



Universidad Central de Venezuela

Facultad de Humanidades y Educación

Escuela de Educación

DISEÑO Y EVALUACIÓN DE UN TALLER DE “SEGURIDAD EN REDES SOCIALES”
DIRIGIDO A LOS DOCENTES DE EDUCACIÓN MEDIA GENERAL DE INFORMÁTICA.

Tutora:

Almeida, Grecia.

Autora:

Ávila Pérez, Paula C.

Ci. 20.616.641

Caracas, Julio 2015.



Universidad Central de Venezuela



Facultad de Humanidades y Educación

Escuela de Educación

**DISEÑO Y EVALUACIÓN DE UN TALLER DE “SEGURIDAD EN REDES SOCIALES”
DIRIGIDO A LOS DOCENTES DE EDUCACIÓN MEDIA GENERAL DE INFORMÁTICA.**

Trabajo de Grado presentado ante la Universidad Central de Venezuela para optar a

Licenciatura en Educación, Mención Desarrollo de los Recursos Humanos

Tutora:

Almeida, Grecia.

Autora:

Ávila Pérez, Paula C.

Ci. 20.616.641

Caracas, Julio 2015.



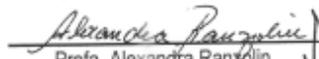
VEREDICTO

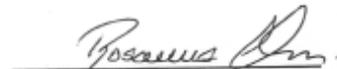
Quienes suscriben, miembros del jurado designado por el Consejo de la Escuela de Educación en su sesión 1571 de fecha 10-06-2015 para evaluar el Trabajo de Licenciatura presentado por **PAULA C., ÁVILA PÉREZ C.I. 20.616.641**, bajo el Título: **DISEÑO Y EVALUACIÓN DE UN TALLER DE "SEGURIDAD EN REDES SOCIALES" DIRIGIDO A DOCENTES DE EDUCACIÓN MEDIA GENERAL DE INFORMÁTICA**, para optar el Título de **LICENCIADO EN EDUCACIÓN**, dejan constancia de lo siguiente:

1. Hoy 22-07-2015 nos reunimos en la sede de la Escuela de Educación para que su(s) autor(es) lo defendiera(n) en forma pública.
2. Culminada la Defensa Pública del referido Trabajo de Licenciatura, conforme a lo dispuesto en el Art. 14 del "Reglamento de Trabajos de Licenciatura de las escuelas de la Facultad de Humanidades y Educación" adoptando como criterios para otorgar la calificación: rigurosidad en el razonamiento, coherencia en la exposición, claridad y pertinencia en los procesos metodológicos empleados, adecuación del sustento teórico, así como la calidad de la exposición oral y de las respuestas dadas a las preguntas formuladas por el jurado, **acordamos calificarlo como:**

APLAZADO APROBADO otorgándole la mención:
SUFICIENTE DISTINGUIDO SOBRESALIENTE

3. Las razones que justifican la calificación otorgada son las siguientes: la importancia y relevancia del tema desarrollado, la metodología el análisis de los resultados, conclusiones y recomendaciones son un gran aporte al área de estudio TIC, redes Sociales y Educación.


Prof. Alexandra Ranzolin


Prof. Rosanna Chacín

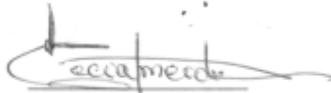

Tutor. Grecia Almeida



APROBACIÓN DEL TUTOR

Quién suscribe, Profesora Grecia Almeida, de la Universidad Central de Venezuela, adscrito a la Escuela de Educación, en mi carácter de tutora del Trabajo de Grado titulado **"DISEÑO Y EVALUACIÓN DE UN TALLER EN "SEGURIDAD EN REDES SOCIALES" DIRIGIDO A LOS DOCENTES DE EDUCACIÓN MEDIA GENERAL DE INFORMÁTICA"**, realizado por la ciudadana Paula C Ávila Pérez, C.I. 20.616.641, manifiesto que he revisado en su totalidad la versión definitiva de los ejemplares de este trabajo y certifico que se le incorporaron las observaciones y modificaciones indicadas por el jurado evaluador durante la discusión del mismo.

En Caracas a los 27 días del mes de Julio de 2015.



Profa. Grecia Almeida

Ci.11.993.622.

DISEÑO Y EVALUACIÓN DE UN TALLER EN “SEGURIDAD EN REDES SOCIALES” DIRIGIDO A LOS DOCENTES DE EDUCACIÓN MEDIA GENERAL DE INFORMÁTICA.

Autora:

Ávila Pérez, Paula C.

CI. 20.616.641

Tutora:

Profa. Almeida, Grecia.

Año:

Julio, 2015.

RESUMEN

La presente investigación aporta el diseño de un taller en “Seguridad en Redes Sociales” dirigido a los docentes de educación media general pertenecientes a la cátedra de informática, la propuesta fue evaluada por un panel de expertos que tuvieron la tarea de valorar los cuatro componentes (análisis, tecnología, diseño y evaluación) que integran el taller según el modelo ADITE (Polo, 2003); incluyendo en la estimación los medios didácticos computarizados diseñados y propuestos. La investigación fue Descriptiva con un diseño de Campo- Tecnológico. La razón de diseñar el plan de formación en la temática es a raíz de la carente inclusión del tema dentro de las líneas curriculares, y programas de actualización docente, así como la preocupante por el incremento de los ciberdelitos como grooming, sexting, phishing y cyberbullying; quiénes se han convertido en todo un fenómeno social; se buscó apoyar las líneas de formación en función a las demandas educativas contemporáneas tanto en entornos virtuales como reales.

Palabras Claves: Redes Sociales, Seguridad en Redes Sociales, Formación Docente, Modelo ADITE y Ciberdelitos.

DESIGN AND EVALUATION OF A WORKSHOP ON “SECURITY NETWORKS” FOR TEACHERS OF GENERAL EDUCATION MEDIA IN COMPUTER.

Author:

Paula C Ávila Pérez.

20.616.641

Tutor:

Profa. Grecia Almeida.

Date:

July, 2015.

ABSTRACT

The present investigation is the design of a workshop in “Security Networks” aimed at teachers of general secondary education belonging to the department of computer science, the proposal was assessed by a panel of experts who had the task of assessing the four components (analysis, technology, design and evaluation) that make up the workshop as the ADITE (Polo, 2003) model; including estimating the computerized teaching aids designed and proposed. The research was descriptive with a design of field-technology. The reason for designing the training program on the subject is due to the inclusion lacking of the item lines within the curriculum and teaching programs as well as concern for the rise in cybercrime as grooming, sexting, and cyberbullying phishing; who have become a social phenomenon; we sought support lines training according to contemporary educational demands both in virtual and real.

Keywords: Social Networks, Social Media Security, Teacher Training, Model ADITE and Cybercrime.

DEDICATORIA

El presente trabajo de grado me gustaría dedicárselo a mis padres, abuelos y tías; a ellos por siempre apoyarme y creer en mí cuando a veces yo no lo hice, alentarme a levantarme ante cada obstáculo que se me presentó en la carrera y sobre todo por apoyarme a que tomará mis propias decisiones y aprendiera de mis procesos.

También me gustaría, dedicar este trabajo a mi persona, pues tengo la propiedad para hablar del camino de estos cinco años y medio de carrera, de lo que fue mi vida universitaria y mi rol discente. En cuarenta y cinco minutos de defensa no podre resumir, todo el proceso de ser bachiller y sentirme licenciada, pero sí puedo decir al defender el presente trabajo de grado, que me siento orgullosa de lo que he logrado y en el tiempo que lo hice, además de la profesional en la que me he convertido tanto a nivel personal como profesional.

Solo puedo decirles y decirme, gracias por estar y por no rendirnos fue un trabajo en equipo.

AGRADECIMIENTO

Empezaré agradeciendo nuevamente a mi mamá y a mi negra (abuela), como mujeres han secado mis lágrimas y celebrado mis victorias con propiedad, también a mi abuelo y papá quienes siempre me decían que no me rindiera. Así como agradecer a mis tías y madrinas, porque siempre han sabido cómo sacarme una sonrisa.

A mis hermanas de vida, fieles compañeras que conocí en la casa que vence las sobras, que saben con propiedad que es ser ucevista pasar paros, semana del estudiante, protestas, consejos y evaluaciones, una amistad que creció en este espacio y que ha sembrado raíces, fuera de ella. Agradeceré con muchísima propiedad a mi Tutora, ya que me apoyo en un momento importante de la carrera y se comportó durante el proceso como una verdadera profesional comprometida, con su trabajo además de la Profa. Norelkis Riera, quién conjuntamente a la Profa. Grecia Almeida, me decían “Aquí vamos a ser felices”, cuando entre en el proceso de la tesis.

No me van alcanzar las gracias ni mucho menos los reconocimientos, por su gestión y apoyo, me reservare el nombre de estos seres porque las mejores personas que conocemos así como las vivencias, tienen vida en el anonimato y en mi memoria. Son los y las anónimas más extraordinarios que la vida me regalo y que yo escogí, y me atrevo a decir que fue la mejor elección.

Gracias miles, por estar y jamás abandonar.

ÍNDICE GENERAL

PP

INTRODUCCIÒN.....	1-3
-------------------	-----

CAPÍTULOS

CAPÍTULO I: EL PROBLEMA

1.1 Planteamiento del Problema.....	4-12
1.2 Objetivos de la Investigación.....	13
1.2.1 Objetivo General.....	13
1.2.1 Objetivos Específicos.....	13
1.3 Justificación de la Investigación.....	14-17
1.4 Limitaciones de la Investigación.....	18

CAPÍTULO II: MARCO TEÒRICO

2.1 Antecedentes.....	19-23
2.2 Bases Legales.....	24-27
2.3 Bases Teóricas.....	27-56
2.3.1 Sociedad de la Información.....	27-28
2.3.2 Sociedad del Conocimiento.....	28-29
2.3.4 Tecnología de la Información y Comunicación (TIC).....	30-31
2.3.4 Rol del Docente dentro de las TIC.....	32-34
2.3.5 El Internet.....	35-36
2.3.6 La web 2.0.....	36-38

2.3.7 Las Redes Sociales.....	38-42
2.3.8 La Seguridad en Redes Sociales.....	42
2.3.8.1 Los Perfiles de usuario.....	42-47
2.3.8.2 Los Delitos cibernéticos.....	47-49
2.3.9 El Taller.....	49-51
2.3.10 Aproximación del Modelo ADITE.....	51-55

CAPITULO III: MARCO METODOLÒGICO

3.1 Nivel de la Investigación.....	56-57
3.2 Diseño de la Investigación.....	57-58
3.2.3 Técnicas e Instrumentos de Recolección de Datos.....	58-68
3.2.1 Instrumentos.....	58-67
3.2.2 Técnicas.....	67-68

CAPÍTULO IV: LA PROPUESTA

4.1 Componentes del Diseño.....	69- 97
4.1.1 Componente Análisis.....	71-79
4.1.2 Componente Tecnológico.....	79-81
4.1.3 Componente Evaluación.....	81
4.1.4 Componente Diseño.....	82-86
4.1.4.1 Descripción de las Actividades.....	78-97

CAPÍTULO V: ANÁLISIS DE LOS RESULTADOS

Análisis del Cuestionario de Juicio de Experto.....	98-105
5.1 Componente Análisis.....	98-99
5.2 Componente Tecnológico.....	100-101
5.3 Componente Diseño.....	101-103
5.4 Componente Evaluación.....	103-105

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.....	106-110
Recomendaciones.....	111-113

REFERENCIAS BIBLIOGRAFICAS.....	114-120
--	----------------

ANEXOS

Entrevista al Prof. Vito Lacasella.....	121-132
Cuestionario Validación de Instrucción.....	133-144
Cartas de los Validadores.....	145-147
Instrumento Completo para la Validación de Experto.....	148-195
Cartas de los Expertos.....	196-198

ÍNDICE DE TABLAS, FIGURAS Y ESQUEMAS

PP

Tablas

1. Objetivos del Contenido de Informática.....	9
2. Semejanzas y Diferencias de la Sociedad del Conocimiento y la Sociedad de la Información.....	29
3. Principales Redes Sociales.....	40
4. Ventajas y Desventajas de los perfiles públicos y privados.....	44-45
5. Operalización de variable.....	61- 65
6. Clasificación de los contenidos del Taller	75

Figuras

1. Esquema modelo ADITE.....	52
2. Componente Análisis.....	53
3. Componente Diseño	54
4. Componente Tecnología.....	54
5. Componente Evaluación.....	55
6. Adaptación del modelo ADITE.....	70

Esquemas

1. Competencia del Rol Docente en las TIC.....	33
2. Aportes de la web 2.0.....	37
3. Línea del tiempo de las Redes Sociales.....	38
4. Esquema del Talle: Plan de Formación del Taller.....	84- 86

ÍNDICE DE GRÁFICAS

	PP
Componente Análisis.....	99
Componente Tecnología.....	100
Componente Diseño	102
Componente Evaluación.....	104

INTRODUCCIÓN

El impacto de las redes sociales ha sido paulatino y contundente dentro de nuestra sociedad, ha influido no sólo dentro de los procesos de interacción sino además en los comunicativos; ampliando de forma significativas los medios para expresar nuestras opiniones, deseos, contenidos e imágenes. Nos hemos convertido en una sociedad en red e híper conectada, ya que a nivel mundial contamos con tabletas, smartphones y computadoras quiénes tienen acceso al internet permitiendo encontrar contenidos audio- visuales recreativos para todo tipo de usuarios de una manera muy sencilla.

La influencia de estos espacios se ha logrado incluir dentro de espectros políticos, económicos, culturales y por supuesto educativos. Dentro de la educación su influencia ha sido de tal magnitud que ha generado cambios dentro de las tendencias pedagógicas en pro a su incorporación dentro de los procesos de Aprendizaje-Aprendizaje, creando teorías como el conectivismo, que no solo apoya la idea de su incorporación sino además la emplea para el almacenamiento de aprendizajes y contenidos dentro de grandes bases de datos que nos aportan el internet y la web 2.0.

Ahora bien, estos espacios ajustados dentro de la práctica docente han generado experiencias positivas y enriquecedoras, empleándose en su mayoría dentro de la educación superior universitaria y muy poco dentro de la pre-universitaria. Una etapa de alguna manera descuidada, en cuanto a la formación en este eje de temáticas. En Venezuela, contamos con una alta penetración dentro de las redes sociales, sobre todo por parte de los grupos etarios que pueden legalmente aperturar cuentas en los web site.

Con la masiva afluencia dentro de ellos han surgido fenómenos de ciber delitos, donde las víctimas o los victimarios, son los usuarios en ocasiones por su desconocimiento o imprudencia. Lo cierto, es que se ha convertido en una situación que con el tiempo ha ido progresando y nuestro país no escapa de ello, esto se confirmó con la entrevista realizada al profesor Vito

Lacasella (2015), quién nos aseveró que dentro de sus prácticas en talleres en el tema de seguridad en redes sociales, se ha encontrado con niños de sexto grado víctimas de ciberbullying ocurriendo lo mismo dentro de la educación media general no sólo con casos de ciberbullying, sino además, de sexting; donde los discentes comparten fotos con contenido erótico o semi-erótico.

Lo agravante de la situación es que los docentes no saben cómo atacar el problema y se les está presentando en el aula. No obstante, es un problema que pasa a lo curricular, ya que una de las razones por los que docentes de informática, no cuentan con tal formación, es porque ni siquiera es un contenido contemplado dentro del Currículum Básico Nacional (CBN). Lo que hace que exista una transversalidad del problema.

Hacemos referencia al docente de informática, porque es quien posee la mayor competencia en el área para brindar el contenido de seguridad en redes sociales dentro de su práctica, además que forma a los discentes de los grupos etarios que pueden crear legalmente cuentas en los web site. Con el presente diseño se busca proponer un plan de formación dentro del contenido de seguridad en redes sociales dirigido a los docentes de educación media general en el área de informática. El mismo, poseerá los conceptos y herramientas básicas para que él discente pueda saber cómo abordar el tema de una manera didáctica. Es un problema que se puede atacar, pero es necesario partir con su facilitador base.

Desde el aspecto metodológico se contó con la autora Polo (2003), quién propone un modelo de tercera generación llamado ADITE, que sirve para el diseño de un medio computarizado compuesto por cuatro dimensiones claves: Análisis, Tecnología, Diseño y Evaluación. Estos a su vez contienen sub-dimensiones que nos permite entender que aspectos se desarrollan dentro del diseño instruccional. Por las características de la propuesta se le ejecutó una serie de adaptaciones. La investigación es descriptiva y de campo- tecnológica.

La investigación llega hasta la propuesta y evaluación por un panel de expertos que tuvo la tarea de valorar el diseño, materiales y medios audiovisuales. La investigación cuenta con cinco

capítulos que dan vida, sustento teórico y metodológico. Estos son: Capítulo I, da lugar a la presentación del planteamiento del problemas, los objetivos ha abarracar por parte de la investigación, la justificación como autora del porque es importante el diseño del taller y las limitaciones encontradas dentro del proceso investigativo, seguido del Capítulo II, que compone todo el aspecto teórico de la investigación ya que en el se ubican los antecedentes, las bases legales y teóricas del mismo.

Posterior a ellos está el Capítulo III, el cual posee el aspecto metodológico indicando nivel y tipo de investigación así como las técnicas e instrumentos aplicar. Una vez claro lo anterior, se pasa al Capítulo IV, quien posee la propuesta completa del plan de formación para ser apreciado.

Finalmente presentamos el Capítulo V, que compone el análisis de la validación de experto, las conclusiones y recomendaciones de la investigación. De esta manera presentamos sistemáticamente las cinco partes del trabajo de licenciatura. El lector podrá no solo apreciar los capítulos mencionados, sino además los anexos y las referencias bibliográficas.

CAPÍTULO I

EL PROBLEMA

1.1 Planteamiento del Problema:

La educación para un país es un elemento de gran importancia, sobre todo para el desarrollo social, tener una población con oportunidades de estudios es la garantía de un país con ocasión de trabajo calificado y de desarrollo económico. Para un docente, la tarea de formar no es sencilla, dado que en ella, existen factores como la familia, la política, economía y contextos sociales que influyen dentro del proceso formativo.

Las tecnologías y la innovación, le dieron un nuevo sentido a la sociedad y a las relaciones humanas. Hoy en día, contamos con las TIC, el Internet, la Web 2.0 y las Redes Sociales para relacionarnos, investigar y hasta para enterarnos de noticias al otro lado del mundo en tiempo real. Estas herramientas, han influido tanto en los aspectos políticos, económicos, sociales, culturales como en los educativos.

En especial, dentro de la educación han generado la creación de nuevos paradigmas y pedagogías entorno a ellas. El doctor en ciencias en computación de la universidad de Chile, Sánchez (2012), en su artículo “Usos educativos del Internet”, expone:

Internet constituye uno de los componentes de las llamadas Nuevas Tecnologías de Información y Comunicación (ntic). Dichas tecnologías penetran diversos ámbitos de la vida humana, desde la empresa hasta el hogar. Su inserción se encuentra fuertemente vinculada a los cambios sociales, políticos y económicos de las últimas décadas.

La escuela y el liceo no se encuentran ajenos a este proceso. Cerrar la posibilidad de ingreso de tecnologías como Internet a la educación implica desconocer y enajenarse de los cambios e innovaciones que se están generando en nuestra sociedad. (pág.2)

Esto implica, que se espera del docente mayor responsabilidad y compromiso a la hora de actualizar y desarrollar las competencias en los temas según el contexto y lo que los discentes del momento demanden, es tan así la relevancia de las competencias docentes en la TIC, que la UNESCO crea el proyecto “Estándares UNESCO de Competencia en TIC para Docentes” (ECD-TIC), exponiendo:

Hoy en día, los docentes en ejercicio necesitan estar preparados para ofrecer a sus estudiantes oportunidades de aprendizaje apoyadas en las TIC; para utilizarlas y para saber cómo éstas pueden contribuir al aprendizaje de los estudiantes, capacidades que actualmente forman parte integral del catálogo de competencias profesionales básicas de un docente.

Los docentes necesitan estar preparados para empoderar a los estudiantes con las ventajas que les aportan las TIC. Escuelas y aulas –ya sean presenciales o virtuales– deben contar con docentes que posean las competencias y los recursos necesarios en materia de TIC y que puedan enseñar de manera eficaz las asignaturas exigidas, integrando al mismo tiempo en su enseñanza conceptos y habilidades de estas. Las simulaciones interactivas, los recursos educativos digitales y abiertos (REA), los instrumentos sofisticados de recolección y análisis de datos son algunos de los muchos recursos que permiten a los docentes ofrecer a sus estudiantes posibilidades, antes inimaginables, para asimilar conceptos.

Las prácticas educativas tradicionales de formación de futuros docentes ya no contribuyen a que estos adquieran todas las capacidades necesarias para enseñar a sus estudiantes y poderles ayudar a desarrollar las competencias imprescindibles para sobrevivir económicamente en el mercado laboral actual. (pág. 2)

Por esta razón, enajenarse no es la solución más idónea sobretodo en el rol de formadores. Dentro de la educación estas herramientas se han convertido en una necesidad, para generar nuevos entornos de aprendizaje así como estrategias. El uso del internet, en el sistema educativo, es un derecho respaldado por organismos internacionales como la ONU, ya que para el 2009 lo declararon un derecho humano.

Al contemplarse la incorporación de dichas herramientas dentro la educación formal y las competencias en TIC, la actualización docente debe estar a la par. Hoy en día podemos compartir experiencias, opiniones, vivencias o conocimientos de un área en específico, imágenes y videos; sin importar el uso horario o las distancias geográficas. Es por ello que el docente debe

implementar y saber usar los espacios de la web 2.0. Torres (2006), en su artículo “Web Educativa 2.0”, expresa:

Los máximos exponentes de esta nueva Web 2.0 quizás sean los blogs, weblogs o bitácoras, con su correspondiente versión educativa: los edublogs como una muy fácil y gratuita forma de poder escribir periódica, personal o colectivamente en Internet, permitiéndose el debate o los comentarios sobre cada uno de los temas o mensajes que se vayan produciendo.

La web 2.0, brinda interactividad y retroalimentación; invitando a los docentes a aplicarlos en su práctica, tanto a nivel pre-universitario como universitario. Por tal motivo, un docente debe tener competencias cognitivas, aptitudinales y procedimentales en estos nuevos tiempos orientados a herramientas como las TIC, el internet, la web 2.0 y sobretodo en el uso seguro de las redes sociales. Se hace énfasis en el uso seguro de las redes sociales, ya que es un espacio que se ha prestado para cometer ciberdelitos, precisamente por el uso inadecuado que en ocasiones como usuarios se les da a dichos espacios de socialización.

Queda claro que la desinformación docente no radica en el conocimiento o manejo del internet, la web 2.0 o las redes sociales, ya que el boom de estos espacios ha sido de tal impacto que de forma paulatina estos se han visto en la obligación o necesidad de incorporarse a ellos ya sea con intensiones informales de socializar o en aras de aplicar una estrategia formal con su equipo de discentes. Y esto lo podemos respaldar con la investigación ejecutada por ComScore Inc. compañía líder mundial en medición digital, quienes realizan una publicación sobre “El Crecimiento de las redes sociales en América Latina” en el 2011, indicando:

En Junio de 2011, mil cien millones de personas (de edad 15 o superiores accediendo a internet desde sus hogares o trabajo) visitó un sitio de redes sociales a nivel mundial, un aumento del 22% desde Junio 2010. El 81,4% de todos los usuarios de Internet visitan destinos de redes sociales, representando una de las principales actividades online a nivel mundial.

Si contamos con este crecimiento poblacional dentro de ellas, en líneas generales podemos afirmar que el desconocimiento de estos espacios, no se posee. Sin embargo, navegar en ellas sin la debida formación en seguridad, podría generar más problemas que beneficios, ya que en ellos

se cometen delitos como Ciber-bullying, Grooming, Sexting, Fhising o Plagio de Identidad; es decir, es más un tema asociado al cómo lo hacen. En la actualidad el docente debería conocer e impartir estos temas, tanto para sus discentes como en aras de canalizar estas situaciones dentro y fuera del aula apoyando a la familia como actor importante que esta incluido dentro del proceso educativo.

Es así, por lo que el docente debe tener una formación calificada en “Seguridad en Redes Sociales” antes de siquiera aplicarlas como una estrategia educativa. Conceptos como password, piratas informáticos, ransomware o los expuestos antes no debería ser ajenos, sobre todo por las demandas educativas actuales. Por su puesto, el impartir estos contenidos está relacionado al currículo básico o programas diseñados en cada país y su sistema educativo.

Dado que Venezuela es uno de los mercados con mayor penetración en redes sociales dentro de la región de Centro América, contando con una población de 3.1 millones de audiencia, en el 2011, liderando redes como Facebook y Twitter (ComScore Inc), la formación en seguridad en redes sociales se hace una necesidad formativa, ya que tenemos índices importantes de consumo de estos espacios, lo que garantizar que estos usuarios naveguen y socialicen teniendo claros los aspectos básicos de la seguridad en redes sociales, es una obligación. Para saber si el tema se contempla, es necesario investigar cómo se estructura el sistema educativo venezolano y cuál programa contempla tal contenido.

El sistema educativo venezolano, está compuesto por tres etapas: I. Educación pres-escolar (1-7 años), II. Educación primaria (7-12 años) y III. Educación media general (7º, 8º y 9º, que va de los 12-15 años) y diversificado (4to. Y 5to, año y va de los 16-18 años). En ella se cuenta con docentes calificados, en cada área del saber, por lo que los contenidos expuestos anteriormente, pertenecen al área de informática o computación. La diferencia entre cada asignación, es que computación se ve en la segunda etapa de educación básica mientras que informática es a partir de educación media general.

Si partimos del hecho que para abrir cuentas legalmente en espacios como Gmail, Facebook, Twitter e Instagram; se debe ser mayor a los 13 años, política establecida por estos mismos web site, entonces, debemos asumir que es él docente de Informática de educación media general quién tiene la responsabilidad de formarse e impartir el tema de seguridad en redes sociales, ya que maneja en su mayoría a los grupos etarios que pueden abrir cuentas en estos espacios virtuales.

Es por ello que se cree oportuno que la educación media general sea una etapa clave para dar inicio con una educación crítica sobre el cómo deben hacer uso de las redes sociales de una manera segura, pese a, para ello debemos partir con formar o actualizar al docente en tal temática y él de esta área. Con esto no se busca descartar que docentes de otras áreas manejen o apliquen los conocimientos expuestos en su labor, lo que se busca es precisar, en qué área del conocimiento se ubica con mayor propiedad este tipo de temas u contenidos, que son propios a unas competencias docentes, por lo que se recomienda que sea el de informática de la educación media en general quién sea el facilitador clave para actualizar.

Ahora bien, quedando claro qué docentes deben formarse, así como el área del saber en él que debe estar ubicado y cuál etapa sería la más pertinente, para estos temas; es necesario conocer si se tiene planificado impartir este contenido, en tal etapa. Por tal razón, se consultó con el “Programa de Estudios y Manual del Docente (tercera etapa) Matemática–Física (1984)”, se debe aclarar que se consultó este programa en específico ya que es en la asignatura de matemática dónde se contempla según el Currículo Básico Nacional vigente (1994) los objetivos entorno a la enseñanza de la informática. (Ver tabla 1).

Tabla N° 1:

Objetivos Generales y Específicos de la Asignatura de Matemática-Física, de la tercera etapa de educación, en el contenido de informática.

Grado	Objetivos Generales	Objetivos Específicos
7°	XIII. Estudiar nociones elementales de Informática.	33. Diferenciar los conceptos de dato, información y procesamiento de datos.
		34. Analizar la estructura y funcionamiento de los computadores.
		35. Señalar las características básicas que identifican a un computador.
		36. Estudiar diferentes aplicaciones de los computadores.
8°	XV. Estudiar las nociones elementales de informática.	28.1 Introducir los símbolos usados en los diagramas de flujo
		28.2. Utilizar diagramas de flujo.
		29.1. Reconocer los Pasos a seguir para resolver problemas utilizando el computador.
		29.2. Reconocer los diferentes lenguajes de un computador.
9°	X. Estudiar nociones elementales de la Informática.	27. Distinguir los subsistemas que conforman un computador.
		28. Identificar las actividades fundamentales de la programación.

Nota: Elaboración de la autora. Fuente: Programa de Estudio y Manual del Docente- Tercer etapa. Asignatura de Matemática-Física (1984). Ministerio de Educación. Caracas

El cuadro anterior es un esbozo de los objetivos previstos a cumplir dentro de la educación media general, haciendo alusión a los contenidos que deben ser impartidos, lo que nos permite tener una referencia sobre las competencias conceptuales que el docente, que ya no es él de matemática, sino el de informática debe trazar para abordarlos, así como los contenidos alusivos. Con ello podemos analizar, que la formación gira en torno a los aspectos claves y principales de un computador, así como ejecutar una actividad dentro en ellos de una forma sencilla y secuencial.

Claro está, estos objetivos vienen aunados a un contexto educativo particular, al que me atrevería aseverar que ha cambiado, no solo a nivel político u económico sino además a nivel cultural y por ende educativo, por tal razón se puede entender que tal tema no este entre los objetivos, no obstante, se tienen un necesidad que atender con respecto a la temática.

Las datas anteriores nos dieron un esbozo del consumo de las herramientas de las TIC o las web 2.0, por lo que no podemos interpretar que existe desconocimiento, a pesar de que estos temas tampoco estén contemplados, queda evidencia de que existe un conocimiento empírico de ellos, por el uso que les dan. Ahora el cómo lo hagan, es un tema propio de seguridad en redes sociales y si nos basamos en el crecimiento de los ciber delitos, pues tenemos mayor propiedad para indicar que es un tema dónde mayor énfasis a nivel de docencia de debe hacer.

La importancia de este tema tanto a nivel curricular como en competencia docente, no es un mero capricho, a pesar de que en Venezuela no hay data pública de estos delitos; en primera instancia porque no se denuncian y en segunda porque el docente no sabe qué hacer con ellos cuando sucede en el aula y en ocasiones prefiere ignorar, se está convirtiendo en una situación real que está afectando no solo a los discentes, sino además, los docentes por lo que cada vez busca ayuda de instituciones o personal externo para que los guíe, en la capacitación u orientación ante tales situaciones.

Hablar de TIC, es también hablar de seguridad, a pesar de que el país ha buscado estar a la par de estas demandas establecidas y ha enmarcando dentro de su normativa legal incorporar sanciones en delitos cibernéticos como lo es la “Ley Contra los Delitos Informáticos”, aún existen vacíos informativos y formativos para dar vida y realidad a estas acciones, el acompañamiento del docente en ellas, es una de las clave para lograr su propagación en el aula y en la vida cotidiana.

Es una realidad de la que no escapamos como sociedad al establecer leyes y creer que con eso se soluciona; la educación cómo en todo proceso es clave, pero sin docentes formados en esta temática es imposible garantizar ciudadanos críticos en el uso de los espacios virtuales.

Hoy en día la tarea de actualización docente es exigente pues las competencias en esta era digital producto de la sociedad del conocimiento y de la información, van orientadas al dominio de los nuevos entornos digitales así como el uso de sus herramientas, pero de una forma crítica y

segura. La docencia como carrera indiscutiblemente no puede enajenarse a estas permutas que impulsan las tecnologías, como lo indica Zianni y Nessier (2014):

Como docentes del área las tics en el ciclo básico de las carreras universitarias, entendemos que la informática debe cruzar transversalmente los currículos –en ambos niveles de formación–, y ser utilizada en las demás asignaturas. Pero su uso no debe limitarse a contribuir a la enseñanza de otras materias, pues como disciplina tiene contenidos propios que requieren de un espacio curricular específico, además de docentes identificados con dicha área.

La incorporación de las tecnologías informáticas ha significado un adelanto incuestionable, pero también su uso inadecuado ha introducido manifestaciones inapropiadas para la sociedad. (pág. 129).

El tema de la seguridad en redes sociales, es importante por la connotación personal que conduce, por lo que es necesario iniciar acciones que estimulen la formación docente en esta temática, y para ello se debe partir con diseñar un plan de formación que incluya los elementos básicos y las herramientas para abordarlo. Es por ello que se propone diseñar y evaluar un taller en “Seguridad en Redes Sociales” dirigido a los docentes de informática, caracterizando a la investigación, por aportar una propuesta, que deje un precedente metodológico y teórico, a futuras investigaciones en esta área.

Es importante que se tenga presente que docentes informados y formados, apoyan la formación de discentes responsables y críticos en su seguridad dentro de los entornos virtuales. Con ello, no dejamos de reconocer que la familia es un actor importante dentro del proceso de formación en especial en este tipo de temáticas, sin embargo, consideramos que el docente de informática puede contribuir posteriormente a la formación u orientación discente-familia, por tal motivo, no anulamos la participación de la familia sino que consideramos que el docente de informática es la clave inicial del proceso de actualización en temáticas que ya son una necesidad en nuestra sociedad en red. A partir de ello, surgen las siguientes interrogantes:

- 1- ¿Existe presencia de delitos cibernéticos en Venezuela, en la etapa de educación media general?
- 2- ¿Cuáles son los fundamentos teóricos en el contenido de seguridad en las redes sociales?
- 3-¿Cuáles elementos formativos debe poseer la propuesta para el diseño del taller en “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática?
- 4- ¿Cómo realizar la evaluación formativa para el diseño del taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática?

1.2 Objetivos de la Investigación:

1.2.1 Objetivo General:

Proponer el diseño del taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática.

1.2.2 Objetivos Específicos:

1. Fundamentar mediante la entrevista experto, la pertinencia de la formación en el tema seguridad en redes sociales, para el apoyo de la actualización de los docentes de educación media general de informática
2. Analizar los fundamentos teóricos en el tema seguridad en redes sociales.
3. Diseñar el taller “Seguridad en Redes Sociales” dirigido a los docentes de educación media general de informática.
4. Evaluar mediante la validación de experto, el diseño del taller en seguridad en redes sociales dirigido a los docentes de educación media general de informática.

1. 3 Justificación de la Investigación:

Hemos venido explicando detalladamente la situación existente entre la relación formación docente y el tema de Seguridad en Redes Sociales, así como las carentes investigaciones o propuestas en esta temática. También hemos resaltado que el contenido ya hoy por hoy, en esta era digital, es obligatorio dentro de las aulas de clases, específicamente en educación media general, dado que ahí inician con mayor énfasis el consumo de espacios como Facebook, Twitter, Instagram y Correo electrónico. Aunque existen algunos docentes que si han incorporado estos espacios en sus aulas, no lo hacen teniendo presente los elementos de seguridad.

Se necesita la masificación de estas acciones, dentro de la educación venezolana, ya no es suficiente que algunos docentes sepan o lo apliquen, es necesario que en su mayoría o totalidad lo hagan con prudencia y con la formación adecuada. Como dijimos, el acceso a las redes sociales es cada vez mayor, Manzano (2012) en su artículo “Cifras del internet en Venezuela” indica que en los últimos registros proporcionados por la “Comisión Nacional en Telecomunicaciones” existe en el país una población de 12 millones de usuarios en internet, liderando el Distrito Capital:

El Distrito Capital domina en penetración de internet (92,90% de su población). Además es la entidad con mayor crecimiento interanual con un alza 3,08% en el primer trimestre de 2013, seguido de Miranda (3,09%), Nueva Esparta (1,80%) y Carabobo (1,35%). El estado con menos usuarios de internet es Amazonas con 26.335 y el mayor es Miranda con 2.872.240.

Estos datos empíricos son relevantes, ya que exponen el impacto de estas redes en el país de forma general. Ahora bien, para afianzar la importancia de la propuesta, debemos conocer como es el comportamiento de los usuarios en estos espacios virtuales, como en Venezuela no hay data sobre ello se consulto con la publicación del portal de Universia, quien expone los resultados brindados por la encuesta realizada en Colombia, país hermano, por el “Centro de Investigaciones

Pew” en el 2013 quiénes consultaron con una muestra de 802 adolescentes entre 12 y 17 años y a sus padres, arrojando:

... un 91% aseguró mantener contacto con miembros de su familia, un 98% con amigos del colegio, un 30% con profesores y maestros, y un 33% con personas que nunca han visto en la “vida real”.

Un 91% de los adolescentes incluye una foto suya en su perfil, un 71% da a conocer el nombre de la escuela o instituto al que asisten, y un 20% revela su número de teléfono celular. Por otra parte, el 71% expone su ciudad de residencia, el 82% su fecha de cumpleaños, el 92% su nombre real, el 53% la dirección de su cuenta de correo electrónico, el 62% su situación sentimental, y el 24% aseguró haber subido un video de sí mismo en esta red... mientras que un 26% de estos adolescentes incluye información falsa en su perfil para “desorientar” a los curiosos y proteger así su identidad.

Estas estadísticas exponen una aproximación del panorama en el comportamiento en estas redes por parte de la población adolescente, pudiendo asumir esto cómo referencia para Venezuela, con respecto a cómo los usuarios se desenvuelven en ellas, quedando claro que tienden a brindar mucha información privada y poco a proteger su identidad. Estos comportamientos son preocupantes, ya que el acepten personas que jamás han visto, los hace vulnerables a delitos cibernéticos o ciber acoso. Y son estos aspectos, lo que el docente con la formación adecuada pueden apoyar y orientar como facilitador.

Es aquí donde empieza el fuerte de la investigación y la razón fundamental de realizar la propuesta, aunque podríamos preguntarnos ¿Qué tiene de innovador una propuesta, de formación docente, en el tema de seguridad en redes sociales? .Ya que claramente pareciera que deberían ser los discentes y no los docentes. Por lo que como investigadora planteo ¿Quién debe impulsar el proceso de retroalimentación?, ¿Quién es el encargado de guiar los procesos formales en el aula? y ¿Quién termina siendo un modelo a seguir para los discentes?

Como investigadora la respuesta es clara, el Docente. Él debe ser una guía y hasta propiciar los procesos formales, si bien el proceso es de retroalimentación es constante, sí el docente no está formado en temas de interés y actualizados, sí no aporta nada nuevo al proceso; se hace

partícipe de la desmotivación y hasta la deserción escolar. Los discentes no encuentran el interés de aprender algo que no le sea útil en la vida cotidiana. Ya no nos podemos aislar en el uso de la seguridad en redes sociales, debido a que es un tema importante y aplicable dentro de la vida cotidiana tanto de docentes como de discentes.

Debemos asumir el compromiso de ser garantes de disminuir las tasas de ciber-bullying o sexphsing, dentro de la población adolescente. La innovación de la propuesta es aportar en primera instancia un diseño del taller sobre el tema de seguridad en redes sociales, partiendo con los guías y bases, es decir, con los docentes de educación media general de informática. Rivera Sandoval (2011), expone:

La falta de formación docente para el uso de las tics ha sido una problemática, la cual muchas de las veces inicia desde la apatía por aprender, la falta de capacitación, la falta de recursos económicos para poder darle mantenimiento a las computadoras y esto implica por supuesto un obstáculo en el proceso enseñanza-aprendizaje (pág. 1)

Sandoval (2011), insiste en que “El docente debe desarrollar la habilidad para buscar, interpretar y discriminar información proveniente de las TIC para aplicarla de acuerdo a las necesidades específicas de aprendizaje de sus alumnos” (pág.2). Volvemos a recalcar hablar de la formación en las TIC, sin duda alguna incluye formación en seguridad en estos espacios. Es así como insistimos, los docentes del área de informática son los que más a la vanguardia en estos contenidos deben estar.

