REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD VALLE DEL MOMBOY
DECANATO DE LA FACULTAD DE INGENIERÍA
INGENIERÍA EN COMPUTACIÓN
CARVAJAL ESTADO TRUJILLO

ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA DE LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO

AUTORES:
YORDY ROMERO VALERA
YOANIS JESÚS PÉREZ MACHADO
TUTOR: ING. IVAN PÉREZ

JUNIO, 2018

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD VALLE DEL MOMBOY
DECANATO DE LA FACULTAD DE INGENIERÍA
INGENIERÍA EN COMPUTACIÓN
CARVAJAL ESTADO TRUJILLO

ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA DE LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO

Trabajo Especial de Grado, presentado como requisito para optar al título de Ingeniero de Computación

AUTORES:
YORDY ROMERO VALERA
YOANIS JESÚS PÉREZ MACHADO

TUTOR: ING. IVAN PÉREZ

Carvajal, 2018.

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD VALLE DEL MOMBOY
DECANATO DE LA FACULTAD DE INGENIERÍA
INGENIERÍA EN COMPUTACIÓN
CARVAJAL ESTADO TRUJILLO

APROBACIÓN DEL TUTOR

En mi carácter de tutor del Trabajo Especial de Grado, titulado: ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA DE LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO, presentado por: YORDY ROMERO VALERA y YOANIS JESÚS PÉREZ MACHADO. Considero que el mismo reúne los requisitos necesarios para ser sometido a la evaluación correspondiente, razón por la que apruebo la entrega del mismo y solicito nombramiento del jurado examinador correspondiente.

En CARVAJAL, a los 04 días del mes de Julio de 2018.

Tutor 4.884.156

iii

AGRADECIMIENTO

En este Día, al finalizar esta meta, quiero expresar mi más sincero agradecimiento, a todas aquellas personas que me orientaron y ayudaron.

A Dios, por ser mi guía y sabiduría en los momentos ms difíciles de esta investigación.

A mi tutor, Ing. Iván Pérez, quien se convirtió en un profesor consejero y amigo. Gracias por tu dedicación y orientación, por brindarme su apoyo en el trabajo elaborado. Muchas gracias.

A mis maestros. Claribel, Corina, Hellys, Sandra, Carlos, Larry, betzabeth por su gran apoyo y motivación para la culminación de nuestros estudios profesionales y para la elaboración de este trabajo, por su tiempos compartidos y por impulsar el desarrollo de nuestra formación profesional. Muchas Gracias.

A todas aquellas personas, que de alguna u otra forma me acompañaron para la culminación de este logro.

A TODOS MUCHAS GRACIAS…

AUTORES:
YORDY ROMERO VALERA
YOANIS JESÚS PÉREZ MACHADO

DEDICATORIA

Hoy siento una inmensa alegría, porque uno de mis sueños se ha realizado.

A mi Señor Jesús, quien es mi Dios Todopoderoso y Padre Celestial, el cual es fuente de toda sabiduría y amor, quien me dio la fuerza en los momentos más difíciles y cruciales de mí vida.

A mi padre, el Sr. Domiciano Romero, sé que en estos momentos te sientes muy orgulloso por el logro que hoy alcanzo. Gracias por sr un padre ejemplar y siempre brindarme tu amor y apoyo incondicional, enseñándome a ser constante en los momentos más difíciles. Te Amo.

A mi madre, Yoly Valera de Romero, quien fue la mujer que dios uso para darme la vida, gracias por tu amor, comprensión y todas las oraciones que me mantuvieron luchando, a pesar de muchas veces no tener fuerzas. Gracias por tu ejemplo de superación. Te amo.

A mi novia, María José Arango Suárez, quien es mi compañía perfecta y por supuesto mi ayuda idónea, Gracias porque siempre me apoyas en mis locuras, hazañas y en mis decisiones más importantes. Gracias por ser mi esperanza y ánimo en los momentos más difíciles. Este logro es de Ambos porque eres parte de mi vida. Te Amo.

A mi sobrina, Valeria Valentina Romero Araujo, un rayito de luz en momentos difíciles. Dios te bendiga hoy y siempre, hasta que Dios decida separarnos. Te Amo.

A mi hermano, Yovanny Romero Valera, con este logro espero haberte cumplido tu petición, Gracias por tu carisma y alegría que me regalas a diario. Siempre te llevare en mi corazón y recuerda siempre luchar por tus metas como tú me enseñaste, no importa si son altas como el cielo, si quieres puedes alcanzarlas.

A mi abuela, María de Valera, Gracias por tus sabios consejos, por tu cariño incondicional.

A mis tíos y tías, Orlando, José, Gregorio, Rafa, Bernabé, Samuel, Carlos, Dairi, Leonor, Carolina, Yarelis. Gracias por su apoyo incondicional y ejemplo de superación. Los Aprecio.

A mis primos y primas, quienes son mi fuente de alegría, que este triunfo sirva de ejemplo para sus vidas, En especial para ti Greiry Rodríguez que me brindaste tu apoyo y consejos siempre serás la mejor prima. Los Quiero.

A mi suegra y cuñado, Marleny Peña, José Arango, por sus buenos deseos y palabras de aliento y de superación en todo momento.

A mis amigos, Jesús Machado, Carlos Trujillo, Hugo Gil, Gracias por estar siempre a mi lado y brindarme una amistad sincera en toda mi vida. Juntos ayudaron hacer este sueño realidad. Siempre formaron parte de mi vida.

A mis padres espirituales, mis pastores Presidente de la Iglesia Pentecostal Unida de Venezuela Reverendo Alirio Ferreira y la pastora Lcda. Yajaira de Ferreira, quienes han sido de mis ayudas más grandes. Gracias por su ejemplo intachable, en todos los aspectos de sus vidas. Dios los bendiga en todo momento.

a mis maestros, aquellos que marcaron cada etapa de nuestro camino universitario, y que me ayudaron en asesorías y dudas presentadas

Y por último, pero no menos importante, a todas aquellas personas que ahora no menciono, pero siempre están presentes en mi corazón, les doy gracias por formar parte de este momento tan importante en mi vida.

YORDY ROMERO VALERA

DEDICATORIA

A Dios. Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre, Pilar Elena Machado. Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor. Te amo.

A mis hermanos, Juan José Godoy Machado, Ivana Paola Rodríguez Machado, por estar conmigo y apoyarme siempre, los quiero mucho. Te amo.

A mis abuelos, Ernesto José Machado, Elsy Escorihuela, por quererme y apoyarme siempre, esto también se lo debo a ustedes.

A mi novia, Yoselin Betania Pacheco, Gracias porque siempre me apoyas en mis sueños, metas y en mis decisiones más importantes. Gracias por ser mi felicidad y ánimo en los momentos difíciles. Este logro es para ti. Te amo.

A mis amigos. Que nos apoyamos mutuamente en nuestra formación profesional y que hasta ahora, seguimos siendo amigos: Hugo Leonardo Gil, La Empresa Inproandes C.A, LOS SEÑORES Henry Esposito, Amalio Esposito y Juan Carlos Godoy, Karley Hernández, a Yordy Romero por haberme ayudado a realizar este trabajo.

Finalmente, a Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben que siempre están presentes en mi corazón. Gracias por su apoyo incondicional así mí.

YOANIS JESÚS PÉREZ MACHADO

ÍNDICE GENERAL

LISTA DE TABLAS Y GRÁFICOS

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD VALLE DEL MOMBOY
DECANATO DE LA FACULTAD DE INGENIERÍA
INGENIERÍA EN COMPUTACIÓN
CARVAJAL ESTADO TRUJILLO

ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA DE LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO

AUTORES:
YORDY ROMERO VALERA
YOANIS JESÚS PÉREZ MACHADO
TUTOR: ING. IVAN PÉREZ
Año: 2018

RESUMEN

Esta investigación se desarrolló para cumplir con el objetivo de determinar el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo. Se trató de una investigación descriptiva, con diseño de campo. La población estuvo constituida por 500 integrantes de la Facultad de Ingeniería de la Universidad Valle del Momboy, de los cuales 200 pertenecen a Ingeniería en Computación, por lo que se decidió tomar una muestra a conveniencia y al azar del 10% para un total de 20 sujetos entre profesores y estudiantes.Se aplicó un instrumento de 43 ítems. El mismo fue validado por un panel de expertos y su confiabilidad resultó muy alta 0,9 con el Coeficiente de Cronbach. Se concluye que el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, es muy bajo para denunciar el ciber-delito, pero igualmente muy poco contribuyen con los conocimientos adquiridos y habilidades desarrolladas para demostrar y aclarar la ocurrencia del mismo. Sin embargo, no basta el conocimiento y habilidad para manejar software y hardware de última generación, debido a que cada día cobra vigencia la necesidad de desarrollo empresarial y apertura de nuevos empleos como alternativa básica liberadora, no antagónica al desenvolvimiento laboral de jóvenes profesionales, donde la percepción de la realidad les ofrece oportunidades para contribuir con la justicia y paz ciudadana.

Palabras clave: delito – ciber – acoso – estudiantes - universitarios.

INTRODUCCIÓN

Aunque el estudiante de ingeniería en computación se forma durante la escolaridad para el análisis de sistemas de información, uso de lenguajes de programación, diseño y uso de hardware y software para lograr avanzadas aplicaciones temáticas y científicas, esa misma formación no le exenta de la posibilidad de ser objeto o conocer el delito del acoso cibernético o ciberacoso definido como ‘’amenazas, hostigamiento, humillación u otro tipo de molestias realizada por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación’’ (Pinto, 2018), es decir, internet, telefonía móvil, correo electrónico, mensajería instantánea, video consolas online, entre otros y cuando esto ocurre con menores se denomina ciberbulling, todo con la finalidad de socavar la autoestima o dignidad personal, además de dañar el estatus social.

De hecho, mientras que la tecnología busca favorecer la vida e interacción humana, el mismo acceso globalizado de la información facilita a personas maniobrar palabras, frases y hasta introducir nuevo vocabulario como phising, carding, o ciberbullying, que son parte del paisaje digital en los últimos años y le atañen cierto grado de compromiso legal al profesional de la computación en función de aclarar o demostrar la ocurrencia o falsedad del mismo ante la sociedad y organismos competentes.

Con base en lo expresado, se fijó como propósito de investigación determinar el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo. Tal objetivo se desarrolló en cinco capítulos compuestos por:

En el Capítulo I, El Problema, se describe la problemática planteada en la empresa, los objetivos generales y específicos, además de la justificación, presentando claramente las razones por los cuales se cumple el estudio.

En el Capítulo II, Marco Teórico Referencial, donde se reseñan los antecedentes basados en investigaciones relacionadas con el tema tratado, los fundamentos teóricos y las referencias conceptuales, con la finalidad de exponer las bases teóricas que sustentan la investigación, bases legales y Operacionalización de la variable.

En el Capítulo III, Marco Metodológico, se describe el tipo de investigación, la población, la muestra, las técnicas de recolección de datos, y las técnicas de análisis de datos, con las cuales se indica la forma como se usarán los instrumentos para recabar datos y presentar los resultados.

Capítulo IV, Análisis de Resultados, donde se desarrollan los objetivos propuestos a través de la aplicación del instrumento de recolección de información y el análisis de los hallazgos.

Capítulo V, Conclusiones y Recomendaciones, donde se muestran los resultados obtenidos.Por último, se presentan las referencias bibliográficas y los anexos, con lo cual se finaliza el estudio.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

Planteamiento del Problema

Los adelantos y avances tecnológicos a nivel mundial, no solamente han facilitado la calidad de vida y comercio global, sino también han dado lugar a vacíos estratégicos y jurídicos que los Estados tardaron en enfrentar siendo necesario un cambio de paradigma y tratados internacionales para lograr una implementación apropiada a las estrategias para la prevención, protección y persecución de quienes participan en actos de Ciberguerra y Ciberacoso.

Este tipo de Ciberdelincuencia ha ocasionado que los Estados coordinen esfuerzos para prevenir ataques informáticos en los sistemas de información de los recursos básicos como el petróleo, material radiactivo-nuclear que pueden llegar a ser manejados remotamente, esto es, sin intervención de personas físicas. Al respecto, se tiene como ejemplo el caso de Stuxnet, un troyano instalado en el sistema operativo Windows de Irán, con un sistema llamado Scada producido por la compañía Siemens; este troyano estaba planificado para la destrucción de la infraestructura crítica del gobierno iraní (Aguilar, 2011).

Indudablemente, la Ciberdelincuencia no solamente busca la confrontación del conflicto gubernamental, sino también, contra civiles, ciudadanos comunes, inclusive niños, niñas, adolescentes y hasta estudiantes universitarios. De hecho, Rodríguez (2012: 54) explica ‘’los ciberdélitos son una nueva realidad cotidiana con casos que tienen que ver con ciberbullying o ciberacoso, existiendo una abundante y variada casuística: delitos contra la intimidad, estafas, daños por intrusión en sistema ajenos, distribución de pornografía, entre otros’’.

En el caso del acoso cibernético o Ciberacoso, según un estudio publicado por la Universidad de Guadalajara de México, uno de cada cinco estudiantes universitarios sufre o ha sufrido alguna vez ciberacoso entre iguales. La encuesta, realizada entre más de 2.000 jóvenes del Centro Universitario de Ciencias Económico-Administrativas, revela que el 38% de estudiantes recibe insultos permanentemente por la red; el 29% fue ridiculizado; el 25% fue acosado sexualmente; el 15% recibió amenazas y 18% sufrió el robo de sus contraseñas. También se confirma que el celular es actualmente la herramienta más utilizada para ejercer el ciberhostigamiento. Según la Universidad de Guadalajara, el acceso a Internet a través del smartphone permite prolongar el acoso de manera casi ilimitada, lo que sin duda genera efectos psicológicos devastadores en la víctima (Pinto, 2015).

En Colombia, Redondo y col. (2017) explica que desde hace aproximadamente dos años, comenzó el interés por estudiar los comportamientos asociados con el ciberbullying, no siendo esto suficiente para identificar las problemáticas asociadas a este hecho, destacando además las escasas investigaciones psicológicas sobre el tema en el ámbito universitario colombiano y los pocos estudios publicados que se relacionan con su impacto psicológico.

Sin embargo, el acoso cibernético en las universidades no siempre se da entre estudiantes, por cuanto también es percibido contra docentes o profesores al convertirse estos en víctimas acosados. Según Pérez (2013), cada vez es mayor el abuso contra el maestro y de acuerdo a investigación realizada en el Reino Unido, 35% de profesores han sido víctimas de ciberacoso por parte de los estudiantes utilizando las redes sociales con el apoyo de la familia.

