescubrir el grupo social: Una teoría de la categorización del yo. Madrid: Ediciones Morata.

GIONES, A. y SERRAT I BRUSTENGA, M. (2010). “La gestión de la identidad digital: una nueva habilidad informacional y digital”. BiD: textos universitaris de biblioteconomia i documentació. Nº 24. Recuperado el 30 de junio del 2010 de http://www.ub.edu/bid/24/giones2.htm

FREIRE, J. (2009). "¿Las personas debemos tener identidad digital? Cómo construirla [Sesión web de la Generalitat de Catalunya]". Nómada: reflexiones personales e información sobre la sociedad y el conocimiento abierto. Recuperado de http://nomada.blogs.com/jfreire/2009/03/las-personasdebemos-tener-identidad-digital-cmo-construirla-sesin-web-de-la-generalitat-decatalunya.html

MOSCOVICI, S., MUGNY, G. y PÉREZ, J.A. (Eds.) (1991). La influencia social inconsciente: estudios de psicología social experimental. Barcelona: Editorial Anthropos.

BARTOLOMÉ, M. (Coord.) (2002).Identidad y Ciudadanía: Un Reto a la Educación Intercultural. Madrid: Narcea

MERCADO, A. y HERNÁNDEZ, A.V. (2010). “El proceso de construcción de la identidad colectiva”. Convergencia. Revista de Ciencias Sociales. Nº 53, 2010. Universidad Autónoma del Estado de México. Recuperado de http://convergencia.uaemex.mx/rev53/pdf/13_Asael%20Mercado%20Maldonado.pdf

MOLINA, F. (2011) “Educación, Multiculturalismo e Identidad”. Recuperado de http://red.pucp.edu.pe/ridei/wp-content/uploads/biblioteca/inter30.PDF

Bibliografía

Olga Isaza (2019). Representante a.i. de Unicef Perú. 42% de menores de 15 años se conecta a Internet en el Perú. Recuperado el 06 de febrero del 2019 de https://elcomercio.pe/peru/unicef-familias-deben-generar-entorno-virtual-seguro-jovenes-noticia-605140-noticia/

Ayuda en Acción (2018). Ciberbullying: ¿qué es y cómo lo prevenimos? Recuperado el 06 de agosto del 2018 de https://ayudaenaccion.org/ong/blog/educacion/ciberbullying/

Sabe the Children (s.f.). Grooming: Qué es, Cómo detectarlo y prevenirlo. Recuperado de https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

Pantallas Amigas (s.f.). Qué es el Sexting. Recuperado de https://www.sexting.es/que-es-el-sexting/

Intra Med (2018). Sexting: Peligro en niños y adolescentes. Recuperado el 02 de noviembre del 2018 de https://www.intramed.net/contenidover.asp?contenidoid=93210

Clara Borges (2019). Gerente de Marketing B2B en Rock Content. Cultura digital: ¿cuáles son sus características e influencias en la sociedad? Recuperado el 16 de agosto del 2019 de https://rockcontent.com/es/blog/cultura-digital/

Comunidad RIIAL (2016). ¿Qué es Cultura Digital? Es la expresión que nace por el hecho de vivir en un entorno influido por las TICs. Recuperado el 01 de agosto del 2016 de http://www.riial.org/que-es-cultura-digital-es-la-expresion-que-nace-por-el-hecho-de-vivir-en-un-entorno-influido-por-las-tics/

Guillermo Cánovas, N.U. (2015). Cultura Digital y su Uso Saludable de la Tecnología. Recuperado de https://www.bejob.com/wp-content/uploads/2017/11/bejob_guias_cultura-digital-uso-saludable-de-la-tecnologia.pdf

KiVa School (s.f.). KiVa: Un Método Eficaz Contra el Acoso Escolar. Recuperado de http://www.kivaprogram.net/ssc-en/news/kiva-un-m%C3%A9todo-eficaz-contra-el-acoso-escolar

Eva Adán García (s.f.). El método KiVa finlandés contra el acoso escolar. Recuperado de http://webs.ucm.es/BUCM/revcul/e-learning-innova/148/art2039.pdf

Instituto Iberoamericano de Finlandia (s.f.). Educación en Finlandia: KiVa, programa finlandés anti acoso escolar. Recuperado de https://madrid.fi/wp-content/uploads/2015/04/Educacio%CC%81n-en-Finlandia-KIVA.pdf

HABERMAS, J. (1987). Teoría de la acción comunicativa, vol. 1. Racionalidad de la acción y racionalización social. Madrid: Taurus.

TAJFEL, H. (1984). Grupos humanos y categorías sociales: Estudios de psicología social. Barcelona: Herder

MOSCOVICI, S. (1985). Psicología social: pensamiento y vida social; psicología social y problemas sociales. Barcelona: Ediciones Paidós Ibérica.