Proponer el diseño de un taller, sirve cómo una referencia dentro del sistema educativo, para su posterior incorporación y aplicación a los programas, así como darle a la escuela de Educación de la Universidad Central de Venezuela, una propuesta innovadora en un tema a la vanguardia de las necesidades de esta era digital pues así como las TIC son una obligación en la formación docente según organismos como UNICEF y ONU, la formación en seguridad en redes sociales es igual.

El énfasis de aplicar la estrategia del taller, para propiciar aprendizajes cooperativos, entendido como “... los alumnos trabajan juntos para maximizar su propio aprendizaje y el de los demás” (Johnson, Johnson y Holubec 1999). Es porque la propuesta del diseño se orienta a generar una actualización a los docentes de educación media general de informática, partiendo de sus experiencias. El taller se define como:

...una forma de enseñanza aprendizaje donde se construyen colectivamente los conocimientos con una metodología participativa, dinámica, coherente, tolerante frente a las diferencias; donde las decisiones y conclusiones se toman mediante mecanismos colectivos, y donde las ideas comunes se tienen en cuenta. (Añorga Morales, J. y otros, 1995 cit. Sequera y Agüero, 2011)

Para ello se realizó la planificación de los objetivos, contenidos, estrategias y recursos pertinentes al tema “Seguridad en Redes Sociales”, con fin de alcanzar el aprendizaje cooperativo, por parte de los docentes. La investigación posee factibilidad ya que responde a una necesidad actual, se orienta a la formación de una población que no está aislada de sistema educativo y puede llegar a disminuir tasas del acoso en la red, ciber-bullying y sexting/sexphsing, además de que los docentes pueden apoyar la lucha contra el fenómeno del acoso cibernético.

Esta investigación es innovadora para el país, la sociedad venezolana y para la casa que vence las sombras, la Universidad Central de Venezuela y sobre todo para la escuela de Educación, escuela promotora de la formación de los futuros docentes de aula, es una investigación que brinda una herramienta instruccional a la vanguardia de las necesidades y sobre todo sigue la razón central de un docente, que es la de seguir aprendiendo cada día. Es así como no solo sustentamos su relevancia, sino además, su importancia pues es un aporte significativo para seguir apoyando la formación y actualización docente en el área de informática, que en esta era digital, juega un papel indispensable dentro la educación formal.

1.4 Limitaciones de la Investigación:

Por el alcance de la investigación, la misma sólo será una propuesta a validar, por lo que no se plantea la ejecución del taller por el factor tiempo y planificación. Dado que el desarrollo teórico e investigativo, fue extenso se tomó la decisión de solo llegar hasta la validación y de esta manera darle dedicación y relevancia al plan de formación; sumado a esto la aplicación del taller implicaba una mayor logística y no se contaba con los recursos, sin embargo, se buscó dar la relevancia valorativa que la propuesta requiere. Con ello dejamos claro a futuras investigaciones que con la presente investigación tendrán una base metodológica del plan de formación y la validación del mismo, de esta manera contarán con los recursos bases para su posterior aplicación.

CAPÍTULO II

MARCO TEÒRICO

Este capítulo está constituido por los antecedentes, las bases legales y teóricas de la investigación, siendo una continuación de los elementos expuestos tanto en el planteamiento como en la justificación. De esta manera se puede brindar la respuesta al objetivo específico número uno y dos que hacen referencia a los fundamentos teóricos del tema “Seguridad En Redes Sociales”, así como exponer el arqueo teórico de la investigación.

2.1 Antecedentes de la Investigación:

Los antecedentes representan trabajos previos que tienen vinculaciones con la investigación. Fidias (1999), define los antecedentes, como: “...refiere los estudios previos y tesis de grado relacionadas con el planteamiento del problema, es decir, investigaciones realizadas anteriormente y que guarden alguna vinculación con el problema de estudio.” (pág. 38-39).

Teniendo presente que el problema gira en torno, a tres ámbitos estelares: 1) Las Redes Sociales, 2) La Seguridad en Redes Sociales y 3) La Formación docente, en seguridad en redes sociales, cómo proceso de actualización. En el primer antecedente, nos apoyaremos en el ámbito metodológico con el diseño de curso basado en la tecnología de la información comunicación (TIC), dentro de la Universidad Simón Bolívar, realizada por Álvarez (2003), exponiendo:

En Venezuela, se han dado importantes experiencias en pro de la incorporación de la información en la escuela, proyectos como los liderizados desde CENAMEC (Una computador para cada escuela) y QUORUM (capacitación de docentes) entre otros, dan cuenta de lo escrito, sin embargo, se puede fácilmente constatar que el paradigma vigente dentro del aula continua siendo docente “buen expositor” (pág. 6)

En su propuesta toma el enfoque constructivista, basado en la teoría del aprendizaje socio-cultural de Vigotsky y el aprendizaje significativo de Ausubel. Teniendo por objetivo general “Formular una metodología para el diseño de cursos de actualización tecnológica dirigido a docentes acerca del uso de las TIC en educación” (pág. 14).

Punto clave de la investigación, pues de este antecedente, asumimos los referentes de su metodología para ser aplicado dentro del taller, con respecto al fundamento teórico de Ausubel y la metodología del trabajo, pues aun juegan un impacto dentro del proceso E-A. Además de que el diseño del curso, sirve como guía del plan de formación a diseñar del taller, en seguridad en redes sociales, contenido que es parte de las TIC y que así como el trabajo anterior, está orientado a la formación y actualización docentes, pero no para la etapa universitaria, sino para nuestro caso la pre universitaria.

Seguido a ello, nuestro segundo antecedente sustenta el aspecto práctico con respecto a la inclusión de las redes sociales dentro de la práctica docente, es por ello que consultamos a De Haro (2009), quién expone en su artículo “Redes sociales aplicadas a la práctica docente”, dónde narra su experiencia en la aplicación de las redes sociales dentro de la educación secundaria.

Esta estrategia piloto se realizó en el 2008, en el centro “Amor de Dios” de Barcelona-España, para las etapas de secundaria. En ella, se desarrolló una red social, para las asignaturas de informática y matemática, de diversos niveles de bachillerato, utilizando una muestra para la primera de 50 discentes y para la segunda de 100. Con la primera la interactividad era exclusivamente para la asignatura, mientras que en la segunda recibían comentarios de su perfil y de los contenidos que estos compartían, por supuesto coherentes a la asignatura.

Lo que arrojó por efecto un incremento en los miembros de la asignatura de matemática dentro de esta red. Ya para el 2009, se manejaba dentro de ella una población de 314 miembros de los cuales 10 docentes y el resto discentes, lo que representa un claro éxito para la experiencia de incluir las redes sociales dentro de los aspectos formativos.

El éxito, según el autor, radicó en la motivación que sintieron los discentes por los contenidos que se encontraban, además, de la posibilidad de desarrollar relaciones entre estos, actuando en ellas el aprendizaje formal e informal, lo que permite “el incremento en la eficacia del aprendizaje de los alumnos” (De Haro, 2009:6). El autor aparte de lo expuesto antes asevera que:

Hasta ahora los intentos de utilizar las redes sociales en la práctica de la docencia se han limitado a experiencias aisladas realizadas con alumnos de educación superior, así como en la formación de profesores, y de forma mayoritaria para cursos individuales, formado por un profesor y sus alumnos. Las redes sociales utilizadas con fines estrictamente educativos en la educación pre-universitaria son prácticamente inexistentes. (pág. 1)

Ciertamente, lo que expone De Haro (2009), tuvo pertinencia en ese momento y aún tiene vigencia, dentro de los presentes contextos, ya que aún las acciones son pequeñas dentro de la educación media general, lo que va a la mano de la carente inclusión de estos contenidos en los currículos formales; así como en la actualización o formación docente, específicamente los pertenecientes al área de informática.

Por consecuencia, es un problema transversal que va de lo macro a lo micro pues sin docentes formados, no podemos esperar discentes educados en los usos apropiados de estas redes. El aporte del autor, es teórico y nos da un esbozo sobre cómo se puede abordar la situación y sobre los posibles resultados positivos que se pueden obtener con su aplicación desde la experiencia de Haro (2009).

Su iniciativa parte de una necesidad, similar a la de esta propuesta. La carente inclusión de estos contenidos o herramientas dentro de la educación pre-universitaria, es una realidad de la que no escapamos como docentes. La formación y disposición de los docentes, es la clave para el éxito de estos aprendizajes.

El uso de las TIC, la web 2.0 y las redes sociales, han generado la importancia de la formación en “Seguridad dentro de las Redes Sociales”, volviéndolo un contenido obligatorio en estos nuevos contextos educativos, marcando una pauta pedagógica. Para finalizar, se consultó con nuestro tercer antecedente que es la monografía de Sánchez (2010).

Realizada para optar por el título de ingeniería electrónica y telecomunicaciones, en la Universidad Autónoma de Hidalgo-España. Enfocada en “Seguridad en Redes”. El autor hace un desarrollo teórico, de tipo documental, sobre la relevancia que tiene la seguridad en redes, expresando:

La seguridad en redes es de dos tipos: físicas y lógica. En la primera, se debe estar atento y tomar medidas preventivas como son desastres naturales, inundaciones, terremotos, incendios, así como también en las instalaciones eléctricas, etc. En la segunda, se debe tener cuidado con aquellas personas que no están autorizadas para el acceso de la información, y es aquí donde entran los piratas informáticos, un ejemplo de ellos son los hackers, crackers, etc. (pág. 7).

Por su puesto para el diseño del taller, el interés radica en aquellos ataques denominados como “lógicos” por el autor. Por ser los ataques más comunes dentro de las redes sociales, por su parte el objetivo general que se establece para la elaboración su monografía es: “Describir y analizar los factores que intervienen en la seguridad en redes, a partir de los usuarios que buscan la mayor protección y confiabilidad de información en su red, utilizando herramientas y políticas de seguridad, para alcanzar ese fin” (pág.10). Para su investigación desarrolla conceptos como: password/contraseñas, identificación y autenticación, que son hackers, crackers, piratas informáticos y virus, además, de cómo contrarrestarlos.

Conceptos que nos sirven de apoyo dentro de los contenidos que poseerá el taller en seguridad en redes sociales, el aporte de está monografía, nos permite brindar un sustento teórico, sobre la relevancia que posee el contenido, traspolado para las redes sociales, dado que los conceptos antes expuestos son claves para el desarrollo del taller. Los docentes, necesitan formarse en ellos para poder ser guías posteriores. Por ello usamos esté antecedente. Sánchez (2010) asume que los riesgos dentro de las redes son reales, por lo que afirma:

“...la seguridad no debería ser un problema, ni en las redes, ni en la vida cotidiana, pero como no se tiene conciencia social, algunos humanos, ya sea por avaricia, por curiosidad mala, por ambición, etc., pierden aquellos valores como la generosidad, amabilidad, sencillez, etc., por lo cual se debería vivir en armonía...” (pág.130).

Apoyándonos en Sánchez, al expresar que la seguridad en teoría no debería ser un problema, pero en la práctica se ha convertido en uno, por lo que se considera que la educación puede jugar un impacto relevante ante tal fenómeno. El generar la conciencia y la responsabilidad como cibernauta, debería ser un trabajo de la escuela y las familias pues ellas cumplen un rol significativo dentro de la sociedad. Estas redes se han hecho parte de nosotros como ciudadanos, por lo que no es responsable como docentes enajenarnos de ser parte de la formación en estos conocimientos. En este contexto el diseño del taller, puede apoyar la solución de la carencia de formación docente en el tema de seguridad en redes sociales.

Las tres investigaciones ayudan a abordar los ejes centrales de la propuesta, ya que la investigación de De Haro (2009), es un vivo ejemplo de cómo una experiencia piloto en la tercera etapa de educación básica, bien organizado puede generar resultados positivos y estimular el aprendizaje de los discentes en los contenidos, el autor lo aplicó con redes sociales como medio, pero nosotros podemos trasladar esta experiencia, apostando al diseño del taller en seguridad en redes sociales, ya que puede traer igual o mayores respuestas positivas con respecto a la participación. Mientras que el Rubén Bustamante (2010), en su aporte teórico de los conceptos para el taller así como la clasificación que tienen los delitos cibernéticos considerados ataques “lógicos”.

Por último El trabajo de Álvarez (2003), aporte la estrategia y la fundamentación teórica con respecto al diseño del curso dirigido a docentes, lo que nos permite emplearlo para el diseño del plan de formación. De esta manera los aportes suman una confirmación desde lo teórico y lo metodológico sobre lo factible de la presente propuesta.

2.2 Bases Legales de la Investigación:

La normativa central que rige los sistemas políticos, económicos, sociales y educativos en Venezuela es la Constitución de la República Bolivariana de Venezuela (CRBV), aprobada en 1999. Enmarcando elementos indispensables dentro de la educación, cómo por ejemplo:

Artículo 102 °

La educación es un derecho humano y un deber social fundamental, es democrático, gratuito y obligatorio... El Estado, con la participación de las familias y la sociedad, promoverá el proceso de educación ciudadana, de acuerdo con los principios contenidos en esta Constitución y en la ley.

Artículo 103°

Toda persona tiene derecho a una educación integral de calidad, permanente, en igualdad de condiciones y oportunidades, sin más limitaciones que las derivadas de sus aptitudes, vocación y aspiraciones. La educación es obligatoria en todos sus niveles, desde el maternal hasta el nivel medio diversificado...

La C RBV, como carta magna, obliga a las demás leyes a regirse en torno a ella, la educación en el país represente un derecho humano, esto implica educar al hombre tanto en los entornos sociales como los digitales. La incorporación de la tecnología e innovaciones dentro de los procesos formales, no sólo incluye las TIC, sino además, todos los elementos que mejoren e influyan en la calidad de vida y educación del venezolano. En el siglo XXI la educación y la tecnología, van a la par pues no puede funcionar una sin las herramientas que le aportan a la otra. El uso de estas herramientas también se contempla en la Ley Orgánica para la Protección del Niño y el Adolescente (LOPNA) (2007), exponiendo:

Artículo 73.

Fomento a la Creación, Producción y Difusión de Información Dirigida a Niños y Adolescentes. El Estado debe fomentar la creación, producción y difusión de materiales informativos, libros, publicaciones, obras artísticas y producciones

audiovisuales, radiofónicas y multimedias dirigidas a los niños y adolescentes, que sean de la más alta calidad, plurales y que promuevan los valores de paz, democracia, libertad, tolerancia, igualdad entre las personas y sexos, así como el respeto a sus padres, representantes o responsables y a su identidad nacional y cultural. (p. 69)

Estas normativas hacen énfasis a la relevancia del Estado como garante de la formación y orientación de los procesos formales, indicando como política la aplicación y creación de medios audiovisuales y multimedia. Sumado a esto el aspecto de la seguridad, se contempla en la Ley Orgánica de Telecomunicaciones (2000):

Artículo 2.

Los objetivos generales de esta Ley son:

Defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de telecomunicaciones, en adecuadas condiciones de calidad, y salvaguardar, en la prestación de estos, la vigencia de los derechos constitucionales, en particular el del respeto a los derechos al honor, a la intimidad, al secreto en las comunicaciones y el de la protección a la juventud y la infancia. A estos efectos, podrán imponerse obligaciones a los operadores de los servicios para la garantía de estos derechos....

Artículo 12.

En su condición de usuario de un servicio de telecomunicaciones, toda persona tiene derecho a:

La privacidad e inviolabilidad de sus telecomunicaciones, salvo en aquellos casos expresamente autorizados por la Constitución o que, por su naturaleza tengan carácter público...

Que se le proporcione adecuada y oportuna protección contra anomalías o abusos cometidos por los prestadores de servicios de telecomunicaciones o por cualquier otra persona que vulnere los derechos establecidos en esta Ley.

Aunado a esto, se cuenta con la “Ley contra Delitos Informáticos” quien se encarga de enmarcar lo tipificado como delito y cuáles son los aspectos legales a contemplar así cómo su penalidad según sea delito, quiere decir, que para el Estado la seguridad en redes es relevante, tanto es así que lo especifica en el Capítulo II De los Delitos, en el Capítulo III: De los delitos

contra la privacidad de las personas y de las comunicaciones y el Capítulo IV: De los delitos contra niños, niñas o adolescentes, que va desde el artículo 20 al 24, se tipifica dentro de la normativa penalidades para delitos como el Sexting, Grooming, Phishing, por ejemplo:

Artículo 20. Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21. Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22. Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Artículo 23. Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas 7 advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24. Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Con los artículos anteriores, se expone cómo actualmente si contamos con la normativa jurídica para afrontar el fenómeno de delitos cibernéticos, pero como en todo proceso sin la difusión y formación, sería ley muerta, debido a que no haremos uso de los derechos que nos amparan como ciudadanos. La formación en seguridad en redes sociales cada vez se hace una necesidad y contenido imperante dentro de nuestro Currículo, contamos con la ley ahora hace falta la formación en ello.

2.3 Bases Teóricas de la Investigación:

Las bases teóricas se definen de la siguiente manera "... un conjunto de conceptos y proposiciones que constituyen un punto de vista o enfoque determinado, dirigidos a explicar el fenómeno o problema" (Fidias (1999:39). En las bases teóricas se desarrolló los elementos conceptuales del proyecto. La incorporación del tema "Seguridad en Redes Sociales", en la formación docente, no es una necesidad aislada, pues proviene de las demandas educativas que han surgido con los cambios contextuales, es así como pasamos a presentar las bases conceptuales y teóricas de la investigación:

2.3.1 Sociedad de la Información:

Valentini (2002) la presenta cómo:

El surgir de la Sociedad de la "Información" se debe al hecho de poder transformar la información digital en valor económico y social, en **conocimiento útil**, creando nuevas industrias, nuevos y mejores puestos de trabajo y mejorando la forma de vida de la sociedad en su conjunto a través de un desarrollo basado en el uso del conocimiento, apostando a **convertir el conocimiento en PBI**.

Por lo tanto cuidado con que el concepto de información nos haga perder de vista el sentido real de esta transformación, si hablamos de Sociedad de la Información en realidad estamos hablando de una sociedad que se propone manejar de forma diferente todo lo que tiene que ver con la gestión del conocimiento.

Lo expuesto por Valentini (2002), se entiende que la Sociedad de la Información, es la base para el desarrollo del conocimiento de una economía globalizada. Por ser aquella dónde el conocimiento tácito pasa hacer explícito, empleando la innovación y la tecnología que impacta directamente en la economía y en el desarrollo social, es decir, se asevera que esta sociedad toma auge con el desarrollo y evolución de las nuevas Tecnologías de la Información y Comunicación (TIC), de la era post-industrial, donde el hombre desarrolla la necesidad de hacer del conocimiento tácito una fuente económica.

Según Valentini (2002), la Sociedad de la Información se caracteriza por estar compuesta de los siguientes elementos:

1- **Nuevos entornos sociales, económicos y tecnológicos** productos de la Globalización y la innovación,

2- **Usuarios**, (ciudadanos, empresas, gobiernos, entre otros) quienes acceden a la información mediante una infraestructura que permite su conexión en red,

3- **Infraestructura**, que son las condiciones técnicas que permite el acceso a los contenidos (redes, terminales, servidores y ancho banda)

4- **Contenidos**, que es la información, los servicios y los productos a los que se puede acceder a través de la infraestructura. Básicamente esta sociedad brinda las bases para la búsqueda de la información de una manera accesible.

2.3.2 Sociedad del Conocimiento:

Esta sociedad, es la consecuencia de la sociedad de la información, sin embargo la presente se entiende como:

... una sociedad en la que las condiciones de generación de conocimiento y procesamiento de información han sido sustancialmente alteradas por una revolución tecnológica centrada sobre el procesamiento de información, la generación del conocimiento y las tecnologías de la información. Esto no quiere decir que la tecnología sea lo que determine; la tecnología siempre se desarrolla

en relación con contextos sociales, institucionales, económicos, culturales, etc. . .
(Castell, 2002)

Es decir, la Sociedad del Conocimiento, surge de la creación de los nuevos conceptos, teorías e hipótesis, que parten de un previo proceso de investigación, donde las tecnologías juegan un papel importante, más no, central, como lo aclara Castell (2002) es más el producto de las demandas externas las que impulsan el desarrollo a los nuevos conocimientos en aras de satisfacer las constantes necesidades sociales y mundiales, que con cada era y revolución han ido mutando. Ambas sociedades tienen elementos semejantes como claramente divergentes. Y los podemos apreciar a continuación (Ver tabla 2):

Tabla N° 2:

Semejanzas y diferencias de la Sociedad de la Información y la Sociedad del Conocimiento.

Semejanzas	Diferencias	
	Sociedad de la Información	Sociedad del Conocimiento
1. Son producto de las demandas sociales, económicas, políticas y educativas. 2- La tecnología juega un papel importante, para el desarrollo de las mismas. 3- La Globalización e innovación son el motor del desarrollo de ambas sociedades. 4- Son el producto de la evolución social de los países sub y desarrollados. 5-Ambas marcan un hito de la era industrial y la era digital.	1- Se basa en el desarrollo de la infraestructura para la obtención de información. 2- La tecnología y los recursos, son clave para la obtención de la información. 3- Surge de la era post-industrial. 4- Se asocia con la producción, creación, desarrollo y distribución de la información. 5- Se basa en los datos, la infraestructura, contenido.	1- Parte de la información para la creación o mejora de nuevos conocimientos. 2- Las personas con la clave para la creación y desarrollo del conocimiento. 3- Adquiere mayor auge en los 90. 4- Proviene del análisis, exploración y comprobación del conocimiento, para su posterior aplicación. 5- Se basa en las capacidades cognitivas de crear e innovar.

Nota: Elaboración de la autora. Fuente: Valentini López (2002). La Sociedad de la Información en América Latina y el Caribe: TIC y un nuevo Marco Institucional, y Castell, M (2002). La dimensión cultural del Internet. Ambos documentos en línea.

Al Analizar los contextos en que ambas surgieron, sus características, semejanzas y diferencias básicas, apostaríamos que se está en la transición de una era digital, producto de la sociedad de la información y del conocimiento, que se enfoca más en el desarrollo de nuevas tecnologías que contribuyan no solo al desarrollo social, sino también intelectual del ser humano.

2.3.3 Tecnologías de la Información y Comunicación (TIC):

Se puede apostar que se está en una era social, donde las tecnologías han influido en los ámbitos económicos, políticos, sociales y hasta culturales. Tanto es así que hasta la forma en la que hoy nos relacionamos está fuertemente vinculada a las tecnologías.

La década de los 80 y 90 representan una etapa potencial para el progreso de la tecnología y creación de nuevos conocimientos. Donde la incorporación de las TIC marca un hito, creando nuevos paradigmas mundiales, apostando al progreso e innovación social. Las TIC, según Vita (2008) cit. Gil (2002) y Ochoa & Cordero (2002), no son más que:

... según Gil (2002)... un conjunto de aplicaciones, sistemas, herramientas, técnicas y metodologías asociadas a la digitalización de señales analógicas, sonidos, textos e imágenes, manejables en tiempo real. Por su parte, Ochoa y Cordero (2002), establecen que son un conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes y canales de comunicación, relacionados con el almacenamiento, procesamiento y la transmisión digitalizada de la información. (Vita Montiel (2008) cit. Gil (2002) y Ochoa & Cordero (2002)

Ambas definiciones de las TIC, se consideran acertadas dado que toman los elementos claves, definiéndolas como aplicaciones, sistemas, herramientas y metodologías asociadas a la digitalización, derivadas de herramientas como hardware y software; que ayudan a lograr mayor accesibilidad a la información e interacción para producir nuevos conocimientos, promovidos por las necesidades sociales: de interacción e investigación.

Las TIC se pueden ver en entornos y escenarios sociales, culturales, organizativos, educativos, políticos y económicos; tanto en el país como a nivel internacional en el siglo XXI, de una forma masiva y hasta podríamos decir que cotidiana. Si bien cada uno de estos espacios y contextos son particulares para cada país, en la educación las TIC han jugado un papel relevante para el progreso dentro de la enseñanza y aprendizaje de una manera bilateral. En este contexto las autoras Puelles y Risco (2009), exponen:

El Sistema Educativo se encuentra inmerso en procesos de cambios sociales propiciados por la innovación tecnológica y, sobre todo, por el desarrollo de las TICs. Estos cambios hacen surgir nuevas concepciones de las relaciones tecnología-sociedad y a su vez de las relaciones tecnología-educación... por esta causa, ha existido la necesidad de adaptar y redefinir, los modelos pedagógicos.

Tomar en consideración los escenarios de aprendizaje propiciados por las TICs puede facilitar la concepción de ambientes de aprendizaje adecuados a las nuevas coordenadas espacio-temporales donde el papel protagónico lo desempeñe el estudiante sin obviar el rol de guía del profesor.

Las perspectivas que ofrecen las TICs en cada uno de los nuevos entornos de aprendizaje implican cambios organizativos en cuanto a la combinación de estos escenarios y los servicios integrados de aprendizaje (campos virtuales, proyectos institucionales de innovación tecnológica, etc.). Se trata de nuevas tendencias centradas en enriquecer y mejorar la calidad del curriculum y de la formación.

Las autores exponen dos elementos claves, uno de ellos es la contribución de las TIC para los cambios dentro de los modelos pedagógicos, uniéndose dentro del proceso y contribuyendo a que sea más dinámico para lograr el aprendizaje significativo deseado. Cada proceso histórico ha producido cambios dentro de la educación, y ahora con la incorporación de las tecnologías de información y comunicación se eliminaron fronteras y uso horario, haciendo más alcanzable la información. Aspecto que refleja como hoy en día podemos crear entornos y campos virtuales para la enseñanza.

Por otro lado las autoras hacen mención del rol docente y el del discente, el cual se cree que está la clave del éxito o fracaso de estas herramientas para la educación. Ambos roles cambiaron, exigiendo más por parte de ellos con el aprendizaje cooperativo, obligándolos hacer uso de espacios virtuales, procesos de retroalimentación y convertirse en seres activos dentro de la investigación. El del discente por su parte deja de ser pasivo y receptor únicamente, para ser activo, emisor y receptor constante, es por ello que el proceso de enseñanza- aprendizaje (E-A) pasa hacer más aprendizaje-aprendizaje (A-A), cambiando los modelos pedagógicos tradicionales.

2.3.4 Rol del Docente dentro de las TIC:

El docente cumple un rol importante para la presente investigación, es por ello que haremos énfasis es en él, dado que se ha visto significativamente afectado, y obligado a salir de los paradigmas tradicionales, para probar las nuevas tendencias las nuevas herramientas que ofrecen en otros entornos; elementos donde la resistencia al cambio ha repercutido de una forma más visible que la del discente. Otra razón, por la que se hará énfasis en este rol, es porque el trabajo se centra es en la actualización del mismo. Es así, como sustentaremos con Cabrero (2001), la relevancia de este rol, ya que él expresa que:

...el profesor desempeñará una función de evaluador y selector de información adaptada a sus estudiantes, es decir, será un soporte de información y de acceso a recursos para los propios estudiantes.

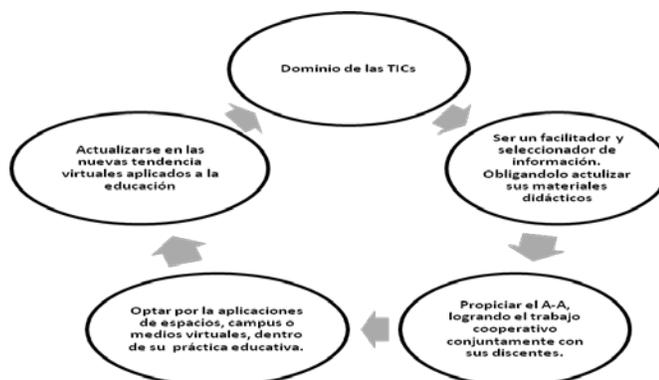
Ello supone también que el profesor realice una serie de esfuerzos para garantizar que todos los participantes en el proceso tengan las mismas garantías para su incorporación, independientemente de sus posibilidades de acceso a la tecnología, de su localización física, de su nivel de comprensión del lenguaje, o de su habilidad y pericia para interaccionar con el sistema...

Cabrero (2001), expone de una forma precisa cómo el docente se convierte en un “diseñador de situaciones de aprendizaje”. A la par de esto el Estado debe garantizar una educación que responda a las demandas internacionales, es decir, se requiere un docente constantemente actualizado y formado.

Con lo expuesto por Vita (2008), Puelles y Risco (2009) y Cabrero (2001); se podrá entender como las TIC han transformado los procesos pedagógicos tradicionales y sobretodo han impactado en las nuevas competencias del docente. Ya Básicamente el rol del docente pasa a transformarse y exigir el desarrollo de nuevas competencias no solo pedagógicas, sino también, informáticas, esas competencias son: (Ver esquema 1)

Esquema N° 1:

Competencias del Rol Docente dentro de las TIC.



Nota: Elaboración de la autora. Fuente: Cabrero (2001). Aplicación de las Tic: ¿Esnobismo o Necesidad Educativa?

Por supuesto estas competencias van a la mano de la formación docente en el uso de estas herramientas. Lo que se ha convertido no solo en una constante preocupación como se ha venido planteando, sino también, pasa hacer un problema dentro de la educación. Las causales sobre los elementos que inciden en la falta de formación docente, son multi-factoriales y ya hemos expuesto algunas.

Para Venezuela, como se mencionó en los antecedentes, tiene un trasfondo curricular, a pesar de que el docente si posee las competencias, la carencia de este contenido en los programas formales influye directamente en como ellos puedan manejar el contenido dentro de las aulas de clases. Cuando se le pregunto al profesor Vito Lacasella, en la entrevista: ¿Cómo percibe la formación docente con respecto a este tema?, ya que se sabe que existe la inquietud, pero ¿Realmente poseen la formación en este tema?, su respuesta inmediata fue:

“No, no tienen la formación, de hecho fíjate que una de nuestras estrategias en EPM Venezuela (Educación para los Medios en Venezuela), la estrategia que maneja para la enseñanza de la alfabetización mediática digital, proponemos que no solo debemos formar a los chicos. Hay que formar a los docentes y que hay que formar a las familias; hay que hacer un trabajo en conjunto...” (Vito Lacasella, entrevista personal, 2015, Enero 21)

Además analiza las bases del problema exponiendo que el mismo viene de lo macro a lo micro, es decir de lo curricular a la formación docente. En esta entrevista podemos rescatar cuando Lacasella (2015), expone:

“...en la actualidad en el Currículo Venezolano, especialmente en el área de informática, no se da eso. Dicho por los mismos profesores que conozco de informática.

Ahí se da es un saber instrumental, es decir, como manejar una PC, Word, abrir Windows, claves, etc. Pero manejar ese de tema de seguridad, son los profesores que sienten la necesidad de dar esa información y se la dan a los muchachos...” (Vito Lacasella, entrevista personal, 2015, Enero 21).

Es decir, para el país la falta de formación docente en el tema de las TIC, inicia en el currículo, pasa por la falta de recursos para la dotación de equipos, luego por la desmotivación personal del docente en actualizarse en los conocimientos nuevos y finalmente recae en la falta de organización o políticas públicas que promueven la actualización periódica del personal docente. Afectando así los procesos educativos. Básicamente esto es lo que podemos rescatar de la entrevista realizada al profesor Vito Lacasella. Ante este aspecto Martín, Lucena y Díaz (2002:256), exponen:

... la falta de formación de los docentes junto con la ausencia de las TIC en los centros, urge la necesidad de formar a los profesionales de la enseñanza en TIC, ya que en la actualidad el aprendizaje de nuestros alumnos está dominado por la tecnología de la que disponen en sus hogares o a la que acceden en otros lugares, y que usan de un modo acrítico e irreflexivo.

La falta de formación docente afecta de una forma relevante e incide en la calidad de educación que se brinda, sobretodo en el uso de las TIC y en los espacios virtuales que estas ofrecen, abriendo la posibilidad de que haya un uso inadecuado en estas herramientas. La formación como en todo, es clave para solventar estas situaciones. Que dificultan el proceso A-A.

2.3. 5 El internet:

En las TIC funcionan otras herramientas importantes, una de ellas es el internet, quién nace también de las demandas culturales, responsables de que sea posible el acceso a la información de una forma sencilla, así como lograr procesos de interacción dentro los espacios virtuales, Castell (2002), explica su origen en la producción cultural:

..Internet no es solamente ni principalmente una tecnología, sino que es una producción cultural... es, pues, la combinación de cuatro culturas que se apoyan mutuamente. Cuatro culturas que son distintas, pero que se van reforzando, que son unas responsables de las otras: la cultura universitaria de investigación, la cultura *hacker* de la pasión de crear, la cultura contracultural de inventar nuevas formas sociales, y la cultura empresarial de hacer dinero a través de la innovación.

El internet, como híper red conectada a ordenadores, móviles, tabletas o dispositivos con acceso a él, proviene de la demanda en la búsqueda de información y de acortar las distancias mundiales. Es por ello que Castell (2002), expone que es una producción de cuatro culturas, quienes interactúan constantemente dentro de las sociedades, a nivel mundial. Caracterizadas por ser un canal de comunicación, universal, omnifuncional, bidireccional y de gran alcance. Influyendo de una manera significativa dentro de la educación, Calero (2010) asevera a su vez:

Internet es también, una forma de motivación para la lectura y la investigación al presentar al usuario una interfaz atractiva, con recursos de sonido, imágenes, videos, animaciones y proporcionarle innumerables posibilidades como el acceso a informaciones actualizadas de las más diversas áreas del conocimiento; permitiendo ingresar virtualmente a las bibliotecas, museos, periódicos centros de investigación de todo el mundo. (pág. 37)

Otros de sus usos educativos se ven, por ejemplo: 1. En el acceso a sitios educativos, 2. Para conseguir materiales de consulta, 3. Como una enciclopedia global abierta, 4. Para generar el trabajo y el aprendizaje colaborativo, por medio de espacios virtuales, 5. Permite el acceso a software educativos y 6. Para obtener información curricular y evaluativa, entre otros usos que se le puede dar al internet (Sánchez, 2012).

Con Castell (2002) y Calero (2010), se puede rescatar que el internet como herramienta propia de las TIC, también, proviene de una demanda de la interconexión y de la búsqueda de información de una forma global, rápida y sencilla. Lo que nos permite entender como cada herramienta que se ha venido desarrollando, convirtiéndose en el producto de la necesidad del ser humano de crecer y conquistar hasta los entornos virtuales.

2.3.6 Web 2.0:

Con el internet en los 60 se creó la web 1.0, quién permitía la lectura y la escritura pero la misma era estática, de baja interactividad y con dificultad para creación; es por ello que al no cumplir con las demandas de los cibernautas para el 2003 se desarrolla una nueva versión denominada trayendo como nueva propuesta, la posibilidad de socializar, compartir, editar, publicar videos o imágenes haciendo posible obtener comentarios en estas publicaciones.

La web 2.0, sin duda alguna marcó un antes y un después, para los usuarios dentro de las TIC y en el internet. Dando grandes avances por ser un espacio de lectura, escritura e interactividad, permitiendo un mundo de posibilidades, que bien enfocadas pueden traer aportes positivos y significativos en todos los ámbitos, en especial dentro de la educación. Pues la oportunidad de crear, publicar y compartir información dentro de esta web y diversos espacios, ha estimulado el enriquecimiento de los procesos de aprendizaje. Para Castaño Garrido (2007), los beneficios de la web 2.0 dentro de la educación, se simplifican de la siguiente manera: (Ver esquema 2)

Esquema N° 2:

Aportes de la web 2.0 dentro de la educación.



Nota: Elaboración de la autora. Fuente: Castaño Garrido, J (2007). Educar con redes sociales y web 2.0. [Artículo en Línea].

Con apoyo de los autores expuestos, podemos afirmar que estos espacios deben ser incorporados también dentro de la educación formal en todos los niveles educativos lo cual hemos visto que bien canalizados aportan grandes herramientas dentro de la formación del discente ya que estos hacen uso frecuente de estas herramientas tanto para la investigación como para su entretenimiento.

Anteriormente hicimos mención al rol del docente dentro de las TIC. Para la web 2.0, de igual forma se requiere un docente formado en las herramientas y los espacios que se promueven dentro de sus plataformas, es decir, se requiere un docente 2.0, ante esto Peña, Córcoles y Casado (2006) exponen:

La comunidad docente debe estar abierta a estos nuevos sistemas de aprendizaje y debe ser capaz de informar y formar al profesorado de los usos docentes de Internet. La utilización de las herramientas que proporciona la web 2.0 no debe ser una complicación para el docente, sino que debe ayudarlo en su trabajo. (pág. 5)

En especial la docencia debe estar a la par de las demandas educativas y de las herramientas que pueden ayudar a su práctica, enajenares, es rechazar los nuevos aportes y retrasar todas las generaciones que pasen por sus manos o lo que es peor causar desmotivación dentro del proceso de aprendizaje y deserción. Para crear un nuevo docente 2.0 que pueda responder a las dudas concretas y reales, además de servir como guía para la buena aplicación de estos espacios con una

consciencia más responsable y crítica como ciberusuario se requiere traspasar los libros tradicionales, la pizarra y la libreta dentro de su práctica.

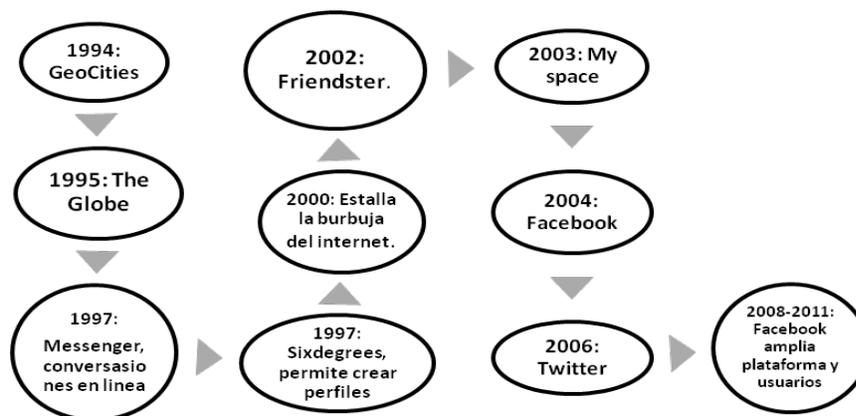
Ya se ha visto como la sociedad de la información dio pie a la sociedad del conocimiento y esta por su parte a la creación de las Tic, el internet y la web 2.0. Por lo que se tiene claro, cómo cada uno de estos espacios ha influido dentro de la educación formal e informal, y se han hecho parte de la vida cotidiana de los seres humanos, sobre todo aquellos con acceso a estas herramientas.

2.3.7 Las Redes Sociales:

Pero dentro de la web 2.0, dio apertura a la creación de las redes sociales. Su evolución se puede ver en la siguiente línea del tiempo. (Ver esquema 3)

Esquema N° 3:

Línea del Tiempo: Redes Sociales.