En Venezuela, argumenta Pérez (2013), la escases de cifras oficiales y trabajos científicos respecto a la problemática del ciberacoso a nivel universitario, bien sea con profesores o estudiantes, aunque se estima que

cada 9 de 100 habitantes sufre de algún tipo de violencia y en efecto se han reportado casos de profesores agredidos físicamente por alumnos y sus padres. En efecto es notorio que la mayoría de estudiantes universitarios disponen de teléfonos celulares convertidos en objetos imprescindibles para mantener sus relaciones sociales durante muchas horas con impacto abusivo, obsesivo y hasta problemático o adictivo que facilita participar en actos de ciber acoso, ya sea para acosar, hostigar o intimidar a otros, o simplemente convertirse en cibervíctimas.

Es importante recordar que la etapa universitaria representa un periodo de transición para que el estudiante logre la independencia familiar, obtenga nuevas amistades, empleo o reconocimiento social, eventos que pueden llevar a un cambio del uso de internet, celular y redes sociales desde la perspectiva positiva hacia una esfera negativa relacionada con el ciberacoso, situación que convierte a este grupo en una población especial para el estudio de los comportamientos relacionados con el cibereacoso, más aun si se trata de estudiantes de ingeniería de computación cuya formación proporciona herramientas para reconocer o modificar contraseñas, bases de datos, entre otras acciones que alteran o recuperan evidencias cibenéticas.

Sin embargo, ante tales realidades de los ciberdélitos y cibereacoso, el estudiante o ingeniero en computación, no solamente está en el derecho de defenderse como miembro de un Estado Político para vivir en paz, sino que también tiene la posibilidad de orientarse por una salida profesional poco conocida como lo es la actuación como perito en el área cibernética, dada la variedad de temas informáticos por enfrentar en una actividad que renta honorarios profesionales debido al aumento de delitos cibernéticos.

Tomando en cuenta lo anteriormente expuesto se formula la siguiente interrogante:

¿Cómo se da el fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo?

Objetivos de la Investigación

Objetivo General

- Determinar el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo.

Objetivos Específicos

- Identificar el índice de acoso cibernético en los miembros de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo.
- Diagnosticar la reacción personal ante el delito de acoso cibernético dentro y fuera de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo.
- Identificar la capacidad de colaboración para enfrentar incidentes de impacto público de acoso cibernético.

Justificación de la investigación

Esta investigación tiene como propósito fundamental determinar el manejo realizado al fenómeno del acoso cibernético, por estudiantes de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, por cuanto el ciberacoso aumenta el grado de inseguridad en la víctima, provocando sentimientos de poca defensa y desprotección al desconocer a la persona agresora que se inclina en generar sentimientos de impotencia.

Desde el punto de vista teórico, en el estudio se considera al acoso como un problema social complejo cuyo autor está mentalmente perturbado debido a una relación íntima previa por el acosado, y quien manifiesta su conducta con carácter repetitivo, agresivo y poderoso para dominar al agraviado y obligarle a cumplir con los pedidos o deseos del perpetrador. Es amplía la gama del impacto del acoso sobre la víctima, resaltando al respecto

los trastornos psicológicos, daños a la propiedad, dificultades económicas, lesiones físicas y asalto sexual.

A nivel práctico, el estudio abre la posibilidad al participante de ingeniería en computación, para especializarse con los conocimientos y habilidades que ayuden en los juicios y tribunales a esclarecer delitos cibernéticos relacionados con el bullying donde el canal principal son las computadoras, teléfonos inteligentes, tablets, internet, redes sociales, entre otros dispositivos que almacenan los datos que proporcionan las evidencias electrónicas irrefutables esenciales para resolver el conflicto.

Desde el punto de vista social, se justifica el estudio al permitir reconocer la responsabilidad social del perfil del estudiante de ingeniería en computación para evitar espionajes, fraudes, robos de información, manipulación de datos y programas, entre otros que pueden ocasionar grandes pérdidas económicas y laborales. Es la escolaridad de la carrera de ingeniería en computación la que facilita la adquisición de tales habilidades profesionales y por tanto, la pericia personal debe ser cuidadosa en su uso y aplicación.

En lo metodológico se justifica el estudio al seguir los lineamientos del Trabajo de Grado de la Facultad de Ingeniería de la Universidad Valle del Momboy, con el uso de la Encuesta de Obsesión Intrusiva Relacional (ORI-82) de Spitzberg y Cupach (2014) retomando la Subescala de Contacto Mediado, que se compone de 30 reactivos con formato de respuesta tipo Likert de cinco opciones, validadas internacionalmente. Este instrumento considera como dimensiones: Vigilancia remota, Búsqueda de interacción, Desprestigio social, Acercamiento gradual y Hostigamiento Sexual.

Delimitación de la investigación

La presente investigación se realizó en un tiempo comprendido de Febrero a Mayo del 2018, es importante señalar que esta etapa se considera suficiente para cubrir los objetivos previstos en la investigación y corresponde al año escolar 2017- 2018. Es prudente señalar que el investigador durante este tiempo estuvo inmerso de manera continua, organizada y sistemática en los procesos de diagnostico, diseño de registro y análisis de la información obtenida.

En cuanto al espacio y la población objeto de estudio se considera la parroquia Carvajal del Municipio San Rafael de Carvajal en el Estado Trujillo Venezuela, y dentro de ellos los estudiantes de la Escuela de Ingeniería de la Universidad Valle del Momboy, los cuales se seleccionaron de manera aleatoria.

CAPÍTULO II
MARCO TEÓRICO REFERENCIAL

El contenido de este capítulo está referido a los antecedentes y las teorías que sustentan la realización de este estudio, los cuales requieren ser conceptualizados; así como, relatados a través de experiencias producto a otras investigaciones que sirvan de aporte al mismo para fortalecer y profundizar los conocimientos sobre las dimensiones de la variable.

Antecedentes de la investigación

Según Arias (2012: 106) los antecedentes de la investigación “reflejan los avances y el estado actual del conocimiento en un área determinada y sirven de modelo o ejemplos para las futuras investigaciones”, es decir, se refieren a los estudios previos que guardan relación con el objeto de investigación. A continuación se presentan algunos trabajos de investigación que fundamentan y sustentan el presente estudio.

En Colombia, Redondo y col (2017) realizaron ‘’Impacto Psicológico del Ciberbullying en Estudiantes Universitarios’’, con el objetivo de determinar la prevalencia del ciberbullying entre los participantes del estudio, así como conocer el impacto psicológico tanto en cibervíctimas como en ciberagresores, analizando además las diferencias de género de dicho impacto. La muestra estuvo constituida por 639 estudiantes de la Universidad Pontificia Bolivariana, seccional Bucaramanga, con una media de edad de 17,6 años (chicos N = 303, chicas N = 334). Para ello se emplearon los siguientes instrumentos: (a) Escala de ciberagresiones; (b) Escala de cibervictimización; y (c) Symptom Assessment-45 Questionnaire (SA-45). Los resultados evidencian que un 27,5% de la muestra ha sido agredida en alguna ocasión, así como que 26,7% ha sido acosador durante el último año.

Por otro lado, los resultados demostraron que existe un impacto psicológico (escalas del SA-45) tanto en las cibervíctimas, como en los ciberagresores. Respecto a las diferencias de género en ciberbullying se evidenciaron solo en algunas escalas (primordialmente depresión, ansiedad, sensibilidad interpersonal y somatización), aunque no fueron significativas entre los síntomas psicológicos reportados en este estudio (salvo en las escalas relacionadas con Somatización y Ansiedad fóbica).

Queda demostrado como aporte de este estudio que en cualquier momento de la vida un estudiante o profesional puede ser acosado o acosador a través del ciberespacio y esto por ende genera efectos psicológicos que deben atenderse y denunciarse ante los organismos competentes, valiéndose para ello de la credibilidad de expertos.

La investigación realizada en México por el Instituto Nacional de Estadística y Geografía (INEGI, 2018) revela que los universitarios son quienes más sufren hostigamiento virtual, pues del total de quienes han sido víctimas de esto, el 39.1 por ciento son estudiantes de nivel superior, 28.5 son de nivel medio superior, 17.7% son de nivel básico y 8.3 por ciento no tienen escolaridad.De los estudiantes de nivel superior, quienes más sufren acoso son los hombres con 39.1%; en el nivel medio superior, también sobresale que son los varones los más acosados con 31,1%.En lo que respecta al nivel básico, tanto hombres como mujeres sufren ciberacoso y en el caso de las personas que no reportan escolaridad, la mayor parte son varones.Asimismo quienes más sufren acoso son las personas de 20 a 29 años de edad, seguidos por el grupo de 12 a 19 años; en tercer lugar el grupo de 30 a 49 años y el grupo con menor problema por acoso virtual es el de personas mayores de 50 años.

Se considera como aporte de este estudio a la presente investigación lo relevante de demostrar que los hombres adultos contemporáneos menores de 30 años, son blanco fáciles para el ciberacoso ya sea relacionado con

aspectos laborales, de romance, familiar o sexual, que colocan en riesgo su estabilidad emocional, seguridad física y bienestar ciudadano.

Retana, B. y Sánchez, R. (2015) realizaron ‘’Acoso Cibernético: Validación en México del ORI-82’’ con el propósito de validar en México la subescala de la Encuesta de Intrusión Obsesiva Relacional de Contacto Mediado (Spitzberg&Cupach, 2014). Para ello participaron 717 personas (504 mujeres y 204 hombres) que reportaron haber sido víctimas de acoso. Se realizó el procedimiento de validez y confiabilidad de Reyes Lagunes y García y Barragán (2008) y se obtuvo una medida con propiedades psicométricas robustas e interesantes, identificándose cinco factores: vigilancia remota, búsqueda de interacción, desprestigio social, acercamientos y violencia. El instrumento resultó válido y confiable en la cultura mexicana y puede ser utilizado por clínicos para evaluar el tipo de acoso percibido por sus pacientes, así como ser ampliado, corregido y reaplicado para fines de investigación.

Se toma como aporte de esta investigación al presente estudio el modelo de escala para determinar índice de ciberacoso, la cual sirvió de guía en la elaboración del instrumento para recolectar información en la Facultad de Ingeniería de la Universidad Valle del Momboy.

En Ecuador, Cañarte (2017) presentó ‘’Cyberbullying: el acoso a través de las redes sociales en jóvenes universitarios’’, basada en una investigación cualitativa, descriptiva y transversal, en los estudiantes de la Facultad deInformática de la Universidad Laica “Eloy Alfaro” de Manabí, en la ciudad de Manta, República deEcuador, durante el periodo 2015, a fin de determinar las experiencias de victimización a través de lasnuevas tecnología en jóvenes universitarios. La población de estudio estuvo conformada por 50jóvenes. El análisis se llevó a cabo a partir de categorías en lugar de variables dependientes eindependientes.

En la serie se obtuvo que el 80.0 % de las mujeres plantearon haber sido molestadaso acosadas por internet, el 60.0% en los hombres; actos de violencia por medio de las nuevastecnologías que prevaleció fue el insulto, el 100 % de los cyber acosados han sido en algún momentomolestados por medio del internet como insultos, acoso sexual. Infortunadamente, el acoso y el cyberacoso son conductas violentas que se han naturalizado. El uso de redes sociales, como forma deinteracción humana, ha supuesto una prolongación de actividades delictivas.

Se demuestra como aporte de este estudio a la presente investigación el acto del insulto como principal forma de agresión a través del móvil celular y demás redes sociales tan utilizadas por estudiantes universitarios dentro y fuera de la Facultad de Ingeniería de la Universidad Valle del Momboy.

En España Polo del Río y col. (2017) realizó ‘’Abuso del móvil en estudiantes universitariosy perfiles de victimización y agresión’’, con la finalidad de estudiar las repercusiones sociales,personales y comunicacionales del abuso del móvil de los estudiantesuniversitarios, y profundizar en los diferentes perfiles del ciberacoso,analizando quién presenta más problemas personales y sociales con eluso del móvil: ¿víctimas o agresores? También si el número de horasde uso del móvil tiene un efecto sobre dichos problemas. La muestra(1200 estudiantes) fue seleccionada mediante muestreo polietápicopor conglomerados de entre las distintas Facultades de la Universidadde Extremadura.

Los datos fueron obtenidos a través de las Escalasde Victimización (CYB-VIC) y Agresión (CYB-AGRES) a través delTeléfono Móvil y el Cuestionario de Experiencias relacionadas con elMóvil (CERM). Los resultados muestran que el uso abusivo del móvilgenera conflictos en los jóvenes de ambos sexos; aunque las chicasmanifiestan más problemas comunicacionales y emocionales que loschicos. Además, la edad, el campo de conocimiento, el perfil víctima/agresor y las horas de uso del móvil son

variables determinantes sobrelos conflictos comunicacionales y emocionales derivados del usoabusivo del móvil.

Se considera como aporte fundamental de esta investigación al presente estudio la importancia de usar racionalmente la telefonía móvil a modo de minimizar el impacto negativo cuando se transmiten mensajes o se establecen conversaciones con personas conocidas o desconocidas con todo el derecho a vivir una vida libre de violencia.

BASES TEÓRICAS

De acuerdo a Arias (2012), constituyen “un conjunto de conceptos y proposiciones que constituyen un punto de vista o enfoque determinado, dirigido a explicar el fenómeno o problema planteado”. Pueden subdividirse de acuerdo a su naturaleza en psicológicas, filosóficas, pedagógicas, legales, entre otras. En este caso se considera el tema del ciberacoso y el rol del ingeniero en computación para reconocer el mismo.

Acoso Cibernético o Ciberacoso

En su conceptualización general, el ciberacoso implica el uso de las tecnologías de la información y la comunicación como plataforma de una conducta intencional, repetida y hostil de un individuo o de un grupo para hacer daño a otros (Ortega, Calmastra, y Mora, 2008). El ciberacoso es el acoso virtual y al igual que el acoso interpersonal, está el acosador, la víctima y los testigos.Es importante saber que a pesar del aparente anonimato de los ciberacosadores, su cuenta queda registrada en internet y pueden ser ubicados.El ciberacoso es una forma de violencia realizada a través de las tecnologías.