BARTOLOMÉ, M. (2000). La construcción de la identidad en contextos multiculturales. Madrid: Centro de Investigación y Documentación Educativa (CIDE)

Apéndice A - Glosario de Términos

- Plataforma Digital: Es un lugar de Internet, portal o cibersitio, que sirve para almacenar diferentes tipos de información tanto personal, negocio u ocio.
- Red Social: Es una plataforma digital con una estructura social compuesta por un conjunto de usuarios (tales como individuos u organizaciones) que están relacionados de acuerdo a algún criterio (relación profesional, amistad, parentesco, entre otras). El tipo de conexión representable en una red social es una relación diádica o lazo interpersonal.
- Usuario: Es una persona que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc, dichos usuarios deberán identificarse.
- Cuentas de usuario: Para que un usuario pueda identificarse, el usuario necesita una cuenta, en la mayoría de los casos asociados a una contraseña.
- Información Personal: Es la información relacionada con la cuenta de usuario, con la que puede usarse para identificar, contactar o localizar a una persona en concreto, o puede usarse, junto a otras fuentes de información para hacerlo. Esta información suele ser regulada según legislación del país.
- Cibernético: Es todo lo que se relaciona con la tecnología computacional, especialmente con la Internet.
- Espacio Cibernético (Ciberespacio): Es el ámbito de información que se encuentra implementado dentro de los ordenadores y de las redes digitales de todo el mundo. Es virtual, inexistente desde el punto de vista físico donde las personas o sujetos, públicas o privadas, desarrollan comunicaciones a distancia, exponen sus competencias, generan interactividad para diversos propósitos.
- Identidad Digital: Es la identidad online o reivindicada en el ciberespacio por un individuo, organización o dispositivo electrónico. Está formada tanto por los datos privados y públicos del usuario, como también por sus

acciones (opiniones, fotos, navegación, etc.), pero también por las publicaciones que otros han hecho sobre él.

- Delitos Informáticos o Cibernéticos (Ciberdelitos): Son todos los delitos que se cometen haciendo uso equipos informáticos, internet y en ocasiones, también software malicioso o malware. El concepto de delito cibernético está asociado a la expansión y uso de la Internet.
- Delincuente Informático o Cibernético (Ciberdelincuente / Atacante): Es la persona que realiza actividades delictivas en la Internet, como robar información, acceder a redes privadas, estafas, acoso, abuso y todo lo que tiene que ver con los delitos e ilegalidad.
- Acoso Virtual (Ciberbullying / Ciberacoso): Es el uso de plataformas digitales con la intención de acosar psicológicamente a terceros entre iguales: niños, jóvenes, adolescentes; donde el agresor y la víctima del acoso tendrán la misma edad y compartirán un contexto social (no se trata de acoso o abuso sexual, ni intervendrán personas adultas, pues, en este caso, estaríamos hablando de otro tipo de ciberdelito).
- Engaño Pederasta (Grooming / Online Grooming): Es una serie de conductas y acciones emprendidas por un adulto, a través de Internet, con el objetivo deliberado de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las preocupaciones del menor y poder abusar sexualmente de él. En algunos casos, se puede buscar la introducción del menor al mundo de la prostitución infantil o la producción de material pornográfico.
- Sexting (Sexteo): Se refiere al envío de mensajes sexuales, eróticos o pornográficos, por medio de teléfonos móviles. Inicialmente hacía referencia únicamente al envío de SMS de naturaleza sexual, pero después comenzó a aludir también al envío de material pornográfico a través de smartphone y ordenadores.
- Uso Responsable del Internet: Hace referencia a la manera correcta navegar por Internet, siguiendo las buenas practicas, para prevenir que los delincuentes cibernéticos atenten.

- Cultura Digital: Es la forma de relacionamiento social y generación de conocimiento que la influencia de las TIC genera en los comportamientos y manifestaciones comunicativas, culturales y sociales, cuya característica básica es su relación con la información y la forma en que hoy en día las personas interactúan con un mundo interconectado; la interacción con las nuevas tecnologías, el uso de redes sociales, la tecnología GPS y muchos otros factores son los que han dado origen a esta llamada cultura digital.
- Inicio de Sesión Único (Single Sign On / SSO): Permite a los usuarios tener acceso a múltiples plataformas digitales ingresando solo con una cuenta de usuario a los diferentes sistemas y recursos. El SSO es de gran utilidad cuando existen diferentes sistemas a los que es posible acceder mediante una única contraseña y se desea evitar el ingreso repetitivo de estas cada vez que el usuario se desconecte del servicio.
- Dispositivo (Hardware): Son las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Los cables, así como los gabinetes o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico. Es dispositivo puede ser estático (p.ej. una computadora de escritorio) o móvil (p.ej. una laptop, Tablet, Smartphone, etc).
- Aplicación (Software / Programas): Es un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas. La interacción entre el software y el hardware hace operativo un ordenador, es decir, el software envía instrucciones que el hardware ejecuta, haciendo posible su funcionamiento.
- Red Privada Virtual (VPN): Es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

- Cortafuego (Firewall): Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- Malware (Malicious Software): Es un software malicioso que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. Es el término principal que se utiliza para hablar de todas las amenazas informáticas. Dentro de esta categoría se cuenta con diferentes clasificaciones bastante más específicas de las amenazas, como la de los troyanos, los gusanos, los virus informáticos, el adware, el spyware, ransomware, entre otras
- Antivirus: Son programas cuyo objetivo es detectar y eliminar virus informáticos. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e internet, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de los mismos.