Nota: Elaboración de la autora. Fuente: Marketing Directo (2011). Breve Historia de las Redes Sociales.

Las Redes Sociales, son otro producto de la necesidad de conectarse, comunicarse y crear vínculos con otras personas de una forma rápida y sencilla. Creando nuevos espacios para compartir no solo información, sino también, opiniones, fotos y videos; lo que implica dentro de los procesos sociales, una nueva forma para interactuar. Las Redes Sociales, se definen como:

... aquel lugar virtual que les permite a individuos la interacción social, el intercambio constante de información, intereses, ideas y opiniones. Es una comunidad en constante construcción y remodelación a fin de ser cada vez más completa frente a las necesidades de los internautas (usuarios de internet), quienes buscan un sitio apropiado para convivir con demás personas que, como ya se dijo, comparten sus mismos gustos y aficiones, pero al mismo tiempo relacionarse con gente. (Perdomo, 2011:8)

Perdomo (2011) indica que es una “comunidad en constante construcción”, pues cada día se incorporan millones de usuarios a estas redes y se hacen parte del proceso de socialización, en estos entornos virtuales. Estas redes son creadas con diversos fines que pasan desde el entretenimiento hasta para hacer marketing de marcas y mercados reconocidos ya que en ellas es factible conocer personas, realizar chat, compartir o mandar imágenes y videos además de crear perfiles y hacer estos espacios más personalizados y públicos.

Y así como un proceso Darwiniano, sólo aquellas que fueron capaces adaptarse mejor a las necesidades globales han tenido la oportunidad de crecer dentro del mercado aumentado día a día la población que hace vida en ellas. Las redes más usadas actualmente son: (Ver tabla 3)

Tabla N° 3:

Principales Redes sociales.

Red Social	Año de fundación	Creador	Características	Números de usuarios actualmente (2014)	Logo
Facebook	2004	Mark Elliot Zuckerberg	<ul style="list-style-type: none"> -Se crea con un gran espacio para compartir vivencias. -Permite aceptar amigos de todos lados del mundo. -Crear un perfil y hacerlo público o privado. - Se puede subir videos, imágenes y etiquetar a los amigos aceptados en tu perfil. -Se puede jugar dentro de la misma red. 	Aprox. 1.28 billones	
Twitter	2006	Jack Dorsey	<ul style="list-style-type: none"> -Microbloggin. - Publicaciones en 140 caracteres. -Permite las publicaciones de imágenes. -Permite estar enterada al instante de sucesos, hechos o aconteceres a nivel local, regional y mundial. -Hashtag, para crear temas de interese. 	Aprox. 255 millones	
Youtube	2005	Chad Hurley, Steve Chen y Jaweb Karim)	<ul style="list-style-type: none"> -Permite subir y publicar videos, de cualquier tipo de temas. -Aloja una variedad de video clips de películas y programas de televisión, videos musicales, y vídeos caseros. 	Aprox. 1 Billón	
Instagram	2010	Kevin Systrom y Mike Krieger	<ul style="list-style-type: none"> -Es una aplicación gratuita para publicar fotos y videos. -Aplicación gratuita para smarphon. -Comprado en el 2012 por Facebook. - Permite la aplicación de filtros a las fotos, etiquetar a seguidores o hacer publicaciones directas. 	Aprox. 200 millones	
Google+	1997	C- fundadores: Sergey Brin y Larry Page	<ul style="list-style-type: none"> -Es una red social, perteneciente a google, que permite la publicación de videos, imágenes y comentarios. -Crear círculo de amistades, familia y trabajadores. 	Aprox. 540 millones	

Nota: Elaboración de la autora. Resumen de las principales redes sociales, con sus características, fundadores y número de usuarios actualmente. Fuente en Línea: Go&web.com

Es claro que las redes sociales han establecido nuevos esquemas de comunicación e interacción. Impactando en todos los ámbitos sociales, en especial en la educación, su

incorporación se ha ido masificando con el pase de los años, de una forma importante, tanto para los procesos formales como informales. Por esta razón, no se puede enajenar la docencia de las redes sociales, sobretodo en esta era digital, donde son tan usados y visitadas.

Las redes sociales han sido utilizadas en la educación superior sobretodo como un espacio para propagar el aprendizaje colaborativo, Nieves Roberto (2011) nos explica: “La intervención virtual se hace evidente con la aplicación de las redes sociales, mensajes electrónicos y participación de eventos que están mediados por dispositivos influenciados por sistemas de entornos informáticos, los cuales en su conjunto conforman los ambientes virtuales” (pág. 19).

Torres y Alcántar (2011), con respecto a esto también manifiestan “El uso de las redes sociales en las universidades del mundo ha facilitado la comunicación y el aprendizaje colaborativo y ha introducido nuevas formas de trabajo entre los actores de los procesos de formación”. Estas en su mayoría han sido aplicadas es en la educación universitaria y poco para la pre- universitaria (media general).

Lo cierto es que las redes sociales, bien aplicadas son una herramienta útil dentro de la educación, tanto en la etapa pre- universitaria como en la universitaria. Ya en universidades en España, se ha incorporado la asignatura de redes sociales. Y los resultados han sido beneficiosos. Lo que nos obliga a pensar que Venezuela, por su parte no puede quedarse atrás. Empero, para que esto suceda, la formación y participación docente es necesaria, para que propuestas como la presente y muchas más, sean posibles y reales a la práctica. En este orden de ideas Torres y Alcántar (2011), expresan:

Para que las redes puedan convertirse en parte de la transformación educativa, es importante resaltar que el docente tiene un papel significativo, puesto que participa en el proceso de generar conocimientos junto con el estudiante de forma construida y compartida...el esfuerzo del profesor está centrado en ayudar al estudiante a desarrollar talentos y competencias utilizando nuevos esquemas de enseñanza, lo cual lo convierte en un guía del proceso de enseñanza-aprendizaje.

De esta manera como investigadora se considera, que para lograr la incorporación de esta temática, tanto en la formación universitaria como en la pre, se debe partir con la formación

docentes, en especial a los de educación media general, ya que estos darán la base formativa para la educación posterior. Esta educación debe ser integral, es decir, debe tocar todos los aspectos necesarios y básicos sobre la temática, es aquí donde la seguridad juega un papel esencial, ya que no podemos decir que hay una formación completa, sino se brindan las herramientas principales para mantener la seguridad como usuarios, sobretodo en estos entornos de socialización virtual.

2.3.8 La Seguridad en las Redes Sociales:

El tema de seguridad en redes sociales, no se le ha dado la relevancia educativa que merece. Actualmente los cibernautas, ven estos espacios más como medios de entretenimiento o socialización, que como un medio de aprendizaje, y en ocasiones hacen uso de ellos de forma irresponsables exponiendo no sólo su identidad e integridad como personas, sino también, inconsciente o conscientemente se han hecho parte de ciber delitos como ciberbullying, ciberacoso o fraudes. Es por ello, que si hablamos de educar en redes sociales y formar al docente en ellas, indiscutiblemente también se debe hablar de educar al docente en el tema de Seguridad en Redes Sociales.

La formación en seguridad en redes sociales, se ha convertido en una necesidad imperante. Si bien no se cuenta con una definición, se puede dar una aproximación de ella. Se entiende por seguridad en redes sociales, como la protección de los datos personales, contenidos, información, integridad y autonomía del usuario. Para alcanzar esta seguridad, se debe ser consciente y crítico de los contenidos que se publican y a quienes se acepta como amigos en estas cuentas, es decir, esta seguridad depende en su mayoría de la precaución o formación que tenga el usuario a la hora de conectarse y hacer público sus datos personales.

2.3.8.1 Los perfiles de usuario:

Las redes sociales permiten crear o formar vínculos con nuevos usuarios o con su círculo de amigos frecuentes, pero en dichos espacios virtuales se permite la creación de perfiles, donde la

persona puede cargar los siguientes aspectos privados: nombre, edad, sexo, foto, aficiones y gustos, formación académica, profesión e incluso orientación sexual (Herrero, Moreno y Martin, 2003).

No obstante si se posee perfiles públicos, esta información es accesible tanto para conocidos como para extraños, como usuario se está exponiendo y convirtiéndose en una víctima potencial de delitos cibernéticos, los hackers o piratas informáticos buscan precisamente personas con perfiles públicos, por lo fácil que es acceder a ellas y a su información. Los autores Herrero, Moreno y Martin (2003), exponen con respecto a ello:

Al menos el 40% de los usuarios de redes sociales tiene abierto el acceso a su perfil a todo el que pase por ellas, sin restricción alguna de privacidad. Entre los menores de 18 años, este porcentaje se eleva al 77%, según un estudio reciente de la AEPD y el Instituto de Tecnologías de la Comunicación.

Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona. Se desconoce en gran medida que los perfiles pueden ser archivados, facilitando la creación de bases de datos de personas con fines ilícitos y del valor que éstos pueden llegar a alcanzar en el mercado.

Los perfiles de usuario se han convertido en una carta de presentación, pero sin la debida formación esta carta más que beneficiarnos como usuarios lo que hace es perjudicar la seguridad. No solo exponemos la integridad o seguridad personal, sino también, la de nuestros amigos o familiares más cercanos, ya que por medio de nosotros también pueden acceder a ellos, ya sea en imágenes o en información privada.

Es por esta razón que siempre se aconseja que si se es un usuario particular, es decir, que no tiene fines empresariales o de mercadotecnia, poseer un perfil privado, ya que resguarda la información que en estas redes se suban, además de no aceptar en ellas personas que no conoces dentro de los entornos físicos. Analizando lo que indican los autores anteriores y lo que se ha venido exponiendo, como investigadora presento las siguientes cinco ventajas y desventajas de los perfiles públicos y privados: (ver tabla N° 4)

Tabla N° 4:

Ventajas y Desventajas de los Perfiles públicos y privados.

	Perfil Público	Perfil Privado
Ventajas	1. Permiten acceder fácil a ti, de personas conocidas como desconocidas.	1. Solo pueden acceder a ti personas que conozcas o le des acceso a tu perfil.
	2. Tus publicaciones, llegan a gran cantidad de personas.	2. Solo a quienes pertenecen a tu círculo de amigos o seguidores, pueden ver tus publicaciones y comentarlas.
	3. Las publicaciones de eventos tanto corporativos como personales, pueden tener gran publicidad, con perfiles abiertos pues grandes números de personas conocidas como desconocidas pueden acceder a él.	3. Puedes invitar por estos espacios a las personas cercanas a ti a tus fiestas o eventos. De esta manera exclusivamente solo el que tú quieras puede ser parte de él.
	4. Permite la propagación de informaciones a gran escala.	4. Tu información solo llega a quienes desees.
	5. Permite hacer nuevas vinculaciones o amistades con personas de todos lados del mundo.	5. Permite respetar tu espacio personal y mantiene tu vida privado en resguardo, ya que solo lo que desees y a quienes desees que las vean podrán acceder.
Desventajas	1. Tanto personas conocidas como no conocidas, pueden acceder a tu perfil y ver tus publicaciones y fotos.	1. Si eres una corporación o estás interesado en vender una marca o producto, esto podría dificultar el acceso a él.
	2. Cuando acceden a él personas que no conoces ni están dentro de tu círculo de amistades, no sabemos bajo cual intención hacen el acceso a él, lo cual puede generar situaciones incómodas o negativas para el usuario.	2. Si eres una corporación o estas interesado en la organización de un evento a gran escala, los perfiles privados no permiten que esto sea posible pues solo conocerán de este evento quienes tengas como seguidores o amigos, no público externo que esté interesado en participar.
	3. Corres riesgo de ser una víctima de delitos como: Sexphising, Ciber bullying, Plagio de Identidad y Phishing o ser expuesto ante piratas informáticos con hackers.	
	4. Las características primordial de las redes sociales, es que permite crear un círculo o red con personas tanto conocidas como desconocidas. Al tener el perfil público puedes exponer también a	

	tus amistades cercanas como a familiares, pues pueden ser localizados o vistos en tu perfil de una forma sencilla.	
	5. Algunas corporaciones, hacen uso de las redes sociales, para los procesos de selección, si este está abierto y es tu cuenta personal podrías exponer de una forma negativa ante estos.	

Nota: Análisis y construcción de la autora. Resumen de las principales ventajas y desventajas de tener perfiles públicos o privados, en las redes sociales.

Con la tabla anterior, se presenta de forma sistemática cinco ventajas y desventajas de tener perfiles públicos o privados, exponiendo claramente que éstas radican en su mayoría en los intereses del usuario o corporación. En general, los adolescentes son la población que más comenten estas indiscreciones en sus perfiles, agregan a personas que no conocen, abriéndoles una puerta de su intimidad. En este contexto, Blanco (2013), en su artículo “Así funcionan los delitos y secuestros 2.0”, manifiesta:

Oficiales especializados en delitos informáticos de España, México, Venezuela y Brasil coinciden en que las más graves filtraciones del resguardo de grupos familiares de clase media ocurren después que sus miembros adolescentes pecan de imprudentes al revelar ingresos, propiedades, rutinas y privacidades.

Los expertos en seguridad personal en la era 2.0 instan a los usuarios a no subir fotografías de su lugar de residencia en los perfiles públicos ya que "una foto de una reunión de amigos en una habitación del hogar puede otorgarle a delincuentes claras señales de pertenencias de valor, estatus de vida y niveles de seguridad". Además aseveran que no es prudente subir imágenes de viajes realizados; y mucho menos de la fachada de la residencia porque "le facilitan al malhechor los detalles que necesita para planificar su cometido".

Durante el 2012 amplias investigaciones contra la extorsión y secuestro en Venezuela, México y Colombia determinaron que la mayoría de los actos vandálicos interactivos más comunes tenían su centro de operaciones en Facebook, pues allí los antisociales se dedicaban a seleccionar víctimas –con las que se vinculaban a través de perfiles falsos, rastrear activistas políticos, detectar vulnerabilidades a través de las fotografías públicas y precisar el lugar "del acto" para raptar a las próximas víctimas o cometer otras acciones.

Otra investigación con respecto a esta situación, fue la realizada por Symatec empresa líder en el desarrollo de programas y aplicaciones para la seguridad del ordenador en el uso del internet, quien atendiendo las necesidades expuestas por organismos internacionales como la Organización de Estados Americanos (OEA), desarrolló el informe sobre las “Tendencias de Seguridad Informática en América Latina y el Caribe”.

Con el fin de indicar, como se comporta el “ecosistema informático”, para ejecutar acciones de seguridad cibernética, esta publicación se realizó en junio de 2014 avalada por organizaciones como: AMERIPOL, Anti-Phishing Working Group (APWG), La Corporación de Internet para la Asignación de Nombres y Números (ICNN), Lacnic y Microsoft, exponiendo en el informe lo siguiente:

Los incidentes denunciados con mayor frecuencia dirigidos contra usuarios individuales involucraron phishing, seguido de robo de la identidad de una persona para cometer fraudes financieros o a través de las redes sociales. El último tipo de incidente parece ir de la mano de la expansión de las redes sociales y sus comunidades de usuarios, que en la actualidad existen en todos los Estados Miembros de la OEA en números crecientes, y se refleja en el aumento de la cantidad de denuncias de incidentes que involucran difamación, amenazas y cyber-bullying (acoso en la Web)... cada vez más frecuente el uso de ransomware (secuestro cibernético).

Lo cierto es que cada vez, las Naciones se sienten obligadas a pensar en la seguridad cibernética. En este mismo orden de ideas, el informe de la compañía TREND MICRO, avalado por la OEA publicado en el 2013 expresa “En un mundo interconectado, es necesario buscar un equilibrio entre disfrutar la comodidad que ofrecen las tecnologías de la información y minimizar las oportunidades que su uso les ofrece a los delincuentes cibernéticos” (pág. 3) Además aseveran:

Cada país aborda de manera distinta la seguridad cibernética, dependiendo de su panorama económico, político y cultural imperante. Algunos países consideran la seguridad cibernética principalmente como un asunto de seguridad nacional y defensa. Otros opinan que tiene un mayor impacto en el desarrollo económico o en la competitividad internacional. Otros más la ven

como un factor clave para la educación, la interacción social y la gobernanza centrada en los ciudadanos. (pág. 19)

La seguridad cibernética, es cada vez más una preocupante para la educación, pues sin las herramientas necesarias, cualquiera podría ser vulnerado dentro de estos espacios virtuales. Lo indispensables de estos entornos es el uso consciente de ellos para evitar ser víctima de delitos informáticos.

2.3.8.2 Los Cibercriminosos:

Los más frecuentes son:

- ✓ Sextorsión: Para los autores Molina, García y Aperador (2012), es “una forma de explotación sexual en la cual se chantajea a una persona por medio de imágenes de si mismo desnudo o desnuda que ha compartido a través de Internet o mediante sexting”. El sexting por su parte es “envío de imágenes de desnudos de uno misma vía telefónica, móvil e internet, normalmente ocultando el rostro”. Cabe desatacar que también imágenes con contenido erótico, puede considerarse una forma de Sextorsión. Con esta información privada la persona es extorsionada u obligada chantajes ya sea monetarios o de índole sexual, por parte de su malhechor.

En Venezuela, este delito según la experiencia del profesor y doctor Lacasella, expone que se han hecho presente con la manipulación y distribución de imágenes eróticas o sub-pornográficas, por parte de la población discente, son casos que se han presentado y son alarmantes, pero la razón por la que no hay data de ello es por el miedo a denunciar cuando se es víctimas de estos delitos.

- ✓ Ciber bullying: Para Santander Alejandro (2013), el ciber bullying es un subtipo de violencia que se practica dentro de las redes sociales, expone ante ello “se conoce como el acoso escolar cibernético (ciber acoso o Cyberbullying), una violencia que de a poco se ha transformado en el desafío de las escuelas en estos tiempos debido al masivo acceso y contacto permanente de los jóvenes”. Actualmente, el ciber acoso ha

aumentado progresivamente a nivel mundial, por ejemplo: La organización Pantallamigas, recolecta los siguientes datos:

-En Chile (2011), se registro que el 878 % de los estudiantes chilenos de 7° curso básico (12 años) a 4° medio (17 años) ha sido víctima de ciber bullying por Internet. Investigación realizada por Universidad Andrés Bello.

- En Argentina (2011) El 19% de los menores de entre 9 y 17 años de Mendoza (Argentina) sufrieron bullying por Internet o por celular, en forma de insultos, burlas o amenazas. El 11% reconoce haberlo ejercido sobre otros. Investigación realizada por el Observatorio Internacional de la Violencia Escolar - UCA

- En EE.UU. (2011), El ciber bullying aumentó en los EE. UU. Más del 80% en 10 años. Los investigadores apreciaron un auge desde el 6% que había en 2000 al 9% en 2005 y al 11% en 2010. Investigación realizada por CCRC, Universidad de New Hampshire.

-En Venezuela, según la experiencia de Lacasella (2015), es un delito que inicio en la etapa de bachillerato, pero hoy en día se solicita de su apoyo en charlas dentro de la educación primaria, ya que niños de cuarto grado están siendo víctimas de este delito, situación que es preocupante pues es una clara consecuencia de no asumir políticas formativas preventivas.

Hay más investigaciones y tasas sobre este fenómeno a nivel mundial, lo que nos indica que es un fenómeno que se está propagando muy rápido y ni docentes ni discentes cuentan con la formación adecuada para contrarrestar y reorientar. Muchas de sus víctimas al sentirte acorralada, tienden a optar por el suicidio.

- ✓ Phishing: Para Castro Luis (2013), este delito se define como "...término empleado en el mundo de Internet para referirse a una estafa diseñada para obtener información confidencial, como lo son números de tarjetas de crédito, claves de acceso, datos de

cuentas bancarias u otros datos personales.”. Este se enfoque en las llamadas estafas online ya sea bancarias o de transacciones en páginas de compra o venta de artículos, se denomina “phishing” porque el pirata informático pesca en la red a sus víctimas. Este delito también se vincula con el plagio de identidad, dado que en este también ocurre una estafa en la identidad de un usuario, es decir, este es plagiado y tienden a utilizar su información bancaria para hacer transacciones.

- ✓ **Grooming:** Para Cortejoso David (2013), se entiende “como el conjunto de acciones que lleva a cabo un adulto a través de las TIC para ganarse la confianza de un menor, con el fin de obtener un posterior beneficio de índole sexual”. Este tipo de delitos se asocia a patologías como la pedofilia, pederastias y pornografía infantil.

Quiénes comenten estos delitos tiene diversas denominaciones, sin embargo las básicas son: Hackers o piratas informáticos, estas personas obtienen datos de usuarios de forma fraudulenta dentro de la red, y dependiendo de sus intenciones hacen uso indebido de la información obtenida.

Venezuela cuenta con la “Ley de Delitos Informáticos” que sanciona este tipo de delitos, pero es el desconocimiento sobre la misma, lo que repercute en no saber cómo actuar ante estas situaciones, no cabe duda que en la medida en que exista mayor formación e información, sobre estos delitos, se podrá generar mayor consciencia sobre cómo evitarlos. La docencia juega un papel clave dentro de la formación en esta área, es por ello que se entiende que es por estos por donde debe partir la formación.

2.3.9 El Taller:

Se insiste en la importancia en la formación en este aspecto dentro de la educación formal, en primera instancia para los docentes. Ya que estos como guía de aula pueden iniciar campañas en contra de ciber-bullying o fraudes de identidad, así como contribuir a crear una consciencia sobre la correcta usabilidad de estos espacios en pro a garantizar la de seguridad personal, dentro de estos espacios, tanto el aula como en los hogares.

Los docentes son la base para iniciar la formación de estos contenidos, es por ello que su formación en ellos es indispensable para partir. El tema de seguridad en redes sociales, no es un tema difícil para planificar, ni mucho menos para elaborar un diseño para impartirlo, como se ha venido haciendo énfasis la propuesta en el diseño de un taller para ejecutar el proceso de formación, para qué es un El taller, lo definiremos como:

... un lugar donde se trabaja y se elabora. Es una forma de enseñar y aprender mediante la realización de algo. Se aprende desde lo vivencial y no desde la transmisión. Predomina el aprendizaje sobre la enseñanza. Se trata entonces de un aprender haciendo, donde los conocimientos se adquieren a través de una práctica concreta. Es una metodología participativa en la que se enseña y se aprende a través de una tarea conjunta. (Careaga, Sica, Cirillo y Da Luz, 2006:5)

El taller, permite la participación y el aprendizaje cooperativo, lo cual es indispensable para abordar este tipo de temáticas, las redes sociales no son desconocida, pues son un tema cotidiano, el punto es que muchas veces se hace uso de ellas exponiendo la seguridad.

La estrategia principal del taller es partir de los conocimientos previos, hasta llegar desarrollar las herramientas necesarias para garantizar la seguridad en redes sociales; debe ser visto como un proceso de actualización docente. El taller, en si tiene características que se deben tomarse en cuenta a la hora de realizar el diseño, esta son:

1. Se basa en la experiencia de los participantes.
2. Es una experiencia integradora donde se unen la educación y la vida, los procesos intelectuales y afectivos.
3. Está centrado en los problemas e intereses comunes del grupo.
4. Implica una participación activa de los integrantes.
5. Puede utilizar diversas técnicas, especialmente la discusión en grupo.
6. Se debe trabajar con grupos pequeños. (Careaga, Sica, Cirillo y Da Luz, 2006:6)

Con estas características, se desarrollara el diseño del taller elaborando su planificación en un cuadro que contenga los objetivos, metas, temarios, actividades, recursos requeridos o materiales y el tiempo estimado de cada actividad. Posterior a ello se explicara cada actividad y el fin por el cual se ejecuta. Los talleres, son pertinentes para la realización de procesos de formación o

actualización, sirven para manejar grupos pequeños y para temas específicos. Los talleres son también un Medio Instruccional (MI) o Diseño Instruccional (DI), pero estos diseños están aunados a modelos pedagógicos.

2.3.10 Modelo ADITE:

Un diseño instruccional permite de manera sistemática, planificada y dinámica organizar los contenidos de curso, taller, diplomado, blog, infografía que se quiere diseñar bajo un objetivo de instruccional, ya que el requisito indispensable es que esté orientado a un proceso de instrucción formativa, es por esta razón por la que se tomará el modelo de Marina Polo (2003), que indica en su artículo “Aproximación del Modelo ADITE”, define el Diseño Instruccional (DI), como:

...un proceso dialéctico, sistémico y flexible, cuyas múltiples fases y componentes de planificación se abordan y se trabajan de forma simultánea. Asimismo, el Diseño Instruccional requiere de la aplicación de un proceso de análisis y evaluación, para seleccionar adecuadamente los medios y estrategias de enseñanza, de manera que permitan la construcción y reelaboración de aprendizajes significativos por parte de la población-usuario, en función de los tipos de conocimientos que deberán aprehenderse. (pág. 68)

Cuando la autora hace mención sobre lo dialéctico, está haciendo referencia al ordenamiento lógico de los objetivos y contenidos pues entre ellos debe haber coherencia; cuando dice que debe ser flexible es porque su diseño debe tomar fundamentos teóricos constructivistas, ya que en la actualidad los teóricos vanguardistas exponen la relación activo del discente o público dentro del proceso de aprendizaje, quiere decir que estos construyen el proceso conjuntamente con el facilitador o docente.

Por último cuando habla de que debe ser sistémico hace referencia de la posibilidad de interrelacionar, objetivos, contenidos y estrategias de una forma armoniosa, así como aquellos procesos que van surgiendo sin ser planificados. El esquema que la autora propone para el modelo ADITE es el siguiente: (ver figura N°. 1)

Figura N°.1:

Modelo ADITE:



Fuente: Figura extraída del artículo: Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas.

Al ver el esquema una pregunta clave sería ¿Qué tiene de innovador este modelo?, concurre, que el aporte de este modelo es la interrelación de los componentes algo que por ejemplo no se trata en los modelos de primera generación (1960) ni en los de segunda generación (1970), así como la incorporación del elemento tecnológico, con este modelo se propone no solo la incorporación de las TIC dentro del DI, sino además, crear entornos virtuales para el aprendizaje.

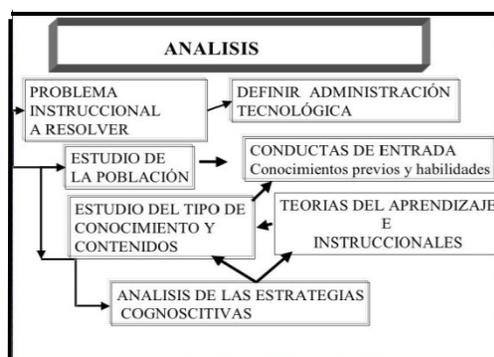
Las posturas de un Medio Computarizado para el Aprendizaje (MCA) tienen años siendo defendidas por autores como Dorrego (1995) y Polo (2001). Villasana (2006) en su tesis de postgrado, también expone:

El avance de las TIC en el ámbito educativo, ha suscitado el surgimiento de lo que hoy conocemos como entornos virtuales de enseñanza y de aprendizaje que, aprovechando las potencialidades de las TIC, ofrecen nuevos espacios de enseñanza y aprendizaje libre de restricciones que imponen el tiempo y el espacio en la enseñanza presencial y capaces de asegurar una continua comunicación entre estudiante y docente. Estos entornos hoy en día son utilizados en diferentes instituciones, también permiten complementar la enseñanza presencial con actividades virtuales... (pág. 60)

Las TIC, sin duda alguna se han incorporando de manera masiva dentro de los procesos de aprendizaje creando nuevos espacios dinámicos. El modelo ADITE, propone la incorporación de las tecnologías para hacer del DI, pero entendido como un Medio Instruccional Computarizado (MIC), es por ello que Polo (2003), toma los aportes de Tennyson (1993) y Dorrego (1995) además de hacer una adaptación a los modelos de tercera generación (1980) y los de cuarta generación (1990) y crea los siguientes cuatro sub-dimensiones: (ver figuras N°.2-3-4-5)

Figura N° 2:

Componentes del elemento Análisis.

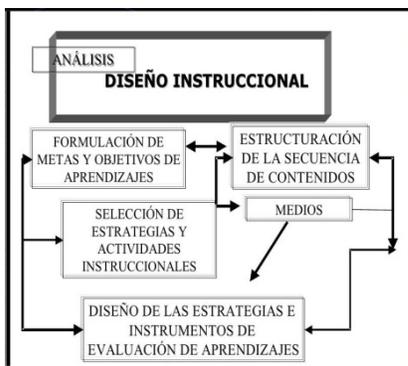


Dentro de la sub- dimensión de Análisis, encontramos que se despliega siete (7) elementos indispensables que giran en torno a entender el problema institucional plateado, la población que la misma atenderá así como las conductas de entrada que estas deberán poseer antes del proceso de formación. Este componente además interrelaciona las tecnologías a emplear así como las teorías de aprendizaje que fundamentan el medio didáctico computarizado. En está sub-dimensión se busca entender el problema para dar pie a la base de los componentes sub siguientes.

Fuente: Figura extraída del artículo: Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas.

Figura N° 3:

Componentes del elemento Diseño.

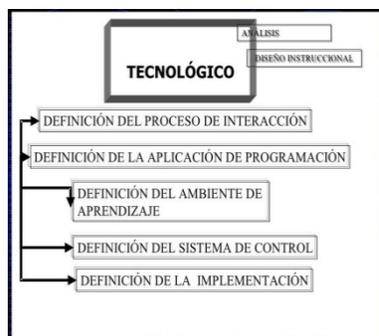


Fuente: Figura extraída del artículo: Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas

La sub dimensión diseño, en nuestro caso juega un papel importante ya que como hemos venido planteando representa el fuerte de la investigación, tal como lo muestra el esquema en esta se desarrollan todos los elementos inherentes al diseño de un MDC, ya que en él se traza y expone las metas, objetivos, estrategias, planificación, actividades, medios tecnológicos a emplear así como la estructura secuencial que lleva el diseño instruccional a realizar.

Figura N°.4:

Componentes del elemento Tecnológico.



Fuente: Figura extraída del artículo: Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas.

Cada sub-dimensión, representa una parte de su modelo y se trabajan de forma integrada. Estas pueden ser entendidas además como cada componente de un taller que busca integrar la

tecnología o espacios como las redes sociales con procesos de formación o actualización. La innovación de este modelo es precisamente la inclusión de estas herramientas al proceso de A-A, por lo que se integra y trabaja a la mano de los componentes anteriores y el siguiente.

Figura N°.5:

Componentes del elemento Evaluación.



Fuente: Figura extraída del artículo: Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas.

Finalmente el componente evaluación, se centra en el diseño y aplicación de la evaluación post diseño instruccional, el mismo tiene el fin de medir si fueron alcanzados los objetivos y metas desde la evaluación de los participantes o público al que se planifico que fuera dirigido el medio. Esta etapa sirve de referencia para la mejora continua del proceso ya que como todo aprendizaje su crecimiento es continuo y los resultados obtenidos en la aplicación de evaluación de todo el MDC, se puede tomar la decisión una mejora posterior o una continua aplicación.

CAPÍTULO III

MARCO METODOLÒGICO

Esta fase es concebida con el “Cómo” de toda investigación, en este capítulo se indica el diseño, nivel, procedimientos, técnicas e instrumentos que se emplearon, para hacer el análisis de la evaluación de la propuesta formativa del taller en seguridad en redes sociales. Con ello claro, damos inicio a las:

3. 1 Nivel de la Investigación:

El nivel de la investigación según Arias (2009:46), lo define con el “... grado de profundidad con que se aborda un objeto o fenómeno”. Por la profundidad del fenómeno planteado, se considera que el nivel es Descriptiva, la cual consiste en “... la caracterización de un hecho, fenómeno o grupo con el fin de establecer su estructura o comportamiento”

En los capítulos precedentes, hemos dejado claro como la imprudencia de usuarios o el mal uso de las redes sociales o espacios en la web, han dado pie al crecimiento de ciberdelitos a nivel mundial, haciendo presentes en Venezuela, y es precisamente la carente formación del tema por parte del docente de informática de educación media general una causal para que los discentes desconozcan la temática o no usen estos espacios de una forma crítica y responsable. Dado que se debe partir con el facilitador, la propuesta gira en torno a la actualización del mismo.

La investigación trae un planteamiento claro de la situación, por ello, expone de una forma descriptiva, el fenómeno a trabajar; lo que servirá para proyectar acciones académicas que pudiesen ser implementadas en investigaciones posteriores.

Con esto no solo demostramos que la investigación posee una naturaleza descriptiva, que brinda el panorama de una situación en nuestro contexto venezolano, teniendo por motivo firme dejar de ignorar la situación ya que sería irresponsable. La indagación realizada, nos afianza que el diseño del presente taller servirá tanto como un aporte a las líneas de investigación de nuestra casa madre (UCV), como al Currículum Básico Nacional, donde estas temáticas carecen, demandando una actualización dentro del currículum oculto, de cada institución y docente.

3.2 Diseño de la Investigación:

Para Arias (2009:48), entiende esta sección como "... la estrategia que adopta el investigador para responder el problema planteado". La investigación está diseñada para ser de Campo-tecnológica. Se dice que es de campo ya que está comprendida como "... consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna".

Por ser una propuesta a validar por expertos, la recolección de los datos fue directamente con ellos y con la entrevista realizada al profe. Lacasella, la cual podrán apreciar mejor en los anexos y en los extractos indicados en el capítulo anterior. Además de los sustentos factuales tomados por encuestadores respetadas como ComScore Inc. o Pew, con respecto a la temática de forma documentaria.

Y exponemos que es Tecnológica, porque como se ha venido desglosando la propuesta esta enmarcada en el Modelo ADITE, quién está compuesto de cuatro etapas de las que despliegan sub-dimensiones que se tomaron en cuenta a la hora de desarrollar la propuesta en la misma queda evidencia de la incorporación de las tecnologías dentro del proceso diseño y planificación dónde se indica como deberán ser aplicadas para el taller en seguridad en redes sociales. Este elemento viene ligado a la "Investigación Tecnológica" la cual se define, como:

La investigación tecnológica comprende con mayor énfasis la transformación, cuyo fin es obtener conocimiento para lograr modificar la realidad en estudio, persiguiendo un conocimiento práctico. “Como resultado de una investigación tecnológica se obtienen conocimientos que establecen con detalle: acciones, requisitos, características, diseño, materiales, costos, responsables, métodos, instrumentos, y demás circunstancias, que describen el qué y el cómo, con lo que se promueve el logro de los objetivos, generalmente predeterminados en el área de producción” (García Córdoba, 2007, p.81).

Para nuestra propuesta las tecnologías, son un medio para lograr los objetivos establecidos para el taller así como la meta propuesta, por tal motivo el elemento tecnológico no solo se vincula por la implementación de la tecnología sino además porque el contenido que se propone desarrollar es uno propio de las TIC. De esta manera sustentamos el hecho de que el diseño de nuestra investigación es de tipo Campo-Tecnológico, ya que recauda información de la fuente directa y a su vez en la propuesta se emplean estas herramientas.

3.3 Técnicas e Instrumentos:

En las técnicas e instrumentos, se responderán las preguntas sobre cuáles instrumentos se emplearan y cuál será la evaluación de los mismos, presentando así a continuación:

3.3.1 Instrumentos:

Los instrumentos permitirán recolectar toda la información posible, sustentando los argumentos expuesto en todo el documento. Hurtado Barrero (2012:161) conceptualiza los instrumentos como “...la herramienta con la cual se va a recoger, filtrar y codificar la información, es decir, el con qué”.

En esta investigación se manejarán dos tipos de instrumentos uno de ellos será de registro, con la aplicación de la entrevista a Vito Lacasella, quién es: Licenciado en Comunicación Social mención Audiovisual (Universidad Central de Venezuela) y posee un doctorado en Comunicación Social mención Audiovisual (Universidad Central de Venezuela), además de ser en el encargado de la sección de Arte-Visión (Universidad Simón Bolívar), Gerente de Producción encargado de LA SIMONTV canal de tv de la Universidad Simón Bolívar así como es miembro de la ONG “Educación para los Medios”. La entrevista, se define como:

... más que un simple interrogatorio, es una técnica basada en un diálogo o conversación “cara a cara”, entre el entrevistador y el entrevistado acerca de un tema previamente determinado, de tal manera que el entrevistador pueda obtener la información requerida. (Arias, 2006:73)

Esta sirvió para fundamentar con el experto, la relevancia del tema seguridad en redes sociales, dado que en Venezuela no se cuenta con información sobre ella, decidimos recurrir a un experto para confirmar su presencia dentro del país y sobretodo en la educación formal así como evidencia de delitos cibernético. Los extractos de la misma fueron presentados en el marco teórico y en los anexos.

Para este caso la entrevista será de tipo semi-estructurada, este tipo de entrevistas son aquellas en las que aún cuando existe un previo guión de preguntas, el entrevistador tiene la oportunidad de agregar nuevas durante la entrevista, según se considere para abarcar el motivo y seguir en curso la dinámica en la que se desarrolle la entrevista (Arias, 2005:74). La estructura y las respuestas obtenidas en la misma serán transcritas y presentada en los anexos.

La entrevista fue grabada y posteriormente transcrita, este proceso Rodríguez (2014) indica la ejecución de la entrevista debe ser como un conversatorio, que servirá para recabar la información que se busca, tal como se hizo con la del Prof. Lacasella. De esta manera como ya hemos presentado en las bases, extractos de la entrevista, conocimos cuales delitos, son los más frecuentes así como la base donde se fundamenta el problema sobre el tema de seguridad en redes sociales, según Lacasella (2015).

Para nosotros la ejecución de la entrevista, no represento ninguna dificultad, sino por el contrario genero beneficios, no sólo por la información obtenida, sino por la experiencia que generó a la investigadora de conocer a manos de un especialista, su vivencia en este contenido dentro del sistema educativo. El segundo instrumento que se empleó fue el cuestionario, definido como:

... un conjunto de preguntas relacionadas con el evento de estudio. Su característica es que tales preguntas pueden ser dicotómicas, de selección, abiertas, tipo escala o tipo ensayo. Un mismo cuestionario puede albergar diversidad de preguntas según se requiera para obtener la información pertinente acerca del evento de estudio. (Hurtado de Barrera, 2012:165)

Por consiguiente, se diseñara un cuestionario que abarque los cuatro componentes del modelo ADITE, dicho instrumento es pertinente por su rápida aplicabilidad, para la evaluación de los diseños instruccionales, ya que el factor tiempo muchas veces juega un papel importante, a la hora de obtener resultados y más si hablamos de que el mismo fue aplicado a un grupo de expertos. En este caso, se elaboró uno mixto debido a que estará constituido tanto por preguntas cerradas como por espacios para realizar las observaciones.