Igualmente, el delito del acoso cibernético o ciberacoso definido como ‘’amenazas, hostigamiento, humillación u otro tipo de molestias realizada por

un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación'' (Pinto, 2018), es decir, internet, telefonía móvil, correo electrónico, mensajería instantánea, video consolas online, entre otros y cuando esto ocurre con menores se denomina ciberbulling, todo con la finalidad de socavar la autoestima o dignidad personal, además de dañar el estatus social. Es una problemática que se ha venido acentuando dada la facilidad con la que se utilizan diversos medios, como los correos electrónicos, chats, mensajes de texto y, recientemente, redes sociales.

Como antecedente, vale la pena mencionar que cuando se empezó a estudiar el fenómeno del ciberacoso en la literatura científica este se identificaba bajo el término acoso online (Finkelhor, Mitchell y Wolak, citados en Ortega, 2010) y se analizaba el riesgo de la Internet para la población juvenil. Entre los riesgos estaban "las amenazas y las conductas violentas" realizadas por medio de la Red (p. 9). Así, a finales del año 2006, en el Congreso de la Sociedad de Psicólogos Londinenses, el equipo de investigación de Peter K. Smith presentó los primeros datos bajo el nombre de cyberbullying.

Respecto a los elementos característicos del ciberacoso, Ortega, Del Rey y Casas (2013b) identifican tres: la agresión puede suceder en cualquier momento y en cualquier lugar, con la consecuente dificultad de desconectarse del contexto, ya que los canales de comunicación siempre están abiertos; la agresión puede ser observada por una gran cantidad de espectadores, un número indefinido de veces; es posible que las víctimas nunca lleguen a conocer a sus agresores, debido al anonimato que permiten los medios que se utilizan.

El agresor, al igual que en el bullying, es alguien que puede tener alguna problemática familiar o personal. En el caso del ciberbullying también pueden ser personas que no tienen amigos y por lo tanto utilizan una computadora o cualquier dispositivo móvil para acosar, intimidar o agredir a

otros, incluso, llegan a alterar sus horarios para dormir, pues se desvelan por estar al pendiente de su víctima.

Kowalski y Limber (2007), explicanque aunque no hay una agresión de tipo física como en el bullying, el ciberbullying afecta emocionalmente a las víctimas, pues alguien que es bombardeado por ofensas, amenazas o insultos ve mermada su salud, al no poder dormir, tener pesadillas y terrores nocturnos, sobre todo si la víctima es un niño.Alguien que es víctima de ciberbullying constantemente está revisando su celular o sus redes sociales para ver si han dicho algo en contra de él o, por el contrario, puede ser el último que se entere de lo que se está hablando sobre su persona.

Maple, Short y Brown (2011) refieren que el acoso cibernético inflige la misma cantidad de daño psicológico que el real y que muchas víctimas sufren de trastorno de estrés postraumático. Por sus parteKowalski y Limber (2007) reportan que el acoso cibernético, es un tipo de acoso más indirecto y relacional que otro tipo de maltrato. Ciertamente, muchas agresiones cibernéticas son relacionales; buscan provocar un daño en el círculo de amistades de la víctima con la difusión de rumores y secretos, suplantación de la identidad o bien en su percepción de pertenencia a un grupo.

En lo referente al tipo de ciber agresiones McKennay col (2002)la clasifica en: 1) hostigamiento (envío repetido de mensajes ofensivos a la víctima); 2) denigración (difusión de rumores falsos sobre la víctima); 3) suplantación de la identidad (envío de mensajes maliciosos haciéndose pasar por la víctima); 4) violación de la intimidad (difusión de secretos o imágenes embarazosas de la víctima); 5) exclusión social (exclusión deliberada de la víctima de grupos virtuales) y 6) ciber-persecución (envío repetido de mensajes amenazantes a la víctima).

Más recientemente, Ogilvie (2012) refiere que el acoso cibernético puede adoptar diversas formas:

(a) Acoso por e-mail es la forma más común, implica el envío de correos electrónicos no solicitados, que pueden referir el odio, mensajes obscenos o amenazantes (McGraw, 1995). Además el envío de correos electrónicos no deseados, también conocidos como spam, o el envío de virus de manera repetitiva para intimidar al receptor. El acoso a través de e-mails incorpora las características de las llamadas telefónicas y el envío de cartas, por la inmediatez y el anonimato que garantiza el e-mail.

(b) El acecho por el internet, se refiere a que las personas visitan los sitios web que fueron utilizados por la víctima para grabar sus movimientos virtuales. Con esta información, lo que se hace es subir datos falsos sobre la persona en los sitios web que frecuentan y en otros sitios web como pueden ser los pornográficos (Gilbert, 1999).

(c) Acecho por en el manejo de la computadora, este es el más grave de las tres formas, y se produce cuando el acosador explota el funcionamiento de Internet y el sistema operativo con el fin de asumir el control de la computadora de la víctima. Un ejemplo de ellos es prender la cámara o abrir las unidades de CD-ROM por mencionar un ejemplo.

Es importante mencionar que el acoso cibernético puede comenzar por medio de apoyos cibernéticos pero pronto puede cruzar a más formas físicas de acoso (Spence-Diehl, 2003), esto implica que tanto los acosadores físicos como los acosadores cibernéticos pueden reaccionar agresivamente cuando son rechazados, humillados o despreciados por la víctima (Reno, 1999).

Aunque se ha encontrado esta vinculación entre tipos de acosos (físico y cibernético, por ejemplo), en el mediado por el uso de la tecnología no se necesita de ninguna confrontación física para alcanzar el nivel de angustia en la víctima (Reno, 1999). Esto se da puesto que el mundo de internet crea una falsa sensación de intimidad entre el acosador y la víctima y por lo tanto da lugar a una mala interpretación del acosador (McKenna, Green &Gleason, 2002) a la vez que -en la mayoría de los casos-, la víctima en línea no es

capaz de medir la intención de la persona con la que se comunica, debido a que el Internet proporciona un medio para compartir penas y alegrías con un oyente sin rostro (Finn, 2004); por lo tanto, la víctima puede darse cuenta muy tarde que está siendo objeto de acoso por parte de su acosador.

Dentro de este contexto, el ciberacoso puede darse a través de:

Vigilancia remota: Puede darse con el monitoreo, vigilancia y hostigamiento de la víctima y consiste en una plataforma híbrida de contribución de vídeo más avanzada y completa, utilizando el sistema, las fuerzas de campo pueden capturar y transmitir perfectamente vídeo de alta calidad en vivo a sus centros de mando, aprovechando las redes 3G / 4G, Wi-Fi, Ethernet y satelitales disponibles.

Un sistema completo de Vigilancia remota a distancia por Internet, no necesita un ordenador para transmisión de imágenes y sonido a través de Internet, tampoco para su visualización. Hoy en día sirve cualquier teléfono Móvil, PDA, Televisor con un decodificador o cualquier ordenador conectado a Internet. Un sistema de Televigilancia permite con una simple contraseña, visualizar, escuchar o hablar desde un lugar remoto (Henostroza, 2016).

ICAM es la manera fácil de configurar video vigilancia remota, usando el smartphone para mantener un ojo en nuestras cosas mientras estamos fuera. Ya sea usando smartphones de Apple o Android.Cualquiera con un ordenador y un smartphone puede crear su propio sistema de video vigilancia con un poco de esfuerzo y sin gastar mucho dinero.

Búsqueda de interacción: Puede ocurrir con la notificación reiterada de mensajes que busquen alterar el estado de bienestar del acosado. Sin embargo, en la actualidad es más fácil buscar personas y encontrarlas, ya sea utilizando los buscadores oficiales de las plataformas sociales, como Facebook y Twitter, o usando otras herramientas de búsquedas como Google o Bing. Sin duda una potente herramienta para buscar personas en redes

sociales es el Social Searcher. Lo único que debe hacerse es introducir las palabras clave en el buscador Social. Luego, la herramienta mostrará los resultados de las menciones en todas las redes sociales más importantes, como Facebook, Twitter, Google+, Instagram y Tumblr (Henostroza, 2016).

WinkPeopleSearch, esta herramienta te permite encontrar a las personas que buscas en las diferentes redes sociales. Se puede buscar ingresando los datos, como su nombre, ubicación, escuela, trabajo, intereses, y mucho más.WinkPeopleSearch es igual que un motor de búsqueda normal, pero se centra buscar los perfiles que están en línea en todos los sitios sociales (Henostroza, 2016).

Por su parte, PeekYou es un motor de búsquedas de personas que te permite encontrar a cualquier contacto en las diferentes redes sociales de manera rápida y sencilla. Para ello debe colocarse en el recuadro su nombre, apellido y el país, si no está el tuyo en las opciones, selecciona “Mundo”.

Desprestigio social: Participar en las redes sociales ocasiona beneficios, por ejemplo, permiten dar a conocer opiniones, intereses, logros, para las organizaciones, así como los productos, servicios y los beneficios de utilizarlos en lugar de los de la competencia. Las redes sociales también abren la puerta para recibir quejas y comentarios negativos acerca de las personas y las organizaciones (Picazo-Vela, 2016).

La humillación pública no tiene hoy límites, el usuario más anónimo de las redes sociales puede ver arruinada su vida cuando se convierte en diana de los justicieros virtuales. Cualquier frase desafortunada, opinión chocante o desliz en alguno de esos canales basta para ser llevado, sin posibilidad de defensa, a un patíbulo digital.Existen muchos ejemplos del uso de las redes sociales para desprestigiar personas, organizaciones o para quejarse de la calidad de una empresa (Picazo-Vela, 2016).

Acercamiento gradual: En el entorno del ciberacoso existen los “stalkers”, término relacionado con aquellos que acechan, persiguen y acosan físicamente a su víctima (o más de una). Buscan estar atrás del otro en todo momento, sin importar si lo incomodan o se entrometen demasiado en su vida (Papa, 2015). Dentro de la psicología de este tipo de acosador, se asume que se divierte con malicia, obsesión, maldad, hostilidad, enfado, celos o culpa. El objetivo de un stalker es acceder a una persona que quiere o le gusta aunque no sea correspondido.

De acuerdo con Papa (2015), los stalkers se dividen en dos grandes grupos: psicóticos y no psicóticos. Esto quiere decir entonces que los acosadores en gran medida tienen trastornos o desequilibrios mentales. Las subcategorías de stalkers son:

El rechazado: Persigue a la víctima con la intensión de vengarse de un rechazo, como por ejemplo, cuando una chica no acepta salir con un chico.

El resentido: El objetivo de la persecución es asustar a la víctima por algo que ha pasado entre ambos, también puede ser por un rechazo, pero no en todos los casos. Puede deberse a la envidia o a los celos, por ejemplo.

El enamorado: El acosador en esta categoría está convencido de que la víctima es su alma gemela, el amor de su vida y que deben vivir y hasta morir juntos.

El pretendiente: Otro de los stalkers es aquél que cumple con la idea anterior de la media naranja pero a su vez tiene características adicionales, como ser falta de habilidades sociales, introversión, creencia de que está en su derecho de tener intimidad con cualquier persona que comparta sus intereses y gustos, entre otros. En la mayoría de los casos, la víctima tiene otra relación estable.

El depredador: Vive las 24 horas del día espiando a su víctima, está pendiente de todos sus actos, se aprende de memoria cada paso, conoce los

lugares y personas que frecuenta, puede revisar hasta la basura o las gavetas del otro. Todo ello para encontrar el momento y el sitio adecuado para atacar (sobre todo sexualmente).

Hostigamiento sexual: El hostigamiento y acoso sexual (HAS), se presenta de diferentes formas en el contexto de una sociedad digitalizada y se destaca que quienes más han experimentado llamadas y mensajes no deseados, y recepción de contenidos multimedia de parte de contactos con identidades falsas son el grupo que cuenta con una escolaridad de nivel universitario(Vélez, 2016).

El análisis del HAS en las redes sociodigitales permite, visibilizar las formas y mecanismos que se utilizan para violentar cotidianamente a jóvenes universitarios y obliga a trabajar en el cumplimiento irrenunciable de los derechos humanos de quinta generación; en particular el derecho a existir digitalmente, a la reputación digital y a la estima digital (Vélez, 2016).

Es relevante considerar a las humanidades digitales como un espacio para debatir una estrategia digital en aras de la construcción de Internet como un espacio libre de este tipo de violencias y plantear mecanismos organizacionales que eviten se generen, toleren y reproduzcan en ámbitos de educación superior y en la sociedad en su conjunto.

Reacción personal ante el delito de acoso cibernético

El delito es una transgresión de la ley, de la norma socialmente establecida.La respuesta institucional al delito se rige por los principios y la ética de la Justicia: persecución del delito y castigo del delincuente. La pena pretende laretribución del daño, y contribuir a la seguridad; y a su vez, pretende tambiénefectos disuasorios y la rehabilitación del delincuente.

Tanto la enfermedad mental como la conducta delictiva son dos eventualidades que se presentan con frecuencia relativamente alta, en algún

momento de la vida de muchas personas. Existe una amplia gama de conductas delictivas, y una gran diversidad también de enfermedades mentales, por lo que en ningún caso se espera una relación simple entre ambos fenómenos (Hernández Monsalve, 2011).

Enfermedad mental y delito son fenómenos de distinta naturaleza, pero hay ciertos aspectos de la realidad que los vincula: hay enfermos que cometen delitos, y delincuentes que presentan problemas de salud mental. Esta circunstancia plantea importantes dilemas y controversias que atañen a aspectos teórico-conceptuales (ej. la responsabilidad jurídica del enfermo mental ante el delito), y a aspectos prácticos (ej. la respuesta institucional al enfermo que comete el delito, o al recluso con enfermedad mental: pena vs tratamiento) (Hernández Monsalve, 2011).

La enfermedad mental presupone una eventualidad conla que el sujeto seencuentra, que acontece al margen de su voluntad, que proporciona sufrimiento y cierto grado de merma en la capacidad del sujeto para gestionar de formaadecuada su propia vida, que en los casos más graves puede producir una seria reducción o pérdida de la capacidad para decidir y obrar libremente. Antela enfermedad mental la sociedad dispone los recursos de las instituciones sanitarias y sociosanitarias, hoy en el contexto de la salud mental comunitaria (Hernández Monsalve, 2011).

Una de las cuestiones más inquietantes es la contribución de la enfermedad mental a la producción de delitos. Es un tema controvertido, abierto adebate, sobre el que se suele discutir más desde los prejuicios que desde el conocimiento de la realidad. Tradicionalmente las posiciones extremas hanestado encuadradas entre quienes ven en todo delitoindicios de enfermedadmental (posición que ha conducido a la «psiquiatrización» de conductas disruptivas, antisociales, consideradas de entrada «casos psiquiátricos») y entre quienes tienden a judicializar y penalizar las conductas sintomáticas de los pacientes «criminalización» de pacientes mentales.