Antes de diseñar los cuestionarios, se realizó la operalización de la variable, para entender cuáles eran las categorías a evaluar dentro del instrumento. Una operalización de la variable según Sabino (2007:57) es "...cualquier característica o cualidad de la realidad que es susceptible de asumir diferentes valores". Las variables son aquellas categorías o conceptos que como su nombre lo indican varían, es decir poseen dimensiones, indicadores que permiten generar los ítems para entender como debe ser abarcada cada variable. Con esto claro, presentamos la operalización del segundo objetivo específico:

Tabla N° 5:

Operalización de la Variable:

Objetivo	Variable	Componente	Sub-dimensiones	Ítems
<p>Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática</p>	<p>-Diseño Instruccional. (Modelo ADITE)</p>	<p>- Análisis.</p>	<p>-Problema Institucional. -Estudio de la Población. -Estudio del Tipo de Conocimiento. -Teorías del aprendizaje. - Análisis de las Estrategias cognoscitivas.</p>	<p>1. ¿Cómo es definido el problema de actualización del docente de informática, dentro del tema en seguridad en redes sociales? 2. ¿Cómo son definidas las características de la población a la que va dirigido el taller en seguridad en redes sociales? 3. ¿De qué manera se establecen los conocimientos y habilidades previas que debe poseer el docente de informática para a participar dentro del taller? 4. ¿Cómo se justifican las teorías de aprendizaje dentro del taller en seguridad en redes sociales? 5. ¿Cómo es el análisis de las estrategias dentro del taller en seguridad en redes sociales? 6. ¿De qué</p>

			-Administración de las Tecnologías.	manera se indica la administración de las tecnologías a emplear durante el taller de seguridad en redes sociales?
--	--	--	-------------------------------------	---

Objetivo	Variable	Componentes	Sub-dimensiones	Ítems
Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática.	-Diseño Instruccional. (Modelo ADITE)	- Tecnología.	- Definición del Proceso de Interacción -Definición del Ambiente de aprendizaje.	7. ¿De qué manera es definido el tipo de interacción que tendrán los participantes del taller en seguridad en redes sociales? 8. ¿Cómo se define el ambiente de aprendizaje donde los participantes del taller en seguridad en redes sociales, interactúan? 9. ¿Cómo considera el proceso de interacción y el ambiente de aprendizaje?

Objetivo	Variable	Componente	Sub-dimensiones	Ítems
<p>Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática.</p>	<p>-Diseño Instruccional. (Modelo ADITE)</p>	<p>- Diseño.</p>	<p>- Formulación de las Metas y Objetivos.</p> <p>-Estructura secuencial de los contenidos.</p> <p>-Selección de las estrategias y actividades instruccionales.</p>	<p>10. ¿Cómo están redactadas las metas del taller y de cada contenido?</p> <p>11. ¿Cómo están redactados los objetivos del taller?</p> <p>12. ¿De qué manera es presentada la coherencia entre las metas y los objetivos?</p> <p>13. ¿Cómo se presenta la secuencia en los contenidos del taller?</p> <p>14. ¿De qué manera es la continuidad en cada uno de los contenidos?</p> <p>15. ¿Cómo es presentado el esquema de los temas del taller en seguridad en redes sociales?</p> <p>16. ¿Cómo considera la selección de las estrategias a emplear durante el taller?</p> <p>17.¿Cómo percibió fue la aplicación del video durante el taller?</p> <p>18. ¿Existe una selección correcta de las actividades grupales para los</p>

			<p>-Diseño de las estrategias instruccionales e instrumentos de evaluación de aprendizaje.</p>	<p>participantes del taller “Seguridad en Redes Sociales”?</p> <p>19. ¿Cómo es el diseño de la presentación colectiva multimedia?</p> <p>20. ¿Fue la presentación colectiva Multimedia visualmente agradable para los participantes?</p> <p>21. ¿Es empleado el video para apoyar los contenidos y generar reflexión, sobre el tema de seguridad en redes sociales?</p> <p>22. ¿Considera adecuada la selección de los videos a emplear para el taller en seguridad en redes sociales?</p>
--	--	--	--	--

Objetivo	Variable	Componente	Sub-dimensiones	Ítems
Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática.	-Diseño Instruccional. (Modelo ADITE)	- Evaluación.	-Evaluación de las estrategias”.	<p>23. ¿Cómo está diseñado el instrumento post-taller?</p> <p>24. ¿Existe el orden dentro de los instrumentos de evaluación post-taller?</p> <p>25. ¿Cree que el presente instrumento abarca la evaluación de los contenidos, estrategias, medios computarizados y dominio conceptual y grupal del facilitador durante el desarrollo del taller?</p>

Claro lo que se evaluaría, se diseñaron dos cuestionarios, uno de ellos será aplicado a un primer panel de expertos encargados de validar si el instrumento del cuestionario posee pertinencia, congruencia y efectividad, para ser presentado finalmente al segundo panel de expertos, quienes evaluarán finalmente el diseño del taller. Para este primer panel, fueron dos docentes en el área de Estadística y otro en el de Tecnología. Estos expertos se tomaron de manera arbitraria, cumpliendo con las siguientes características:

- Tienen competencias en área de metodología de la investigación y diseño de instrumentos.
- Son miembros de la escuela de educación de la UCV.
- Son docentes de la escuela de educación.

Las docentes colaboradoras fueron:

- Profa. Carla Noguera- Departamento de Estadística e Informática aplicada a la Educación.
- Profa. Johanalí González- Departamento de Estadística e Informática aplicada a la Educación.
- Profa. Luzmara Urbina- Departamento de Estadística e Informática aplicada a la Educación.

Una vez procesada la información se realizó las recomendaciones aportadas por las docentes antes mencionadas, hechas las correcciones se pasó al segundo tiempo, que será la aplicación del cuestionario a los expertos, ellos tendrán la tarea de finalmente validar desde el área de Educación, Comunicación e Internet y Contenido, la eficacia y efectividad del diseño del taller: “Seguridad en Redes Sociales, dirigido a los docentes pertenecientes al área de Informática, de la etapa de educación media general”.

Para la elección de este panel se busco tres docentes que cumplieran con las siguientes competencias:

- Docentes que manejen y apliquen las Redes Sociales en su práctica Docente.
- Conozca y hayan trabajado el tema de Seguridad en Redes Sociales.
- Tengan dominio en el diseño de talleres.
- Tengan competencia en el área de Educación orientado a los medios audiovisuales o en redes sociales.

Para esta fase se contó con la colaboración de los siguientes expertos:

- Profa. Alejandra Ranzolin- ININCO-UCV.
- Profa. Norelkis Riera- Escuela de Educación –UCV
- Profe. Vito Lacassela- ININCO-UCV.

Una vez culminado el proceso de validación, se pasará a procesar los datos y generar las conclusiones, lo cual será presentado en el capítulo siguiente. Este instrumento final también podrá ser visualizado en los anexos.

3.3.2 Técnica de Procesamiento:

Como técnica se empleara: 1- Transcripción de la entrevista de experto 2- Validación del instrumento mediante el juicio de experto y 3- Análisis de frecuencia. En primera instancia será validación del cuestionario, para sustentar que el mismo, sirva para evaluar de manera eficiente el diseño del taller, la validación se entiende como “el grado en que un instrumento realmente mide la variable que pretende medir” (Hernández, Fernández y Baptista, 1991:243). Una vez realizado ello se pasara, a surtir el cuestionario para ejecutar la técnica de juicio de experto, quien según Correa (2006) se aplica de la siguiente manera:

1. Se selecciona tres (03) expertos de metodología de la investigación para que evalúen de manera independiente los ítems o preguntas del instrumento en términos de relevancia o congruencia, claridad en la redacción y la tendenciosidad o sesgo en su información.
2. Cada experto recibe información escrita acerca de: a) Propósito del instrumento; b) Objetivo general; c) Objetivos específicos; y d) Sistema de variables e indicadores.
3. Cada experto recibe una planilla de validación de datos en donde se recogió la información suministrada por él. Dicha planilla contiene los siguientes aspectos por ítem o pregunta: Congruencia, claridad, tendenciosidad y observación. (ver anexo 02)
4. Se recoge y se analiza las planillas de validación y se toma las siguientes decisiones: a) En los ítems o preguntas donde exista un 100% de coincidencia favorable entre los expertos quedaron incluidos en el instrumento; b) Los ítems o preguntas donde exista un 100% de coincidencia desfavorable entre los expertos

quedaron excluidas del instrumento; c) Los ítems o preguntas donde exista coincidencia parcial entre los expertos se revisa, reformula y es nuevamente validados.

Obtenidas las repuestas de los veinte y cinco ítems que compone el cuestionario de Validación de Experto, se realizará un análisis de frecuencia, dividió en los cuatro componentes que posee el taller y según las respuestas obtenidas por los tres expertos, lo que nos permitirá contrastar las respuestas generales obtenidas en el instrumento, de esta manera analizaremos y compararemos según la escala de estimación escogida y se dará las conclusiones y recomendaciones pertinentes. Este análisis será presentado en el capítulo V.

CAPÍTULO IV

LA PROPUESTA

En las bases teóricas, cuando se expuso el modelo ADITE fueron presentados las sub-dimensiones este comprendía los aspectos que deben ser tomados en cuenta para su desarrollo dentro del Diseño Instruccional (DI) o Medio Didáctico Computarizado (MDC). No obstante, para nuestro DI es necesario realizar una serie de adaptaciones, ya que el mismo posee las siguientes características:

1- Es un taller, diseñado para la modalidad presencial.

2- Dirigido a los docentes de Informática, de la etapa de educación media general.

3-La herramienta de las TIC que se planifica emplear será el video, presentación colectiva multimedia y el proyector multimedia.

4- Es una propuesta de diseño de taller, la cual se validará mediante evaluación de experto, con ello aclaramos que no será implementado el taller posteriormente, sino que se llegará hasta el diseño y evaluación del modelo.

Expuestas estas características, se puede denotar que hay sub-dimensiones, que no será necesario ni aplicar ni desarrollar, ya que no se adaptan a la propuesta que se viene desarrollando en el planteamiento, marco teórico y legal previamente presentados. Dicho esto, como autora se propone que el modelo ADITE, para el diseño del taller con modalidad presencial, por sus particulares expuestas, deberá ser así: (ver figura N°.6)

Figura N° 6:

Adaptación del Modelo ADITE, para el Diseño del Taller: Modalidad presencial.



Fuente: Adaptación de la autoría del Modelo ADITE, extraído de: Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas.

De esta manera realizamos el proceso de adaptación de las sub-dimensiones, que son factibles para el diseño de nuestro taller y que además se acoplan con armonía al modelo de Polo (2003). Lo importante del modelo, es que su propuesta vanguardista de incorporar a las TIC, dentro de lo DI, lo cual no solo se está adaptando a las necesidades educativas de esta nueva sociedad, sino además, demuestra la versatilidad en aplicación que posee el mismo, algo que los DI de primera y segunda generación no presentaban. Ahora bien para entrar por completo en el DI del taller, se explicara cada una de las sub-dimensiones presentadas.

4.1 Componentes del Diseño:

4.1.1 Componente de Análisis:

En este componente se desarrolló el problema institucional, estudio de la población (conductas de entradas y habilidades), estudio del tipo de conocimiento y contenido, fundamentos teóricos, análisis de las estrategias cognoscitivas y administración de la tecnología. En este aspecto Polo (2003), expone que esta dimensión ayuda a conocer que se espera conocer o lograr con el medio, es por ello que afirma:

Cuando se diseña un medio instruccional basado en tecnologías o computarizado, hay que saber qué se espera de él, qué tipo de necesidad educativa va a solucionar, cuáles son las características de la población a la cual va dirigido, qué tipos de conocimientos se mediarán. Por lo tanto, las teorías del aprendizaje y de la instrucción deben ser analizadas en esta fase. (pág. 72)

El problema institucional; como se expuso en el planteamiento del problema, la sociedad del conocimiento y de la información dejó claro que las TIC, deben ser incorporadas en todos los aspectos geopolíticos que una sociedad demanda, donde la educación no escapa de ello. Tanto es así que organismos internacionales como la ONU establece el internet como un derecho humano, lo que incidió directamente que tanto en países desarrollados como sub-desarrollados lo incorporaran de forma progresiva en todos sus espectros yendo de lo macro a lo micro.

En Venezuela, en su marco normativo se incorpora como una obligación de Estado, sin embargo, al realizar la investigación documental se encontró que dentro del aspecto educativo al ir de lo macro que es lo curricular a lo micro que es la formación discente y docente, donde el tema de seguridad en redes sociales no se da, y una de las razones es porque el Currículo Nacional, no lo contempla lo que ata de manos a la práctica y formación docente para darlo y para tener los conocimientos técnicos en ello.

El tema de las redes sociales, se ha convertido en un fenómeno global, por ejemplo el país es uno de los mercados con mayor penetración dentro de la región de Centro América, con una población de 3,1 millones de audiencia, en el 2011, liderando redes como Facebook y Twitter.

Con esta referencia factual, se nota que existe uso constante de estas redes sociales, lo que ha permitido el desarrollo de un fenómeno social llamado ciber violencia, hoy en día algunas de las estadísticas de incidencias de estos delitos son:

-En Chile (2011), se registro que el 87,8 % de los estudiantes chilenos de 7° curso básico (12 años) a 4° medio (17 años) ha sido víctima de ciber bullying por Internet.

- En Argentina (2011) El 19% de los menores de entre 9 y 17 años

-En Venezuela, según la experiencia de Lacasella (2015), es un delito que inicio en la etapa de bachillerato, pero hoy en día se solicita de su apoyo en charlas dentro de la educación primaria

Además de ellos Blanco (2013), indica: “Durante el 2012 amplias investigaciones contra la extorsión y secuestro en Venezuela, México y Colombia determinaron que la mayoría de los actos vandálicos interactivos más comunes tenían su centro de operaciones en Facebook”. Estos datos, fueron expuestos en el capítulo II, los retomamos, ya que son datos factuales del ciberbullying uno de los delitos que mayor propagación a nivel mundial ha traído, así como la implicación que tiene el Facebook como medio para incurrir en delitos.

Con estos datos y el testimonio que nos brindó el profesor Vito Lacasella (2015), nos permitió conocer desde su experiencia dictando charlas tanto en instituciones privadas como públicas, la detección de delitos mencionados. Por lo que podemos sustentar, en Venezuela existe la necesidad de la formación en este eje de temáticas, ya que él nos expuso que la situación se ha agravado al punto de que ya niños de cuarto grado son víctimas de tales delitos así como los discentes de la tercera etapa de educación media general, donde se ha propagado el fenómeno del sexting con la publicación de “fotos eróticas y sub-pornográficas”.

Quiere decir que Venezuela no escapa de esta realidad mundial, tenemos discentes y docentes que poseen la nueva tecnología con teléfonos o tablets inteligentes con acceso a internet y conexión a redes sociales como el correo, Facebook, Gmail, Twitter y sin darse cuenta se prestan para ser partícipes de ciberbullying, como por ejemplo.

Y si a esto le sumamos el comportamiento en estas redes, expuesto en la investigación de “Centro de Investigaciones Pew” en el 2013, tenemos mayores razones de creer, que el crecimiento de tales delitos, se asocia al cómo hacen uso de ello y una baja formación e información en delitos cibernéticos y seguridad en redes sociales.

Es un problema de valores y formación, que debemos apropiarnos de forma responsable. Ante tal situación y según lo que nos afirmó el profesor Lacasella (2015), la formación docente es indispensable y más los del área de Informática quienes poseen las competencias técnicas para proporcionarlos. Es por ello que taller va dirigido a esta población, ya que estos no solo potenciaría los conocimientos y el rol discente sino además de la familia, pues serviría de facilitador para ambos actores.

“La población”, en el párrafo anterior dimos un abre boca de la población a la que está orientado el taller. Los docentes de Informática, por ser los que cuentan curricularmente con las competencias técnicas para dar contenidos referentes a las TIC, es decir temas como el uso y manejo del internet, páginas como redes sociales y la previsión que se debe tener al ser parte de los miembros de esta “Social Network”, precisamente por ello es que proponemos una actualización docente en tema de seguridad en redes sociales, ya que por el uso que la población tiene de ellas, no podemos decir que hay desconocimiento de su tema, mas sí de el Ser críticos a la hora de subir fotos o publicar videos, o aceptar amigos en sus círculos sociales en entornos virtuales.

Son esas situaciones la que exponen a los usuarios y amigos a ser víctimas de ciber delitos. Ahora bien, la razón particular por la que se considera que debe ser el docente de esta área en la etapa de educación media general, es porque los delitos como sexting o ciberbullying agravado

donde más se denotan, además de que legalmente dan clases a los grupos etarios que tienen derecho acceder a estas cuentas, pues para ser parte de ellas deber ser mayor a los 13 años de edad.

Si bien es un problema que ya se está detectando desde antes, el conocimiento en seguridad tiene otra modalidad y concepción, ya que no es igual formar a niños que adolescentes; y los docentes de Informática se encuentran con el contexto de la población adolescente. Por esta cognición se busca darle las herramientas que requieran para que ellos posterior a su formación sirvan como formadores de formadores en el tema de seguridad en redes sociales. Sumado a esto la población debe contar con las siguientes “*conductas de entrada*”:

1. Debe ser docente de Informática de la etapa de educación media general.
2. Tener el dominio del uso del Computador, el Internet y las Redes Sociales.
3. Poseer cuenta en alguna de las siguientes redes sociales: Facebook, Twitter, Gmail, Google+, Hotmail, Youtube, Instagram, entre otras.
4. Debe emplear estas cuentas, dentro de su práctica docente o haber tenido una experiencia en el uso de ella dentro de la educación.

Concreto los aspectos anteriores es necesario pasar a definir el “*Tipo de Conocimiento*”, para el tipo de conocimiento Polo (2003), lo divide en declarativos, procedimental y factual. Por supuesto en conformidad con su clasificación, se estableció el tipo de aprendizaje y el análisis de las estrategias que tengan mayor pertinencia con el tema y generen el aprendizaje esperado. Polo (2003) define cada tipo, así:

Se consideran conocimientos declarativos los llamados “saber qué”. Son aquéllos de datos, hechos, conceptos y principios. Pozo (citado por Díaz y Hernández, 1999) los ha clasificado en conocimiento factual y conocimiento conceptual. El factual es el referido a datos y hechos que suministran información... Los conocimientos procedimentales se corresponden con el “saber hacer”, e implican la ejecución de procedimientos, estrategias, técnicas, habilidades, destrezas y

métodos. Están basados en la realización de acciones, por lo que remiten a conocimientos prácticos.

Los conocimientos actitudinales remiten a esos que deben suscitarse con el modelaje, la persuasión y la enseñanza de procesos para fomentar cambios en los mapas mentales que cercan el pensamiento de los alumnos. (pág. 73-74)

Para el tema los contenidos se clasificaran de la siguiente manera: (ver tabla nº6)

Tabla Nº 6:

Clasificación de los contenidos del Taller:

Declarativos/Conceptual/Factual	Procedimentales	Actitudinales
<ul style="list-style-type: none"> -Qué son las Redes Sociales. -Que es la Seguridad en Redes Sociales. - Clasificación de las Redes Sociales. -Población de las Principales Redes Sociales, a nivel Mundial. -Ventajas y Desventajas de los perfiles públicos y privados, dentro de las redes sociales. 	<ul style="list-style-type: none"> - Analizar y exponer los principales ataques en estas redes: <ul style="list-style-type: none"> -Sextorsión. -Ciber bullying. - Plagio de Identidad. - Phishing - Grooming. - Análisis general de cada video que se presente durante el taller. 	<ul style="list-style-type: none"> - Reflexionar sobre la importancia del tema seguridad en redes sociales. - Reflexionar, sobre los delitos más comunes dentro de las redes sociales.

Nota: Elaboración de la autora. Clasificación de los Contenidos, del taller en “Seguridad en Redes Sociales”.

Los “*Fundamentos Teóricos*”, en el caso del taller serán desde dos visiones que hoy en día en esta nueva era trabajan en conjunto, sobretodo dentro del proceso de aprendizaje en las redes sociales o TIC. Dicho lo anterior, el primer fundamento teórico será dado por Ausubel (1983), quien expone su teoría del “Aprendizaje Significativo”, en él se indica que para garantizar un verdadero aprendizaje significativo se debe partir con los conceptos o conocimientos previos de la persona.

Esto a manera de propiciar un proceso metacognitivo exitoso, para ello se debe contar con un contenido y material adecuado, donde tanto a nivel visual como conceptual llame la atención del discente y genere la motivación requerida. Esto lo podemos aplicar hasta para la formación en adultos. Ausubel (1983) expone:

...el aprendizaje del alumno depende de la estructura cognitiva previa que se relaciona con la nueva información, debe entenderse por "estructura cognitiva", al conjunto de conceptos, ideas que un individuo posee en un determinado campo del conocimiento, así como su organización. En el proceso de orientación del aprendizaje, es de vital importancia conocer la estructura cognitiva del alumno; no sólo se trata de saber la cantidad de información que posee, sino cuales son los conceptos y proposiciones que maneja así como de su grado de estabilidad. (pág. 1)

Es decir, si queremos formar en “seguridad en redes sociales”, debemos partir de antemano con saber si los participantes saben y utilizan de forma frecuente las redes sociales, tanto en su vida cotidiana como dentro de sus prácticas en aula. Es así, como se inicia de un conocimiento base, para hablar de la seguridad dentro de estas redes y exponer sobre los delitos, generando un engranaje entre lo que saben y lo nuevo por descubrir. El aprendizaje significativo:

...ocurre cuando una nueva información "se conecta" con un concepto relevante ("subsuntor") pre existente en la estructura cognitiva, esto implica que, las nuevas ideas, conceptos y proposiciones pueden ser aprendidos significativamente en la medida en que otras ideas, conceptos o proposiciones. (Ausubel, 1983:2)

Para lograr tal aspecto, como antes hicimos mención los materiales y los contenidos juegan un papel relevante, ya que estos se convierte en el canal o medio por el que el participante hace el engrane solo lo que sabe y lo nuevo por aprender. Para ello el facilitador, debe exponer los nuevos conceptos y preceptos de una forma clara, creativa e innovadora. Se debe lograr estimular el aprendizaje para que el mismo se fije en el cerebro y no se olvide de manera rápida. Es por ello que el autor expone:

Que el material sea potencialmente significativo, esto implica que el material de aprendizaje pueda relacionarse de manera no arbitraria y sustancial (no al pie de la letra) con alguna estructura cognoscitiva específica del alumno, la misma que debe poseer "significado lógico" es decir, ser relacionable de forma intencional y sustancial con las ideas correspondientes y pertinentes que se hallan disponibles en la estructura cognitiva del alumno...

Cuando el significado potencial se convierte en contenido cognoscitivo nuevo, diferenciado e idiosincrático dentro de un individuo en particular como resultado del aprendizaje significativo, se puede decir que ha adquirido un "significado psicológico" de esta forma el emerger del significado psicológico no solo depende

de la representación que el alumno haga del material lógicamente significativo, "sino también que tal alumno posea realmente los antecedentes ideativos necesarios" (Ausubel, 1983: 55)

Con respecto a los materiales se empleará las presentaciones colectivas multimedia, el proyector multimedia, los materiales didácticos diseñados y el video como herramienta para generar conocimientos y afianzarlos de una forma didáctica. Con respecto al contenido será expuesto como algo sustancial y no arbitrario, es decir, se comenzará con lo que los participantes ya conocen y los asociaremos con lo nuevo, de manera que sea percibido como una continuidad y no como un conocimiento nuevo obligatorio aprehender.

Ausubel (1983), sin duda alguna expone una teoría aplicable y válida para el diseño de nuestro taller, dado que la misma, visualiza el aprendizaje como un proceso dinámico que ocurre de una forma bilateral, ya que el docente o facilitador no puede inferir que sabe todo o que el discente no sabe nada. Ambos deben partir por una base de conceptos para conjuntamente crear nuevos.

Claro esto, la otra teoría que sirve de complemento será la propuesta de la teoría es el Conectivismo, una que a pesar de exponer que tiene sus propias raíces de origen, puede trabajar en equipo con la teoría de Ausubel (1983), ya que mientras este expone que el aprendizaje significativo emana del material y del concepto que se exponga, la nueva propuesta hace énfasis en el que mismo ocurre pero por medio de la colaboración dentro de la "Social Network" (redes sociales) o su almacenamiento está dentro de base de datos.

Es decir, el conectivismo se incluye las tecnologías y las redes sociales como una nueva tendencia para el aprendizaje, como señala Polo (2003) en su modelo y según lo presente, es un proceso similar al que expone Ausubel, pero incluye a las tecnologías dentro del proceso no solo para generarlas sino además para almacenarlo. En fin son teorías, que más que encontrarse se adaptan o se complementan dentro de la investigación y sobre todo al proceso de aprendizaje que al fin y al cabo es el objetivo final de los tres autores y el interés personal de la presente autora.

El exponente base de esta propuesta es Siemens (2008), quien expone que esta es una nueva corriente epistemológica, a tiene ciertamente un inicio en posturas como el conductismo,

cognositivismo y constructivismo, en cuanto a la tendencia del aprendizaje, sin embargo, aporta nuevas ideas con respecto a cómo ocurre y cómo se almacena, ya que no es mentira que las nuevas tendencias de esta era giran es torno a las tecnologías, redes sociales e internet, es un poco lo que se expuso ante sobre las nuevas competencias que debe tener el docente para adaptarse a los procesos dentro del aula. Siemens (2008), define el Conectivismo como:

...la aplicación de los principios de redes para definir tanto el conocimiento como el proceso de aprendizaje. El conocimiento es definido como un patrón particular de relaciones y el aprendizaje es definido como la creación de nuevas conexiones y patrones como también la habilidad de maniobrar alrededor de redes/patrones existentes.

El Conectivismo aborda los principios del aprendizaje a numerosos niveles – biológico/neuronal, conceptual, social/externo

Es decir el proceso puede ocurrir tanto de forma colectiva como a nivel personal, es decir, discente y explorador. Ya que como hemos indicado el enfoque de esta tendencias es precisamente incluir las tecnologías como parte de la “distribución de cognición y conocimiento” (Siemens, 2008). Es decir, el conocimiento no solo reside en el individuo sino también en la interacción con otras personas o en fuentes de información como bases de datos, blog, exploradores, entre otros. Sin duda alguna, lo innovador de esta propuesta o teoría es el papel clave que juegan las tecnologías para alcanzar el aprendizaje o construir conocimiento.

Por ejemplo Siemens (2008) expone que las tecnologías se orientan al “Trabajo cognitivo en la creación y visualización de patrones, en extender e incrementar nuestras habilidades cognitivas y en Mantener información en una forma de rápido acceso (por ejemplo, buscadores, estructuras semánticas, etc.)”. Y de alguna manera, tiene un buen punto, la generación 2.0 y próximamente la 3.0, tiene en gran medida almacenado sus archivos, videos, libros, artículos y trabajos dentro de sus computadoras, en la nube con el internet o dentro de espacios corporativos.

En estos espacios confían, una parte importante de sus conocimientos e investigaciones sintiéndose seguros de que estos se ubiquen ahí, lo que quiere decir, es que los discentes emplean las TIC, las redes sociales y el internet para generar, compartir u obtener conocimientos y

aprendizajes el docente dentro del aula debería hacerlo, de manera de poder captar su atención; si no se pierde entre sus prácticas antiguas y no genera esa chispa requerida por parte del estudiante.

Con ello no buscamos aseverar que la práctica docente esta descontextualizada o que lo tradicional está mal, lo que buscamos exponer es que no podemos cerrar las puertas las nuevas tendencias ni mucho menos no aprobar supuestos como los que aporta esta nueva tendencia del Conectivismo. La era digital es una realidad, las redes sociales se han convertido en todo un espacio para la interacción y hasta para compartir información así como los blogs o weblogs son espacios para la educación y sobre todo para generar aprendizaje significativos en red.

Para las “*Estrategias cognoscitivas*”, se entiende por ellas aquellas estrategias que se planifica emplear en el diseño, para hacer del proceso de enseñanza uno más dinámico y como se estableció previamente poder hacer del proceso dialéctico, flexible y sistemático. En este punto uniremos también la “*Administración de la Tecnología*”, debido a que se consideran que ambas van de la mano el diseño de nuestro taller presencial. Aclarando esto, cubrimos este componente presentando las estrategias y tecnologías serán aplicadas en el taller: (esto se apreciara mejor en el componente Diseño)

Estrategias y Tecnología a emplear:

- Aplicación de medios audiovisuales (videos, imágenes, presentación colectiva multimedia y proyector multimedia.)
- Actividades grupales (exposición, organización de contenidos, feedback).
- Actividades individuales (lluvia de ideas, opiniones, exposición de experiencias, etc.)

4.1.2 Componente Tecnológico:

El componente Tecnológico juega un papel relevante dentro del diseño del taller, en este se habla de los medios computarizados de las TIC, que se emplearán para presentar un contenido y

lograr los objetivos declarativos, actitudinales y procedimentales propuestos en nuestros taller.

Polo (2003) entiende este componente como:

...es de importancia determinante, pues abarca las dimensiones disciplinaria e interdisciplinaria de los recursos humanos requeridos para la producción de un curso mediado por las tecnologías.... No obstante, desde el punto de vista pedagógico, cada sub-componente debe ser estudiado y analizado por el educador o diseñador de la instrucción, lo que implica un proceso de comunicación permanente entre los miembros del equipo. (pág. 76)

El proceso de análisis lo hemos cubierto en su totalidad, antes de iniciar esta exposición se hablo de que era necesario realizar ciertos ajustes para que el modelo se adaptará a lo que va a diseñar, es por ello que algunos sub-componentes de esta dimensión serán editados ya que no se van aplicar dentro del diseño del taller. Expuesto lo anterior, "*El proceso de Interacción*", en este aspecto Polo (2003) emplea el modelo de Galvis (1992), ejecutando una seria de adaptaciones, donde define este punto como:

La interacción centrada en el alumno remite al binomio estudiante instrucción. Esta forma de interactuar atañe a los procesos que el ambiente tecnológico, basado en un entorno multimedia, proporciona al estudiante para que se generen respuestas de ambos lados y, en consecuencia, se logre el aprendizaje... (pág. 77)

La interacción se puede realizar por íconos (iconos de navegación- Hipervínculos), de forma pictóricas (Fotos, ilustraciones), Sonoros (música, efectos de sonidos), Dispositivos de entrada (uso del ratón y el teclado), Dispositivos de salida (Pantalla y efectos de sonido). Como ya se expuso antes el taller será presencial, sin embargo, se empleará el uso de presentación colectiva multimedia, la presentación de videos, para dar inicio y afianzar algunos contenidos.

Podemos decir que la interacción en primera instancia será interactivo de tipo presencial facilitador-docente, pictórica pues se les presentaran imágenes asociativas al tema a exponer empleando Dispositivos de Salida, pues utilizaremos un computador, y pantalla de reproducción donde se verán la presentación así como los videos a mostrar. Es por ello que el "*Ambiente de*

Aprendizaje” básicamente será el espacio dispuesto para el proceso de taller, ya que en gran medida y el proceso de feedback será dado en ese espacio de forma presencial.

El mismo deberá ser un aula con cabida de quince a veinte personas, que posea acceso a internet o en su defecto se cuente con enchufes para laptop, proyectores multimedia y cornetas, el mismo deberá poseer una buena iluminación para que la presentación colectiva multimedia y los videos se puedan percibir de manera adecuada.

4.1.3 Componente Evaluación:

Este es una de los componentes más relevantes, ya que en él se permite verificar que tan apropiado es el diseño, los contenidos, las estrategias y medios, en este componente se percibe el todo del DI o MIC. Es al que Polo (2003) denomina como:

Es el componente que estará presente en cada uno los elementos que conforman los demás. El proceso estará montado sobre tres sistemas: la evaluación de los aprendizajes, la evaluación de la tecnología y la evaluación del ADITE. (pág. 79).

Este así como el componente tecnológico, sufrió ciertas modificaciones, precisamente por las características predominantes ya expuestas del taller. Para nosotros las sub-dimensiones son: *“Evaluación de las estrategias”* y *“Especificación de la Evaluación Formativa de los componentes del diseño”*; será mediante un cuestionario, diseñado por la investigadora y evaluado por los profesionales escogidos. El diseño de dicho cuestionario se podrá apreciar en los anexos.

4.1.4 Componente de Diseño:

Dejamos de último el componente de Diseño, porque es el más extenso ya que tiene el fuerte de la investigación, este así como el de Análisis si se aplica completo, solo que se adapta a MI que se propone. El diseño del MI, está constituido por “*Formulación de las Metas y Objetivos*”, “*Estructura secuencial de los objetivos*”, “*Selección de las Estrategias y Actividades instruccionales*” aquí se incluye los Medios y el “*Diseño de las estrategias e instrumentos de evaluación de aprendizaje*”. Esto lo presentaremos a continuación:

✓ Nombre del taller:

Taller “Seguridad en Redes Sociales”: Conceptos Básicos y Herramientas para su abordaje en aula.

✓ Meta del Taller:

Dar a conocer los conceptos básicos y las herramientas claves sobre el tema “Seguridad en Redes Sociales”, a los docentes pertenecientes al área de Informática en la etapa de educación media general. Una vez finalizado el taller el docente contara con nociones superiores del tema y con estrategias para abordar la temática y al mismo tiempo habremos apoyado la calidad en la formación docente.

✓ Objetivos:

- Describir los aspectos conceptuales básicos en torno al tema “Seguridad en Redes Sociales”.
- Analizar la importancia de los principales ataques y herramientas para abordar el tema de seguridad en redes sociales.
- Reflexionar sobre la importancia de la inclusión del tema de Seguridad en Redes Sociales, dentro de su práctica docente dentro de esta etapa escolar.

✓ **Duración:**

Una de sesión de siete (7) horas y media, dividida en tres bloques, donde las horas en aula, se toman de 45min. Aclarado lo siguiente se presentará así:

- ✓ Bloque #1: Inicio y desarrollo del taller, duración de: 3h.
- ✓ Bloque #2: Break, duración: 1h y 15min. Es decir en total: 60min.
- ✓ Bloque #3: Desarrollo y Final del Taller, duración: 2h y 30min.

✓ **Esquema del Taller:**

PLAN DE FORMACIÓN DOCENTE PARA EL TALLER
“SEGURIDAD EN REDES SOCIALES”

META	TEMARIO	ACTIVIDAD	RECURSOS REQUERIDOS	TIEMPO ESTIMADO
	Presentación Inicial	1- Se les dará la Bienvenida y solicitará que se identifiquen, colocando su nombre en los identificativos. Para ello se contarán los recursos necesarios. 2- Presentación inicial de todos los participantes y del facilitador.	Marcador. Imperdible. Cartón (para colocar sus nombres)	15´
Conocer las expectativas por parte de los participantes con respecto al taller.		3- Exposición por parte de los participantes, las expectativas del taller. 4- Revisión de los objetivos y agenda desarrollar.		15´
Exponer las definiciones básicas.	Redes Sociales: Definiciones y tipos.	5- Se hace una pregunta abierta: ¿Qué son las redes sociales? (El facilitador debe estimular a que respondan al menos tres participantes para entrar en contexto).	Ninguno.	10´
		6- Se proyecta la presentación colectiva multimedia con la definición de redes sociales. Y un cuadro con las redes sociales y la población con la que cuenta a nivel mundial. Datos factuales del 2014. 7- Se les presentará un cuadro sobre la clasificación de las redes sociales.	Presentación Colectiva Multimedia. Computador. Proyector Multimedia.	25´
Presentar la definición de “Seguridad en Redes Sociales”	Seguridad en Redes Sociales I: Definición.	8- Se hace una pregunta abierta: ¿Cuáles casos han conocido o escuchado sobre delitos cibernéticos? (el facilitador debe estimular a que respondan al menos tres participantes para entrar en	Presentación Colectiva Multimedia. Computador.	15´

		<p>contexto)</p> <p>9- Se proyecta presentación colectiva multimedia con la definición de seguridad en redes sociales y las tasas de los delitos cibernéticos más frecuentes. Para ello se les facilitara un material didáctico. (ver Anexo N° 2)</p>		
<p>Conozcan que los delitos más frecuentes dentro de las redes sociales.</p>	<p>Seguridad en Redes Sociales II: Tipos de ataques.</p>	<p>10- Actividad en Grupo#1: Exponer sobre los delitos cibernéticos más comunes dentro de las redes sociales. Para esto se les proporcionara un material de apoyo, previamente diseñado. (Ver Anexo 3)</p>	<p>Papel Bond. Marcadores. Tizas. Colores.</p>	<p>40´</p>
<p>Generar reflexión sobre los delitos y sus consecuencias</p>	<p>Seguridad en Redes Sociales III: Reflexión general.</p>	<p>11- Presentación del video: “Lo Malo de las Redes Sociales Si no se controla webmsmall” (Tiempo: 8´05´´)</p> <p>12- Análisis del video e identificación de los delitos ya expuesto. -Se les preguntara a los participantes que opinan del video.</p>	<p>Computador. Cornetas. Proyector Multimedia. Video.</p>	<p>20´</p>
		Break		<p>60´</p>
<p>Generar reflexión sobre cómo nos comportamos dentro de las redes sociales.</p>	<p>Aceptar un amigo en la red.</p>	<p>* 13- Presentación del Video: Caperucita 2.0: ¿Deberías agregar a extraños a tus redes sociales? (Tiempo: 2´07´´) * 14- Discusión y análisis del video.</p>	<p>Computador. Cornetas. Proyector Multimedia. Video.</p>	<p>12´</p>

Indicar la ventaja y desventaja de los perfiles públicos y privados.	Perfiles público y privados. Ventajas y desventajas.	15- Presentación colectiva multimedia: Ventajas y Desventajas de las los perfiles públicos y privados.	Computador. Presentación Colectiva Multimedia.	15´
Elaborar una recomendación de forma conjunta, sobre cómo ser un mejor usuario.	Como ser un mejor usuario.	* 16-Actividad Grupal #2: “140 Caracteres una Recomendación”	Papel Bond. Marcadores. Tizas. Colores. Teipe.	20´
Elaboración de cinco estrategias docentes para abordar el tema de seguridad en redes sociales.	Cinco estrategias	* 17- Con la reflexión anterior, todos con la guía y participación del facilitador extraerán de forma breve cinco estrategias concretas de cómo abordar el tema de seguridad en redes sociales.	Papel Bond. Marcadores. Tizas. Colores.	10´
	Reflexión Final.	18- Presentación del Video Final: Recomendaciones para el Uso Seguro del Internet y las Redes Sociales, con seguridad. (Tiempo: 5´01´´) 19- Analizar el video con las siguientes preguntas: ¿Cómo aplicar este contenido en el aula?	Computador. Cornetas. Proyector Multimedia. Video.	15´
		20- Actividad Final: Que te llevas en la maleta. 21- Aplicación de la Evaluación post-taller. (Modelo puede ser apreciado en el Anexo)	Papel Bond. Marcadores. Pruebas.	35´
			Tiempo Total	295

4.1.4. 1 Descripción de las actividades:

Las actividades 1, 2, 3, 4 permitirán a los participantes conocerse entre sí, además de situar la agenda a tratar en el taller. Es de esta manera como se da inicio al taller.

- **Actividad #5:** Pregunta de Inicio.

Una vez iniciado el proceso y presentado los participantes, se dará pie para que empiece el tema, partiendo con la pregunta: ¿Qué son las redes sociales?

Esta pregunta le permite al facilitador, conocer que tanto manejan sobre el tema, y sobre las redes que más usa la población docente, permitiendo partir de sus experiencias o conocimientos sobre ello. Las experiencias previas en este caso son importantes ya que le brindan al facilitar la poca o mucha receptiva que se tienen sobre estas o sobre su aplicación dentro de las aulas. Una vez obtenido la información base, el facilitador pasa a la siguiente actividad.

- **Actividad #6:** Presentación de Láminas

La presente actividad se basa en la presentación colectiva multimedia, el concepto de redes sociales y los tipos de redes sociales, así como la población que posee cada una. Para el concepto apoyándose Perdomo, D (2011). El concepto de “Redes Sociales”, comprendidas como:

... aquel lugar virtual que les permite a individuos la interacción social, el intercambio constante de información, intereses, ideas y opiniones. Es una comunidad en constante construcción y remodelación a fin de ser cada vez más completa frente a las necesidades de los internautas (usuarios de internet), quienes buscan un sitio apropiado para convivir con demás personas que, como ya se dijo, comparten sus mismos gustos y aficiones, pero al mismo tiempo relacionarse con gente. (Perdomo, 2011:8)

Para los tipos de Redes Sociales, usaremos la tabla N° 3, presentada en el marco teórico, por supuesto esta tabla debe ser adaptada para una presentación multimedia. La tabla será:

Principales Redes sociales.

Red Social	Año de fundación	Creador	Características	Números de usuarios actualmente (2014)	Logo
Facebook	2004	Mark Elliot Zuckerberg	<ul style="list-style-type: none"> -Se crea con un gran espacio para compartir vivencias. -Permite aceptar amigos de todos lados del mundo. -Crear un perfil y hacerlo público o privado. - Se puede subir videos, imágenes y etiquetar a los amigos aceptados en tu perfil. -Se puede jugar dentro de la misma red. 	Aprox. 1.28 billones	
Twitter	2006	Jack Dorsey	<ul style="list-style-type: none"> -Microbloggin. - Publicaciones en 140 caracteres. -Permite las publicaciones de imágenes. -Permite estar enterada al instante de sucesos, hechos o aconteceres a nivel local, regional y mundial. -Hashtag, para crear temas de interés. 	Aprox. 255 millones	
Youtube	2005	Chad Hurley, Steve Chen y Jaweb Karim	<ul style="list-style-type: none"> -Permite subir y publicar videos, de cualquier tipo de temas. -Aloja una variedad de video clips de películas y programas de televisión, videos musicales, y vídeos caseros. 	Aprox. 1 Billón	
Instagram	2010	Kevin Systrom y Mike Krieger	<ul style="list-style-type: none"> -Es una aplicación gratuita para publicar fotos y videos. -Aplicación gratuita para smarphone. -Comprado en el 2012 por Facebook. - Permite la aplicación de filtros a las fotos, etiquetar a seguidores o hacer publicaciones directas. 	Aprox. 200 millones	
Google+	1997	Co-fundadores: Sergey Brin y Larry Page	<ul style="list-style-type: none"> -Es una red social, perteneciente a google, que permite la publicación de videos, imágenes y comentarios. -Crear círculo de amistades, familia y trabajadores. 	Aprox. 540 millones	

Nota: Elaboración de la autora. Resumen de las principales redes sociales, con sus características, fundadores y número de usuarios actualmente.

● **Actividad # 7:** Clasificación de las Redes Sociales.

Cabe destacar el cuadro que presentaremos a continuación es un esbozo para el facilitador, dado que igual que la tabla anterior, el mismo es extenso para presentarse en una presentación colectiva multimedia. Sin embargo, servirá para estudiar y presentar de forma verbal y sintetizada la clasificación de las redes sociales. La presentación final de esta tabla, podrá ser vista en los anexos.

Clasificación de las Redes Sociales.

Por su público objetivo y temática	Por el sujeto principal de la relación	Por su localización geográfica	Por su plataforma
<p>-Redes sociales horizontales: Son aquellas dirigidas a todo tipo de usuario y sin una temática definida. Por ejemplo: Facebook, Twitter, Orkut, Identi.ca.</p>	<p>-Redes sociales humanas: Son aquellas que centran su atención en fomentar las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades. Por ejemplo: Koornk, Dopplr, Youare y Tuenti.</p>	<p>-Redes sociales sedentarias: Este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Por ejemplo: Rejaw, Blogger, Kwippy, Plaxo, Bitacoras.com, Plurk.</p>	<p>-Red social MMORPG y metaversos: Normalmente contruidos sobre una base técnica Cliente-Servidor (WOW, SecondLife, Lineage).</p>
<p>-Redes sociales verticales: Están concebidas sobre la base de un eje temático agregador. Tienen por objetivo el de congregar en torno a una temática definida a un colectivo concreto. A su vez pueden clasificarse en:</p>	<p>-Redes sociales de contenidos: Las relaciones se desarrolla uniendo perfiles a través de contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador. Por ejemplo: Scribd, Flickr, Bebo, Friendster.</p>	<p>-Redes sociales nómadas: Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Por ejemplo: Latitud, Brighkite, Fire Eagle y Scout.</p>	<p>-Red social web: Su plataforma de desarrollo está basada en una estructura típica de web. Algunos ejemplos representativos son MySpace, Friendfeed y Hi5.</p>

<p>a. Redes sociales verticales profesionales: Están dirigidas a generar relaciones profesionales entre los usuarios. Por ejemplo: Viadeo, Xing y Linked In.</p> <p>b. Redes sociales verticales de ocio: Su objetivo es congregarse a colectivos que desarrollan actividades de ocio, deporte, usuarios de videojuegos, fans, etc. Por ejemplo: Wipley, MinubeDogster, Last.FM y Moterus.</p> <p>c. Redes sociales verticales mixtas: Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales entorno a sus perfiles. Por ejemplo: Yuglo, Unience, PideCita, 11870.</p>	<p>-Redes sociales de inertes: Conforman un sector novedoso entre las redes sociales. Su objeto es unir marcas, automóviles y lugares. Entre estas redes sociales destacan las de difuntos, siendo éstos los sujetos principales de la red.</p> <p>El ejemplo más llamativo es Respectance.</p>		
--	--	--	--

Nota: Elaboración de la autora. Fuente: Flores Cueto, J (2009). Redes Sociales.

● **Actividad #8:** Pregunta abierta.

Las actividades anteriores serán la base, para que en estas actividades se inicie el tema sobre la seguridad en redes sociales, que es el eje central del taller. Es por ello que se realizan las siguientes preguntas abiertas: ¿Cuáles casos que han conocido o escuchado sobre delitos cibernéticos?

Las respuestas a estas preguntas le permitirían al facilitador, tener una base sobre los conocimientos que tienen los participantes del tema y sobre los delitos cibernéticos más frecuentes en estos espacios virtuales. De este punto partir y entrar a fondo en el tema.

- **Actividad #9:** Presentación colectiva multimedia - Definición de “Seguridad en Redes Sociales”.

Partiendo de la información anterior el facilitador pasará a presentar una lámina sobre la definición de “Seguridad en Redes Sociales”. Se le presentará datos recolectados por la autora, sobre el porcentaje de los delitos más comunes en estos espacios según la empresa líder en el desarrollo de programas y aplicaciones para la seguridad del ordenador en el uso del internet, “Symatec” quien lo expone en el informe sobre las “Tendencias de Seguridad Informática en América Latina y el Caribe” (para ello se le dará un material de apoyo, el mismo podrá verse en los anexos). Para dar inicio a los delitos se realiza la actividad siguiente.

- **Actividad # 10:** Actividad Grupal “Presenta sobre los delitos cibernéticos más comunes dentro de las redes sociales”.

En esta actividad se divide a los participantes en cinco grupos de cuatro personas, y se les pide al azar que seleccionen, uno de los siguientes temas:

- Sextorsión.
- Cyberbullying.
- Plagio de Identidad.
- Phishing
- Grooming.

Para ello se les dará la información de cada tema a los equipos, con el fin de que estos se organicen y de una forma sencilla expongan al resto de los participantes el tema que les toco. Contarán con 20´ para organizarse y 5´cada grupo para exponer. Esta actividad se hace con objetivo de generar un proceso de retroalimentación donde son los mismos participantes los encargados de construirlos con la guía y herramientas que propicia el facilitador. (Para ello se le dará un material de apoyo, el mismo podrá verse en los anexos).

● **Actividad #11 y # 12:** Presentación y Análisis del Video.

Se le presenta a la audiencia el segundo video, llamado “Lo Malo de las Redes Sociales Si no se controla webmsmall.” obtenido en línea. En él se demuestra de una forma muy jocosa y sencilla, cada uno de los errores que fácilmente cometemos dentro de las redes sociales, deslices que nos pueden colocar en situaciones que exponen tanto nuestra integridad física como virtual por estas redes. Estos errores, son comunes en los usuarios que las visitan. Usuarios de diversas edades que exponen de una manera innecesaria su vida privada.

El video como medio didáctico permite dos cosas: 1- Que los docentes entiendan la necesidad de formación en seguridad en redes sociales, dado que pueden guiar a sus discentes a que sean más críticos y prudentes a la hora de usarla y 2- Sirve como un medio, para enseñar o ejemplificar una situación latente dentro de la sociedad. Como lo sustenta Acevedo (2012:44):

El video dada sus características es utilizado por los docentes como un instrumento o elemento motivador dentro de los procesos de enseñanza y aprendizaje, ya que al presentar la información en un formato distinto a los tradicionales, los estudiantes suelen incentivarse...

De esta manera no solo se logran los objetivos, sino además, se generara la discusión necesaria sobre el tema, traer conceptos desconocidos y demostrar que delitos como: Sextorsión, Cyberbullying, Plagio de Identidad y Phishing; son delicados y lo que es peor nuestros discentes se exponen a ellos con el mal uso que le den a estas redes. Es así como se aportan tanto elementos conceptuales como estratégicos para abordar la temática, por parte de ellos en aula. Con el apoyo del video se plasma la exposición de cada equipo sobre lo delitos cibernéticos.

Break: Tiempo de descanso y comida para los participantes, mientras el facilitador prepara el segundo bloque de actividades y contenidos.

● **Actividad # 13 y #14:** Presentación de Video y Análisis.*

Antes de explicar estas actividades, es imprescindible aclarar que la razón por la que estas poseen asteriscos (*), es porque pueden ser o no aplicadas a la hora ejecutar el taller, es decir el facilitador tendrá la oportunidad de decidir de acuerdo al tiempo si es posible su aplicación o no.

No obstante, Para continuar el tema y activar a los participantes de nuevo después del break, se les presente el segundo video llamado “Caperucita 2.0: ¿Deberías agregar a extraños a tus redes sociales?”, obtenido en línea. Este presenta de una forma ejemplifica lo que puede suceder cuando agregamos a nuestros perfiles personas que no conocemos, una acción muy común hoy en día sobre todo por la población adolescente. Una vez presentando el video, se da pie al análisis del mismo, por parte de los participantes.

- **Actividad #15:** Presentación colectiva multimedia.

Se presentara el siguiente cuadro con cinco desventajas y ventajas de tener un perfil público o privado dentro de nuestras redes sociales. Hay que tener en cuenta que el beneficio de estos espacios, depende en gran medida en el buen uso que le demos que de las configuraciones que presenta cada página o red social, ya que cada usuario es autónomo y administrador de su perfil o cuenta. Al igual que los cuadros anteriores se le recomienda al facilitador, que lo sintetice de manera de ser propuesto en la presentación colectiva multimedia, sin embargo, en la diseñada para la propuesta, hay presencia de un ejemplo de cómo podría sintetizar el siguiente cuadro en sus anexos.

Ventajas y Desventajas de los Perfiles públicos y privados.

	Perfil Público	Perfil Privado
Ventajas	1. Permiten acceder fácil a ti, de personas conocidas como desconocidas.	1. Solo pueden acceder a ti personas que conozcas o le des acceso a tu perfil.
	2. Tus publicaciones, llegan a gran cantidad de personas.	2. Solo a quienes pertenecen a tu círculo de amigos o seguidores, pueden ver tus publicaciones y comentarlas.
	3. La publicaciones de eventos tanto corporativos como personales, pueden tener gran publicidad, con perfiles abiertos pues grandes números de personas conocidas como desconocidas pueden acceder a él.	3. Puedes invitar por estos espacios a las personas cercanas a ti a tus fiestas o eventos. De esta manera exclusivamente solo el que tú quieras puede ser parte de él.
	4. Permite la propagación de informaciones a gran escala.	4. Tu información solo llega a quienes desees.
	5. Permite hacer nuevas vinculaciones o amistades con personas de todos lados del mundo.	5. Permite respetar tu espacio personal y mantiene tu vida privado en resguardo, ya que solo lo que desees y a quienes desees que las vean podrán acceder.
Desventajas	1. Tanto personas conocidas como no conocidas, pueden acceder a tu perfil y ver tus publicaciones y fotos.	1. Si eres una corporación o estás interesado en vender una marca o producto, esto podría dificultar el acceso a él.
	2. Cuando acceden a él personas que no conoces ni están dentro de tu círculo de amistades, no sabemos bajo cual intención hacen el acceso a él, lo cual puede generar situaciones incómodas o negativas para el usuario.	2. Si eres una corporación o estas interesado en la organización de un evento a gran escala, los perfiles privados no permiten que esto sea posible pues solo conocerán de este evento quienes tengas como seguidores o amigos, no público externo que esté interesado en participar.
	3. Corres riesgo de ser una víctima de delitos como: Sexphsing, Cyberbullying, Plagio de Identidad y Phishing o ser expuesto ante piratas informáticos con hackers.	
	4. Las características primordial de las redes sociales, es que permite crear un círculo o red con personas tanto conocidas como desconocidas. Al tener el perfil público puedes exponer también a tus amistades cercanas como a familiares, pues pueden ser localizados o vistos en tu perfil de una forma sencilla.	
	5. Algunas corporaciones, hacen uso de las redes sociales, para los procesos de selección, si este está abierto y es tu cuenta personal podrías exponer de una	

	forma negativa ante estos.	
--	----------------------------	--

Nota: Elaboración y análisis de la autora. Resumen de las principales ventajas y desventajas de tener perfiles públicos o privados, en las redes sociales.

•Actividad #16: Actividad Grupal #2: “140 Caracteres una Recomendación” *.

De igual manera a las actividades 13 y 14 poseen asteriscos (*), porque pueden ser o no aplicadas a la hora ejecutar el taller, es decir el facilitador tendrá la oportunidad de decidir de acuerdo al tiempo si es posible su aplicación o no.

Para esta actividad a los grupos anteriores, se les pedirá que escojan e indique en 140 caracteres, una recomendación sobre el uso correcto de sus perfiles dentro de las redes sociales. Esto deberán escribirlo en una hoja de papel bond, y el representante deberá exponer ¿Por qué escoger esa recomendación? y ¿Por qué la considerarla importante, para mantener la seguridad dentro de las redes sociales? .Lo importante es que no deberán repetirse, lo que obliga el trabajo colaborativo de todos los participantes.

De esta manera, estimularemos los pensamientos críticos de los participantes tanto individual como grupalmente, lo que ayudara a fijar la importancia del tema y de la formación de él tanto para ellos como para los discentes. Se espera además que esta actividad complemente las anteriores, quienes están enfocadas en primera instancia que se focalice cuales aspectos de los que se han hecho mención se ha incurrido o si sean expuesto como usuarios de una manera que puedan ser víctimas de estos delitos. En segunda instancia que identifiquen si dentro de su aula se han presentado estas situaciones o algún discente ha sido víctima; si logran identificar esto en sus aulas, una vez culminado el taller contarán con las herramientas para enfrentar la situación y ser ellos guías para mejorarla.

- **Actividad #17:** Cinco Recomendaciones para el Docente.*

De igual manera a las actividades 13, 14 y 16 poseen asteriscos (*), porque pueden ser o no aplicadas a la hora ejecutar el taller, es decir el facilitador tendrá la oportunidad de decidir de acuerdo al tiempo si es posible su aplicación o no.

Como una de las actividades finales, el facilitador conjuntamente con los participantes escribirá en una lámina de papel bond, cinco estrategias que puede emplear el docente en el aula a la hora de que se presente una situación ligada a los delitos en redes sociales, las ideas deberán ser expuestas de forma corta y concreta; de manera de hacer el proceso rápido pero enriquecedor.

- **Actividad #18:** Presentación de video final

La presentación del video final, titulado: Recomendaciones para el “Uso Seguro de Internet y las Redes Sociales, con seguridad” este video se obtuvo en línea. En él se presentan diez recomendaciones sobre el uso correcto de las redes sociales, en aras de mantener nuestra seguridad como usuario. Estas recomendaciones son:

- Mantén tu equipo de software maliciosos y no abras mensajes o ficheros extraños, pueden conducirte a virus.
- No expongas tus datos ni información personal.
- Cuidado con las fotos e imágenes que se carguen en los perfiles, pueden dar tu imagen o la de terceros.
- Evita generar o ser parte de provocaciones u conflictos por estos espacios.
- Gestiona tu privacidad, exponerse lo menos posible, es de personas críticas e inteligentes.
- No compartas claves.
- Cuidado con el uso inadecuado de la webcam.
- Mantén un espíritu crítico en estas redes, es necesario contrastar información.

- No aceptes a desconocidos como amigos dentro de estos entornos.
- No concretes citas a solas con desconocidos.

• **Actividad # 19:** ¿Qué te llevas en la maleta?

Una vez visto el video, se para analizar las diez recomendaciones, se darán las siguientes preguntas: Se dará cierre con la pregunta ¿Qué te llevas en la maleta?. Cada participante de forma breve expresará que se lleva al finalizar el taller.

• **Actividad #20:** Evaluación post-taller.

Antes de que los participantes se vayan, se les proporcionara la evaluación post-taller, que le servirá al facilitador que tan pertinente fue su gestión, los contenidos y estrategias y las impresiones que se llevan. (El diseño de esta evaluación será presentado en los anexos).

El fin general de todas las actividades propuestas, es en primera instancia, lograr cada objetivo. ¿Cómo?, desarrollando cada actividad, pues cada una tiene aspectos conceptuales donde se les indicarán las nociones básicas de conceptos asociados a las redes sociales y la seguridad dentro de ellas, así mismo los procedimentales con las actividades en grupos, donde tendrán que socializar y consensuar con sus equipos de trabajos lo que se les pide, de esta manera se genera el aprendizaje cooperativo (Johnson, Johnson y Holubec 1999), antes expuesto.

CAPÍTULO V

ANÁLISIS DE RESULTADOS

En el capítulo III, hicimos referencia que el análisis de los resultados sería por medio del método estadístico análisis de frecuencia. El mismo será empleado, para conocer de manera general cómo fue la frecuencia en las respuestas en la validación de experto, es importante recordar, que los expertos evaluarían el taller en función a los cuatro componentes del modelo ADITE. Estos cuatro componentes: Análisis, Tecnología, Diseño y Evaluación, permitirán saber en una escala de estimación, que va de: Muy Adecuado (M-A), Adecuado (A), Poco Adecuado (P-A) e Inadecuado (I); cómo está diseñado el taller en “Seguridad en Redes Sociales”, dirigido a los docentes pertenecientes al área de Informática, de etapa de educación media general”.

Los expertos contaron con el plan de formación, descripción de las actividades, materiales didácticos y los links de los videos que se planifico emplear para el taller. Todos estos recursos fueron el anexo de instrumento a llenar. De esta manera cada validador, contó con el material completo para ejecutar el proceso de evaluación de una forma crítica, pertinente y objetiva. Teniendo lo anterior presente, damos continuación para el análisis de cada componente.

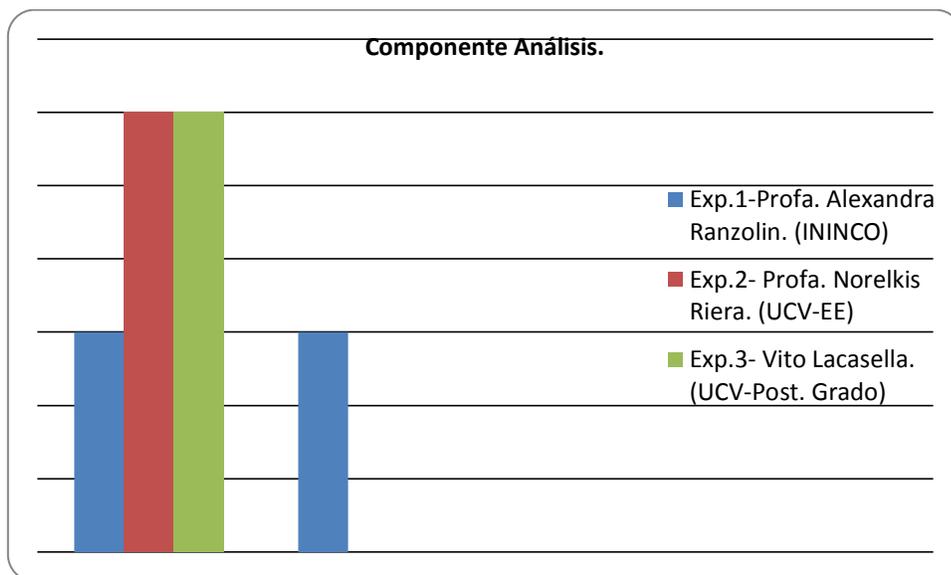
5.1 Componente Análisis:

Este aspecto estuvo compuesto de los siguientes ítems:

1. ¿Cómo es definido el problema de actualización del docente de informática, dentro del tema en seguridad en redes sociales?
2. ¿Cómo son definidas las características de la población a la que va dirigido el taller en seguridad en redes sociales?
3. ¿De qué manera se establecen los conocimientos y habilidades previas que debe poseer el docente de informática para a participar dentro del taller?

4. ¿Cómo se justifican las teorías de aprendizaje dentro del taller en seguridad en redes sociales?
5. ¿Cómo es el análisis de las estrategias dentro del taller en seguridad en redes sociales?
6. ¿De qué manera se indica la administración de las tecnologías a emplear durante el taller de seguridad en redes sociales?

Los ítems abarcaron la evaluación de este componente, las respuestas obtenidas según su escala, fueron las siguientes:



Fuente: Elaboración de la Autora.

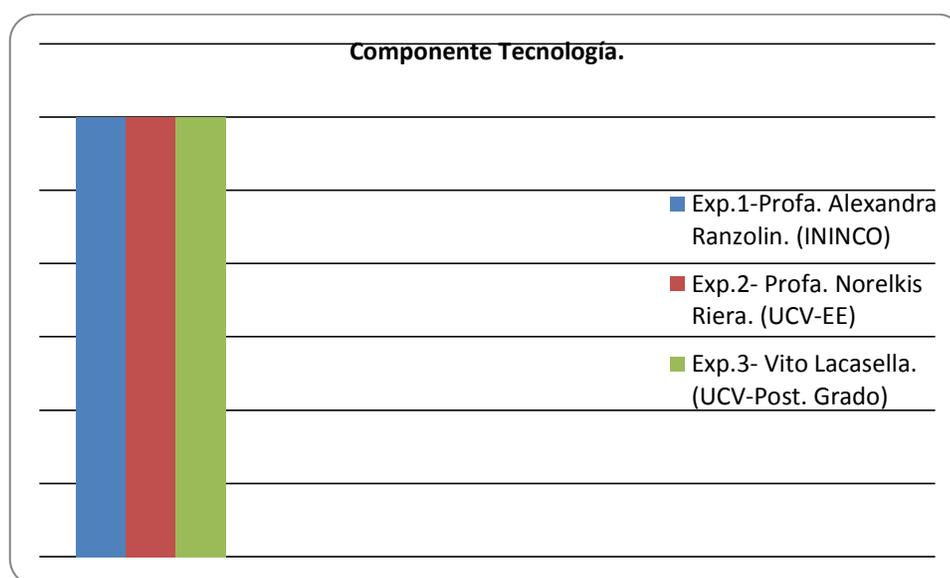
El gráfico anterior, indicó de manera general que los tres expertos concibieron en que el componente análisis, se presentó “Muy Adecuado” (M-A), sin embargo la Profa. Rozolini, considero que tres de sus ítems eran “Adecuados” ya que sus observaciones en esta dimensión fueron orientadas hacia la redacción así como errores de transcripción. Correcciones de forma que fueron tomadas en cuenta y ajustadas, para la presentación final del diseño y recursos que posteriormente el lector pudo apreciar en la propuesta.

5.2 Componente Tecnología:

Para el presente componente, según la adaptación que se le ejecutó al modelo ADITE, sólo se considero la definición del tipo de interacción, ambiente y como desde la experiencia del validador consideraba la planificación de la misma. Los ítems para este componente, fueron:

7. ¿De qué manera es definido el tipo de interacción que tendrán los participantes del taller en seguridad en redes sociales?
8. ¿Cómo se define el ambiente de aprendizaje donde los participantes del taller en seguridad en redes sociales, interactuaran?
9. ¿Cómo considera el proceso de interacción y el ambiente de aprendizaje?

De igual manera, se manejó la escala de estimación anterior. En este aspecto los resultados fueron:



Fuente: Elaboración de la Autora

Para este componente, de forma unánime los tres expertos consideraron que la planificación y definición de los ítems tomando en cuenta el recurso con los que contaron fue “Muy Adecuado” (M-A), sin ningún tipo de correcciones u observaciones. Esto nos indica que así como el

componente anterior el taller cubre con las expectativas y pautas establecidas previamente, en ambos componentes. Lo que sin duda alguna es positivo, no solo para los resultados de la investigación sino además para el diseño final presentado.

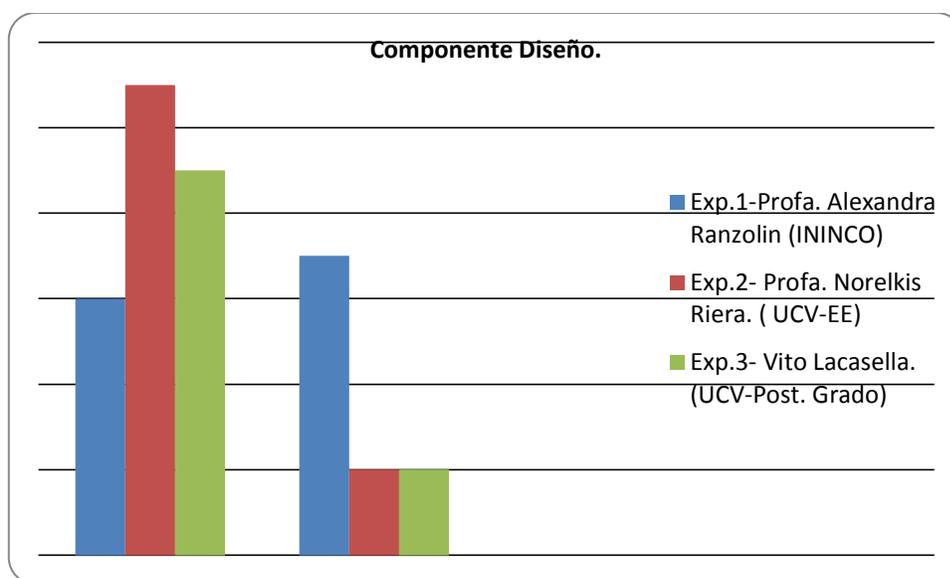
5.3 Componente Diseño:

Este componente, representa en casi su totalidad el plan de formación es decir es el capítulo anterior, fue la evaluación que conto con mas ítems y recursos, ya que en la misma se contendría el plan de formación y materiales didácticos, incluyendo el links de los videos propuestos para el taller. Es un componente clave, pues representa el fuerte de toda la propuesta, para el de igual manera se manejo la misma escala de estimación. Para esta dimensión, los ítems planteados fueron:

10. ¿Cómo están redactadas las metas del taller y de cada contenido?
11. ¿Cómo están redactados los objetivos del taller?
12. ¿De qué manera es presentada la coherencia entre las metas y los objetivos?
13. ¿Cómo se presenta la secuencia en los contenidos del taller?
14. ¿De qué manera es la continuidad en cada uno de los contenidos?
15. ¿Cómo es presentado el esquema de los temas del taller en seguridad en redes sociales?
16. ¿Cómo considera la selección de las estrategias a emplear durante el taller?
17. ¿Cómo es el diseño de la presentación colectiva multimedia?
18. ¿Cómo percibió los videos para apoyar los contenidos del taller seguridad en redes sociales?
19. ¿Existe una selección de actividades grupales para los participantes del taller “Seguridad en Redes Sociales”? ¿De qué manera?

20. ¿Fue la presentación colectiva multimedia visualmente agradable para los participantes? ¿De qué manera?
21. ¿Es empleado el video para apoyar los contenidos y generar reflexión, sobre el tema de seguridad en redes sociales? ¿De qué manera?
22. ¿Existe una selección de los videos para el taller en seguridad en redes sociales? ¿De qué manera?

A continuación presentamos los resultados de la validación dentro de este componente:



Fuente: Elaboración de la Autora

Este componente así como los anteriores recibió una valoración entre “Muy Adecuado” (M-A) y “Adecuado (A), ya que si bien en la mayoría de los ítems la estimación se orientó hacia lo máximo de la escala, las observaciones fueron enfocadas por los tres expertos en que quizás habrían muchas actividades dentro del taller y algunas podían ser opcionales, así como correcciones dentro de la presentación colectiva multimedia. La Profa. Riera, propuso además la

incorporación de infografías, para potenciar el material, elemento que a la hora de aplicar el taller el facilitador podrá tomar en cuenta.

Es indispensable aclarar, que para los ítems 19, 20, 21, 22; antes de la escala de estimación se presento la opción SI y NO. Ya que los mismos están redactados para resaltar antes si hay existencia o ausencia de las mismas y de qué manera era. Para las cuatro preguntas los tres expertos indicaron que Si había presencia y estaban definidas entre M-A y A.

Dispuesto lo anterior, se consideró que fueron pertinentes las recomendaciones que proporcionaron los expertos, ya que en cierto modo para su aplicación el facilitador podría tomarlas en consideración por tal razón, en el capítulo IV y en el modelo final del diseño, se tomó en cuenta poner opcionales cuatro de las actividades planteadas, además de realizar las correcciones a la presentación. La incorporación de la infografía se deja a criterio del facilitador, a la hora de implementar el taller.

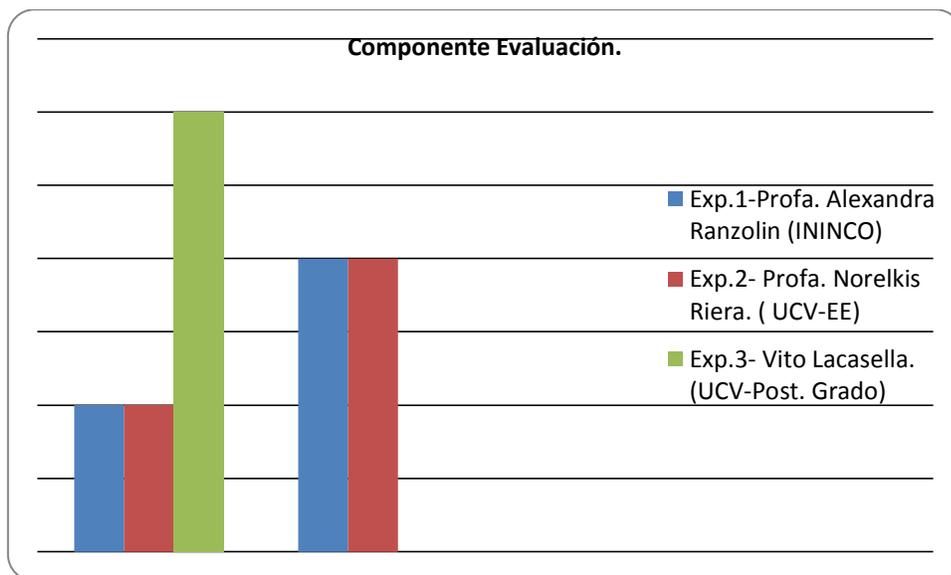
En general, más que observaciones fueron recomendaciones por parte del panel de expertos, se cree que de igual forma, recibió una buena ponderación el diseño del mismo, lo que nos indica como investigador, que la factibilidad y pertenencia del plan de formación es óptimo.

5.4 Componente Evaluación:

Este representa el componente final del modelo, en este punto así como en el de tecnología solo se evaluaría, la pertinencia del diseño del modelo de evaluación post- taller. Por tal motivo, los ítems planteados fueron:

23. ¿Cómo está diseñado el instrumento post-taller?
24. ¿Existe el orden dentro de los instrumentos de evaluación post-taller? ¿De qué manera?
25. ¿Cree que el presente instrumento abarca la evaluación de los contenidos, estrategias, medios computarizados, didácticos y el dominio del tema y grupal del facilitador? ¿De qué manera?

De igual manera que en los ítems antes mencionados, para el 24 y 25 se planteo antes la opción SI y NO, ya que los mismos están redactados para resaltar antes si hay existencia o ausencia de las mismas y de qué manera era. Para ver los resultados finales, hacemos presentación de la gráfica.



Fuente: Elaboración de la Autora.

Para los ítems 24 y 25, obtuvieron un SI, con referencia a si había presencia y con respecto a qué manera dos de los expertos manifestaron que era “Adecuada” mientras que uno coloco que todos los planteamientos fueron “Muy Adecuados”. Las recomendaciones fueron de forma dentro del instrumento, las cuales de igual manera se ejecutaron.

En general se puede afirmar que el objetivo central de la investigación fue logrado, recordando que él mismo era “Proponer un diseño de taller en “Seguridad en Redes Sociales”, dirigido a los docentes en el área de informática, pertenecientes a la etapa de educación media general”. En esta propuesta se pauto realizar el diseño y la evaluación, lo cual fue logrado y podremos afirmar que exitosamente.

En general la propuesta se ubica entre M-A y A, respondiendo al objetivo logrado, que es la carente formación docente en el tema de seguridad en redes sociales. Con la validación de experto podemos medir que el plan de formación propuesto es capaz de llenar los vacíos curriculares existentes hoy en día no solo dentro de nuestro CBN, sino además, dentro de la formación del docente de informática, en la etapa media general.

El modelo ADITE (Polo, 2003), permite que en cuatro componentes o etapas se ejecute el diseño y evaluación de un medio instruccional, para este caso emplear el video fue importante ya que el mismo de una manera didáctica apoyó y presento contenidos dentro del taller, lo que se cree que si se llegara a su aplicación permitiría generar en el público participante la reflexión esperada. La idea de crear el presente plan de formación es responder a las líneas y necesidades educativas que presenta nuestra sociedad en red, y sobre todo nuestro sistema escolar. Con la validación, quedó claro no solo la pertinencia, claridad, efectividad y factibilidad del plan de formación propuesto en los capítulos anteriores así como la decantación teórica del mismo.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

En función a la investigación realizada y a los datos obtenidos mediante la validación de experto, podemos concluir lo siguiente:

Se logró fundamentar mediante la entrevista experto, la presencia de delitos cibernéticos dentro del sistema de educativo, sobre todo a nivel de educación media general esto a razón de que no se cuenta ni con data ni con testimonios transcritos sobre el tema. El poder lograr este objetivo, no solo abrió el panorama sobre el tema y la situación sino además conocer desde la experiencia del profesor Lacasella la razón curricular del problema de formación docente así como el trabajo mancomunada que la familia como actor del proceso debe tener.

Con este panorama claro, pudimos desplegar los fundamentos teóricos con respecto al tema de formación en “Seguridad en Redes Sociales”, dentro del marco tanto en el aspecto legal como en el teórico, quedando claro que la formación dentro del tema era una necesidad inherente, en el que ni la docencia ni familias pueden escapar pues el fenómeno de la ciber violencia se está propagando a nivel mundial, y las victimas cada vez crecen tanto en la población de adolescentes como dentro de la adulta.

La decantación teórica, nos permitió afirmar lo que Cabrero (2001) expone con respecto al rol del docente dentro de las web 2.0, y no es más que asumir la responsabilidad y el compromiso de generar nuevos conocimientos y guiar a la construcción de los mismos empleando las TIC. El docente juega un papel importante dentro del proceso educativo, ya que tiene el adeudo de generar nuevos espacios de aprendizaje y formarse en los contenidos que cada era y generación

demanda. Las redes sociales, han calado dentro de la educación y dentro de los procesos comunicativos de manera hasta cultural y de forma globalizada.

Por lo que el tema de la formación en la seguridad dentro de ellas no es un mero capricho, es una necesidad, se posee tasas factuales sobre la población que se ve afectada a raíz del uso inadecuado no solo que le dan a sus cuentas sino ídem a sus perfiles e usuario. Lo que es preocupante, es que este tipo de contenidos no están dentro del CBN, ya que impacta directamente en la formación conceptual y práctica del docente de informática.

Las redes sociales permiten crear o formar vínculos tal como lo exponen Herrero, Moreno y Martin, 2003. Sin embargo, en cómo empleamos dichos espacios es nuestra responsabilidad como ciudadanos críticos. Para ello se ejecuto una decantación en las bases conceptuales sobre el tema de seguridad en redes sociales.

No solo se logró este objetivo, sino además permitió reflexionar sobre la relevancia que posee la incorporación del mismo, ya que si contamos con leyes que protejan sobre este tipo de delitos, así como tasas de tal hecho, su formación conceptual es esencial para lograr una práctica efectiva por parte del docente de informática.

A fin de diseñar un plan de formación que tomará las vertientes conceptuales del tema de seguridad en redes sociales y las hiciera sencilla de aprehender por parte de los participantes para ello se empleó el modelo ADITE. Quién nos sirvió de referente para el diseño del taller, en el se ejecutaron adaptaciones para cubrir con las características que la propuesta planteaba.

Sirvió para enfocar la propuesta en cuatro componentes básicos (análisis, tecnología, diseño y evaluación) que dieron vida al plan de formación y respondieron a cada una de las interrogantes sobre los elementos que debe poseer un DI. Lo enriquecedor en este objetivo, era presentar una propuesta donde se empleará un medio propio de las TIC y las redes sociales, como los fue el video, quien valió como una estrategia para generar reflexión y contenido.

El plan de formación, era la propuesta y vida de la presente investigación, por lo que este aspecto podemos concluir que fue factible diseñar un DI dirigido a los docentes, como un plan de formación, esbozando materiales y escogiendo videos, que no solo capten y generan nuevos conocimientos, sino además, sean capaz de buscar emanar reflexión sobre la incorporación del tema dentro del aula, así como brindar las herramientas para afrontar situaciones propias de la ciber violencia.

Parte del compromiso de la docencia es la constante actualización en temáticas propias de educación y de la vida actual. El proponer un taller en seguridad en redes sociales sería un primer paso para lograrla, ya que diseñar un plan de formación es tomar en cuenta desde el temario hasta los recursos y el tiempo para brindar un contenido, la idea con ello es organizar de forma sistemática; el proceso sin dejar de hacerlo flexible y dinámico, ya que la idea es afianzar de forma significativa el proceso siendo el participante el que lo engrane con sus conocimientos previos (Ausubel, 1983).