Dentro de la categoría delictiva, el ciberacoso puede constituir un delito penal, y de acuerdo con Romero (2015), los delitos por medios electrónicos o digitales pueden integrarse en dos grandes grupos:

Delitos contra el sistema informático: Hurto, robo, revelación de secretos, y otro conjunto de delitos que ya no es tan frecuente encontrar, al menos con carácter general, perfectamente tipificados, como el denominado hurto de tiempo, destrucción de logiciales y datos, delitos contra la propiedad (material, terminales, cintas magnéticas,...).

Delitos cometidos por medio del sistema informático: Manipulaciones fraudulentas de logiciales, informaciones contenidas en bases de datos, falsificaciones, estafas, Hurto de uso, este delito suele producirse cuando se utilizan los equipos informáticos de una organización para fines privados (trabajos externos, simple diversión). Se trata, en definitiva, de la utilización de unos equipos si tener derecho a ello o para un uso distinto de lo autorizado, y en el que lo lacerado no es la propiedad, sino el uso del equipo con otros fines no autorizados.

Denuncias: En todo caso, la víctima del cibesacoso en Venezuela puede hacer sus denuncias en los organismos competentes. El término denuncia es utilizado para hacer referencia al acto mediante el cual un sujeto avisa o establece frente a las autoridades correspondientes que se ha cometido algún tipo de delito o crimen. La denuncia puede tomar muy diversas formas, especialmente cuando hablamos de los ámbitos judiciales y legales en los cuales se conforman un número de reglas y procedimientos para establecer una denuncia. La acción de denunciar o de realizar una denuncia puede también darse fuera del ámbito jurídico o legal y el término puede usarse también de manera informal cuando una persona denuncia o avisa de algún error en alguna situación de la vida cotidiana.

En el ámbito jurídico venezolano, existen artículos relacionados al Código Penal; Ley Orgánica de Prevención, Condiciones y Medio Ambiente

de Trabajo (LOPCYMAT); Ley Orgánica del Trabajo, los Trabajadores y las Trabajadoras; Ley de Estatuto de la Función Pública; Ley Orgánica Sobre el Derecho de las Mujeres a Una Vida Libre de Violencia; La Ley Orgánica para la Protección de Niñas, Niños y Adolescentes (LOPNNA) que por ejemplo, en su Artículo 32 hace referencia al Derecho a la integridad personal, el cual establece que “Todos los niños, niñas y adolescentes tienen derecho a la integridad personal. Este derecho comprende la integridad física, síquica y moral”.

También, en Venezuela, existe la Ley Especial contra los Delitos Informáticos, la cual tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley, sin embargo no hace planteamiento explícito de protección en cuanto al acoso cibernético.

La Ley Especial Contra Delitos Informáticos establece en su artículo 20 que la persona que viole la privacidad de otra a través de medios electrónicos puede perder su libertad hasta por seis años.

> Artículo 20 Ley Especial Contra Delitos Informáticos. 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 de otro sobre las cuales 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.

Vale la pena hacer referencia a que el ciberacoso puede incluir varios ámbitos conocidos, como por ejemplo: El acoso académico, el profesional o laboral, social y el amoroso. Sin embargo, no debe olvidarse que si no se hace nada para frenar este tipo de situaciones de acoso cibernético, esto servirá como refuerzo de una actitud negativa como también el mal manejo

de herramientas que bien pudiesen servir para muchos aspectos positivos de la vida, es decir, es preferible siempre darle un buen uso enfocando dichas herramientas tecnológicas como medios eficaces para divulgar informaciones de interés para la sociedad (Ávila, 2015).

A tales efectos, tanto el estudiante como el profesional, está en el deber de ser un buen ciudadano implementando el respeto, la tolerancia, valores familiares y supervisión a los menores. Lo mejor es tener una actitud de asertiva, entendiendo que es el comportamiento comunicacional en el cual la persona no agrede ni se somete a la voluntad de otras personas, sino que manifiesta sus convicciones y defiende sus derechos. Expresarse consciente, congruente, directa y equilibradamente, con el fin de comunicar nuestras ideas y sentimientos sin la intención de herir o perjudicar al prójimo (Ávila, 2015).

En Venezuela, las denuncias de ciberacoso pueden hacerse a través de:

Cuerpo de Investigaciones Científicas, Penales y Criminalísticas, con su Página Web: www.cicpc.gov.ve. Al respecto, cuenta con la División Contra Delitos Informáticos es la Oficina del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas especializada en combatir delitos que afecten el patrimonio económico de personas naturales y jurídicas, también aquellos que vayan de detrimento o afecten la personalidad, moralidad y salud psicológica de las personas, siempre y cuando el medio de comisión sea a través del uso de tecnología de información.

Sus funciones son:Identificar al (los) autor (es) del caso investigado; Iniciar las averiguaciones correspondientes a los delitos informáticos; Estudiar el surgimiento de nuevas modalidades de delitos informáticos; Instruir y sustanciar expedientes para ser remitidos a los organismos jurisdiccionales competentes; Apoyar a las diferentes dependencias de la institución en la investigación de los delitos informáticos; Realizar las

diligencias necesarias para el esclarecimiento de los casos iniciados por delitos informáticos; Diseñar estrategias dirigidas a la detección de organizaciones dedicadas a actividades ilícitas por medios informáticos.

Ministerio Público, con su Página Web: www.ministeriopublico.gob.ve, además el Ministerio Público (MP) creó una oficina o división para recibir las denuncias de extorsión promovidas por funcionarios de este organismo.El número de atención telefónica del Ministerio Público es el 0800-FISCA-00 / 0800-34722-00.

Defensoría del Pueblo, con su Página Web: www.defensoria.gob.ve y el apoyo de las Comisarías policiales, las Casas de la Mujer en todo el país, los Juzgados de Paz, Prefecturas o Jefaturas Civiles, la División de Protección en Materia de Niños, Niñas y Adolescentes del Cuerpo de Investigación con competencia en la materia (CICPC), los Cuerpos de Policía Nacional, Estadales y Municipales y los Tribunales de Municipio en localidades donde no existan los organismos anteriormente mencionados.

Instituto Nacional de la Mujer, con sus oficinas específicas en diferentes municipios en todo el país, en el 0800-Mujeres / 0800-6853737 del Instituto Nacional de la Mujer, informan sobre a cuál se debe acudir de acuerdo a la cercanía del caso las 24 horas del día –, pero si ocurre que al llegar no le quieren tomar la denuncia, entonces la víctima debe solicitar el nombre y apellido de la persona receptora y posteriormente denunciarla por no cumplir con sus funciones.

Refuerzo de la conducta del agresor:El silencio es siempre cómplice del maltrato, como la pasividad o el no rechazo de este tipo de violencia beneficia siempre al maltratador.

Apoyo al agresor:Es necesario destacar la importancia de la recompensa y el castigo en la conducta pues todasnuestras acciones dependen de estas dos reacciones: si recibimos recompensa por algo

quehacemos y nos sentimos bien, seguiremos haciéndolo; si por el contrario recibimos un castigo,dejaremos de hacerlo, por lo que los centros nerviosos que controlan la recompensa y el castigoserán de suma importancia para el control de nuestras actividades y motivaciones.

Manejo de herramientas con víctima:Hoy día, a pesar de los beneficios de las telecomunicaciones, también hay un lado malo al enseñarse a utilizarlas con fines criminales, sobre todo en cuestión cibernética por cuanto, la gran mayoría de transacciones financieras se realizan electrónicamente invisible al ojo de los usuarios y casi que a la velocidad de la luz por lo que se torna difícil controlar todo lo que pasa en determinado momento (Castellanos, 2016).

Debido a que hay personas que aún no están familiarizadas con los actos bancarios cibernéticos, los delincuentes suelen aprovechar esta situación, para robarlos, por lo cual es muy importante estar alerta de los movimientos de la cuenta. En efecto, según Castellanos (2016), las técnicas más utilizadas son el phishing, el smishing y el malware.

En el phishing, los delincuentes suplantan la página Web de la entidad, envían correos electrónicos o genera una ventana emergente invitando al cliente a ingresar a la pagina e ingresar sus datos financieros o la autenticación de la cuenta. Sobre la página fraudulenta, el delincuente captura la información del cliente y la almacena para su uso fraudulento que puede utilizar directamente o vender a otros delincuentes.

El smishing es una práctica en la que los delincuentes hacen uso de los mensajes de texto de los celulares y la ingeniería social para engañar a las personas y obtener información financiera o información útil para el robo de identidad y los delincuentes generalmente ofrecen premios.Por su parte, el softwatre espía (malware), es una modalidad en la que los delincuentes monitorean las actividades del usuario del computador, como las páginas que visita o el tipo de información busca, e incluso la información que escribe en

el teclado y los contenidos de sus correos electrónicos.Lo más grave es que cuando el usuario utiliza su computador para acceder a Internet y hacer sus transacciones bancarias, el software va capturando y enviando la información al delincuente sin que el cliente se dé cuenta (Castellanos, 2016).

La instalación del software espía se puede realizar a través deun hardware (como USB o CD) o se instala automáticamente, sin que el usuario se dé cuenta, cuándo baja programas de sitios no seguros o abre correos electrónicos que no sabe de donde provienen. Una vez con los datos del cliente, el delincuente puede realizar las siguientes transacciones electrónicas: transferencias a cuentas del mismo banco, transferencias a cuentas de otro banco, pagos a terceros (servicios públicos, celulares), compras o pagos por Internet a través de PSE o compras con tarjeta de crédito por Internet (Castellanos, 2016).

Pericias del ingeniero o estudiante de computación para enfrentar incidentes de acoso cibernético.

Los delitos más frecuentes a través delas computadoras y conocidos también como “Cyber-crimes” o delitos ciberneticos o electrónicos, fraude, robo de identidad, secuestro express y lavado de dinero, legitimación yblanqueo de capitales, entre otros que resultan interminable e incluso infinitos pues cada día se conocennuevas modalidades y delitos hasta de “terrorismo cibernético” “pánico financiero en lasredes”, “robo de información vital”, “comercio de pornografía infantil”, “prostitución virtual”, “chantajes y extorsiones”, y hasta “matoneo u hostigamiento”.

Se han dado casos de chicas que publican su fotos en las redes con trajede baño y estos pillos con un programa especial las modifican para que aparezca totalmentedesnuda y luego la contactan y le envían estas fotos modificadas a suvíctima para obligarla apagar para no publicarlas en las

redes y enviárselas a sus conocidos o a sus padres. Muchaschicas ingenuas hasta acceden a tener relaciones sexuales bajo intimidación, y algunos casos quehasta con extraños, por físico miedo deser expuestas en su intimidad.

Todo esto representa es un delito muy grave y va enaumento, es más, se han conocido casos de reclutamiento de posibles víctimas de tráficointernacional de personas, ofreciendo através de páginas y blogs, oportunidadesde ser modelos en el exterior ganandomiles de dólares. Pero en fin, el estudiante o profesional de computación, gracias a su formación, puede encontrar las herramientas de software idóneas frente al ciberfraude, combinando para ello aspectos como la experiencia y proactividad.

Auditoría Informática: Puede definirse como el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas y de acuerdo a las normativas informáticas y generales prefijadas en la organización. Según Romero (2015), su objetivo es evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

En perspectiva de Romero (2015), la auditoría informática cubre tres áreas fundamentales:

1. Aspectos generales relativos a la seguridad. La seguridad operativa de los programas, seguridad en suministros y funciones auxiliares, seguridad contra radiaciones, agresiones y posibles sabotajes, seguridad físicas de las instalaciones, del personal informático, entre otros.

2. Aspectos relativos a la confidencialidad y seguridad de la información. Estos aspectos se refieren no sólo a la protección del material, la logística, los soportes de la información, sino también al control de acceso a la propia información (a toda o a parte de ella, con la posibilidad de introducir modificaciones en la misma).

3. Aspectos jurídicos y económicos relativos a la seguridad de la información. En este grupo de aspectos se trata de analizar la adecuada aplicación del sistema de información en la empresa en cuanto al derecho ala intimidad y el derecho a la información, y controlar los cada vez más frecuentes delitos informáticos que se cometen en la empresa.

Recuperación de archivos eliminados: Cuando se vacía la papelera de reciclaje de windows no quiere decir que elarchivo esté eliminado completamente, simplemente se le está diciendo al sistemaoperativo que el espacio está disponible nuevamente para que se vuelva a escribirsobre él. Por eso, cuando se guardan más archivos, o al hacer otras cosas en elordenador, este espacio se vuelve a llenar (García, 2014).

Esto quiere decir que se tiene una ventana limitada de tiempo para recuperar unarchivo: preferentemente de forma inmediata después de hacerlo. Cuantas másactividades se lleven a cabo después de borrar el archivo, más se estaráocupando ese espacio que se indicó a Windows que estaba disponible pero queen realidad está ocupado por el fantasma del archivo borrado. Por lo tanto, loprimero que se debe hacer es dejar de hacer lo que se está haciendo y ponermanos a la obra para recuperar el archivo. Ahora bien, para esto conviene tenerun software especial instalado. A continuación se presenta una selección de loscinco mejores que se pueden descargar de forma gratuita (García, 2014).

Pandora recovery: Aunque la caja de Pandora supuestamente dejó sueltas a todas las desgraciasdel mundo, esta pequeña aplicación gratuita puede ser de mucha utilidad. Tieneun uso muy intuitivo, y aunque su interfaz deja mucho que desear, no es unconcurso de belleza. Pandora recovery permite mirar todos los archivos que sehan borrado recientemente, que todavía se pueden recuperar, además de podersalvar también archivos cifrados y comprimidos (García, 2014).

Recuva: Con un funcionamiento muy similar al de Pandora pero con una interfaz mucho más cuidada y accesible para los usuarios menos duchos en el tema de recuperar archivos o meterse con el funcionamiento de Windows, Recuva es una herramienta completamente gratuita que también permite hacer un escaneo del equipo para seleccionar los archivos que se quieren recuperar. Es una de las más usadas actualmente, y altamente recomendada (García, 2014).