Toda necesidad debe estar acompañada de una propuesta que apueste a superarla y generar cambios constructivistas. Es así como la presente propuesta no solo apuesta a contribuir un nuevo plan de formación, sino además, apuesta a la actualización docente en temas a la vanguardia de las demandas que hoy los discentes 2.0 demanda dentro de su proceso formal en aula. Es importante destacar que la formación dentro de la seguridad en redes sociales, no solo potencia los procesos del aula, sino también los procesos cotidianos e informales, un docente y discente formado en entornos reales y virtuales, son el reflejo de una sociedad que apuesta a la educación ciudadana de su población.

Finalmente con el último objetivo específico la idea era evaluar precisamente la factibilidad, pertinencia, coherencia y diseño del taller en seguridad en redes sociales. Para ello, se buscó un panel de expertos tanto en contenido como en el área de educación, quienes debían evaluar desde los cuatro componentes la calidad del plan de formación, así como la planificación de sus actividades y los recursos didácticos diseñados.

Para ello se diseñó un cuestionario que podrá ser apreciado en los anexos, el mismo estuvo compuesto de veinticinco (25) ítems que abarcaban los cuatro componentes del taller, como vimos en el capítulo anterior en las gráficas; la propuesta se ubicó dentro de las dos escalas de estimación altas, yendo de los “muy adecuado” a lo “adecuado”, con correcciones de forma que fueron atendidas y superadas.

Con ello desde el aspecto metodológico queda evaluado su diseño, sirviendo como referencia a futuras investigaciones que planeen su aplicación, ya que tienen la validación del diseño. En líneas general cada objetivo conjuntamente con su dimensión fue logrado, pues pasando de lo conceptual a lo procedimental y metodológico, logramos el despliegue de cada uno, cumpliendo con lo pautado.

La idea con la presente investigación es promover las primeras bases, para la posterior aplicación del taller en seguridad en redes sociales dirigido a los docentes de informática de educación media general. Ya que la detección de tal necesidad fue no solo precisada sino además entendida desde el aspecto formativo, por lo que al encontrar que no existen talleres del tema dirigido a la docencia se genera la motivación de tal propuesta enfocada en los profesores de informática quienes sirven de facilitadores dentro del área de las TIC.

La formación docente es un compromiso tanto individual como estatal, ya que si bien como profesionales se debe estar a la vanguardia de las nuevas demandas, el Estado como ente político, debe también garantizar espacios de actualización así como las adaptaciones curriculares según lo demande cada generación. El presente DI, es una propuesta que busca aportar desde lo metodológico, el diseño de un taller en la temática y dirigido a la población en específico que se considera más necesita en primera instancia formarse en la nueva tendencia de contenidos como lo es la seguridad en redes sociales.

Como investigadora, se tienen el compromiso de proponer nuevas ideas y desarrollarlas, ideas que fortalezcan y apoyen las demandas instruccionales del momento, por tal motivo, se creyó pertinente el despliegue de la presente investigación tanto para apoyar las nuevas líneas de la

Universidad Central de Venezuela, las de la Escuela de Educación y a la Sociedad Venezolana. Es nuestro compromiso, como profesionales y obligación como ciudadanos, apostar a la formación ya que de cierta manera es la contribución que le damos a nuestra sociedad como seres activos dentro y fuera, de ella.

RECOMENDACIONES

Es necesario indicar una serie de recomendaciones tanto a nivel de la investigación, como docente y a la universidad; con ellas se espera que las investigaciones subsiguientes las tomen en cuenta a la hora de utilizar el referente del presente trabajo de grado. Estas recomendaciones ayudaran a potenciar la práctica docente y minimizar algunas de las interrogantes o debilidades que pudiesen encontrarse dentro de la investigación, por lo que destacamos:

- Al principio de la investigación, se hizo referencia de por el tema de la logística que implicaba la ejecución del taller, se recomienda que con los elementos expuestos y la validación se logre la aplicación del mismo para llevar a la realidad el plan de formación e iniciar el proceso de actualización docente.

- Se recomienda, que se haga en posteriores investigaciones el estudio sobre el rol de la familia como actores dentro del proceso de formación en el tema de seguridad en redes sociales, ya que la presente solo las menciona pero no hace gran énfasis por la delimitación y objetivos planteados. No obstante, recomendamos que se indague con mayor profundidad su rol e importancia, sobretodo en estas temáticas que como se hizo referencia el Prof. Lacasella, es un trabajo mancomunado familia-escuela-discente.

- A la hora de aplicar el taller, el facilitador puede tomar en cuenta, lo expuesto en las actividades que se marcaron como opcionales así como la inclusión de infografías como medio didáctico, ya que fueron dos de las recomendaciones aportadas por el panel de expertos.

- Dado que no existen gran data sobre estos delitos en Venezuela, se recomienda que se realice una investigación, que se aboque a levantarla, sobretodo en estos nuevos contextos.

A los docentes:

- Es necesario que busquen capacitarse en temáticas actuales con respecto al área de las TIC, y sobre todo dentro de la seguridad en redes sociales. Pues cuenta con una población que hace uso frecuente de las mismas y para lograr la educación deseada se debe partir con lo el interés real de los discentes así como en aquellos espacios donde ellos más frecuentan, tanto en la vida real como en la virtual.
- Las redes sociales, hoy en día son una herramienta y un media para desarrollar estrategias formativas, adaptándose a cualquier tipo de temática o área del conocimiento. Por lo que su uso adecuado es una obligación así como la incorporación de estas a nivel tanto universitario como pre-universitario.
- Es necesario promover la formación dentro de temas como el grooming, sexting, phishing, cyberbullying o plagio de identidad, para promover su consciencia en ellos y sobre el uso que de damos a las cuentas dentro de la vida virtual.
- Deben hacer del aprendizaje uno significativo, por lo que conocer los conceptos y estrategias apropiadamente, potencializará su práctica.
- Deben incorporar estos temas dentro de su plan de contenidos anual.
- Debe ser un trabajo a la par con las familias, para ayudar a la formación un ser critico dentro en todas sus dimensiones, ya que la ciber violencia, es un problema también de valores, por lo que el trabajo es de docente, discente y familia, para lograr su erradicación.

A la escuela de Educación de la Universidad Central de Venezuela:

- Promocionar y fomentar, la formación en esta temática a nivel universitario, ya que también existe ciber violencia en esta etapa de formación.
- Incorporar dentro de las líneas curriculares, en las asignaturas propias de este eje de formación, la incorporación de la temática en seguridad en redes sociales.
- Es pertinente que preparen a las generaciones próximas a graduar, para este tipo de situaciones que van a encontrar dentro de su práctica y deben saber cómo canalizarlo, ignorarlo solo agudiza el fenómeno de la ciber violencia.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, J (2003). Aproximación metodológica para el diseño de cursos basados en tecnología de la información y la comunicación en educación (TIC)-(Diagnostico, Propuesta y Factibilidad). Caso: Una experiencia piloto en la Universidad Simón Bolívar con docentes de la Región Capital. Trabajo de asenso para optar al nivel de profesor asistente en el escalafón de asenso de la UCAB. Universidad Andrés Bello. Caracas.

Acevedo, H (2012). Uso del video para el desarrollo del pensamiento crítico. Trabajo de grado para optar por: Magister Scientiarum en Educación. Universidad Central de Venezuela. Caracas.

Ausubel, D (1983). Teoría del Aprendizaje Significativo. [Artículo en línea] Recuperado de: http://www.iprojazz.cl/intranet_profesor/subir_archivo/archivos_subidos/Aprendizaje_significativo.pdf.

Bustamante Sánchez, R (2000). Seguridad en Redes. [Monografía en línea] Recuperado de: <http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf>

Cabrero (2001). Aplicación de las Tic: ¿Esnobismo o Necesidad Educativa? [Artículo en línea] Recuperado de: <http://medios.educativos.umce.cl/externals/documentos/aplicacion-de-TICs-snobismo-o-necesidad.pdf>

Careaga, Sica, Cirillo y Da Luz, (2006). Aportes para diseñar e impetrar talleres. 2da Jornada de Experiencias Educativas en DPMC. [Documentos en línea] Recuperado de: http://www.smu.org.uy/dpmc/pracmed/ix_dpmc/fundamentaciontalleres.pdf

Castell, M (2002). La dimensión cultural del Internet. [Artículo en línea] Recuperado de: <http://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.html>

Castaño, Maíz, Palacios y Villaroel (2007). Características más relevante de la web 2.0. [Artículo en línea] Recuperado de: <http://servicio.bc.uc.edu.ve/educacion/eduweb/vol2n2/art2.pdf>

Castaño Garrido, J (2007). Educar con redes sociales y web 2.0. [Artículo en línea] Recuperado de: <http://servicio.bc.uc.edu.ve/educacion/eduweb/vol2n2/art2.pdf>

Calero, M (2010). Influencia del internet en los estudiantes de primer semestre de carrera de administración del ISTP Argentina. [Maestría en línea] Recuperado de: http://pirhua.udep.edu.pe/bitstream/handle/123456789/1412/MAE_EDUC_073.pdf?sequence=1

Correa, A (2006). Modelo de Control de Gestión Basado en el Cuadro de Mando Integral para la Empresa Representaciones Caribbean COOL C.A. Capítulo III. [Tesis en línea] Recuperado de: <http://www.oocities.org/es/alejandrorcorrea/sem/Capitulo3.htm>

Constitución de la República Bolivariana de Venezuela (1999). Asamblea Nacional Constituyente. Caracas

Currículo Básico Nacional (1984). Ministerio de Educación. Caracas.

ComScore (2011). El Crecimiento de las Redes Sociales en América Latina. [Presentación en línea] Recuperado de: <http://es.slideshare.net/brendatre/el-crecimiento-de-redes-sociales-en-amrica-latina-septiembre-2011>

García Córdoba, Fernando. (2009). La investigación tecnológica. Investigar, idear e innovar en Ingenierías y Ciencias Sociales. México: Editorial Limusa.

Decreto Presidencia N° 825 (2000). [Documento en línea] Recuperado de: http://www.cnti.gob.ve/images/stories/documentos_pdf/decreto825.pdf

De Haro, J (2009). Las redes sociales aplicadas a la práctica docente. Revista de Investigación Didáctica y Multimedia. [Artículo en línea] Recuperado de: <http://www.raco.cat/index.php/DIM/article/view/138928/189972>

Fidias, A (1999). Proyecto de Investigación: Guía para su elaboración. Editorial Espíteme. Ed. 3era. Caracas.

Flores Cueto, J (2009). Redes Sociales. [Documento en línea] Recuperado de: http://mc142.uib.es:8080/rid=1HY8TVCBB-15599LW-1S6Z/redes_sociales.pdf

Educación (2013). Caperucita 2.0: ¿deberías agregar a extraños a tus redes sociales?. [Video en línea] Recuperado de: <https://www.youtube.com/watch?v=Vx7GIKPSE8U>

Hernández, Fernández y Baptista, (1991). Metodología de la Investigación. Editorial Mc Graw-Hill Interamericana S.A. México

Hurtado Barrera, J (2012). El proyecto de Investigación: Comprensión holística de la metodología y la investigación. Ediciones: Quirón, 7ma. Ed. Caracas

Johnson, Johnson. Holubec (1999) El aprendizaje cooperativo en el aula. Editorial Paidós. Buenos Aires.

Latre, F (2010). Las nuevas redes sociales, ¿moda o revolución? Revista Cultura y de cuestiones actuales de la Universidad de Navarra. N°.683 [Revista en línea] Recuperado de: <http://www.unav.es/nuestrotiempo/temas/las-nuevas-redes-sociales-moda-o-revolucion>

Lacasella, V. (2015). Entrevista realizada por la investigadora, sobre la incidencia en el país de los delitos cibernéticos. La transcripción de dicha entrevista se puede ver en el Anexo No. 1.

Ley Orgánica de Educación (2009). Ministerio del Poder Popular para la Educación. Caracas.

Ley Orgánica para la protección del Niño y el Adolescente, (LOPNA) (2007). Asamblea Nacional de la República Bolivariana de Venezuela. Caracas.

Ley sobre uso del Software Libre desarrollado con Estándares Abiertos por toda la Administración Pública Nacional, (2004). Asamblea Nacional de la República Bolivariana de Venezuela, Decreto N° 3.390. Caracas.

Ley Orgánica de Telecomunicaciones (2000). Asamblea Nacional Constituyente. Publicado en la Gaceta Oficial No. 36.920. Caracas

Ley Especial de Delitos Informáticos (2001). Asamblea Nacional Constituyente. Publicado en la Gaceta Oficial No. 37.313. Caracas

Manzano, J (2012). Cifras del internet en Venezuela. [Periódico en línea] Recuperado de: <http://www.elmundo.com.ve/noticias/tecnologia/internet/cifras-del-internet-en-venezuela.aspx>

Martín, Lucena y Díaz (2002). Las actitudes docentes hacia la formación en tecnologías de la información y comunicación (TIC) aplicadas a la educación. [Documento en línea] Recuperado de: <file:///C:/Users/Administrador/Downloads/Dialnet-LasActitudesDeLosDocentesHaciaLaFormacionEnTecnolo-498346.pdf>

Marketing Directo (2011). Breve Historia de las Redes Sociales. [Blog en línea] Recuperado de: <http://www.marketingdirecto.com/actualidad/social-media-marketing/breve-historia-de-las-redes-sociales/>

Merlo Vega, J (2008). Las diez claves de la web social. [Artículo en línea] Recuperado de: [file:///C:/Users/Administrador/Downloads/Dialnet-LasDiezClavesDeLaWebSocial-3012969%20\(1\).pdf](file:///C:/Users/Administrador/Downloads/Dialnet-LasDiezClavesDeLaWebSocial-3012969%20(1).pdf)

Nieves, R (2011). Actitudes de los Profesores Universitarios hacia el uso de los Ambientes Virtuales de enseñanza y aprendizaje. Trabajo de grado para optar por el grado: Magister Scientiarum en Educación. Universidad Central de Venezuela. Caracas.

Núñez, R (2012). Modulo I: Introducción a la seguridad informática [Blog en línea] Recuperado de: <http://rafajavier.blogspot.com/2012/03/electiva-i-seguridad-informatica.html>

Pantalla Amigas (2013). Recomendaciones para el Uso Seguro de Internet y las Redes Sociales, para el uso seguro. [Video en línea] Recuperado de: <https://www.youtube.com/watch?v=t-x73w1N1os>

Perdomo, D (2011). Redes Sociales en Internet. [Tesis en línea] Recuperado de: <http://es.slideshare.net/cubedirubik/tesis-redes-sociales-en-internet>

Peña, Córcoles y Casado (2006). El profesor 2.0: Docencia e Investigación desde la red. [Artículo en línea] Recuperado de: http://www.uoc.edu/uocpapers/3/dt/esp/pena_corcoles_casado.pdf

Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, Nº IV. SADPRO – UCV. Caracas

Puelles y Risco (2009). Tecnologías de Información y Comunicación (TICs) en Programa Social de Alfabetización dirigido a mujeres de de la zona rural de Vice. [Documento en línea] Recuperado de: <http://www.eumed.net/libros-gratis/2013/1241/las-TICs-los-nuevos-escenarios-de-aprendizaje.html>

Programa de Estudios y Manual del Docente (tercera etapa) Asignatura Matemática–Física (1984). Ministerio de Educación. Caracas.

Rey, J (2009). Web 2.0 un Nuevo Entorno de Aprendizaje en la Red. [Artículo en línea] Recuperado de: <http://dim.pangea.org/revistaDIM13/Articulos/pacoruz.pdf>

Rivera Sandoval (2011). Formación docente para el uso de las TIC. [Artículo en línea] Recuperado de: <http://gte2.uib.es/edutec/sites/default/files/congresos/edutec11/Ponencias/Mesa%201-anx/Formaci%C3%B3n%20del%20docente%20para%20el%20uso%20de%20las%20TIC.pdf>

Rincón del Network (2013). Tipos de Redes Sociales. [Video en línea] Recuperado de: <https://www.youtube.com/watch?v=gRKctZjfRLk>

Rodríguez Trujillo, N (2014). Material de Apoyo sobre entrevista. Seminario: Investigación Etnográfica en Educación.

Sánchez Ilabaca, J. (2012). Usos Educativos del Internet. [Documento en línea] Recuperado de: <http://users.dcc.uchile.cl/~jsanchez/Pages/papers/usoseducativosdeinternet.pdf>

Sequera y Agüero. (2011). Actitud de los Estudiantes de Inglés Instrumental la aplicación del taller grupal como estrategia de comprensión lectora. [Tesis en línea] Recuperado de: <http://es.scribd.com/doc/58499932/DIANA-Y-JULIA-Sus-Contextualizaciones>

Symantec (2014). Tendencias de Seguridad Informática en América Latina y el Caribe. [Documento en línea] Recuperado de: http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Siemens, G (2008). Conectivismo: Una teoría de Aprendizaje para la Era Digital. [Articula en línea]. Recuperado de: <https://humanismoyconectividad.wordpress.com/2009/01/14/conectivismo-siemens/>.

Torres, A (2006). Web Educativa 2.0. Revista Electrónica de Tecnología Educativa. [Revista en línea] Recuperado de: <http://edutec.rediris.es/Revelec2/revelec20/anibal20.htm>

Torres y Alcántar (2011). Usos de las Redes Sociales como estrategia de aprendizaje. ¿Transformación educativa? . [Artículo en línea] Recuperado de: <http://www.udgvirtual.udg.mx/apertura/index.php/apertura3/article/view/198/213>

TREND MICRO (2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. [Informe en línea] Recuperado de: http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf

Universia (2013). Los adolescentes no controlan su privacidad en las redes sociales [Portal en Línea] Recuperado de: <http://noticias.universia.edu.ve/en-portada/noticia/2013/06/10/1029493/adolescentes-no-controlan-privacidad-redes-sociales.pdf>

UNESCO (2008). Estándares UNESCO de Competencia en TIC para Docentes. [Documento en línea] Recuperado de: <http://www.oei.es/tic/UNESCOEstandaresDocentes.pdf>

Universidad Pedagógica Experimental Libertador (UPEL) (2003). Manual de Trabajos de Grados de maestría y tesis doctorales. Caracas

Valentini López, P (2002). La Sociedad de la Información en América Latina y el Caribe: TICs y un nuevo Marco Institucional. [Revista en línea] Recuperado de: <http://www.oei.es/revistactsi/numero2/valenti.htm>

Vita Montiel, N (2008). Tecnología de Información y Comunicación para las organizaciones del siglo XXI. Editorial CIGAC. Vol. 5, edc.1. Venezuela.

Villasana P. N (2006). Habilidades sociales en entornos virtuales de trabajos colaborativos. Trabajo de grado para la mención de: Magister en Scientiarum en Educación. Universidad Central de Venezuela. Caracas.

Yotube (2013). Lo Malo de las Redes Sociales Si no se controla webm small. [Video en línea] Recuperado de: <https://www.youtube.com/watch?v=hoqzkHQ9jxw>

Zianni y Nessier (2014). Formación Docente en seguridad TIC. Revista Iberoamericana de Educación [Artículo en línea] recuperado: <http://www.rieoei.org/rie65a07.pdf>

ANEXOS

Entrevista Profe. Vitto Lacasella (2015). Universidad Simón Bolívar. Día: 29-01-2015.

Entrevista al Profe. Vitto Lacasella.

Breve Reseña de su Curriculum Vite:

- Lic. en Comunicación Social mención Audiovisual (Universidad Central de Venezuela)
- Doctorado en Comunicación Social mención Audiovisual (Universidad Central de Venezuela).
- Encargado de la sección de Arte-Visión (Universidad Simón Bolívar).
- Gerente de Producción encargado de LA SIMONTV canal de tv de la Universidad Simón Bolívar
- Miembro de la ONG “Educación para los Medios”.

Lugar: Servicio de Artevisión. Universidad Simón Bolívar.

Fecha: 29-1-2015.

Entrevistadora: Bra. Paula C Ávila P. (Tesisista de la Escuela de Educación de la UCV)

El fin que se busca mediante la presente entrevista, es conocer si en Venezuela se ha presentado la detección del ciberdelito dentro de la educación media general. Esto fue explicado inicialmente por la Profa. Grecia Almeida, quien expone que las investigaciones previas realizadas por la Tesisista Paula C Ávila, con respecto al tema de “Seguridad en Redes Sociales” se detectó que en Venezuela actualmente se carece de data e información sustentable, sobre el fenómeno de Cyberbullying, Grooming, Sexphising, Phishing y Fhising. Por esta razón, se vio la necesidad de entrevistar a un especialista en este campo, quien no solo además maneja data en

sus investigaciones, sino también posee la experiencia por dictar talleres y charlas tanto en liceos públicos como privados sobre la temática. De esta manera se da inicio a la entrevista:

Entrevistadora:

¿Considera que actualmente en Venezuela existen mecanismos formativos para asumir y manejar el tema de seguridad en redes sociales, con respecto a la parte educativa?

Prof. Vitto Lacasella:

“Mira mi respuesta es No, sabes ¿Por qué no?, porque en la actualidad en el Curriculum Venezolano, especialmente en el área de informática, no se da eso. Dicho por los mismos profesores que conozco de informática.

Ahí se da es un saber instrumental, es decir, como manejar una PC, Word, abrir Windows, claves, etc. Pero manejar ese de tema de seguridad, son los profesores que sienten la necesidad de dar esa información y se la dan a los muchachos. He conseguido profesores, por ejemplo en estos días estuve en el Colegio “Santo Tomas de Villanueva” en ese colegio cuando di la charla a los muchachos la profesora me dijo: Profesor yo también trato de darle esto a los muchachos de forma transversal veo como hago, porque sabe que esto no está en el curriculum. Es decir no se da porque no aparece”

Entrevistadora:

Entonces podríamos decir: ¿Qué actualmente es una problemática educativa, el hecho que no se de este dando el tema de “Seguridad en Redes Sociales”?

Prof. Vitto Lacasella:

“Es una condición de Estado, ¿ósea es curriculum, no? Debe venir diga desde arriba mira vamos a incluir esto dentro de la educación. Claro que sí! Evidentemente si es, es un problema que viene de más arriba y los profesores que están abajo, tratan de solventarlo, sienten que está el vacío y tratan de solventarlo”

Entrevistadora:

Teniendo esto presente ¿Cómo percibe la formación docente con respecto a este tema? .Me dijo que habían docentes que tenían la inquietud, pero ¿Realmente poseen la formación en este tema?

Prof. Vitto Lacasella:

“No, no tienen la formación, de hecho fíjate que una de nuestras estrategias en EPM Venezuela (Educación para los Medios en Venezuela), la estrategia que maneja para la enseñanza de la alfabetización mediática digital, proponemos que no solo debemos formar a los chicos. Hay que formar a los docentes y que hay que formar a las familias; hay que hacer un trabajo en conjunto.

Porque el problema de seguridad en el internet es un problema de los tres. Casi siempre cuando hay un problema de seguridad, violencia en las redes sociales o hay un ataque de ciberbullying u acoso alguien. Porque fíjate que una cosa es acoso y otro ciberbullying ok?. Cuando hay ciberbullying “Viene la mamá y va al colegio y dice: ¡Ese es problema de escuela! entonces viene la escuela y dice: ¡No, no eso viene de casa!” .Y resulta que es un problema de todos. Entonces notamos que cuando damos nuestras charlas o los talleres son precisamente los profesores los que aceptan gustosamente que nosotros vayamos y las demos, porque no saben qué hacer.

Si es un problema de internet, es un problema de seguridad o violencia; los docentes no saben cómo intervenir va un poco más arriba con los directores y los directores no saben qué hacer. Lo que dicen es ¡Eso es cosa de muchachos! Levanto la alfombra lo engavetamos y espero que eso se vaya a eliminar. Y resulta que no es así y los profesores se sienten atados, porque no tienen la formación. Lo quieren aprender empíricamente pero no saben qué hacer pues”.

Entrevistadora:

¿Cuál es la etapa que usted considera dentro de la educación formal que más se ve afectada, con respecto a la violencia o inseguridad por estas redes?

Profe. Vitto Lacasella:

“Gua! Déjame decirte que por experiencia”. Hace una aclaratoria: “Esto que te estoy contando son experiencias que he tenido con el intercambio de colegios aquí en Caracas, básicamente, porque es la fuente donde yo trabajo. Cuando nosotros comenzamos nos pedían inicialmente hacer actividades con chamos de tercer año o segundo año; eso es lo que nos pedían a nosotros. Ahora estamos consiguiendo que maestras de cuarto grado nos están pidiendo si podemos hacer actividades con los niños con el internet, porque resulta que a los niños les están dando teléfonos inteligentes que tiene capacidad de sacar fotos, videos que si no tiene acceso a internet ellos saben cómo conectarse en un Wifi, conectarse y subir la cuestión y están consiguiendo problemas de violencia ya a esa edad, o sea que yo te puedo decir con propiedad que desde cuarto grado me están pidiendo actividades con los muchachos, quiere decir, que ya se han detectado estos problemas hasta quinto año de bachillerato”.

Entrevistadora:

Pero pudiéramos decir que donde más se denota este problema, ¿Es en la etapa de educación media general? (aclaratoria de 1er. A 3er. Año)

Profe. Vitto Lacasella:

“Bueno dependiendo de la gravedad. Lo que pasa es que los muchachos no saben cuando están cometiendo un delito informático, los chamos no saben que si yo saco la fotografía de una persona de su Facebook sin pedir permiso y la utilizo para hacer cualquier cosa, eso es un delito informático. Y si yo agarro esa foto y le monto Photoshop y le monto unos cachitos y lo subo después en la red para que mis compañeros se burlen

de él, eso es violencia y hasta tipificado en la Ley Contra Delitos cibernéticos lo puedes buscar son dos capítulos con seis artículos, donde se tipifica bien estas cosas. Y ellos creen que están jugando y resulta que no se imaginan el daño que están haciendo y cualquier cosa que tu hagas en internet o en el mundo virtual trae consecuencias personales, sociales, psicológicas, económicas y legales”.

Y los muchachos no saben eso y lo hacen. Claro! Una simple foto parece algo simple, pero cuando va al nivel más grande puede ser que te empiecen amenazar. Yo me conseguí este martes que paso cuando termine una actividad con un colegio en Caracas, una niña se me acercó y me dijo: “Profesor yo necesito que usted me ayude en algo”, dime cuéntame que paso?: mira este teléfono! ,por whatsapp la estaban amenazando, diciéndole tu eres un caca, no sirves para nada, que haces en este colegio sino te vas te caemos a golpes. Y era una niña de sexto grado y era una amenaza mayor”

Entrevistadora:

Eso sería ¿ciberbullying?

Profe. Vitto Lacasella:

“Eso es ciberbullying, totalmente! Entonces fue reincidente. Porque ciberbullying es cuando tu amenazas una vez y envías otra vez y otra vez y es constantes. Y la niña no sabía qué hacer y yo la aconseje. Mira ¿Tú has hablado con tus papas sobre esto? Y saben lo que me dijo: “No profe, porque si les digo a mis papas me quitan el teléfono” ok. Entonces le explique la gravedad del asunto, y bueno la niña me prometió que hablaría con sus papas, porque era fácil de ubicar había un número, pero la están amenazando. Entonces podemos ir desde un simple juego con una fotografía desde sexto grado donde la están amenazando como una amenaza mayor en bachillerato.

Aunque también los muchachos de quinto año con eso de la fotografía que es el mayor problema que tenemos ahorita también lo hacen, entonces no hay una cosa como clara de

que los mas chiquitos hacen una cosa leve y los más grandes hagan otra puede ser también en viceversa; aquí o a ya te consigues casos”

Entrevistadora:

¿Cuáles son los delitos que más ha conseguido según su experiencia?

Profe. Vitto Lacasella:

“Lo que pasa es que la Ley contra los delitos informáticos, tipifica que cualquier cosa que yo tome sin pedir permiso en las redes sociales y no lo notifique es un delito informático. Una simple copia y pega, es un delito informático ok? Y a los chamos les encanta hacer una copia y pega. Entonces yo les explico mira no se puede hacer esto, ese es el que más veo y el de la fotografía es el más usual y esta todo un fenómeno que se llama sexting que es la difusión de imágenes sub-pornográficas/ eróticas a través de teléfonos celulares. Este fenómenos se está dando mucho gracias primero a que los teléfonos tienen unas cámaras hasta mayores que una cámara digital normal y estos mismos chamos hacen competencias. Te voy a dar un ejemplo de una competencia.

Niñas de segundo año que con sus teléfonos se sacan fotos de los senos y se las mandan por los teléfonos para hacer una competencia para que adivinen de quien son esos senos y el que adivine tiene un premio, no llegue adivinar cuál era el premio. Pero hacen competencias de este tipo, entonces los chamos reciben esas imágenes y lo que hacen es tan culpable como el que genera el contenido, como el que lo reenvía, ok? .Porque también cuando tú distribuyes esa imagen también eres culpable de ese delito y todas esas cosas los muchachos no lo saben y esos son los más usados con las cámaras fotográficas. A veces se toman fotos con sus noviecitos con poses subjetivas y de repente esas fotos pueden llegar a donde no te imaginas. Te voy a dar otro caso, un papa me contó que estaba en un almuerzo de negocios en las mercedes con tres clientes, mientras estaban hablando, tocaron el tema de la difusión de imágenes, la cámara fotográfica, los niños y el internet. Viene el cliente y le cuenta a este papá que le había llegado una página donde

habían unas fotos de unas niñas que estaban con unas poses que tu decías ¡Wuao, como es esto! Viene el señor y le mostro el teléfono con la imagen y esta su hija en esa foto.

Que es lo que pasa la foto no era nada del otro mundo, era una chama en traje de baño con una posición nada subjetiva me cuenta el papá. Pero al principio me dijo iba a salir corriendo a matar a mi hija, pero después vi la foto y vi y no era para tanto. El problema es que esa foto se la mando a su novio, su novio la monto en Facebook y tú sabes que cuando algo llega a red tu pierdes el control se vuelve público y esa chama perdió el control y llego donde no tenía que llegar unos cuantos pasos; tu sabes la teoría de los doce grados de separación, eso llega rapidísimos. Entonces, la fotografía en este momento en los chamos hasta donde yo he detectado por las experiencias es en donde más inconvenientes hay”.

Entrevistadora:

¿Cuando suceden este tipo de situaciones ¿A cuales entes ellos podrían recurrir o que se debe hacer?

Profe. Vitto Lacasella:

“Mira la solución o el aporte que se puede hacer es dependiendo del punto. Como ya te dije es la familia, escuela y el chamo; cada uno de ellos puede hacer una cosa dependiendo si es familia hay una estrategia que puede hacer la familia, si es escuela una que pueden hacer los docentes y directores y otra que pueden hacer los chamos. El procesamiento a seguir si a ti te acosan por internet, es primero que nada No responderle a la persona que te está atacando, no deberías responderle porque esa persona quiere feedback y entre tu mas le respondas mas te vuelve a tocar es más si tu respondes y el ataca puede ser que consigas a otras personas que también se unas al ataque.

Segundo guarda las pruebas y denúncialo, eso es otra cosa los chamos no saben la diferencia entre denunciar y sapiar, no conocen la diferencia, entonces hay que hacer la denuncia no hay otro procedimiento, díselo a tus padres y si sabes que es alguien del

colegio debes ir a donde la directora y esta debería citar a la otra persona, vamos a suponer que fue en el colegio, entonces cita a la otra mamá y si una no quiere pues lamentablemente se pondrá a denuncia va al sistema de protección, distrito LOPNA, cosa que debemos evitar. Por eso trabajamos la prevención, por medio de este proceso de alfabetización mediática que hacemos en las escuelas con el internet, es para prevenir, para que los chicos no caigan en esto. Ya que una vez que un chico cae en esto es grave los problemas psicológicos que se generan del ciberbullying son graves inclusive mucho más fuertes que los que se consiguen del bullying.

Porque haber el ciberbullying es anónimo, es constante 24h al día, tu y yo estamos aquí hablando y no sabes que alguien te está acosando en la red y este diciendo de ti las mil y un cosas y no lo sabes; después la no percepción directa de la persona porque no te está viendo y yo vengo y te acoso y no sabes del otro lado como se está recibiendo eso y yo sigo y capaz que yo esté en la peor depresión que estoy a punto de tirarme por un balcón y no lo sé y el que te está acosando sigue acosando. Y en el bullying no pasa eso porque yo vengo golpeo alguien capaz que una vez este en el suelo yo puedo decir no no lo ataco más y lo dejo, ósea hay un límite, porque estoy viendo lo que pasa y en el internet no, entonces las consecuencias son muy graves y hay que actuar rápidamente y enseñar a los chicos como hacerlo y la única manera que hay es esa, a través de la alfabetización y aprender sus derechos y deberes que hay en el internet.

Claro la ley de delitos informáticos es una manera que tienes para defenderte porque ahí protege tus derechos en el uso del internet y si quieres instancias grande la ONU en el 2012, declaró el internet un derecho humano y después la UNICEF sacó un decálogo para los niños en el uso del internet y para los docentes sacó otro, fíjate que interesante que en el de la UNICEF dice que los niños tienen derecho a usar el internet, pero más abajo dice que los padres deben hacerse seguimiento a lo que los chicos hacen en internet.

Y eso es lo que pasa que no hay seguimiento de nada, siempre me recuerdo a un profesor, siempre me decía la televisión la niñera y culpable de todos los problemas ahora

resulta que es el internet se volvió una niñera electrónica. Para muchos padres es una solución darle el teléfono y juega y quédate ahí. Es una cuestión cultural que no he sabido detectar, pero para un para ver que un chamo agarra un teléfono y ver que ya sabe manejarlo y sabe acceder a la red es un logro ¡Oh, mira mi chamo es una avión, mira como maneja el teléfono o la tableta! .Y se sienten orgullosos, pero el problema es que no todo es un saber instrumental y no está el saber ser, y ahí está el problema”

Entrevistadora:

¿Cree que el profesor de Informática, como el área que mejor se adapta a estas temáticas, cuenta con las competencias para dar este tipo de contenidos?

Profe. Vitto Lacasella:

“Tiene las competencias técnicas y pudieran brindarlo, porque yo me conseguido con profesores de informática que transversalmente lo están haciendo, por amor propio porque saben que hay un vacío en este momento. Pero es que no está en el curriculum en este momento, no existe, por eso es que el ININCO desde hace tiempo que está queriendo hacer incorporar la educación mediática dentro del curriculum y no lo hemos logrado, porque si hablamos de educación mediática en todos los años del bachillerato, también tenemos que hablar del internet y estamos hablando de alfabetizar eso. Fíjate que estoy hablando de alfabetizar mediáticamente no digitalmente, para mí son dos cosas diferentes, yo estoy hablando de formar sujetos consientes y críticos en el momento de tomar decisiones a la hora del uso del internet en la tableta o en lo que sea.

Que chamo diga oye si subo esta foto, que puede pasar, que consecuencias me puede traer u afectar. Que puedo hacer o no, que tipo de consecuencias legales podría traerme, ese el tipo de personas que yo quiero formar y que tratamos de formar a los docentes y a los chamos.

Entrevistadora: Cree que el diseño u aplicación de talleres con respecto al tema de seguridad en redes sociales dirigido a los docentes sería apropiado, para apoyar este tipo de problemáticas?

Sería apropiado, para formar a estos docentes y para que ellos también puedan dar este tipo de información. Fíjate que cuando nosotros damos los talleres a los profesores, yo doy en CECODAC ellos tienen un diplomado contra violencia escolar, y en una de las unidades de ese diplomado es justo violencia en el internet, entonces cuando doy ese diplomado trato de decirle a los profesores mira esto es lo que está pasando esto funciona así, esta son las estrategias que te puedo decir desde mi punto de vista como educar que es lo que puedes hacer yo no soy psicólogo ni psicoterapeuta pero te puedo hablar de algunas estrategias sobre cosas que pudieras hacer para poder disminuir el fenómeno de la violencia, no erradicarlo eso imposible y de hecho hemos conseguido resultados. Yo he aplicado esto en un colegio aquí en Baruta donde alfabetizamos a los padres, chicos y docentes y logramos que páginas que estaban abiertas contra docentes se cerraran y se eliminaran, por lo menos logramos eso. Agarraron conciencia o miedo no lo sé, pero logramos eso y se dieron cuenta que estaba haciendo algo mal. Y los profesores transversalmente con las estrategias que les dimos empezaron a trabajar con los chicos y con los papas en las casas y dio resultado y el colegio quedó contento porque se disminuyó la cuestión. Pero hay un detalle debes ser reincidente no es que lo di hoy y después no lo doy más, debes seguir haciéndolo”.

Entrevistadora:

Entonces para este fenómeno podríamos empezar con ¿La formación docente, para que este mismo posterior formara al docente y a la familia?

Profe. Vitto Lacasella:

“Si pudiera ser, si tu formas al docente ayudas. Aunque porque viene uno de afuera, como me lo dijo a mí una profesora de informática. Es que si lo digo yo o si se los dice el papa, es fastidioso. Pero cuando viene una persona de afuera pareciera que los muchachos, toman en serio como autoridad. Entonces claro esta profesora me dice mira profe esto que usted acaba de explicar yo lo di pero con usted hacen creer como si nunca lo hubieran escuchado. Entonces capaz nunca lo han escuchado, pareciera como si no tuviera la fuerza moral. Pero con usted sienten como el peso de la cuestión.

Pero si evidentemente es una cuestión transversal para los profesores. Tu al trabajar el tema con los profesores, padres y muchachos es igualito, la diferencia está en el después, es decir, que puedes hacer tu como muchacho, como mama y papa o como docente. Cuando tu unes esas tres cosas todo funciona perfecto, yo puedo hacer nada si le dices a un muchacho que no puede tomar fotos sin pedir permiso, y viene la mama y recibe una imagen de una persona toda golpeada en forma de burla y ella se ríe se lo muestra y lo reenvía. Eso que hace es un delito informático, entonces como le dices a tu hijo que no lo haga, nosotros somos modelos y los chamos modelan lo que nosotros hacemos en casa, entonces ahí forma una parte importante de la situación si los tres trabajamos juntos”.

Entrevistadora:

¿Cuál sería su recomendación general final?

Profe. Vitto Lacasella:

“La mía es que los tres actores familia, docente y estudiante deben alfabetizarse mediáticamente en el consumo de internet eso más un piso firme de principios y valores que vienen del hogar que debería venir del hogar, porque yo soy de los piensa que la educación debería venir de la casa que educa, en la escuela se refuerza. Eso Con eso lograríamos que disminuya el fenómeno porque a veces es una cuestión de valores respeto, tolerancia hacia a los demás, a veces no es una cuestión de estar o no alfabetizado, pero si no consigues esto en casa no lo logramos. Si tu sabes cómo funcionan las cosas, eso mas los valores y los tres factores se puede lograr una disminución de este fenómeno”.

Fin de la entrevista.



REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

INSTRUCCIONES PARA LA VALIDACIÓN DE LOS INSTRUMENTOS DE
INVESTIGACIÓN

1. Al validador se le suministrara, además de los instrumentos de validación, también:
 - La página contentiva de los Objetivos de Investigación.
 - El cuadro de la operalización de las variables.
2. Una vez reportadas las recomendaciones por los sujetos validadores, se realiza una revisión y adecuación a las sugerencias suministradas.
3. Finalizado este proceso se puede aplicar el Instrumento.
4. Validar un instrumento implica la correspondencia del mismo con los objetivos que se desean alcanzar. Operalización de las variables (variables, dimensiones e indicadores)



REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

Estimado Validador:

Me dirijo a usted con el fin de solicitar su colaboración como experto para validar el cuestionario anexo, el cual se espera aplicarlo en el desarrollo de la investigación titulada: Evaluación y Diseño de un taller en “Seguridad en Redes Sociales” dirigido a los docentes de informática pertenecientes a la educación media general”.