Undelete plus: Esta joyita es importante dada su funcionalidad más que interesante: PhotoSmartScan, que permite recuperar las fotografías que se han borrado por accidente. Undelete Plus es mucho más específica que las anteriores aplicaciones mencionadas, pero igualmente efectiva. Además, tiene un funcionamiento muy rápido lo que permite solucionar un problema de pérdida de archivos sin dedicarle demasiado tiempo del día. Permite recuperar archivos no solamente del disco duro, sino también de un pendrive o de una tarjeta de memoria de una cámara (García, 2014).

Restoration: Esta herramienta también permite recuperar los archivos de fotografías borradas accidentalmente de una tarjeta de memoria, así como también escanear el rígido para recuperar los archivos borrados desde la papelera de reciclaje. También ofrece, para los más cautelosos que quieren realmente asegurarse que un archivo está perdido para siempre, borrar sin dejar rastro esos archivos que ya no están en la papelera pero que se quiere que desaparezcan de la faz de la vida virtual (García, 2014).

Cifrado Simétrico: Los algoritmos simétricos están basados en la utilización de una sola clavesecreta donde preserva el secreto para cifrar y descrifrar el mensaje. Esa clave escompartida por dos usuarios para poder ver el mensaje cifrado. El emisor y elreceptor utilizan el mismo algoritmo. El emisor envía un mensaje cifrado alreceptor con un algoritmo basado en cifrado simétrico, el receptor descifra la clavemediante el uso de la clave secreta con la que el emisor cifro el mensaje (García, 2014).

BASES LEGALES

SegúnVillafranca (2012), “las bases legales no son más que leyes que sustentan de forma legal el desarrollo del proyecto” explica que las bases legales“son leyes, reglamentos y normas necesarias en algunas investigaciones cuyo tema así lo amerite”.

Es así que la ejecución de esta investigación se enmarca en la Constitución de la República Bolivariana de Venezuela (1999), la cual dispone que todas las convenciones sobre Derechos Humanos tengan caráctervinculante para el país, es decir, prevalecen en el orden interno, siendo sus disposicionesde aplicación directa e inmediata por los tribunales y todos los demás órganos del poderpúblico.

Así mismo, la Constitución incluye una visión de género que se expresa desde elpreámbulo hasta las disposiciones finales, entretejida con el principio de lacorresponsabilidad, e incorpora el lenguaje no-sexista. Ésta establece los principios delacceso y gratuidad de la justicia y el derecho a obtener con prontitud la decisióncorrespondiente; la igualdad de derechos y deberes en las relaciones familiares y elrespeto recíproco entre sus integrantes, así como reconoce, entre otros derechos, laigualdad y equidad de hombres y mujeres en el ejercicio y el acceso al trabajo, el derechode las amas de casa a la seguridad social y el valor al trabajo doméstico.

De la mismamanera, consagra el principio de la igualdad y no discriminación fundadas en la raza, elsexo, el credo o la condición social y en el numeral 2º del mismo artículo, la obligación porparte de los poderes públicos de adoptar medidas positivas a favor de personas ogrupos que puedan ser discriminados, marginados o vulnerables, para que laigualdad ante la ley sea real y efectiva.

El propio constituyente, haciendo eco de los avances en la doctrina más avanzada delderecho, admitió que el principio de igualdad no puede limitarse

a su mera consagraciónen el texto fundamental, sino que corresponderá, entre otros, al legislador, la adopción detodas las medidas necesarias y razonables para hacer de aquél una realidad. Esprecisamente esta norma constitucional, la que admite expresamente la posibilidad deconferir por vía legal tratamiento distinto a aquellos grupos discriminados, marginados ovulnerables, que se encuentren en circunstancias de debilidad manifiesta, no pudiendo portanto considerarse tales medidas contrarias al principio de igualdad, sino más bien en suapoyo y garantía de factibilidad.

Sobre la base de las normas antes señaladas, y partiendodel hecho de que las acciones legislativas positivas están expresamente autorizadas porinstrumentos internacionales y nacionales de protección de los derechos humanos queintegran el ordenamiento jurídico vigente en Venezuela; específicamente, en relación a losderechos de la mujer, la Ley Orgánica Sobre el Derecho de las Mujeres a una Vida Libre deViolencia, constituye una medida de acción positiva, que garantiza –además- la normaconstitucional del derecho a la viday el derecho a que se respete la integridad física,psíquica y moral de la víctima.

Por otra parte nuestra Carta Magna consagra el derechode todas las personas a la protección por parte del Estado a través de los órganos deseguridad ciudadana, frente a situaciones que constituyan amenazas, vulnerabilidad oriesgo para la integridad física de las personas.

DEFINICIÓN DE TÉRMINOS BÁSICOS

La Definición de Términos Básicos consiste en “dar el significadopreciso y según el contexto a los conceptos principales, expresiones ovariables involucradas en el problema y en los objetivos formulados”. (Arias,2012:108). A continuación se presentan definiciones que guardan relacióncon el tema de investigación.

Adware: Un programa adware es aquel que difunde publicidad a través de banners, ventanas emergentes, mientras está funcionando. Gracias a esta publicidad se subvenciona la aplicación. A veces, estos programas incluyen un código de seguimiento, que recoge información sobre los hábitos de navegación del usuario, funcionando como programa espías o spyware. Esto ha generado cierta polémica ya que, en algunos casos, se cede a terceros la información de los usuarios sin su consentimiento.

Antivirus: Programas que se utilizan con el fin de prevenir y detectar posibles infecciones producidas por virus y todo tipo de programas maliciosos, y reparar los daños que éstas hayan podido causar.

Backdoor: En informática, una puerta trasera o backdoor, es una secuencia especial dentro del código de programación mediante la cual el programador puede acceder o escapar de un programa en caso de emergencia o contingencia en algún problema. A su vez, estas puertas también pueden ser perjudiciales debido a que los crackers al descubrirlas pueden acceder a un sistema sin conocimiento por parte del usuario.

Black Hat o Cracker: expertos en seguridad informática que tratan de detectar las debilidades o deficiencias de programas y equipos informáticos, para obtener algún tipo de beneficio.

Bomba Lógica: Programa que se instala en un equipo y se mantiene inactivo, en espera de que se cumplan una serie de requisitos o condiciones, como por ejemplo: que el usuario pulse una tecla o una combinación de teclas concretas, que el reloj del sistema marque una hora determinada, etc. Cuando se ejecutan las condiciones de activación, el programa comienza a llevar a cabo las acciones para las que ha sido diseñado, que pueden ser: ordenar una transferencia bancaria, dañar el sistema, borrar datos.

Cracker: El término cracker o hacker “blachhat” se utiliza para denominar a las personas que emplean sus elevados conocimientos

informáticos para robar información, distribuir virus, introducirse ilegalmente en redes, eliminar la protección anticopia del software comercial, burlar la seguridad de determinados sistemas informáticos.

Crimeware: El concepto crimeware engloba a todos aquellos programas informáticos diseñados para obtener beneficios económicos, mediante la comisión de todo tipo de delitos online. Se considera crimeware el phishing, spam, adware.

Dialer: Programa que se instala en un equipo con el fin de modificar los datos de acceso a internet, para que al realizar la conexión a través de un módem, se utilice un número de tarificación adicional (Los números de tarificación adicional o NTA son aquellos cuyo coste es superior al de una llamada nacional, por ejemplo aquellos que empiezan por prefijos como 806, 907). La utilización de dialers o marcadores telefónicos es lícita si se informa al usuario de los costes, se le avisa del la redirección de la conexión y si se instala el programa con su consentimiento.

Exploit: Programa que aprovecha los fallos de seguridad, defectos o vulnerabilidades de otros programas o sistemas informáticos, con el fin de obtener algún tipo de beneficio o de llevar a cabo una acción concreta, como acceder a recursos protegidos, controlar sistemas sin autorización.

Firewall: Firewall o cortafuegos es un mecanismo de seguridad que regula el acceso entre dos o más redes, teniendo en cuenta la política de seguridad establecida por la organización responsable de la red. Habitualmente se utilizan los cortafuegos para proteger redes internas de accesos no autorizados.

Flood o flooder: Programa utilizado para enviar mensajes repetida y masivamente, mediante correo electrónico, sistemas de mensajería instantánea, chats, forospar así provocar la saturación o colapso de los sistemas a través de los que se envía el mensaje.

Gusano: Los gusanos o worms son programas con características similares a las de los virus, aunque a diferencia de los éstos, son capaces de realizar copias de sí mismos y propagarse, a través de la red para infectar otros equipos, sin la intervención de un usuario. Una de las formas más habituales de propagación de gusanos es el envío masivo de correos electrónicos a los contactos de las libretas de direcciones de los usuarios.

Hacker: Se denominan hackers a los especialistas en tecnologías de la información y telecomunicaciones en general, aunque actualmente, se utiliza este término para referirse a aquellos que utilizan sus conocimientos con fines maliciosos como el acceso ilegal a redes privadas, el robo de información, etc. Según algunos expertos, es incorrecto asociar éste término únicamente con aquellas prácticas fraudulentas.

Hijacking: Se denomina hijacking a las técnicas informáticas que se utilizan para adueñarse o "secuestrar" páginas web, conexiones de internet, dominios, IPs.

Hoax: Un hoax es un mensaje de correo electrónico con información engañosa, que pretende avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc. Los hoaxes se caracterizan por solicitar al destinatario que reenvíe el mensaje a todos sus contactos, así logran captar las direcciones de correo de usuarios a los que posteriormente se les enviarán mensajes con virus, spam, phishing.

Keylogger: Programa o dispositivo que registra las combinaciones de teclas pulsadas por los usuarios, y las almacena para obtener datos confidenciales como contraseñas, contenido de mensajes de correo, etc. La información almacenada se suele publicar o enviar por internet.

Malware: El término Malvare (Acrónimo en inglés de: "Malcious software") engloba a todos aquellos programas "maliciosos" (troyanos, virus,

gusanos) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al sistema informático o al usuario del mismo.

Pharming: Modalidad de estafa online que utiliza la manipulación de los servidores DNS (Domine Name Server) para redireccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales del usuario, como contraseñas, datos bancarios.

Phishing: Fraude tradicionalmente cometido a través de internet, que pretende conseguir datos confidenciales de usuarios como contraseñas o claves de acceso a cuentas bancarias. Para lograr esta información, se realizan envíos masivos de correos electrónicos, que simulan proceder de entidades de confianza. En el mensaje se pide al usuario que, por "motivos de seguridad" o con el fin de "confirmar su cuenta", facilite sus datos personales, claves. En ocasiones, este tipo de datos se solicitan en el mismo mensaje, o se indica al usuario que acceda a la página web de la entidad en cuestión, que es una copia idéntica de la original, donde deberá completar dicha información. Actualmente están surgiendo numerosas versiones de este delito, que se sirven de otro tipo de medios para conseguir los mismos fines. Un ejemplo del nuevo phishing es el SMiShing.

Sexting. Es una nueva forma de relación virtual entre los adolescentes y jóvenes. El término se compone de dos palabras en inglés sex (sexo) y texting, porque comenzó con los mensajes de texto vía celular.Se trata de contenidos muy íntimos, generados por los propios remitentes, mediante la grabación de sonidos, fotos o videos de comportamientos sexuales, desnudos o semidesnudos, normalmente destinados a una pareja sexual o amorosa, aunque también en no pocas ocasiones, a otros amigos, como un simple juego. Sin tener conciencia que esto los expone a graves riesgos.

Scam o Phishing Laboral: Fraude similar al phishing, con el que comparte el objetivo de obtener datos confidenciales de usuarios, para

acceder a sus cuentas bancarias. Consiste en el envío masivo de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen supuestos empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicitan datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.

SMiShing: Es una variante del phishing, que utiliza los mensajes a teléfonos móviles, en lugar de los correos electrónicos, para realizar el ataque. El resto del procedimiento es igual al del phishing: el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falseada, idéntica a la de la entidad en cuestión.

Spam: Consiste en el envío masivo de mensajes no solicitados, con contenido generalmente publicitario, que se realiza a través de distintos medios como: foros, mensajería instantánea, blogs, etc. aunque el sistema más utilizado es el correo electrónico. Para obtener la lista de direcciones de correo, los spammers o remitentes de “mensajes basura”, emplean software especializado o robots que rastrean páginas web en busca de direcciones, compran bases de datos, utilizan programas de generación aleatoria de direcciones, copian las direcciones de listas de correo.

SpearPhishing: Tipo de phishing en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional.

Spyware o Programa Espía: Es un tipo de programa cuyo objetivo es recopilar información del usuario del sistema en el que se instala. Los datos que se recogen suelen estar relacionados con los hábitos de navegación del usuario y se utilizan con fines publicitarios. Aunque la instalación de los programas espías puede realizarse con el consentimiento expreso del usuario, en muchos casos, se instalan sin la autorización de éste, al instalar

otro programa supuestamente inofensivo, o mediante virus o un troyanos, distribuidos por correo electrónico.

Troyano: Programa ejecutable que aparenta realizar una tarea determinada, para engañar al usuario, con el fin de llevar a cabo acciones como controlar el equipo informático, robar información confidencial, borrar datos, descargar otro tipo de malware, etc. La principal diferencia entre los troyanos y los virus es que los troyanos no pueden replicarse a sí mismos.

Víctima: Aquella persona que ha sufrido un perjuicio (lesión física o mental, sufrimiento emocional, pérdida o daño material, o un menoscabo importante en sus derechos), como consecuencia de una acción u omisión que constituya un delito con arreglo a la legislación nacional o del derecho internacional.

Victimario: Es aquel que produce el daño, sufrimiento o padecimiento de la víctima. Es incorrecto asimilar el victimario al delincuente, pues se puede ser victimario por una acción u omisión que no sea antisocial o delictiva, es decir " victimario" es el género y delincuente es la "especie". En la auto victimización, las calidades de victimario y víctima se unen en una misma persona.

Virus: Código informático que se replica a sí mismo y se propaga de equipo en equipo por medio de programas o archivos a los que se adjunta. Para que se produzca la infección, es necesaria la intervención humana, es decir, el usuario debe realizar algún tipo acción como enviar un correo o abrir un archivo. Los virus pueden producir todo tipo de daños en el propio equipo y en la información y programas que éste contiene.

Vishing: Fraude que persigue el mismo fin que el Phishing: la obtención de datos confidenciales de usuarios, pero a través de un medio distinto: la telefonía IP.

White Hat: especialistas en informática que utilizan sus conocimientos con el fin de detectar cualquier tipo de vulnerabilidad, errores o fallos de seguridad, para poder solucionarlos y evitar posibles ataques.

CONCEPTUALIZACIÓN Y OPERACIONALIZACIÓN DE LA VARIABLE

Es el proceso mediante el cual se establecen las características propias de la investigación y consiste en transformar o traducir a un lenguaje entendible, lo que se está investigando (Sabino, 2012:98). En el caso de la presente investigación, se utilizaron los objetivos específicos para identificar las variables y así, poder dar una definición conceptual de las mismas. A continuación, se presenta el cuadro donde se operacionaliza la variable presentada.

Variable: Acoso Cibernético.

Definición conceptual. Es definido por Pinto (2018), como ‘’amenazas, hostigamiento, humillación u otro tipo de molestias realizada por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación’’ es decir, internet, telefonía móvil, correo electrónico, mensajería instantánea, video consolas online, entre otros y cuando esto ocurre con menores se denomina ciberbulling, todo con la finalidad de socavar la autoestima o dignidad personal, además de dañar el estatus social.

Definición operacional. La variable será estudiada a través de las dimensiones: Vigilancia remota, Búsqueda de interacción, Desprestigio social, Acercamiento gradual, Hostigamiento sexual, Denuncias, Refuerzo de la conducta, Auditoria informática, Recuperación de archivos.

OPERACIONALIZACIÓN DE LA VARIABLE

Objetivo General: Determinar el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo.				
Objetivos Específicos	**Variable**	**Dimensiones**	**Indicadores**	**Ítems**
Identificar el índice de acoso cibernético en los miembros de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo.	ACOSO CIBERNÉTICO	Vigilancia remota	Monitoreo, vigilancia, hostigamiento	1 a 9
		Búsqueda de interacción	Notificaciones, mensajes	10 a 15
		Desprestigio social	Saboteos, información sin permiso	16 a 21
		Acercamiento gradual	Conocimiento personal, perjuicios	22 a 25
		Hostigamiento sexual	Imágenes obscenas/pornográficas	26 a 30
Diagnosticar la reacción personal ante el delito de acoso cibernético dentro y fuera de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo.		Denuncias	CICPC Defensoría del Pueblo INAMUJER	31 32 33
		Refuerzo de la conducta	Apoyo al agresor Manejo de herramientas con víctima	34 35
Identificar la capacidad de colaboración para enfrentar incidentes de impacto público de acoso cibernético.		Auditoria informática	Aspectos de seguridad Aspectos de confidencialidad Aspectos jurídicos y económicos	36 37 38
		Recuperación de archivos	Pandora recovery, Recuva Undelete plus, Restoration Cifrado Simétrico	39 – 40 41 – 42 43

Fuente: Pérez y Romero (2018).

CAPÍTULO III

MARCO METODOLÓGICO

En este capítulo se presenta el procedimiento seleccionado por el investigador para responder a las interrogantes planteadas en el estudio. En ese sentido se señala, el tipo y diseño de investigación, el método de investigación, la población, la técnica de recolección de información, la validez y el tratamiento de la información.

Tipo de investigación

De acuerdo al nivel de estudio y sobre la base, al problema planteado, como a los objetivos propuestos, se corresponde con el tipo de investigación descriptiva, dado que la misma, según Tamayo y Tamayo (2012: 49), comprende la caracterización, análisis e interpretación de la naturaleza actual, trabaja sobre realidades de hecho, su propósito fundamental es la interpretación correcta de la realidad.

Diseño de la investigación

El diseño según Ballestrini (2011: 67) consiste en un plan que integra de un modo coherente y adecuadamente técnicas de recolección de datos a utilizar, análisis previos y objetivos, intentando ofrecer de manera clara respuestas a las preguntas planteadas.

Por lo antes mencionado, Tamayo y Tamayo (2012: 42) este tipo de diseño es utilizado cuando los datos se recogen directamente de la realidad, denominándose primarios y su valor radica en que permiten cerciorarse de las verdaderas condiciones en que se han obtenido.

Población y Muestra

Arias (2012:81), señala que la misma “es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación

) define la población finita como “agrupación en la que se conoce la cantidad de unidades que la integran. Además existe un registro documental de dichas unidades”. Para efectos de la presente investigación, la población se considera finita con sus 500 integrantes de la Facultad de Ingeniería de la Universidad Valle del Momboy, de los cuales 200 pertenecen a Ingeniería en Computación, por lo que se decidió tomar una muestra a conveniencia y al azar del 10% para un total de 20 sujetos entre profesores y estudiantes.

“implica un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico”, de acuerdo a lo expresado por Hernández y otros (2011: 272).

Arias (2012:67) la define como “el procedimiento o forma particular de obtener datos e información”. En tal sentido, la técnica que se utilizó en esta investigación fue la encuesta,

En relación al instrumento, Arias (2012:68) expresa “son los medios materiales que se emplean para recoger y almacenar la información”. Uno de los más utilizados es el cuestionario, definido como “un conjunto de preguntas con respecto a una o más variables a medir” (Hernández y otros, 2011:310).

Para el presente estudio, se aplicó un cuestionario constituido por preguntas cerradas; este tipo de preguntas según Hernández y otros (2011: 126) presenta entre otras ventajas, ser más fáciles de codificar y preparar para su análisis,

Las preguntas cerradas se presentarán en escala tipo Likert, con cinco

(05) alternativas de respuesta: 1=nunca, 2=Casi nunca, 3=Ocasionalmente, 4=Casi siempre, 5=Siempre. Dentro de este contexto, la primera parte del cuestionario consta se basa en la Encuesta de Obsesión Intrusiva Relacional (ORI-82) de Spitzberg y Cupach (2014) retomando la ESCALA DE ACOSO CIBERNÉTICO compuesta por y tiene como dimensiones: Vigilancia remota, Búsqueda de interacción, Desprestigio social, Acercamiento gradual y Hostigamiento Sexual.

Luego, los ítems 31 a 43 corresponden a las dimensiones denuncias, refuerzo de la conducta, auditoria informática y recuperación de archivos, con sus respectivos indicadores: CICPC, Defensoría del Pueblo, INAMUJER, apoyo al agresor, manejo de herramientas con víctima, aspectos de seguridad, aspectos de confidencialidad, aspectos jurídicos y económicos, pandora recovery, recuva, undelete plus, restoration y cifrado simétrico.

Validezdel instrumento

, Ramírez (2012: 52), así como Hernández y otros (2011: 133) coinciden en que, la validez hace referencia al grado en el cual un instrumento realmente mide la variable que pretende medir.

En esta investigación se consideró la validez de contenido, la cual según Chávez (2012:193) la define como “La eficacia con la cual un instrumento mide lo pretendido”; visto de esta forma, cada uno de los ítems deben ser representativos del contenido a medir.”.

Cabe mencionar que la validez de contenido no se expresa en términos de un índice numérico, sino se basa en la necesidad de discernimiento y juicios independientes entre expertos, quienes deben realizar un análisis cuidadoso y crítico del instrumento de acuerdo con el área específica de contenido teórico. Respecto a la validación del instrumento, el mismo se sometió al juicio de tres (03) expertos: dos en contenido y uno en

metodología, con la finalidad de revisar la pertinencia de los ítems formulados, con la variable, dimensiones e indicadores.

Confiabilidad del instrumento

En cuanto a la confiabilidad, para Chávez (2012:199), consiste “en el grado con el cual se obtiene resultados similares en distintas aplicaciones, ésta mide el grado en que la repetida aplicación del instrumento a una determinada población arroje resultados iguales”. En tal sentido, se tomó el resultado estadístico del instrumento aplicado en la Facultad de Ingeniería de la Universidad Valle del Momboy, para cumplir con la confiabilidad mediante el cálculo del coeficiente AlphaCronbach, expresado a través de la aplicación de la siguiente fórmula:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum Si^2}{St^2}\right]$$

Dónde:

α = Coeficiente de Cronbach

K = Número de reactivos

Si2= Varianza de los puntajes de cada reactivo

St2= Varianza de los puntajes.

$$r_{tt} = \frac{43}{43-1} * 1 - \left(\frac{10,6}{112}\right)$$

$$r_{tt} = 1,02 * (1 - 0,09) = 0,9$$

En cuanto a la escala de interpretación para el coeficiente AlphaCronbach, Pelekais y otros (2012), plantean que la confiabilidad del instrumento se expresa mediante el coeficiente de correlación rtt, que significa correlación del test consigo mismo. Tal como puede observarse en el cuadro, se genera un valor que oscila entre cero (0) y uno (1),

entendiéndose el coeficiente 0 como Muy Baja confiabilidad y 1 Muy alta. En este sentido, considerando los resultados de la fórmula (r_{tt}= 0,9) la puntuación se ubica en la posición **muy alta confiabilidad**.

Escala de Interpretación para el Coeficiente AlphaCronbach

Rango	0,81-1,00	0,61-0.80	0,41-0,60	0,21-0,40	0,01-0,20
Magnitud	Muy Alta	Alta	Moderada	Baja	Muy Baja

Fuente: Pelekais y otros (2012).

Técnicas para el análisis de datos

Una vez aplicado el instrumento y procesados los datos, se analizó estadísticamente la información obtenida, representándola en tablas para una adecuada interpretación. Así mismo, se realizó un análisis en base a parámetros propios de la estadística descriptiva, utilizando la media como medida de tendencia central se utilizará la media y el Baremo de valoración con la finalidad de analizar los resultados por variables, dimensiones e indicadores.

Tal como se evidencia en el cuadro, la alternativa Siempre (S) con un criterio Muy Alto, el cual se ubica en un rango de 4,21 a 5; Casi Siempre (CS) con un criterio Alto en un rango de 3,41 a 4,2; Ocasionalmente (O) con criterio Mediano en un rango de 2,61 a 3,4; Casi nunca (CN) con un criterio Bajo, en un rango de 1,81 a 2,6 y finalmente la alternativa Nunca (N) con un criterio de Muy Bajo, en un rango de 1 a 1,8.

Los criterios son definidos para diferenciarlos con claridad, es así como el muy alto significa el cumplimiento total de cada uno de los indicadores establecidos, el alto indica el acatamiento total de algunos indicadores, siendo estos los más representativos; por su parte, el mediano establece el cumplimiento de algunos indicadores, sin inclinarse de forma relevante hacia alguna en particular, el bajo representa el poco cumplimiento a los

indicadores establecidos; y el muy bajo significa la nulidad de desempeño ante los indicadores propuestos.

Baremo de Valoración

Alternativa	Criterio	Rango
5 = Siempre	Muy Alto	[4,21 a 5]
4 = Casi siempre	Alto	[3,41 a 4,2)
3 = Ocasionalmente	Mediano	[2,61 a 3,4)
2 = Casi nunca	Bajo	[1,81 a 2,6]
1 = Nunca	Muy bajo	[1 a 1,8]

Fuente: Pérez y Romero (2018).

Procedimiento de investigación

Con respecto a esta investigación se procedió de acuerdo a las siguientes fases:

- De forma resumida clara y precisa, se describió el problema planteado, el cual permitió establecer los objetivos que permitieron desarrollar la investigación, seguidamente se justificó la investigación de manera teórica, practica, metodológica y social, para proceder a delimitar, seguidamente se estableció el tiempo y las bases teóricas para la realización de la investigación.
- El siguiente paso fue, describir todas las bases teóricas relacionadas con las variables, es decir realizó una revisión de material como: tesis, artículos, textos.
- Tomando en consideración los pasos de una investigación cuantitativa se comenzó a de sarrollar la metodología a utilizar para el logro de los objetivos planteados como: el tipo de investigación, población instrumento a utilizar, explicación de la validez, cálculo de la confiabilidad y procedimiento para el análisis de los datos.

- Luego se validó el instrumento, con el propósito de realizar su aplicación para proceder formalmente a su aplicación, seguidamente el análisis e discusión de los resultados.
- Finalmente se realizan las conclusiones junto a las recomendaciones con base a los hallazgos de cada objetivo planteado.

CAPÍTULO IV

PRESENTACIÓN DE LOS RESULTADOS

A continuación se presenta el análisis e interpretación de los datos obtenidos de la aplicación del instrumento (cuestionario) en la población objeto de estudio. En ese sentido, se analizó cada dimensión de acuerdo a los indicadores y según las categorías del baremo diseñado.

Tabla 1
Índice de acoso cibernético en los miembros de la Facultad de Ingeniera en la Universidad Valle del Momboy

Ítem	Dimensión	$\overline{X}$ Dimensión	*Rango de* Dimensión	Índice del ciberacoso
1 a 9	Vigilancia remota	1,31	Muy bajo	1,9 Rango: Bajo
10 a 15	Búsqueda de interacción	1,87	Bajo	
16 a 21	Desprestigio social	2,64	Mediano	
22 a 25	Acercamiento gradual	2,80	Mediano	
26 a 30	Hostigamiento sexual	1,7	Muy bajo	

Fuente: Cálculos basados en las respuestas del cuestionario aplicado en Facultad de Ingeniería, grupo de computación. Pérez y Romero (2018).

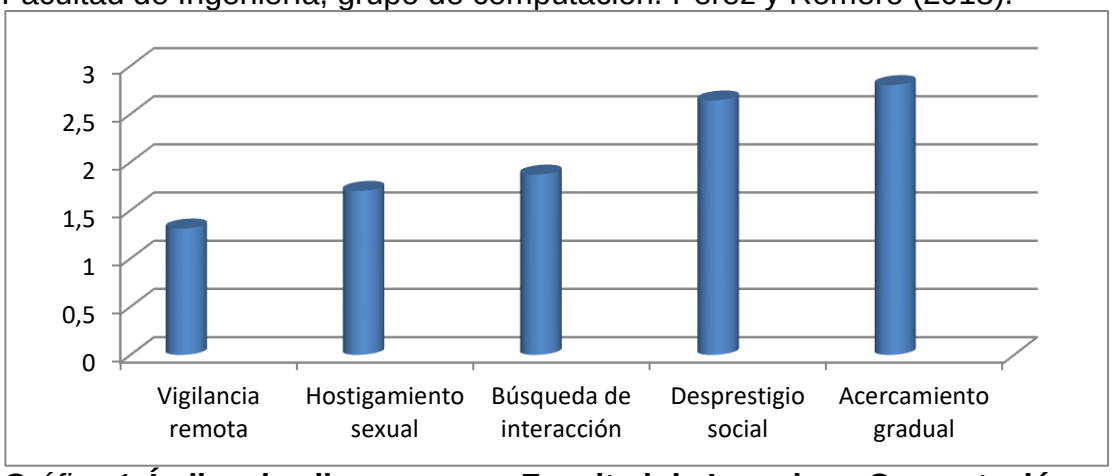

Gráfico 1. **Índice de ciberacoso en Facultad de Ingeniera, Computación.**
Fuente: Tabla 1.