El presente instrumento tiene como finalidad recoger información sobre: Validar por experto el diseño del taller en seguridad en redes sociales dirigido a los docentes de informática pertenecientes a la educación media general”.

Para efectuar la validación del instrumento, sugerimos leer cuidadosamente cada enunciado y sus correspondientes alternativas de respuestas, con la finalidad de establecer la correspondencia de cada ítem, con el indicador que pretende medir. De igual forma agradeceríamos cualquier sugerencia en relación con la construcción de los reactivos en correspondencia con el tipo de instrumento elaborado. De ante mano agradecemos su tiempo y colaboración que despiden por parte de ustedes.

La Investigadora



REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

JUICIO DE EXPERTO SOBRE LA PERTINENCIA DEL INSTRUMENTO

INSTRUCCIONES:

Coloque en cada casilla la letra correspondiente al aspecto cualitativo que le parece que cumpla cada ítem y alternativa de respuesta, según los criterios que a continuación se detallan.

E= Excelente / B= Bueno / M= Mejorarlo / EL= Eliminar / C= Cambiar.

Las categorías a evaluar son: Redacción, contenido, correspondencia y pertinencia. En la casilla de observaciones puede sugerir el cambio o correspondencia.

PREGUNTAS	E	B	M	EL	C	OBSERVACIONES
1. ¿Cómo se presenta el análisis del problema formativo de seguridad en redes sociales?						
2. ¿Cómo son definidas las características de la población a la que va dirigido el taller en seguridad en redes sociales?						
3. ¿Cómo son establecidos los conocimientos y habilidades previas que debe poseer la población para participar en el taller?						
4. ¿Cómo se justifican las teorías de aprendizaje que sustentan el diseño del taller?						
5. ¿Cómo es el análisis de las estrategias que se aplicaran durante el taller?						
6. ¿De qué manera se indica la administración de las tecnologías a emplear durante el taller de seguridad en redes sociales?						

PREGUNTAS	E	B	M	EL	C	OBSERVACIONES
7. ¿De qué manera es definido el tipo de interacción que tendrán los participantes del taller en seguridad en redes sociales?						
8. ¿Cómo se define el ambiente de aprendizaje donde los participantes del taller en seguridad en redes sociales, interactuaran?						
9. ¿Cómo considera el proceso de interacción y el ambiente de aprendizaje?						
11. ¿Cómo están redactados los objetivos del taller?						
12. ¿De qué manera se presenta la coherencia entre las metas y los objetivos?						
13. ¿Cómo se presenta la secuencia en los contenidos del taller?						
14. ¿De qué manera es la continuidad en cada uno de los contenidos?						
15. ¿Cómo es el esquema de los temas a presentar?						
16. ¿Van las estrategias de acuerdo a los objetivos y contenidos del taller en seguridad en redes sociales?						

17. ¿Cómo considera las estrategias van de del taller?						
18. ¿Hay una selección correcta de las actividades grupales e individuales para los participantes?						
19. ¿Cómo es la selección de las estrategias a emplear durante el taller?						
20. ¿Cómo es el diseño de la presentación colectiva multimedia?						
21. ¿Es la presentación colectiva multimedia, visualmente agradable y entendible para los participantes?						
22. ¿Es empleado el video para generar contenido y reflexión, de una manera adecuada?						
23. ¿Cómo percibió los videos para los contenidos del taller seguridad en redes sociales?						
24.¿ Como considero el diseño de la evaluación post-taller, para ser aplicada a los participantes?						

Evaluated by: _____

Name and Surname: _____

C.I.: _____ Firma: _____



REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo, _____, titular de la cédula de identidad N° _____, de profesión _____, ejercitando actualmente como _____ en la institución _____.

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertenecientes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido				
Pertinencia de los ítems				
Organización del contenido y presentación				
Redacción de los ítems.				
Claridad y precisión.				
Coherencia.				

En Caracas a los ___ días del mes de _____ del _____.

ANEXOS

Operalización de la Variable:

Objetivo	Variable	Dimensiones	Indicadores	Ítems
<p>Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática</p>	<p>-Diseño Instruccional. (Modelo ADITE)</p>	<p>-Componente Análisis.</p>	<p>-Problema Institucional. -Estudio de la Población. -Estudio del Tipo de Conocimiento. -Teorías del aprendizaje. - Análisis de las Estrategias cognoscitivas. -Administración de las Tecnología</p>	<p>1. ¿Cómo se presenta el análisis del problema formativo de seguridad en redes sociales? 2. ¿Cómo son definidas las características de la población a la que va dirigido el taller en seguridad en redes sociales? 3. ¿Cómo son establecidos los conocimientos y habilidades previas que debe poseer la población para participar en el taller? 4. ¿Cómo se justifican las teorías de aprendizaje que sustentan el diseño del taller? 5. ¿Cómo es el análisis de las estrategias que se aplicaran durante el taller? 6. ¿De qué manera se indica la administración de las tecnologías a emplear durante el taller de seguridad en redes sociales?</p>

Objetivo	Variable	Dimensiones	Indicadores	Ítems
<p>Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática.</p>	<p>-Diseño Instruccional. (Modelo ADITE)</p>	<p>-Componente Tecnología.</p>	<p>- Definición del Proceso de Interacción</p> <p>-Definición del Ambiente de aprendizaje.</p>	<p>7. ¿De qué manera es definido el tipo de interacción que tendrán los participantes del taller en seguridad en redes sociales?</p> <p>8. ¿Cómo se define el ambiente de aprendizaje donde los participantes del taller en seguridad en redes sociales, interactuarán?</p> <p>9. ¿Cómo considera el proceso de interacción y el ambiente de aprendizaje?</p>

			<p>-Diseño de las estrategias instruccionales e instrumentos de evaluación de aprendizaje.</p>	<p>participantes?</p> <p>19. ¿Cómo es el diseño de la presentación colectiva multimedia?</p> <p>20. ¿Es la presentación colectiva multimedia, visualmente agradable y entendible para los participantes?</p> <p>21. ¿Es empleado el video para generar contenido y reflexión, de una manera adecuada?</p> <p>22. ¿Cómo percibió los videos para los contenidos del taller seguridad en redes sociales?</p>
--	--	--	--	--

Objetivo	Variable	Dimensiones	Indicadores	Ítems
<p>Diseñar el taller “Seguridad en Redes Sociales”, dirigido a los docentes de educación media general de informática.</p>	<p>-Diseño Instruccional. (Modelo ADITE)</p>	<p>-Componente Evaluación.</p>	<p>-Evaluación de las estrategias”.</p>	<p>23. ¿Cómo está diseñado el instrumento post-taller?</p> <p>24. ¿Existe el orden dentro de los instrumentos de evaluación post-taller?</p> <p>25. ¿Cree que el presente instrumento abarca la evaluación de los contenidos, estrategias, medios computarizados y didácticos?</p>



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo Carla Negura, titular de la cédula de
 identidad N° 17.756.782, de profesión
Lic. Cs. Estadística, ejercitando actualmente como
consultora en Métodos Cuantitativos en la institución
CANTU

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertenecientes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido	✓			
Pertinencia de los ítems	✓			
Organización del contenido y presentación	✓			
Redacción de los ítems.		✓		
Claridad y precisión.		✓		
Coherencia.	✓			

En Caracas a los 28 días del mes de marzo del 2015.

Yajaira...
 Firma



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

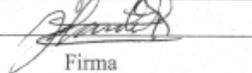
CONSTANCIA DE VALIDACIÓN

Yo, Johnnald González, titular de la cédula de
 identidad N° V-13943037, de profesión
Estadístico, ejercitando actualmente como
Docente en la institución
Escuela de Educación

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertinentes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido		✓		
Pertinencia de los items			✓	
Organización del contenido y presentación		✓		
Redacción de los items.			✓	
Claridad y precisión.			✓	
Coherencia.			✓	

En Caracas a los 23 días del mes de Mayo del 2015.


 Firma



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo LUZARA L. Urbina R., titular de la cédula de
 identidad N. 18540930, de profesión
Magíster en Educación, ejercitando actualmente como
Profesora en la institución
Escuela de Educación (UCV)

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertenecientes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido		✓		
Pertinencia de los ítems		✓		
Organización del contenido y presentación		✓		
Redacción de los ítems.			✓	
Claridad y precisión.			✓	
Coherencia.		✓		

En Caracas a los 15 días del mes de Abril del 2015.

[Firma]
 Firma



REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

VALIDACIÓN DE LOS EXPERTOS

1. Al validador se le suministrará el cuestionario de evaluación además de los siguientes anexos:
 - La página contentiva de los Objetivos de Investigación.
 - Desarrollo del componente Análisis y Tecnología.
 - Planificación del Taller.
 - Link de los vídeos empleados.
 - Presentación Colectiva Multimedia.
 - Materiales Didácticos.
2. Una vez reportadas las recomendaciones por los expertos, se pasará a la revisión y análisis de las respuestas; para posterior elaborar las conclusiones y recomendaciones de la investigación.



REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

Estimado Experto:

Me dirijo a usted con el fin de solicitar su colaboración para validar la pertinencia del diseño del taller de la investigación titulada: Evaluación y Diseño de un taller en “Seguridad en Redes Sociales” dirigido a los docentes de informática, pertenecientes a la educación media general”.

El presente instrumento está compuesto por cuatro componentes: Análisis, Tecnología, Diseño y Evaluación. Componentes propios del modelo ADITE de Marina Polo (2003), el motivo de lograr la presente validación es cumplir con el último objetivo de la investigación que es: Validar por experto el diseño del taller en seguridad en redes sociales dirigido a los docentes de informática, pertenecientes a la educación media general”.

Con ello no solo habremos abarcado todos los aspectos, sino además, se demostrara la factibilidad, coherencia y pertinencia del diseño. Le sugerimos leer cuidadosamente cada enunciado así como revisar los anexos proporcionados de forma se podrá responder cada ítems según considere la alternativa adecuada. De ante mano agradecemos su tiempo, objetividad y sugerencias. Sin más que acotar, presentamos a continuación el cuestionario.

La Investigadora.



REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE HUMANIDADES Y EDUCACIÓN
ESCUELA DE EDUCACIÓN

CUESTIONARIO

Instrucciones:

Estimado experto, se le proporcionarán los recursos necesarios en los anexos. En ellos usted contará con un material audiovisual y diseño instruccional, la idea es que pueda evaluarlos según los componentes: Análisis, Tecnología, Diseño y Evaluación. El presente cuestionario estará contenido de opciones dicotómicas para algunos ítems y escala de apreciación para otros, además de contener un espacio para indicar las observaciones. Las posibles respuestas serán:

Si / No/ M-A= Muy Adecuado / A= Adecuado/ P-A= Poco Adecuado. / I= Inadecuado.

Agradecemos su colaboración, tiempo y objetividad para validar el diseño del taller “Seguridad en Redes Sociales” dirigido a los docentes de informática, pertenecientes a la etapa de educación media general.

Presentamos a continuación los componentes a evaluar

- **Componente Análisis:**

ÍTEMS	M-A	A	P-A	I	Observaciones
1. ¿Cómo es definido el problema de actualización del docente de informática, dentro del tema en seguridad en redes sociales?					
2. ¿Cómo son definidas las características de la población a la que va dirigido el taller en seguridad en redes sociales?					
3. ¿De qué manera se establecen los conocimientos y habilidades previas que debe poseer el docente de informática para a participar dentro del taller?					
4. ¿Cómo se justifican las teorías de aprendizaje dentro del taller en seguridad en redes sociales?					
5. ¿Cómo es el análisis de las estrategias dentro del taller en seguridad en redes sociales?					
6. ¿De qué manera se indica la administración de las tecnologías a emplear durante el taller de seguridad en redes sociales?					

- **Componente Tecnología:**

ÍTEMS	M-A	A	P-A	I	Observaciones
7. ¿De qué manera es definido el tipo de interacción que tendrán los participantes del taller en seguridad en redes sociales?					
8. ¿Cómo se define el ambiente de aprendizaje donde los participantes del taller en seguridad en redes sociales, interactuaran?					
9. ¿Cómo considera el proceso de interacción y el ambiente de aprendizaje?					

- **Componente Diseño:**

ÍTEMS	M-A	A	P-A	I	Observaciones
10. ¿Cómo están redactadas las metas del taller y de cada contenido?					
11. ¿Cómo están redactados los objetivos del taller?					
12. ¿De qué manera es presentada la coherencia entre las metas y los objetivos?					
13. ¿Cómo se presenta la secuencia en los contenidos del taller?					
14. ¿De qué manera es la continuidad en cada uno de los contenidos?					
15. ¿Cómo es presentado el esquema de los temas del taller en seguridad en redes sociales?					
16. ¿Cómo considera la selección de las estrategias a emplear durante el taller?					
17. ¿Cómo es el diseño de la presentación colectiva multimedia?					
18. ¿Cómo percibió fue la aplicación del video durante el taller?					

ÍTEM	SI	NO	¿De qué manera?				Observaciones
			M-A	A	P-A	I	
19. ¿Existe una selección correcta de las actividades grupales para los participantes del taller “Seguridad en Redes Sociales”?							
20. ¿Fue la presentación colectiva multimedia visualmente agradable para los participantes?							
21. ¿Es empleado el video para apoyar los contenidos y generar reflexión, sobre el tema de seguridad en redes sociales?							
22. ¿Considera adecuada la selección de los videos a emplear para el taller en seguridad en redes sociales?							

- **Componente Evaluación:**

ÍTEMS	M-A	A	P-A	I	Observaciones
23. ¿Cómo está diseñado el instrumento post-taller?					

ÍTEMS	SI	NO	¿De qué manera?				Observaciones
			M-A	A	P-A	I	
24. ¿Existe orden de ítems dentro de los instrumentos de evaluación post-taller?							
25. ¿Cree que el presente instrumento abarca la evaluación de los contenidos, estrategias, medios computarizados y dominio conceptual y grupal del facilitador durante el desarrollo del taller ?							



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo, _____, titular de la cédula de identidad N° _____ de profesión _____, ejercitando actualmente como _____ en la institución _____

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertenecientes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido				
Pertinencia de los ítems				
Organización del contenido y presentación				
Redacción de los ítems.				
Claridad y precisión.				
Coherencia.				

En Caracas a los ___ días del mes de _____ del _____.

Firma

ANEXOS

Objetivo General:

Proponer un diseño de taller en “Seguridad en Redes Sociales”, dirigido a los docentes en el área de informática, pertenecientes a la etapa de educación media general.

Objetivos Generales:

1. Analizar los fundamentos teóricos en el tema seguridad en redes sociales.
2. Diseñar el taller “Seguridad en Redes Sociales” dirigido a los docentes en el área de informático de la etapa de educación media general.
3. Evaluar mediante la validación de experto, del diseño del taller en seguridad en redes sociales dirigido a los docentes en el área de informático de la etapa de educación media general.

Componente de Análisis:

En este componente se desarrollará el problema institucional, estudio de la población (conductas de entradas y habilidades), estudio del tipo de conocimiento y contenido, fundamentos teóricos, análisis de las estrategias cognoscitivas y administración de la tecnología. En este aspecto Polo (2003), expone que esta dimensión ayuda a conocer que se espera conocer o lo lograr con el medio, es por ello que afirma:

Cuando se diseña un medio instruccional basado en tecnologías o computarizado, hay que saber qué se espera de él, qué tipo de necesidad educativa va a solucionar, cuáles son las características de la población a la cual va dirigido, qué tipos de conocimientos se mediarán. Por lo tanto, las teorías del aprendizaje y de la instrucción deben ser analizadas en esta fase. (pág. 72)

El problema institucional:

Como se expuso en el planteamiento del problema, la sociedad del conocimiento y de la información dejó claro que las TIC, deben ser incorporadas en todos los aspectos geopolíticos que una sociedad demanda, por lo que la educación no escapa de ello. Tanto es así que organismos internacionales como la ONU y UNICEF establecen el internet como un derecho humano, lo que incide directamente tanto en países desarrollados como sub-desarrollados por lo que la incorporación paulatina en todos sus espectros yendo de lo macro a lo micro es necesaria. En Venezuela, su marco normativo lo incorpora como una obligación de Estado, a pesar de cuando revisamos dentro del aspecto educativa al ir de lo macro que es lo curricular a lo micro que es formación discente y docente, temas como internet, redes sociales y seguridad en redes sociales no se da, y una de las razones es porque el Curriculum Básico Nacional, no lo contempla lo que ata de manos a la práctica y formación docente para darlo y para tener los conocimientos técnicos en ello.

El tema de las redes sociales, se ha convertido en un fenómeno global, por ejemplo el país es uno de los mercados con mayor penetración dentro de la región de Centro América, con una población de 3,1 millones de audiencia, en el 2011, liderando redes como Facebook y Twitter.

Esto es una referencia factual de que hacemos uso constante de estas redes, pero no con el control o consciencia crítica necesario lo que ha consentido el desarrollo de un fenómeno social llamado “*ciber violencia*”; el ciberbullying, sexting grooming; son algunos de los delitos cibernéticos de lo que han sido víctimas la población consumidora de estos espacios virtuales y aunque en el país no se tenga un data de incidencia de ellos, existen testimonios como los que nos brinda el profesor Vitto Lacasella (2015), quien nos expuso que su experiencia dictando charlas tanto en instituciones privadas como públicas, quien ha encontrado casos de ciberbullying y ni docentes ni discentes o padres, saben que hacer al respecto ante esta situación.

Nos expuso que la situación se ha agravado al punto de que ya niños de cuarto grado son víctimas de tales delitos así como los discentes de la tercera etapa de educación media general, donde se ha propagado el fenómeno del sexting con la publicación de “fotos eróticas y sub-pornográficas”. Quiere decir que Venezuela no escapa de esta realidad mundial, tenemos discentes y docentes que poseen la nueva tecnología con teléfonos o tablets inteligentes con acceso a internet y conexión a redes sociales como el correo, Facebook, Gmail, Twitter; sin darse cuenta se prestan para ser partícipes de ciberbullying, como un ejemplo.

Es un problema de valores y formación, del que debemos apropiarnos de forma responsable. Ante tal situación y según lo que nos afirmó el profesor Lacasella (2015), la formación docente es indispensable y más los del área de Informática que poseen las competencias técnicas para proporcionarlos, es por ello que el taller va dirigido a esta población quien requiere de la formación en seguridad en redes sociales en primera instancia. Solo docentes formados y actualizados son garantes de discentes capaces de responder a las situaciones de su contexto, con criterio y responsabilidad.

La población:

Serán los docentes de Informática, por ser quienes cuentan curricularmente con las competencias técnicas para dar contenidos referentes a las TIC y seguridad en redes sociales.

La razón particular por la que se considera que debe ser el docente de esta área en la etapa de educación media general, es porque en ellas es donde se ha hecho más evidente la presencia de delitos como sexting o ciberbullying, además de que legalmente dan clases a los grupos etarios que tienen derecho acceder a estas cuentas, pues para ser parte de ellas debe ser mayor a los 13 años de edad. Sin embargo, para participar en el taller debe contar con las siguientes “**conductas de entrada**”:

1. Debe ser docente de Informática de la etapa de educación media general.
2. Tener el dominio del uso del Computador, el Internet y las Redes Sociales.
3. Poseer cuenta en alguna de las siguientes redes sociales: Facebook, Twitter, Gmail, Google+, Hotmail, Youtube, Instagram, entre otras.
4. Debe hacer uso frecuente de estas cuentas, dentro de su práctica docente o haber tenido una experiencia en el uso de ella dentro de la educación.

Tipo de Conocimiento:

Para el tipo de conocimiento Polo (2003), lo divide en declarativos, procedimentales y factuales. Por supuesto en conformidad con su clasificación, se establece el tipo de aprendizaje y el análisis de las estrategias que tengan mayor pertinencia con el tema y generen el aprendizaje esperado. Para el tema que se están proponiendo en el diseño del taller los contenidos se clasificaran de la siguiente manera: (ver tabla N°5)

Tabla N° 5:

Clasificación de los contenidos del Taller:

Declarativos/Conceptual/Factual	Procedimentales	Actitudinales
<ul style="list-style-type: none"> -Qué son las Redes Sociales. -Que es la Seguridad en Redes Sociales. - Clasificación de las Redes Sociales. -Población de las Principales Redes Sociales, a nivel Mundial. -Ventajas y Desventajas de los perfiles públicos y privados, dentro de las redes sociales. 	<ul style="list-style-type: none"> - Analizar y exponer los principales ataques en estas redes: -Sextorsión. - Ciber bullying. - Plagio de Identidad. - Phishing - Grooming. - Análisis general de cada video que se presente durante el taller. 	<ul style="list-style-type: none"> - Reflexionar sobre la importancia del tema seguridad en redes sociales. - Reflexionar, sobre los delitos más comunes dentro de las redes sociales.

Nota: Elaboración de la autora. Clasificación de los Contenidos, del taller en “Seguridad en Redes Sociales”.

Fundamentos Teóricos:

En el caso del taller serán desde dos visiones que hoy en día en esta nueva era trabajan en conjunto, sobretodo dentro de los procesos de aprendizajes en las redes sociales o Tic. Dicho lo anterior, nuestro primer fundamento teórico será dado por Ausubel (1983), quien expone su famosa teoría del “Aprendizaje Significativo”, en el se indica que para garantizar un verdadero aprendizaje se debe partir con los conceptos o conocimientos previos de la persona.

Esto a manera de propiciar un proceso metacognitivo exitoso, para ello se debe contar con un contenido y material adecuado o significativo, donde tanto a nivel visual como conceptual llame la atención del discente y genere la motivación requerida. Esto lo podemos aplicar hasta para formación en adultos. Ausubel (1983) expone:

...el aprendizaje del alumno depende de la estructura cognitiva previa que se relaciona con la nueva información, debe entenderse por "estructura cognitiva", al conjunto de conceptos, ideas que un individuo posee en un determinado campo del conocimiento, así como su organización. En el proceso de orientación del aprendizaje, es de vital importancia conocer la estructura cognitiva del alumno; no sólo se trata de saber la cantidad de información que posee, sino cuales son los

conceptos y proposiciones que maneja así como de su grado de estabilidad. (pág. 1)

Es decir, si queremos formar en “seguridad en redes sociales”, debemos partir de antemano con saber si nuestros participantes saben y utilizan de forma frecuente las redes sociales, tanto en su vida cotidiana como dentro de sus prácticas en aula. Es así, como partimos de un conocimiento base, para hablar de la seguridad dentro de estas redes y exponer sobre los delitos, generando un engranaje entre lo que saben y lo nuevo por descubrir. El aprendizaje significativo:

...ocurre cuando una nueva información "se conecta" con un concepto relevante ("subsunsor") pre existente en la estructura cognitiva, esto implica que, las nuevas ideas, conceptos y proposiciones pueden ser aprendidos significativamente en la medida en que otras ideas, conceptos o proposiciones. (Ausubel, 1983:2)

Para lograr tal aspecto, los materiales y los contenidos juegan un papel relevante, debido a que se convierten en el canal o medio por el que el participante hace el engrane sobre lo que sabe y lo nuevo por aprender. Para ello el facilitador, debe exponer los nuevos conceptos y preceptos de una forma clara, creativa e innovadora. Se debe lograr estimular el aprendizaje para que el mismo fije en su cerebro y no se le olvide rápidamente. Es por ello que el autor expone:

Que el material sea potencialmente significativo, esto implica que el material de aprendizaje pueda relacionarse de manera no arbitraria y sustancial (no al pie de la letra) con alguna estructura cognoscitiva específica del alumno, la misma que debe poseer "significado lógico" es decir, ser relacionable de forma intencional y sustancial con las ideas correspondientes y pertinentes que se hallan disponibles en la estructura cognitiva del alumno...

Cuando el significado potencial se convierte en contenido cognoscitivo nuevo, diferenciado e idiosincrático dentro de un individuo en particular como resultado del aprendizaje significativo, se puede decir que ha adquirido un "significado psicológico" de esta forma el emerger del significado psicológico no solo depende de la representación que el alumno haga del material lógicamente significativo, "sino también que tal alumno posea realmente los antecedentes ideativos necesarios" (Ausubel, 1983: 55)

Con respecto a los materiales se empleara las presentaciones colectiva multimedia, el proyector multimedia, los materiales didácticos diseñados y el video como herramienta para generar un conocimientos y afianzarlo de una forma didáctica. Con respecto al contenido será

expuesto como algo sustancial y no arbitrario, es decir, partiremos por lo que ya estos conocen y los asociaremos con lo nuevo, de manera que sea percibido como una continuidad y no como un conocimiento nuevo obligatorio aprehender.

Ausubel (1983), sin duda alguna expone una teoría aplicable y válida para el diseño de nuestro taller, dado que la misma, visualiza el aprendizaje como un proceso dinámico que ocurre de una forma bilateral, pues el docente o facilitador no puede inferir “que sabe todo” o “que el discente no sabe, nada”. Ambos deben partir por una base de conceptos para conjuntamente crear nuevos.

Claro esto, la otra teoría sirve de complemento para la propuesta; el conectivismo, puede trabajar en equipo con la teoría de Ausubel (1983), ya que mientras este expone que el aprendizaje significativo emana del material y del concepto que se exponga, la nueva propuesta hace énfasis en el que mismo ocurre pero por medio de la colaboración dentro de la “Social Network” (redes sociales) o el almacenamiento esta dentro de bases de datos.

Es decir, en el conectivismo incluye las tecnologías y las redes sociales como una nueva tendencia para el aprendizaje, como señala Polo (2003) en su modelo y para mi interpretación como autora, es un proceso similar al que expone Ausubel, pero incluye a las tecnologías dentro del proceso no solo para generarlas sino además para almacenarlo. En fin son teorías, que más que encontrarse se adaptan o se complementan dentro de la investigación y sobre todo al proceso de aprendizaje que al fin y al cabo es el objetivo final de los tres autores y el interés personal de la presente autora.

El exponente base de esta propuesta es Siemens (2008), quien expone que esta es una nueva corriente epistemológica, a tiene ciertamente un inicio en posturas como el conductismo, cognositivismo y constructivismo, en cuanto a la tendencia del aprendizaje, sin embargo, aporta nuevas ideas con respecto a cómo ocurre y cómo se almacena, ya que no es mentira que las nuevas tendencias de esta era giran es entorno a las tecnologías, redes sociales y el internet, es un poco lo que se expuso ante sobre las nuevas competencias que debe tener el docente para adaptarse a los procesos dentro del aula. Siemens (2008), define el Conectivismo como:

...la aplicación de los principios de redes para definir tanto el conocimiento como el proceso de aprendizaje. El conocimiento es definido como un patrón particular de relaciones y el aprendizaje es definido como la creación de nuevas conexiones y patrones como también la habilidad de maniobrar alrededor de redes/patrones existentes.

El Conectivismo aborda los principios del aprendizaje a numerosos niveles – biológico/neuronal, conceptual, social/externo

Es decir el proceso puede ocurrir tanto de forma colectiva como a nivel personal, es decir, discente y explorador. Ya que como hemos indicado el enfoque de esta tendencias es precisamente incluir las tecnologías como parte de la “distribución de cognición y conocimiento” (Siemens, 2008). Es decir, el conocimiento no solo reside en el individuo sino también en la interacción con otras personas o en fuentes de información como bases de datos, blog, exploradores, entre otros. Sin duda alguna, lo innovador de esta propuesta o teoría es el papel clave que juegan las tecnologías para alcanzar el aprendizaje o construir conocimiento.

Por ejemplo Siemens (2008) expone que las tecnologías trabajan en “... en la creación y visualización de patrones, en extender e incrementar nuestras habilidades cognitivas y en mantener información en una forma de rápido acceso (por ejemplo, buscadores, estructuras semánticas, etc.)”. Y de alguna manera, tiene un punto.

La generación 2.0 y próximamente la 3.0, tiene en gran medida almacenado sus archivos, videos, libros, artículos y trabajos dentro de sus computadoras, en la nube con el internet o dentro de espacios corporativos. En estos espacios confían, una parte importante de sus conocimientos e investigaciones sintiéndose seguros de que estos se ubiquen ahí, lo que quiere decir, es que los discentes emplean las TIC, las redes sociales y el internet para generar, compartir u obtener conocimiento y aprendizajes el docente dentro del aula debería hacerlo, de manera de poder captar su atención; si no se pierde entre sus prácticas antiguas y no genera esa chispa requerida por parte del estudiante.

Con ello no buscamos aseverar que la práctica docente esta descontextualizada o que lo tradicional está mal, lo que buscamos exponer es que no podemos cerrar las puertas las nuevas

tendencias ni mucho menos no aprobar supuestos como los que aporta esta nueva tendencia del Conectivismo. La era digital es una realidad, las redes sociales se han convertido en todo un espacio para la interacción y hasta para compartir información así como los blogs o weblogs son espacios para la educación y sobre todo para generar aprendizaje significativos en red.

Estrategias cognoscitivas:

Estrategias y Tecnología a emplear:

- Aplicación de medios audiovisuales (videos, imágenes, presentación colectiva multimedia)
- Actividades grupales (exposición, organización de contenidos, feedback).
- Actividades individuales (lluvia de ideas, opiniones, exposición de experiencias, etc.)

Componente Tecnológico:

El proceso de interacción:

En este aspecto Polo (2003) emplea el modelo de Galvis (1992), ejecutando una serie de adaptaciones, donde define este punto como:

La interacción centrada en el alumno remite al binomio estudiante instrucción. Esta forma de interactuar atañe a los procesos que el ambiente tecnológico, basado en un entorno multimedia, proporciona al estudiante para que se generen respuestas de ambos lados y, en consecuencia, se logre el aprendizaje... (pág. 77)

Como ya se expuso antes el taller será presencial, sin embargo, se empleará el uso de la presentación colectiva multimedia y de videos, para dar inicio y afianzar algunos contenidos, es por ello que se puede decir que la interacción en primera instancia será interactivo de tipo presencial facilitador-docente, pictórica pues se les presentaran imágenes asociativas al tema a exponer empleando dispositivos de salida, pues utiliza un computador, y pantalla de reproducción donde se verán las diapositivas así como los videos a mostrar.

Ambiente de aprendizaje:

Básicamente será el espacio dispuesto para el proceso de taller, ya que en gran medida y el proceso de feedback será dado en ese espacio de forma presencial.

El mismo deberá ser un aula con cabida a veinte personas, que posea acceso a internet o en su defecto se cuente con enchufes para laptop, proyectores multimedia y cornetas, el mismo deberá poseer una buena iluminación para que la presentación colectiva multimedia y los videos se puedan percibir de manera adecuada.

- **Nombre del taller:**

Taller “Seguridad en Redes Sociales”: Conceptos Básicos y Herramientas para su abordaje en aula.

- **Meta del Taller:**

Dar a conocer los conceptos básicos y las herramientas claves sobre el tema “Seguridad en Redes Sociales”, a los docentes pertenecientes al área de Informática en la etapa de educación media general. Una vez finalizado el taller el docente contara con nociones superiores del tema y con estrategias para abordar la temática y al mismo tiempo habremos apoyado la calidad en la formación docente.

Objetivos

- Describir los aspectos conceptuales básicos en torno al tema “Seguridad en Redes Sociales”.
- Analizar la importancia de los principales ataques y herramientas para abordar el tema de seguridad en redes sociales.
- Reflexionar sobre la importancia de la inclusión del tema de Seguridad en Redes Sociales, dentro de su práctica docente dentro de esta etapa escolar.

Duración:

Una de sesión de seis (6) horas y media, dividida en tres bloques, donde las horas en aula, se toman de 45min. Aclarado lo siguiente se presentará así:

- Bloque #1: Inicio y desarrollo del taller, duración de: 3h.
- Bloque #2: Break, duración: 1h y 15min. Es decir en total: 60min.
- Bloque #3: Desarrollo y Final del Taller, duración: 2h y 17min.

PLAN DE FORMACIÓN DOCENTE PARA EL TALLER
“SEGURIDAD EN REDES SOCIALES”

META	TEMARIO	ACTIVIDAD	RECURSOS REQUERIDOS	TIEMPO ESTIMADO
	Presentación Inicial	<p>1- Se les dará la Bienvenida y pedirá que se identifiquen, colocando su nombre en los identificativos. Para ello se le darán los recursos necesarios.</p> <p>2- Presentación inicial de todos los participantes y del facilitador.</p>	Marcador. Imperdible. Cartón (para colocar sus nombres)	10´
Conocer las expectativas por parte de los participantes con respecto al taller.		<p>3- Exposición por parte de los participantes, las expectativas del taller.</p> <p>4- Revisión de los objetivos y agenda desarrollar.</p>		15´
Exponer las definiciones básicas.	Redes Sociales: Definiciones y tipos.	<p>5- Se hace una pregunta abierta: ¿Qué son las redes sociales? (El facilitador debe estimular a que respondan al menos tres participantes para entrar en contexto).</p>	Ninguno	10´
		<p>6- Se proyectan las láminas sobre la definición de redes sociales. Y un cuadro con las redes sociales y la población con la que cuenta a nivel mundial. Datos factuales del 2014.</p> <p>7- Se les presentará un cuadro sobre la clasificación de las redes sociales.</p>	Presentación Colectiva Multimedia. Computador. Proyector Multimedia.	25´

<p>Presentar la definición de “Seguridad en Redes Sociales”</p>	<p>Seguridad en Redes Sociales I: Definición.</p>	<p>8- Se hace una pregunta abierta: ¿Cuáles casos han conocido o escuchado sobre delitos cibernéticos?</p> <p>(el facilitador debe estimular a que respondan al menos tres participantes para entrar en contexto)</p> <p>9- Se proyecta en las láminas la definición de seguridad en redes sociales y las tasas de los delitos cibernéticos más frecuentes. Para ello se les facilitara un material didáctico. (ver Anexo N° 2)</p>	<p>Presentación Colectiva Multimedia. Computador.</p>	<p>15´</p>
<p>Conozcan que los delitos más frecuentes dentro de las redes sociales.</p>	<p>Seguridad en Redes Sociales II: Tipos de ataques.</p>	<p>10- Actividad en Grupo#1:</p> <p>Exponer sobre los delitos cibernéticos más comunes dentro de las redes sociales. Para esto se les proporcionara un material de apoyo, previamente diseñado. (Ver Anexo 3)</p>	<p>Papel Bond. Marcadores. Tizas. Colores.</p>	<p>40´</p>
<p>Generar reflexión sobre los delitos y sus consecuencias.</p>	<p>Seguridad en Redes Sociales III: Reflexión general.</p>	<p>11- Presentación del video: “Lo Malo de las Redes Sociales Si no se controla webmsmall” (Tiempo: 8´05´´)</p> <p>12- Análisis del video e identificación de los delitos ya expuesto. -Se les preguntara a los participantes que opinan del video.</p>	<p>Computador. Cornetas. Proyector Multimedia. Video.</p>	<p>20´</p>
		<p>13- Break</p>		<p>60´</p>

<p>Generar reflexión sobre cómo nos comportamos dentro de las redes sociales.</p>	<p>Aceptar un amigo en la red.</p>	<p style="text-align: center;">*</p> <p>13- Presentación del Video: Caperucita 2.0: ¿Deberías agregar a extraños a tus redes sociales? (Tiempo: 2'07'')</p> <p style="text-align: center;">*</p> <p>14- Discusión y análisis del video.</p>	<p>Computador. Cornetas. Proyector Multimedia. Video.</p>	<p>12´</p>
<p>Indicar la ventaja y desventaja de los perfiles públicos y privados.</p>	<p>Perfiles público y privados. Ventajas y desventajas.</p>	<p>15- Presentación de láminas: Ventajas y Desventajas de las los perfiles públicos y privados.</p>	<p>Computador. Presentación Colectiva Multimedia.</p>	<p>15´</p>
<p>Elaborar una recomendación de forma conjunta, sobre cómo ser un mejor usuario.</p>	<p>Como ser un mejor usuario.</p>	<p style="text-align: center;">*</p> <p>16- Actividad Grupal#2: "140 Caracteres una Recomendación"</p>	<p>Papel Bond. Marcadores. Tizas. Colores. Teipe.</p>	<p>20´</p>
<p>Elaboración de cinco estrategias docentes para abordar el tema de seguridad en redes sociales.</p>	<p>Cinco estrategias</p>	<p style="text-align: center;">*</p> <p>17- Con la reflexión anterior, todos con la guía y participación del facilitador extraerán de forma breve cinco estrategias concretas de cómo abordar el tema de seguridad en redes sociales.</p>	<p>Papel Bond. Marcadores. Tizas. Colores.</p>	<p>10´</p>
<p>Reflexión Final</p>	<p>Reflexión Final.</p>	<p>18- Presentación del Video Final: Recomendaciones para el Uso Seguro del Internet y las Redes Sociales, con seguridad. (Tiempo: 5'01'')</p> <p>19- Analizar el video con las siguientes preguntas: ¿Cómo aplicar este contenido en el aula?</p>	<p>Computador. Cornetas. Proyector Multimedia. Video.</p>	<p>15´</p>

		<p>20- Actividad Final: Que te llevas en la maleta.</p> <p>21- Aplicación de la Evaluación post-taller. (Modelo puede ser apreciado en el Anexo N°.5)</p>	<p>Papel Boom. Marcadores. Pruebas.</p>	<p>35´</p>
Tiempo Total		290		

4.3 Descripción de las actividades:

Las actividades 1, 2, 3, 4 permitirán a los participantes conocerse entre sí, además de situar la agenda a tratar en el taller. Es de esta manera como se da inicio a la actualización y socialización, por parte de los docentes de la tercera etapa de educación en el área de informática.

- **Actividad #5:** Pregunta de Inicio.

Una vez iniciado el proceso y presentado los participantes, se dará pie para al inicio del tema, partiendo con la pregunta: ¿Qué son las redes sociales?

Esta pregunta le permite al facilitador, conocer que tanto manejan sobre el tema, y sobre las redes que más usa la población docente, permitiendo partir de sus experiencias o conocimientos sobre ello. Las experiencias previas en este caso son importantes ya que le brindan al facilitar la poca o mucha receptiva que se tienen sobre estas o sobre su aplicación dentro de las aulas. Una vez obtenido la información base, el facilitador pasa a la siguiente actividad.

- **Actividad #6:** Presentación de Láminas

La presente actividad se basa en la presentación de diapositivas, el concepto de redes sociales y los tipos de redes sociales, así como la población que posee cada una. Para el concepto apoyándose en Perdomo, D (2011). El concepto de “Redes Sociales”, comprendidas como:

... aquel lugar virtual que les permite a individuos la interacción social, el intercambio constante de información, intereses, ideas y opiniones. Es una

comunidad en constante construcción y remodelación a fin de ser cada vez más completa frente a las necesidades de los internautas (usuarios de internet), quienes buscan un sitio apropiado para convivir con demás personas que, como ya se dijo, comparten sus mismos gustos y aficiones, pero al mismo tiempo relacionarse con gente. (Perdomo, 2011:8)

Para los tipos de Redes Sociales, usaremos la tabla N° 3, presentada en el marco teórico, por supuesto esta tabla debe ser adaptada para una presentación Power Point. La tabla será:

Principales Redes sociales.