Análisis: Según los resultados obtenidos al aplicar el instrumento entre el grupo de estudiantes y profesores de computación, respectivamente de la Facultad de Ingeniería de la Universidad Valle del Momboy, sede Estovacuy,se encontró con base al baremo diseñado, para la dimensión vigilancia remota una media aritmética de 1,31 lo que indica muy baja existencia de este tipo de acoso cibernético; la dimensión búsqueda de interacción obtuvo por media aritmética 1,87ubicándose en el rango de baja existencia, mientras la dimensión hostigamiento sexual arrojó por media 1,7 en el rango de muy baja existencia de este tipo de ciberacoso.

En cuanto a las dimensiones desprestigio social y acercamiento gradual, sus medias aritméticas (2,64 y 2,80) la ubicaron en el nivel de mediana existencia lo que da a entender que este grupo de estudiantes y profesores encuestados de alguna manera son ciber-saboteados en su reputación, les es robada información privada sin permiso y son expiados por medios electrónicos, aunque sea en un nivel mediano, lo cual perjudica la tranquilidad y calidad de vida. Al igual que en el estudio de Cañarte (2017) en Ecuador, con estudiantes de la Facultad, los actos de violencia por medio de las nuevastecnologías que prevaleció fue el insulto.

Al promediar todos los indicadores se obtuvo como Índice del ciberacoso1.9 para el rango bajo, según el baremo elaborado, lo que permute evidenciar que en la Facultad de Ingeniería se utilizan las nuevas tecnologías de comunicación e información para acosar, hostigar la existencia y permanencia de tales ciudadanos/as, situación que representa un delito que aunque en baja escala, es motivo de atención y sanción penal conforme a los instrumentos jurídicos existentes en un Estado de Derecho.

Conocidos los resultados, vale acotar que al igual que el estudio de Redondo y col (2017) en Colombia, se evidencia que un pequeño porcentaje de la muestra ha sido ciberagredida en alguna ocasión y eso tiene un impacto psicológico tanto en las cibervíctimas, como en los ciberagresores.

Tabla 2
Reacción Personal ante el Delito de Ciberacoso

Ítem	Dimensión	$\overline{X}$ Dimensión	*Rango de* Dimensión	Índice del ciberacoso
31 a 33	Denuncias	1,18	Muy bajo	1,5 Rango: Muy Bajo
34 a 35	Refuerzo de la conducta	1,75	Bajo	

Fuente: Cálculos basados en las respuestas del cuestionario aplicado en Facultad de Ingeniería, grupo de computación. Pérez y Romero (2018).

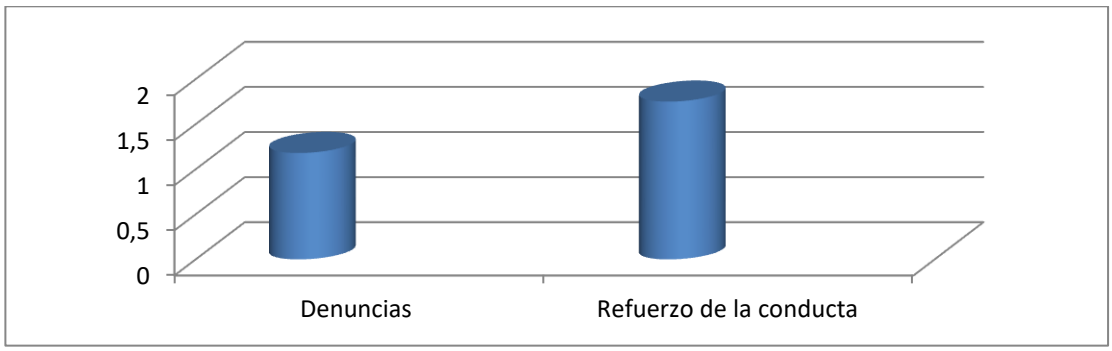

Gráfico 2. **Reacción Personal ante el Delito de Ciberacoso**
Fuente: Tabla 2.

Análisis: Con base a los resultados que permitieron diagnosticar la reacción personal ante el delito de acoso cibernético dentro y fuera de la Facultad de Ingeniera en la Universidad Valle del Momboy, se pudo conocer que la capacidad de denunciar los agredidos o víctimas apuntó 1,18 en el rango muy bajo, mientras el refuerzo de la conducta para que haya continuidad en este tipo de ciberdélito se ubicó en el rango bajo con 1,75 situación que merece mayor atención porque lo ideal para contribuir con la justicia y la paz ciudadana, es denunciar el delito y no apoyarlo en su continuidad, porque como lo dice Polo del Río y col. (2017) en España, el uso abusivo del móvil y demás tecnologías de tele comunicación, genera conflictos en los jóvenes universitarios de ambos sexos; aunque las chicas(mujeres) manifiestan más problemas comunicacionales y

emocionales.

Tabla 3
Capacidad de colaboración para enfrentar ciberacoso

Ítem	Dimensión	$\overline{X}$ Dimensión	*Rango de* Dimensión	Índice del ciberacoso
36 a 38	Auditoria informática	1,61	Muy bajo	1,5 Rango: Muy Bajo
39 a 43	Recuperación de archivos	1,45	Muy bajo	

Fuente: Cálculos basados en las respuestas del cuestionario aplicado en Facultad de Ingeniería, grupo de computación. Pérez y Romero (2018).

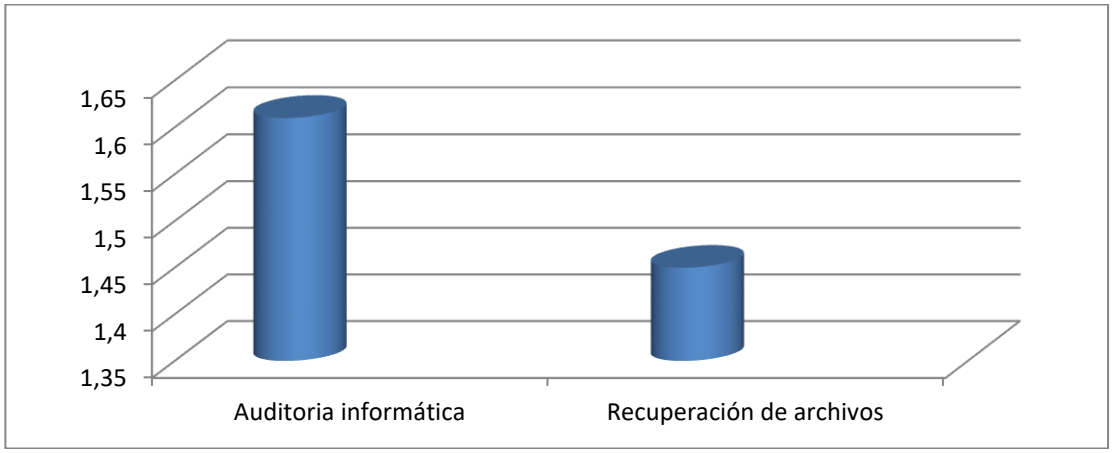

Gráfico 3. **Capacidad de colaboración para enfrentar ciberacoso.**
Fuente: Tabla 3.

Análisis: Con base en los resultados de los ítems del tercer objetivo específico orientado a identificar la capacidad de colaboración del grupo encuestado para enfrentar incidentes de impacto público de acoso cibernético, se conoció que la auditoria informática tiene una aplicación muy baja (media aritmética 1,61) al igual que la colaboración para recuperar archivos es muy baja (media aritmética 1,45).

Al promediar los indicadores, el resultado es 1,5 (rango muy bajo), promedio tomado para inferir que en la Facultad de Ingeniería de Computación de la Universidad Valle del Momboy, es necesario hablarle y

motivar más a quien se está formando profesionalmente en el área de computación para que utilice y perfeccione sus conocimientos en función de impedir, frenar, descubrir y ayudar en la prevención del ciber-delito, al ser ellos/as quienes tienen los conocimientos básicos para convertirse en peritos forenses de la cibernética y como lo demostró el Instituto Nacional de Estadística y Geografía de México (INEGI, 2018) los universitarios son quienes más sufren hostigamiento virtual, especialmente los hombres entre la edad de 20 a 29 años, seguidos por el grupo de 12 a 19 años; en tercer lugar el grupo de 30 a 49 años.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Esta investigación estuvo dirigida a determinar el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, y sus resultados permitieron concluir lo siguiente.

En relación al **primer objetivo** específico orientado a identificar el índice de acoso cibernético en los miembros de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, se encontró un escalamiento de bajo nivel de existencia de ciberacoso entre la comunidad universitaria del área de computación, por lo que se puede decir que los y las estudiantes junto a sus docentes han sido víctimas de solicitudes indecentes de desconocidos, así como del desprestigio social por las redes sociales telemáticas, situación que altera la paz y bienestar ciudadano.

En cuanto al **segundo objetivo** específico orientado a diagnosticar la reacción personal ante el delito de acoso cibernético dentro y fuera de la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, se encontró muy bajo pronunciamiento a la acción de denunciar ante los organismos competentes el ciber-delito, pero tampoco el grupo estudiado se dedica a reforzar las conductas delictivas a través de los medios electrónicos y telemáticos.

Respecto al **tercer objetivo** específico orientado a identificar la capacidad de colaboración para enfrentar incidentes de impacto público de acoso cibernético, se pudo conocer que aunque se trata de estudiantes y profesores del área de computación, los mismos muy poco se inclinan en colaborar o ayudar en la ejecución de auditorías informáticas con herramientas para la recuperación de archivos que sirvan de prueba para corroborar, demostrar y enfrentar el ciberdelito.

Cabe resaltar, no basta el conocimiento y habilidad para manejar software y hardware de última generación, debido a que cada día cobra vigencia la necesidad de desarrollo empresarial y apertura de nuevos empleos como alternativa básica liberadora, no antagónica al desenvolvimiento laboral de jóvenes profesionales, donde la percepción de la realidad les ofrece oportunidades para contribuir con la justicia y paz ciudadana.

Se concluye entonces que el manejo realizado al fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, es muy bajo para denunciar el ciber-delito contribuir con los conocimientos adquiridos y habilidades desarrolladas a demostrar y aclarar la ocurrencia del mismo.

Recomendaciones

Con el fin de enfrentar el fenómeno del acoso cibernético en la Facultad de Ingeniera en la Universidad Valle del Momboy, estado Trujillo, se sugiere:

La Universidad Valle del Momboy en convenio con el CICPC debería ofertar la especialidad en peritaje forense dirigida al ingeniero de computación.

Es necesario instruir a los y las estudiantes sobre la forma de denunciar el delito de ciberacoso y la importancia de no colaborar con el mismo, por

cuanto está sujeto a serias sanciones penales a nivel nacional e internacional.

La comunidad universitaria puede ofrecer sus servicios estudiantiles para reconocer y desnudar el fraude electrónico.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, L. (2011). Introducción. Estado Del Arte De La Ciberseguridad. En Ciberseguridad. Retos Y Amenazas A La Seguridad Nacional En El Ciberespacio. Ministerio De Defensa. Disponible en http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Arias, F. (2012). El Proyecto de investigación. Caracas: Epísteme Editores.

Ávila, K. (2015). Acoso cibernético. Disponible en: http://www.amnistia.ong/group/bolivar/Blog/consideraciones-sobre-acoso-cibernetico

Ballestrini, M. (2011). Como se elabora un proyecto de investigación. Caracas: Ed. Panapo.

Cañarte, T. (2017). Cyberbullying: el acoso a través de las redes sociales en jóvenes universitarios. Disponible en file:///C:/Users/Adm /Downloads/Dialnet-Cyberbullying-6102839.pdf

Castellanos, D. (2016). Consumo Inteligente, Cómo suceden los fraudes electrónicos. Disponible en http://www.finanzaspersonales.co/gaste-eficientemente/articulo/como-suceden-los-fraudes-electronicos/37912

Chávez, N. (2012). Introducción a la investigación educativa. (4a ed). Maracaibo, Venezuela.

Figueroa Campos, M. (2015). Profesora de la Facultad de Psicología de la UNAM.Ciberbullying: perfil de víctimas y victimarios. Disponible en http://ciencia.unam.mx/leer/418/Ciberbullying_perfil_de_victimas_y_victimarios

Finkelhor, D., Mitchell, K. J., y Wolak, J. (2000). Online Victimization: A Report on the Nation's Young People. ERIC (Educational Resources Information Center).

Finn, J. (2004). A Survey of Online Harassment at a University Campus J. Interpersonal Violence, 19 (4) (2004), p. 468 CrossRefView Record in Scopus.

García, L. (2014). La Investigación de Delitos Emergentes en Internet, su Detección y Control. Disponible en http://biblio3.url.edu.gt /Tesario/2014/07/03/Garcia-Ligia.pdf

Gilbert, P. (1999). On Space, Sex and Stalkers Women and performance, 17 (1999), pp. 1-18 View Record in Scopus.

Henostroza, W. (2016). 10 herramientas para buscar personas en redes sociales. Disponible en https://www.webespacio.com/herramientas-para-buscar-personas-redes-sociales/

Hernández Monsalve, M. (2011). Enfermedad mental y delito. Una perspectiva europea. Disponible en: http://www.caritas.es/imagesrepository/CapitulosPublicaciones/4235/07

Hernández, R., Fernández, C. y Baptista, L. (2011). Metodología de la Investigación. México. Mc Graw Hill.

Instituto Nacional de Estadística y Geografía (INEGI, 2018). Módulo sobre Ciberacoso del INEGI. Disponible en https://www.elheraldodechihuahua.com.mx/local/hombres- quienes-sufren-mas-acoso-en-nivel-universitario-1678686.html

Kowalski y Limber, R. (2007). Electronic bullying among middle school students Journal of Adolescent Health, 41 (2007), pp. 22-30.

Maple, C. Short, E. y Brown, A. (2011). Cyberstalking in the United Kingdom, An analysis of the Echo Pilot. Disponible en http://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf

McGraw, (1995). Sexual Harassment in Cyberspace: The Problem of Unwelcome RUTGERS COMP. & TECH, New York (1995).

McKenna, A., Green, M. y Gleason, J. (2002). Relationship Formation on the Internet: What's the Big Attraction? Journal of Social Issues, 58 (1) (2002), pp. 9-31 View Record in Scopus.