Red Social	Año de fundación	Creador	Características	Números de usuarios actualmente (2014)	Logo
Facebook	2004	Mark ElliotZuckerberg	<ul style="list-style-type: none"> -Se crea con un gran espacio para compartir vivencias. -Permite aceptar amigos de todos lados del mundo. -Crear un perfil y hacerlo público o privado. - Se puede subir videos, imágenes y etiquetar a los amigos aceptados en tu perfil. -Se puede jugar dentro de la misma red. 	Aprox. 1.28 billones	
Twitter	2006	Jack Dorsey	<ul style="list-style-type: none"> -Microbloggin. - Publicaciones en 140 caracteres. -Permite las publicaciones de imágenes. -Permite estar enterada al instante de sucesos, hechos o aconteceres a nivel local, regional y mundial. -Hashtag, para crear temas de interes. 	Aprox. 255 millones	
Youtube	2005	Chad Hurley, Steve Chen y Jaweb Karim	<ul style="list-style-type: none"> -Permite subir y publicar videos, de cualquier tipo de temas. -Aloja una variedad de video clips de películas y programas de televisión, videos musicales, y videos caseros. 	Aprox. 1 Billón	
Instagram	2010	Kevin Systrom y Mike Krieger	<ul style="list-style-type: none"> -Es una aplicación gratuita para publicar fotos y videos. -Aplicación gratuita para smarphone. -Comprado en el 2012 por Facebook. - Permite la aplicación de filtros a las fotos, etiquetar a seguidores o hacer publicaciones directas. 	Aprox. 200 millones	

Google+	1997	C- fundadores: Sergey Brin y Larry Page	-Es una red social, perteneciente a google, que permite la publicación de videos, imágenes y comentarios. -Crear círculo de amistades, familia y trabajadores.	Aprox. 540 millones	
----------------	------	--	---	---------------------	---

Nota: Elaboración de la autora. Resumen de las principales redes sociales, con sus características, fundadores y número de usuarios actualmente.

• **Actividad # 7:** Clasificación de las Redes Sociales.

Cabe destacar el cuadro que presentaremos a continuación es un esbozo para el facilitador, dado que igual que la tabla anterior, el mismo es extenso para presentarse en una presentación colectiva multimedia. Sin embargo, servirá para estudiar y presentar de forma verbal y sintetizada la clasificación de las redes sociales.

Clasificación de las Redes Sociales.

Por su público objetivo y temática	Por el sujeto principal de la relación	Por su localización geográfica	Por su plataforma
-Redes sociales horizontales: Son aquellas dirigidas a todo tipo de usuario y sin una temática definida. Por ejemplo: Facebook, Twitter, Orkut, Identi.ca.	-Redes sociales humanas: Son aquellas que centran su atención en fomentar las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades. Por ejemplo: Koornk, Dopplr, Youare y Tuenti.	-Redes sociales sedentarias: Este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Por ejemplo: Rejaw, Blogger, Kwippy, Plaxo, Bitacoras.com, Plurk.	-Red social MMORPG y metaversos: Normalmente contruidos sobre una base técnica Cliente-Servidor (WOW, SecondLife, Lineage).
-Redes sociales verticales: Están concebidas sobre la base de un eje temático agregador. Tienen por objetivo el de congregar en torno a una temática definida a un colectivo concreto. A su vez pueden clasificarse en:	-Redes sociales de contenidos: Las relaciones se desarrolla uniendo perfiles a través de contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador. Por ejemplo: Scribd, Flickr, Bebo, Friendster.	-Redes sociales nómadas: Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Por ejemplo: Latitud, Brighkite,	-Red social web: Su plataforma de desarrollo está basada en una estructura típica de web. Algunos ejemplos representativos son MySpace, Friendfeed y Hi5.

<p>a. Redes sociales verticales profesionales: Están dirigidas a generar relaciones profesionales entre los usuarios. Por ejemplo: Viadeo, Xing y Linked In.</p> <p>b. Redes sociales verticales de ocio: Su objetivo es congregarse a colectivos que desarrollan actividades de ocio, deporte, usuarios de videojuegos, fans, etc. Por ejemplo: Wipley, MinubeDogster, Last.FM y Moterus.</p> <p>c. Redes sociales verticales mixtas: Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales entorno a sus perfiles. Por ejemplo: Yuglo, Unience, PideCita, 11870.</p>	<p>-Redes sociales de inertes:</p> <p>Conforman un sector novedoso entre las redes sociales. Su objeto es unir marcas, automóviles y lugares. Entre estas redes sociales destacan las de difuntos, siendo éstos los sujetos principales de la red. El ejemplo más llamativo es Respectance.</p>	<p>Fire Eagle y Scout.</p>	
--	--	----------------------------	--

Nota: Elaboración de la autora. Fuente: Flores Cueto, J (2009).

• **Actividad #8:** Pregunta abierta.

Las actividades anteriores serán la base, para que en estas actividades se dé inicio al tema sobre la seguridad en redes sociales, que es el eje central del taller. Es por ello que se realizan las siguientes preguntas abiertas: ¿Cuáles casos que han conocido o escuchado sobre delitos cibernéticos?

Las respuestas a estas preguntas le permitirían al facilitador, tener una base sobre los conocimientos que tienen los participantes del tema y sobre los delitos cibernéticos más frecuentes en estos espacios virtuales. De este punto partir y entrar a fondo en el tema.

- **Actividad #9:** Proyección de Láminas- Definición de “Seguridad en Redes Sociales”.

Partiendo de la información anterior el facilitador pasará a presentar una lámina sobre la definición de “Seguridad en Redes Sociales”. Se le presentara datos recolectados por la autora, sobre el porcentaje de los delitos más comunes en estos espacios según la empresa líder en el desarrollo de programas y aplicaciones para la seguridad del ordenador en el uso del internet, “Symatec” quien lo expone en el informe sobre las “Tendencias de Seguridad Informática en América Latina y el Caribe” (ver el material en el Anexo N°2). Para dar apertura a los delitos se realiza la actividad siguiente.

- **Actividad # 10:** Actividad Grupal “Presentar sobre los delitos cibernéticos más comunes dentro de las redes sociales”.

En esta actividad se divide a los participantes en cinco grupos de cuatro personas, y se les pide al azar que seleccionen, uno de los siguientes temas:

- Sextorsión.
- Cyberbullying.
- Plagio de Identidad.
- Phishing
- Grooming.

Para ello se les dará la información de cada tema a los equipos, con el fin de que estos se organicen y de una forma sencilla expongan al resto de los participantes el tema que les toco. Contarán con 20´para organizarse y 5´cada grupo para exponer. Esta actividad se hace con objetivo de generar un proceso de retroalimentación donde son los mismos participantes los

encargados de construirlos con la guía y herramientas que propicia el facilitador. (Ver materia didáctica, Anexo)

- **Actividad #11 y # 12:** Presentación y Análisis del Video.

Se le presenta a la audiencia el segundo video, llamado “Lo Malo de las Redes Sociales Si no se controla webmsmall.” obtenido en línea de la siguiente fuente: <https://www.youtube.com/watch?v=hoqzkHQ9jxw> . En él se demuestra de una forma muy jocosa y sencilla, cada uno de los errores que fácilmente cometemos dentro de las redes sociales, deslices que nos pueden colocar en situaciones que exponen tanto nuestra integridad física como virtual por estas redes. Estos errores, son comunes en los usuarios que las visitan. Usuarios de diversas edades que exponen de una manera innecesaria su vida privada.

El video como medio didáctico permite dos cosas: 1- Que los docentes, entiendan la necesidad de formación en seguridad en redes sociales, dado que pueden guiar a sus discentes a que sean más críticos y prudentes a la hora de usarla y 2- Sirve como un medio para enseñar o ejemplificar, una situación latente dentro de la sociedad. Como lo sustenta Acevedo (2012:44):

El video dada sus características es utilizado por los docentes como un instrumento o elemento motivador dentro de los procesos de enseñanza y aprendizaje, ya que al presentar la información en un formato distinto a los tradicionales, los estudiantes suelen incentivarse...

De esta manera no solo se logran los objetivos, sino además, generar la discusión necesaria sobre el tema, traer conceptos desconocidos y demostrar que delitos como: Sextorsión, Cyberbullying, Plagio de Identidad y Phishing; son delicados y lo que es peor nuestros discentes se exponen a ellos con el mal uso que le den a estas redes. Es así como se aportan tanto elementos conceptuales como estratégicos para abordar la temática, por parte de ellos en aula. Con el apoyo del video se plasma la exposición de cada equipo sobre lo delitos cibernéticos.

Break: Tiempo de descanso y comida para los participantes, mientras el facilitador prepara el segundo bloque de actividades y contenidos.

- **Actividad # 13 y #14:** Presentación de Video y Análisis.*

Antes de explicar estas actividades, es imprescindible aclarar que la razón por la que estas poseen asteriscos (*), es porque pueden ser o no aplicadas a la hora ejecutar el taller, es decir el facilitador tendrá la oportunidad de decidir de acuerdo al tiempo si es posible su aplicación o no.

Ahora bien si desea aplicarse, para continuar el tema y activar a los participantes de nuevo después del break, se les presente el segundo video llamado “Caperucita 2.0: ¿Deberías agregar a extraños a tus redes sociales?”, obtenido en línea de la siguiente fuente: <https://www.youtube.com/watch?v=Vx7GIKPSE8U> . Este presenta de una forma ejemplifica lo que puede suceder cuando agregamos a nuestros perfiles personas que no conocemos, una acción muy común hoy en día sobre todo por la población adolescente. Una vez presentando el video, se da pie al análisis del mismo, por parte de los participantes.

- **Actividad #15:** Presentación de láminas.

Se presentara el siguiente cuadro con cinco desventajas y ventajas de tener un perfil público o privado dentro de nuestras redes sociales. Hay que tener en cuenta que el beneficio de estos espacios, depende en gran medida en el buen uso que le demos que de las configuraciones que presenta cada página o red social, ya que cada usuario es autónomo y administrador de su perfil o cuenta. Al igual que los cuadros anteriores se le recomienda al facilitador, que lo sintetice de manera de ser presentado el Power Point, el cuadro será el siguiente:

Tabla 5: Ventajas y Desventajas de los Perfiles públicos y privados.

	PERFILES PÚBLICOS	PERFILES PRIVADOS
VENTAJAS	1. Permiten acceder fácil a ti, de personas conocidas como desconocidas.	1. Solo pueden acceder a ti personas que conozcas o le des acceso a tu perfil.
	2. Tus publicaciones, llegan a gran cantidad de personas.	2. Solo a quienes pertenecen a tu círculo de amigos o seguidores, pueden ver tus publicaciones y comentarlas.
	3. La publicaciones de eventos tanto corporativos como personales, pueden tener gran publicidad, con perfiles abiertos pues grandes números de personas conocidas como desconocidas pueden acceder a él.	3. Puedes invitar por estos espacios a las personas cercanas a ti a tus fiestas o eventos. De esta manera exclusivamente solo el que tú quieras puede ser parte de él.
	4. Permite la propagación de informaciones a gran escala.	4. Tu información solo llega a quienes desees.
	5. Permite hacer nuevas vinculaciones o amistades con personas de todos lados del mundo.	5. Permite respetar tu espacio personal y mantiene tu vida privado en resguardo, ya que solo lo que desees y a quienes desees que las vean podrán acceder.
DESVENTAJAS	1. Tanto personas conocidas como no conocidas, pueden acceder a tu perfil y ver tus publicaciones y fotos.	1. Si eres una corporación o estás interesado en vender una marca o producto, esto podría dificultar el acceso a él.
	2. Cuando acceden a él personas que no conoces ni están dentro de tu círculo de amistades, no sabemos bajo cual intención hacen el acceso a él, lo cual puede generar situaciones incómodas o negativas para el usuario	2. Si eres una corporación o estas interesado en la organización de un evento a gran escala, los perfiles privados no permiten que esto sea posible pues solo conocerán de este evento quienes tengas como seguidores o amigos, no público externo que esté interesado en participar.
	3. Corres riesgo de ser una víctima de delitos como: Sexphsing, Cyberbullying, Plagio de Identidad y Phishing o ser expuesto ante piratas informáticos con hackers.	
	4. Las características primordial de las redes sociales, es que permite crear un círculo o red con personas tanto conocidas como desconocidas. Al tener el perfil público puedes exponer también a tus amistades cercanas como a familiares, pues pueden ser localizados o vistos en tu perfil de una forma sencilla.	
	5. Algunas corporaciones, hacen uso de las redes sociales, para los procesos de selección, si este está	

	abierto y es tu cuenta personal podrías exponer de una forma negativa ante estos.	
--	---	--

Nota: Elaboración y análisis de la autora. Resumen de las principales ventajas y desventajas de tener perfiles públicos o privados, en las redes sociales.

- Actividad#16: Actividad Grupal #2: “140 Caracteres una recomendación”

De igual manera a las actividades 13 y 14 poseen asteriscos (*), porque pueden ser o no aplicadas a la hora ejecutar el taller, es decir el facilitador tendrá la oportunidad de decidir de acuerdo al tiempo si es posible su aplicación o no.

Para esta actividad a los grupos anteriores, se les pedirá que escojan en e indique en 140 caracteres, una recomendación sobre el uso correcto de sus perfiles dentro de las redes sociales. Esto deberán escribirlo en una hoja de papel bond, y el representante deberá exponer ¿Por qué escoger esa recomendación? y ¿Por qué la considerarla importante, para mantener la seguridad dentro de las redes sociales? .Lo importante es que no deberán repetirse, lo que obliga el trabajo colaborativo de todos los participantes.

De esta manera, estimularemos los pensamientos críticos de los participantes tanto individual como grupalmente, lo que ayudara a fijar la importancia del tema y de la formación de él tanto para ellos como para los discentes. Se espera además que esta actividad complemente las anteriores, quienes están enfocadas en primera instancia que se focalice cuales aspectos de los que se han hecho mención se ha incurrido o si sean expuesto como usuarios de una manera que puedan ser víctimas de estos delitos. En segunda instancia que identifiquen si dentro de su aula se han presentado estas situaciones o algún discente ha sido víctima; si logran identificar esto en sus aulas, una vez culminado el taller contarán con las herramientas para enfrentar la situación y ser ellos guías para mejorarla.

- **Actividad #17:** Cinco Recomendaciones para el Docente.*

De igual manera a las actividades 13, 14 y 16 poseen asteriscos (*), porque pueden ser o no aplicadas a la hora ejecutar el taller, es decir el facilitador tendrá la oportunidad de decidir de acuerdo al tiempo si es posible su aplicación o no.

Como una de las actividades finales, el facilitador conjuntamente con los participantes escribirá en una lámina de papel bond, cinco estrategias que puede emplear el docente en el aula a la hora de que se presente una situación ligada a los delitos d redes sociales, las ideas deberán ser expuestas de forma corta y concreta; de manera de hacer el proceso rápido pero enriquecedor.

- **Actividad #18:** Presentación de video final.

La presentación del video final, titulado: Recomendaciones para el “Uso Seguro de Internet y las Redes Sociales, con seguridad” este video se obtuvo en línea de la siguiente fuente: <https://www.youtube.com/watch?v=t-x73w1N1os>. En él se presentan diez recomendaciones sobre el uso correcto de las redes sociales, en aras de mantener nuestra seguridad como usuario. Estas recomendaciones son:

- Mantén tu equipo se software maliciosos y no abras mensajes o ficheros extraños, pueden conducirte a virus.
- No expongas tus datos ni información personal.
- Cuidado con las fotos e imágenes que se carguen en los perfiles, pueden dar tu imagen o la de terceros.
- Evita generar o ser parte de provocaciones u conflictos por estos espacios.

- Gestiona tu privacidad, exponerse lo menos posible, es de personas críticas e inteligentes.
- No compartas claves.
- Cuidado con el uso inadecuado de la webcam.
- Mantén un espíritu crítico en estas redes, es necesario contrastar información.
- No aceptes a desconocidos como amigos dentro de estos entornos.
- No concretes citas a solas con desconocidos.
- **Actividad # 19:** ¿Qué te llevas en la maleta?

Una vez visto el video, se para analizar las diez recomendaciones, se darán las siguientes preguntas: Se dará cierre con la pregunta ¿Qué te llevas en la maleta?. Cada participante de forma breve expresará que se lleva al finalizar el taller

- **Actividad #20:** Evaluación post-taller.

Antes de que los participantes se vayan, se les proporcionara la evaluación post-taller, que le servirá al facilitador que tan pertinente fue su gestión, los contenidos y estrategias y las impresiones que se llevan. (visible en los anexos)

El fin general de todas las actividades propuestas, es en primera instancia, lograr cada el objetivo conceptual, procedimental y Actitudinal. ¿Cómo?, desarrollando cada actividad, pues cada una tiene aspectos conceptuales donde se les indicarán las nociones básicas de conceptos asociados a las redes sociales y la seguridad dentro de ellas, así mismo los procedimentales con las actividades en grupos, donde tendrán que socializar y consensuar con sus equipos de trabajos lo que se les pide, de esta manera se genera el aprendizaje cooperativo (Johnson, Johnson y Holubec 1999), antes expuesto.

REFERENCIAS BIBLIOGRAFICA

- Educar (2013). Caperucita 2.0: ¿deberías agregar a extraños a tus redes sociales?. [Video en línea] Recuperado de: <https://www.youtube.com/watch?v=Vx7GIKPSE8U>
- Flores Cueto, J (2009). Redes Sociales. [Documento en Línea] Recuperado de: http://mc142.uib.es:8080/rid=1HY8TVCB-15599LW-1S6Z/redes_sociales.pdf
- Johnson, Johnson. Holubec (1999) El aprendizaje cooperativo en el aula. Editorial Paidós. Buenos Aires.
- Pantalla Amigas (2013). Recomendaciones para el Uso Seguro de Internet y las Redes Sociales, para el uso seguro. [Video en línea] Recuperado de: <https://www.youtube.com/watch?v=t-x73w1N1os>
- Perdomo, D (2011). Redes Sociales en Internet. [Tesis en línea] Recuperado de: <http://es.slideshare.net/cubedirubik/tesis-redes-sociales-en-internet>
- Polo, M (2003). Aproximación del Modelo ADITE. Revista Docencia Universitaria, Vol. 1, N° IV. SADPRO – UCV. Caracas
- Rincón del Network (2013). Tipos de Redes Sociales. [Video en Línea] Recuperado de: <https://www.youtube.com/watch?v=gRKctZjfRLk>
- Siemens, G (2008). Conectivismo: Una teoría de Aprendizaje para la Era Digital. [Articula en Línea]. Recuperado de: <https://humanismoyconectividad.wordpress.com/2009/01/14/conectivismo-siemens/>.
- TREND MICRO (2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. [Informe en línea] Recuperado de: http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf.

Presentación Colectiva Multimedia-Taller en Seguridad en Redes Sociales.

Taller "Seguridad en Redes Sociales": Conceptos Básicos y Herramientas para su abordaje en aula



Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Describir los aspectos conceptuales básicos en torno al tema "Seguridad en Redes Sociales".

Objetivos del Taller:



- Describir los aspectos conceptuales básicos en torno al tema "Seguridad en Redes Sociales".
- Analizar la importancia de los principales ataques y herramientas para abordar el tema de seguridad en redes sociales.
- Reflexionar sobre la importancia de la inclusión del tema de Seguridad en Redes Sociales, dentro de su práctica docente dentro de esta etapa escolar.

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Temario:



1. Definición de Redes Sociales.
2. Tipos de Redes Sociales.
3. Clasificación de las Redes Sociales.
4. Seguridad en Redes Sociales:
 - 4.1 Definición.
 - 4.2 Delitos cibernéticos más frecuentes.
 - 4.3 Perfiles públicos y privados: Ventajas y Desventajas.
 - 4.4 Estrategias docentes.
5. Reflexiones Finales.

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Reglas:

- Escuchar las ideas de tus compañeros.
- Teléfonos en vibrador.
- No dejar de participar, en cada actividad.
- Cada idea cuenta.
- No te quedes con ninguna duda.

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

¿Qué son las Redes Sociales?



Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Según Perdomo, (2010) son:

...aquel lugar virtual que les permite a individuos la interacción social, el intercambio constante de información, intereses, ideas y opiniones. Es una comunidad en constante construcción y remodelación a fin de ser cada vez más completa frente a las necesidades de los internautas...

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Principales Redes Sociales:



→ Se fundó en 1997, por los co-fundadores Sergey Brin y Larry Page y cuenta con una población de 540 millones de usuarios (2014).



→ Se fundó en el 2006, por Jack Dorsey y cuenta con una población de 255 millones aprox. (2014)



→ Se fundó en el 2005, con la coproducción de Chad Hurley, Steve Chen y Jaweb Karim y tiene una población de 1 billón de usuarios (2014)



→ Se fundó en el 2010, con la coproducción de Kevin Systrom y Mike Krieger, con una población de 200 millones (2014).

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Principales Redes Sociales:



→ Se fundó en el 2004 por Mark Elliot Zuckerberg y cuenta con una población de 1.8 billones de usuarios (2014).

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Clasificación de las Redes Sociales:

Por su público objetivo y temática

Redes Sociales Horizontales

→ Son aquellas dirigidas a todo tipo de usuario y sin una temática definida. Por ejemplo: Facebook, Twitter, Orkut, Identi.ca.

Redes Sociales Verticales

→ Están concebidas sobre la base de un eje temático agregador. Pueden ser:

-Profesionales: Viadeo, Xing y Linked In.

-Ocio: Wipley, MinubeDogster, Last.FM y Moterus.

- Mixtas: Yuglo, Unience, PideCita.

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Clasificación de las Redes Sociales:

Por el sujeto principal de la relación

Redes Sociales Humanas

→ Son aquellas que centran su atención en fomentar las relaciones entre personas. Por ejemplo: Koornk, Dopplr, Youare y Tuenti

Redes Sociales de contenidos

→ Las relaciones se desarrolla uniendo perfiles a través de contenido publicado. Por ejemplo: Scribd, Flickr, Bebo, Friendster.

Redes Sociales de inertes

→ Su objeto es unir marcas, automóviles y lugares. Por ejemplo: Respectance.

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

¿Cuáles casos que han conocido o escuchado sobre delitos cibernéticos?



Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales:

- Material Didáctico 1: A Exponer...

Seguridad en Redes Sociales: Delitos Cibernéticos

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales:

- Actividad Grupal #1: "Expón sobre los delitos cibernéticos más comunes dentro de las redes sociales".
- Material Didáctico 2: Delitos Cibernéticos más frecuentes.



Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales: Para tu reflexión

- Video 1: "Lo Malo de las Redes Sociales Si no se controla webmsmall."

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Break



Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales: Para tu reflexión

- Video 2: "Caperucita 2.0: ¿Deberías agregar a extraños a tus redes sociales?"



Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales: Perfiles públicos y Privados.

Ventajas

- Perfiles Públicos**
 - Permiten acceder fácil a ti.
 - Tus publicaciones, llegan a gran cantidad de personas.
 - La publicaciones de eventos tanto corporativos como personales, pueden tener gran publicidad.
 - Permite la propagación de informaciones a gran escala.
 - Permite hacer nuevas vinculaciones o amistades.
- Perfiles Privados**
 - Solo pueden acceder a ti personas que conozcas o le des acceso a tu perfil.
 - Solo a quienes pertenecen a tu círculo de amigos o seguidores, pueden ver tus publicaciones.
 - Tu información solo llega a quienes desees.
 - Permite respetar tu espacio personal.
 - Puedes invitar por estos espacios a las personas cercanas a ti a tus fiestas o eventos.

Seguridad en Redes Sociales: Perfiles públicos y Privados.

Desventajas

- Perfiles Públicos**
 - Tanto personas conocidas como no conocidas, pueden acceder a tu perfil.
 - Acceden a él personas que no conozcas ni están dentro de tu círculo de amistades
 - Corres riesgo de ser una víctima de ciber delitos.
 - Algunas corporaciones, hacen uso de las redes sociales, para los procesos de selección...
- Perfiles Privados**
 - Si eres una corporación o estás interesado en vender una marca o producto, esto podría dificultar el acceso a él.
 - No permite, el acceso a eventos que se busque publicar.

Seguridad en Redes Sociales:

- Actividad Grupal #2: “140 Caracteres una Recomendación”

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales:

- Actividad Grupal #3: Construyamos juntos cinco (5) estrategias a emplear por el docente.

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales: Para tu reflexión

- Video Final: “Uso Seguro de Internet y las Redes Sociales, con seguridad”

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Seguridad en Redes Sociales:

¿Qué te llevas en la maleta?

Material Diseñado por: Paula C Avila, P. Correo: paulaca6@gmail.com

Material Didáctico #1.

Seguridad en Redes Sociales: Delitos Cibernéticos



La data de delitos cibernéticos que se manejan, son los siguientes:

Al menos el 40% de los usuarios de redes sociales tiene abierto el acceso a su perfil a todo el que pase por ellas, sin restricción alguna de privacidad. Entre los menores de 18 años, este porcentaje se eleva al 77%, según un estudio reciente de la AEPD y el Instituto de Tecnologías de la Comunicación.

Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona. Se desconoce en gran medida que los perfiles pueden ser archivados, facilitando la creación de bases de datos de personas con fines ilícitos y del valor que éstos pueden llegar a alcanzar en el mercado. (Herrero, Moreno y Martín, 2003)

Esto es un reflejo sobre el uso inadecuado que se le está dando a los espacios en la red y la forma en cómo socializamos hasta con extraños en estos espacios. El consumo que según la investigación realizada por comScore Inc., como compañía líder mundial en medición digital, en su publicación “El Crecimiento de las redes sociales en América Latina” en el 2011, se indica:

En Junio de 2011, mil cien millones de personas (de edad 15 o superiores accediendo a internet desde sus hogares o trabajo) visitó un sitio de redes sociales a nivel mundial, un aumento del 22% desde Junio 2010. El 81,4% de todos los usuarios de Internet visitan destinos de redes sociales, representando una de las principales actividades online a nivel mundial.

Claramente son parte de nosotros estas redes. Venezuela, es uno de los mercados con mayor penetración dentro de la región de Centro América, con una población de 3,1 millones de audiencia, en el 2011, liderando redes como Facebook y Twitter.

Material diseño por la facilitadora: Paula C Ávila Pérez./ correo: paulaca6@gmail.com

Manzano (2012) en su artículo “Cifras del internet en Venezuela” indica que en los últimos registros proporcionados por la “Comisión Nacional en Telecomunicaciones” existe en el país una población de 12 millones de usuarios en internet, liderando el distrito capital:

El Distrito Capital domina en penetración de internet (92,90% de su población). Además es la entidad con mayor crecimiento interanual con un alza 3,08% en el primer trimestre de 2013, seguido de Miranda (3,09%), Nueva Esparta (1,80%) y Carabobo (1,35%). El estado con menos usuarios de internet es Amazonas con 26.335 y el mayor es Miranda con 2.872.240.

Estos datos empíricos son relevantes, ya que exponen el impacto de estas redes en el país de forma general. Ahora bien, para afianzar la importancia de la propuesta, debemos conocer como es el comportamiento de los usuarios en estos espacios virtuales, como en Venezuela no hay estudios sobre ello se consulto con la publicación del portal de Universia, quien expone los resultados brindados por la encuesta realizada en Colombia, país hermano, por el “Centro de Investigaciones Pew” en el 2013 quienes consultaron con una muestra de 802 adolescentes entre 12 y 17 años y a sus padres, arrojando:

... un 91% aseguró mantener contacto con miembros de su familia, un 98% con amigos del colegio, un 30% con profesores y maestros, y un 33% con personas que nunca han visto en la “vida real”.

Un 91% de los adolescentes incluye una foto suya en su perfil, un 71% da a conocer el nombre de la escuela o instituto al que asisten, y un 20% revela su número de teléfono celular. Por otra parte, el 71% expone su ciudad de residencia, el 82% su fecha de cumpleaños, el 92% su nombre real, el 53% la dirección de su cuenta de correo electrónico, el 62% su situación sentimental, y el 24% aseguró haber subido un video de sí mismo en esta red... mientras que un 26% de estos adolescentes incluye información falsa en su perfil para “desorientar” a los curiosos y proteger así su identidad.

Estas estadísticas exponen una aproximación del panorama en el comportamiento en estas redes por parte de la población adolescente, pudiendo asumir esto como referencia para Venezuela, con respecto a cómo los usuarios se desenvuelven en ellas, queda claro que tienden a brindar mucha información privada y poco a mentir en sus perfiles, para proteger su identidad.

Material diseño por la facilitadora: Paula C Ávila Pérez./ correo: paulaca6@gmail.com

Material Didáctico #2.

Seguridad en Redes Sociales: Delitos Cibernéticos



Las Redes Sociales, se define como:

... aquel lugar virtual que les permite a individuos la interacción social, el intercambio constante de información, intereses, ideas y opiniones. Es una comunidad en constante construcción y remodelación a fin de ser cada vez más completa frente a las necesidades de los internautas (usuarios de internet), quienes buscan un sitio apropiado para convivir con demás personas que, como ya se dijo, comparten sus mismos gustos y aficiones, pero al mismo tiempo relacionarse con gente. (Perdomo, 2011:8)

La seguridad en redes sociales así como las TICs, el internet, la web 2.0 y las redes sociales, se ha convertido en una necesidad imperante. Si bien no se cuenta con una definición, se puede dar una aproximación de ella. Entenderemos por seguridad en redes sociales, como la protección de los datos personales, contenidos, información, integridad y autonomía del usuario. Para alcanzar esta seguridad, se debe ser consciente y crítico de los contenidos que se publican y a quienes se acepta como amigos en estas cuentas, es decir, esta seguridad depende en su mayoría de la precaución o formación que tenga el usuario a la hora de conectarse y hacer público sus datos personales.

La seguridad cibernética, es cada vez más una preocupante para las Naciones y para la educación, pues sin las herramientas necesarias, cualquiera podría ser vulnerado dentro de estos espacios virtuales. Lo indispensables de estos entornos es el uso consciente de ellos, los delitos que más se cometen dentro de las redes sociales, son:

Material diseño por la facilitadora: Paula C Ávila Pérez/ Correo: paulaca6@gmail.com

✓ Grooming:



Para Cortejoso David (2013), se entiende como “como el conjunto de acciones que lleva a cabo un adulto a través de las TIC para ganarse la confianza de un menor, con el fin de obtener un posterior beneficio de índole sexual”. Este tipo de delitos se asocia a patologías como la pedofilia, pederastias y pornografía infantil.



✓ Sextorsión:



Para los autores Molina, García y Aperador (2012), es “una forma de explotación sexual en la cual se chantajea a una persona por medio de imágenes de si mismo desnudo o desnuda que ha compartido a través de Internet o mediante sexting”. El sexting por su parte es “envió de imágenes de desnudos de uno misma vía telefónica, móvil e internet, normalmente ocultando el rostro”. Con esta información privada la persona es extorsionada u obligada chantajes ya sea monetarios o de índole sexual, por parte de su malhechor.



Material diseño por la facilitadora: Paula C Ávila Pérez/ Correo: paulaca6@gmail.com

✓ Ciberbullying:



Para Santander Alejandro (2013), el ciberbullying es un subtipo de violencia que se practica dentro de las redes sociales, expone ante ello “se conoce como el acoso escolar cibernético (ciberacoso o ciberbullying), una violencia que de a poco se ha transformado en el desafío de las escuelas en estos tiempos debido al masivo acceso y contacto permanente de los jóvenes”. Actualmente, el ciberacoso ha aumentado progresivamente a nivel mundial, por ejemplo: La organización Pantallamigas, recolecta los siguientes datos:

-En Chile (2011), se registro que el 878 % de los estudiantes chilenos de 7º curso básico (12 años) a 4º medio (17 años) ha sido víctima de ciber bullying por Internet. Investigación realizada por Universidad Andrés Bello.

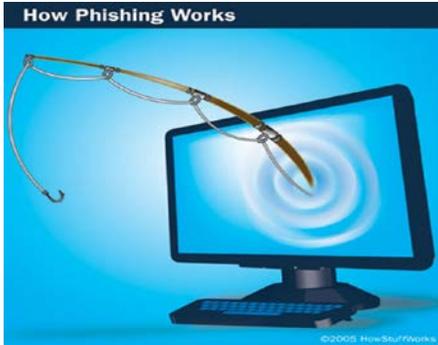
- En Argentina (2011) El 19% de los menores de entre 9 y 17 años de Mendoza (Argentina) sufrieron bullying por Internet o por celular, en forma de insultos, burlas o amenazas. El 11% reconoce haberlo ejercido sobre otros. Investigación realizada por el [Observatorio Internacional de la Violencia Escolar - UCA](#)

- En EE.UU. (2011), El ciber bullying aumentó en los EE. UU. Más del 80% en 10 años. Los investigadores apreciaron un auge desde el 6% que había en 2000 al 9% en 2005 y al 11% en 2010. Investigación realizada por [CCRC, Universidad de New Hampshire](#).

- En Venezuela, según la experiencia de Lacasella (2015), es un delito que inicio en la etapa de bachillerato, pero hoy en día se solicita de su apoyo en charlas dentro de la educación primaria, ya que niños de cuarto grado están siendo víctimas de este delito, situación que es preocupante pues es una clara consecuencia de no asumir políticas formativas preventivas.

Material diseño por la facilitadora: Paula C Ávila Pérez/ Correo: paulaca6@gmail.com

✓ Phishing:



Para Castro Luis (2013), este delito se define como “...término empleado en el mundo de Internet para referirse a una estafa diseñada para obtener información confidencial, como lo son números de tarjetas de crédito, claves de acceso, datos de cuentas bancarias u otros datos personales.”. Este se enfoque en las llamadas estafas online ya sea bancarias o de transacciones en páginas de compra o venta de artículos, se denomina “phishing” porque el pirata informático pesca en la red a sus víctimas. Este delito también se vincula con el plagio de identidad, dado que en este también ocurre una estafa en la identidad de un usuario, es decir, este es plagiado y tienden a utilizar su información bancaria para hacer transacciones.

Quienes comenten estos delitos, tienen diversas denominaciones, sin embargo las básicas son: Hackers o piratas informáticos, estas personas obtienen datos de usuarios de forma fraudulenta dentro de la red, y dependiendo de sus intenciones hacen uso indebido de los datos obtenidos.



Material diseño por la facilitadora: Paula C Ávila Pérez/ Correo: paulaca6@gmail.com

Evaluación post-taller.



Universidad Central de Venezuela
Facultad de Humanidades y Educación
Escuela de Educación



Indicaciones

El siguiente instrumento deberá ser respondido de forma anónima para evaluar la calidad de las estrategias, contenidos, experiencia de aprendizaje y el desempeño de la facilitador (a) durante el taller en taller “Seguridad en Redes Sociales, dirigido a los docentes del área de informático, pertenecientes a la etapa de educación media general”. Se les pide que seleccionen con una equis (x) la opción que mejor le parezca, dentro de la escala de estimación de cada pregunta, solo podrá seleccionar una (1) opción dentro de la escala. Gracias por su colaboración.

1. Con respecto a los contenidos tratados en el taller.

ITEMS	Escala de Estimación			
	Muy Interesantes	Interesantes	Regulares	Malos
¿Cómo considera el tema de “Redes Sociales”?				
¿Cómo percibe el tema de “Seguridad en Redes Sociales”?				

¿Qué le parecieron todos los contenidos expuestos durante el taller?				
--	--	--	--	--

2. Con respecto a las estrategias empleadas:

ITEMS	Escala de Estimación			
	Excelente	Bueno	Regular	Malo
¿Qué le parecieron la organización de los contenidos y estrategias?				
¿Qué le parecieron las estrategias grupales e individuales empleadas?				
¿Qué le parecieron los materiales a emplear en cada una de las actividades?				
¿Cómo percibió las estrategias empleadas dentro del taller?				

3. Con respecto a las actividades:

ITEMS	Escala de Estimación			
	Muy Buenas	Buenas	Regulares	Malas
¿Cómo considera la estrategia del video como medio audiovisual?				
¿Cómo considera las actividades grupales realizadas durante el taller?				
¿Cómo considera las actividades individuales realizadas durante el taller?				
¿Qué le pareció la dinámica general, en la que transcurrió el desarrollo del taller?				

4. Con respecto al desempeño de las facilitadoras:

ITEMS	Escala de Estimación			
	Excelente	Bueno	Regular	Malo
¿Qué le pareció el dominio del facilitador, con respecto a los temas desarrollados?				
¿Qué le pareció el dominio del grupo del facilitador?				
¿Cómo le pareció el dominio de las estrategias del facilitador?				
¿Cómo considera el papel del facilitador durante el taller?				

Recomendaciones y observaciones adicionales:

_____ . ¡Muchas Gracias por su Colaboración! =>



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo, Norelms Alicia Riera Romero titular de la cédula de identidad N° 10626769 de profesión Profesora Lic. Educ. (Magister) TIC. ejercitando actualmente como Profesora UCV - Prof. TIC. en la institución Escuela Educación en la UCV.

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertenecientes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido	X			
Pertinencia de los ítems	X			
Organización del contenido y presentación	X			
Redacción de los ítems.	X			
Claridad y precisión.	X			
Coherencia.	X			

En Caracas a los 20 días del mes de ABR. del 2015.

Firma



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo, M. Claudia Rangelin, titular de la cédula de identidad N° 18.879.679 de profesión Comunicadora Social, ejercitando actualmente como Docente - investigadora en la institución ININCO - UCV.

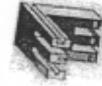
Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertinentes, puede formular las siguientes apreciaciones:

	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Contenido	X			
Pertinencia de los ítems	X			
Organización del contenido y presentación	X			
Redacción de los ítems		X		
Claridad y precisión		X		
Coherencia		X		

En Caracas a los 17 días del mes de abril del 2015.

M. Claudia Rangelin

Firma.



REPUBLICA BOLIVARIANA DE VENEZUELA
 UNIVERSIDAD CENTRAL DE VENEZUELA
 FACULTAD DE HUMANIDADES Y EDUCACIÓN
 ESCUELA DE EDUCACIÓN

CONSTANCIA DE VALIDACIÓN

Yo, VITO LACASELIA, titular de la cédula de identidad
 N° 6964105 de profesión COMUNICADOR SOCIAL
 ejercitando actualmente como DOCENTE POSTGRADO en la
 institución UNIVERSIDAD CENTRAL DE VZLA.

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación al panel de expertos para la Validación de Experto del taller. Una vez de efectuar las observaciones pertinentes, puede formular las siguientes apreciaciones:

Contenido	EXCELENTE	BUENO	REGULAR	DEFICIENTE
Pertinencia de los ítems	X			
Organización del contenido y presentación	X			
Redacción de los ítems.	X			
Claridad y precisión.	X			
Coherencia.	X			

En Caracas a los 23 días del mes de Mayo del 2015

[Firma]
 Firma.