Ogilvie, E. (2012). Cyberstalking. Disponible en http://www.aic.gov.au/documents/4/7/A/%7B47A7FA60-8EBF-498A-BB9E-D61BC512C053%7Dti166.pdfReno, 1999).

Ortega, R., Calmastra, J., y Mora, J. (2008). Cyberbullying. International Journal of Psychology and Psychological Therapy, 8, 183-192. Recuperado de: http:// www.redalyc.org/src/inicio/ArtPdfRed.jsp?iCve=56080204yiCveNum=10533

Ortega, R., Del Rey, R., y Casas, J. A. (2013b). Redes Sociales y Cyberbullying. El proyecto ConRed. Convives Revista Digital, 3(2013, abril), 34-44.

Papa, Y. (2015). La mente del acosador. Disponible en https://lamenteesmaravillosa.com/la-mente-del-acosador/

Pelekais, C. Finol, M., Neuman, N. y Belloso, O. (2012). El ABC de la Investigación. (2a. ed). Maracaibo: Editorial Astro Data AS.

Pérez, V. (2013). Bullying: ¿Qué ocurre cuando el profesor es la víctima?. Disponible en http://www.estampas.com/cuerpo-y-mente/131110/bullying-que-ocurre-cuando-el-profesor-es-la-victima

Picazo-Vela, S. (2016). Las redes sociales: oportunidades y riesgos. Disponible en https://contexto. udlap.mx/ las-redes -sociales-oportunidades-y-riesgos/

Pinto, C. (2015). Ciberacoso y Ciberbullying I. Disponible en http://www. informaticayperitaje.com/ciberacoso-y-ciberbullying-i/

Polo del Río, M., Mendo, S., León, B. y Castaño, E. (2017). Abuso del móvil en estudiantes universitarios y perfiles de victimización y agresión. Departamento de Psicología y Antropología de la Universidad de Extremadura. Disponible en http://www. adicciones.es /index.php/adicciones/article/viewFile/837/843

Ramírez, T. (2012). Como hacer un Proyecto de Investigación. Caracas Editorial Panapo.

Redondo, J., Luzardo, M., Garcia, K. y Cándido, J. (2017). Impacto Psicológico del Ciberbullying en Estudiantes Universitarios: Un Estudio Exploratorio. Universidad Pontificia Bolivariana, seccional Bucaramanga, Colombia. Universidad Miguel Hernández de Elche, España.

Retana, B. y Sánchez, R. (2015). Acoso Cibernético: Validación en México del ORI-82. Acta de Investigación Psicológica - PsychologicalResearch Records, vol. 5, núm. 3, diciembre, 2015, pp. 2097-2112. Universidad Nacional Autónoma de México. Distrito Federal, México.

Rodríguez, Á. (2012). Delitos y guerras informáticas. Corporación Colombia Digital. Disponible en: https:// www.colombiadigital.net /opinion/ columnistas/ cuestion-devoltaje/item/1417-ahora-la-lucha-es-contra-los-ciberdelitos.html

Romero, J. (2015). Auditoría de la seguridad cibernética. Disponible en https://es.slideshare.net/romeprofe/auditora-de-la-seguridad-ciberntica

Sabino, C. (2012). El Proceso de Investigación. Venezuela: Editorial Panapo.

Spence-Diehl, E. (2003). Stalking and Technology: The Double-Edged Sword J. Tech. In Human Services, 22 (1) (2003), p. 5 CrossRefView Record in Scopus

Tamayo y Tamayo, M. (2012). El Proceso de Investigación Científica. (5a Ed). México: Editorial Limusa S.A.

Vélez, D. (2016). Hostigamiento y Acoso Sexual (HAS) en redes sociodigitales. Disponible en http://www.revista.unam.mx/vol.18/num1/art05/

Villafranca, D. (2012). Metodología de la Investigación San Antonio de los Altos. Miranda, Venezuela: Fundaca.

ANEXOS

ESCALA DE ACOSO CIBERNÉTICO

N Nunca	CN Casi Nunca	O Ocasionalmente	CS Casi Siempre	S Siempre

	ÍTEMS VIGILANCIA REMOTA	1 N	2 CN	3 O	4 CS	5 S
Durante los últimos tres meses, has observado que segundas personas se dedican a estar:						
1	Monitoreándole a través de GPS o dispositivos de seguimiento					
2	Monitoreándole usando video encubierto a través de cámaras digitales					
3	Vigilando su computadora usando spyware o el software “TrojanHorse” para infectar su computadora u otras tecnologías de comunicación					
4	Vigilándole a través de dispositivos de audición (p. ej. “bugs” o micrófonos ocultos o dispositivos de grabación de voz)					
5	Intentando desactivar su equipo (p. ej. descargando virus, enviando demasiados mensajes que su sistema no puede manejar, etc.)					
6	Hostigando a su avatar dentro de un grupo cibernético (p. ej., estropeando la identidad de su avatar, siguiéndolo, interfiriendo o realizando otras actividades molestas en un espacio sintético de computadora, etc.)					
7	Alterando su identidad electrónica, es decir su avatar (p. ej. irrumpiendo su sistema y cambiando su firma, información personal, o cómo se retrata usted electrónicamente, etc.)					
8	Asumiendo su identidad o personaje electrónico (p. ej., presentándose a sí mismo con los demás en las salas de chat, tablones de anuncios, pornografía o sitios de solteros, etc.)					
9	Dirigiéndose a otros en forma amenazante (p. ej., haciéndose pasar por usted en el chat y solicitar actos sexuales arriesgados, secuestro, fantasías, etc.)					

ÍTEMS BÚSQUEDA DE INTERACCIÓN	1 N	2 CN	3 O	4 CS	5 S
Durante los últimos tres meses, has observado que segundas					

personas se dedican a estar:						
10	Siguiéndole o notificando en redes sociales (p. ej., pasando tiempo en su Facebook, MySpace, u otros sitios de redes sociales, agregarlo como amigo o de otra manera obteniendo acceso desconocido o no deseado en sus redes sociales, etc.)					
11	Enviando mensajes a través del correo (p. ej. notas, cartas, imágenes, etc. a través del correo)					
12	Contactándose con usted "en vivo" a través de medios electrónicos (p. ej., hostigándole por teléfono, intercambiando chat o mensajes instantáneos, tweets/twitter, etc.)					
13	Dejándole mensajes electrónicos afectuosos (p. ej., expresando su atracción o afecto en correos de voz, correo electrónico, mensajes instantáneos, fax, etc.)					
14	Ciber-acosándole (p. ej., dejando grandes cantidades de mensajes en su correo electrónico, introducirse en su chat o espacio de juego, bloquear su computadora, etc.)					
15	Monitorearle constantemente, etiquetando, donando en su sitio o red social (p. ej., etiquetando sus fotos invitándolo(a) o respondiendo invitaciones a unirse a grupos, escribiendo en su muro, preguntando sobre sus posts, etc.)					

ÍTEMS DESPRESTIGIO SOCIAL		**1 N**	**2 CN**	**3 O**	**4 CS**	**5 S**
Durante los últimos tres meses, has observado que segundas personas se dedican a estar:						
16	"Saboteando" su reputación privada (p. ej., difundiendo rumores sobre usted, sus relaciones o actividades con los amigos, familia, pareja, etc.)					
17	"Saboteando" su reputación de trabajo/escuela (p. ej. difundiendo rumores sobre usted, sus relaciones o actividades en redes organizacionales, boletines electrónicos, etc.)					
18	Obteniendo información privada sin su permiso (p. ej. entrar de forma encubierta a sus archivos de computadora, correo de voz, o los archivos de compañeros de trabajo, amigos o familiares, etc.)					
19	Exponiendo su información privada a otros (p. ej., enviándole un correo a los demás sobre sus secretos, información comprometedora, números privados, etc.)					
20	Pretendiendo ser alguien que ella o él no era (p. ej., representación falsa de él o ella como persona de un sexo diferente, usando una identidad, status o posición falsa, haciéndose pasar por usted, etc.)					
21	"Espiando" su coche, casa u oficina (p. ej., poniendo dispositivos ocultos de audición o grabación, etc.)					

ÍTEMS ACERCAMIENTO GRADUAL	**1 N**	**2 CN**	**3 O**	**4 CS**	**5 S**
Durante los últimos tres meses, has observado que segundas personas se dedican a estar:					

22	Conociéndole primero en línea y después interferir en su vida (p. ej. apareciendo inesperadamente en su trabajo, la puerta principal, el estacionamiento, entrometiéndose en sus conversaciones, etc.)					
23	Conociéndole primero en línea y después perjudicándole (p. ej., se relaciona con usted a través de un servicio de citas en línea y después le sigue, le hostiga, o bien lo acosa)					
24	Conociéndole primero en línea y después seguirle (p. ej., siguiéndole mientras conduce, alrededor del campus o en el trabajo, o en sus actividades sociales o en el gimnasio, etc.)					
25	Conociéndole primero en línea y después le acosa (p. ej. se relaciona con usted a través de un servicio de citas en línea o como conocidos, y luego lo(a) sigue, hostiga, o lo(a) acosa).					

ÍTEMS HOSTIGAMIENTO SEXUAL		**1 N**	**2 CN**	**3 O**	**4 CS**	**5 S**
Durante los últimos tres meses, has observado que segundas personas se dedican a estar:						
26	Enviando mensajes excesivamente reveladores (p. ej. dando inadecuadamente información privada acerca de su vida, cuerpo, familia, pasatiempos, experiencias sexuales, etc.).					
27	Enviando o demandando mensajes excesivamente “necesitados” (p. ej., presionando para que se vean, pidiendo firmemente una cita, discutiendo para que le de “otra oportunidad”, etc.)					
28	Enviando mensajes de hostigamiento sexual (p. ej. describiendo actos sexuales hipotéticos entre ustedes, haciendo observaciones sexuales denigrantes, etc.)					
29	Enviando mensajes o imágenes obscenos/pornográficos (p. ej. fotografías o ilustraciones de personas desnudas, o de personas o animales participando en actos sexuales, etc.)					
30	Dejando mensajes electrónicos agresivos (p. ej., insultar o quejarse en el buzón de voz, email, mensajes instantáneos, fax, etc.)					

ÍTEMS DENUNCIAS		**1 N**	**2 CN**	**3 O**	**4 CS**	**5 S**
Ante el hecho de presenciar o ser objeto de ciberacoso, su reacción personal ha sido.						
31	Presentar la denuncia judicial ante el CICPC.					
32	Presentar la denuncia judicial ante Defensoría del Pueblo					
33	Presentar la denuncia judicial ante INAMUJER de ser el caso					

ÍTEMS REFUERZO DE LA CONDUCTA	**1 N**	**2 CN**	**3 O**	**4 CS**	**5 S**
Ante el hecho de presenciar o ser objeto de ciberacoso, su					

reacción personal ha sido.						
34	Dar apoyo para continuar hostigamiento					
35	Dar apoyo con estrategias digitales informáticas para descubrir a acosador					

ÍTEMS AUDITORIA INFORMÁTICA		1 N	2 CN	3 O	4 CS	5 S
En los casos de ciberacoso, sus conocimientos en el área de computación le han permitido:						
36	Guíar auditoria informática para descubrir violación de seguridad de programas					
37	Guíar auditoria informática para develar violación de datos confidenciales					
38	Guíar auditoria informática para presentar pruebas legales del delito					
39	Ha utilizado Pandora recovery para colaborar como experto informático					
40	Ha utilizado la herramienta RECUVA para colaborar como experto informático					
41	Se ha valido de la herramienta UNDELETE PLUS para colaborar como experto informático en casos de ciberdelitos					
42	Se ha valido de la herramienta RESTORIATION para colaborar como experto informático en casos de ciberdelitos					
43	Le ha servido el CIFRADO SIMÉTRICO para colaborar como experto informático en casos de ciberdelitos					

MUCHAS GRACIAS…

RESULTADOS DE LA APLICACIÓN DEL CUESTIONARIO
CÁLCULO DE LA MEDIA ARITMÉTICA

	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10	P-11	P-12	P-13	P-14	P-15	P-16	P-17	P-18	P-19	P-20	suma	media	
ÍT-1	3	1	1	1	3	1	1	2	1	1	1	1	1	2	1	1	1	1	2	1	1,35	1,311	1,9
ÍT-2	1	1	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	3	1	1	1,25		
ÍT-3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1,15		
ÍT-4	1	1	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	1	2	1	1,2		
ÍT-5	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	2	1	1,15		
ÍT-6	1	1	1	1	1	1	1	1	4	1	1	1	3	1	1	4	1	2	1	1	1,45		
ÍT-7	1	1	1	1	1	1	1	1	4	1	1	1	3	1	1	4	1	2	1	1	1,45		
ÍT-8	1	1	1	1	1	1	1	1	4	1	1	1	3	1	1	4	1	2	1	1	1,45		
ÍT-9	1	1	1	1	1	1	2	1	4	1	1	1	1	1	1	4	1	1	1	1	1,35		
ÍT-10	3	2	2	1	1	1	2	1	3	1	1	1	1	1	1	4	2	2	1	1	1,6	1,875	
ÍT-11	3	2	2	3	1	2	2	1	3	2	1	1	2	1	1	4	4	2	2	1	2		
ÍT-12	1	1	3	2	2	2	1	2	2	2	1	1	3	1	1	1	1	1	2	1	1,55		
ÍT-13	1	2	3	1	2	2	2	3	3	1	1	1	3	1	1	2	4	4	2	1	2		
ÍT-14	1	2	3	1	2	3	2	2	3	2	1	1	3	1	1	2	4	4	2	1	2,05		
ÍT-15	1	2	3	1	2	2	3	1	3	1	1	1	2	2	1	4	4	4	2	1	2,05		
ÍT-16	4	2	2	1	3	3	4	4	3	2	4	5	2	2	2	4	1	1	4	4	2,85	2,808	
ÍT-17	1	4	3	5	3	2	5	4	3	2	4	1	3	2	2	4	1	1	4	1	2,75		
ÍT-18	2	5	2	1	1	1	2	3	2	3	4	5	3	2	1	4	1	3	4	5	2,7		
ÍT-19	3	1	5	5	3	5	2	3	2	3	4	1	3	2	5	4	5	3	4	1	3,2		
ÍT-20	4	5	1	1	2	1	2	1	2	3	3	5	2	2	1	4	1	4	4	5	2,65		
ÍT-21	1	1	5	5	4	5	1	3	1	1	1	5	1	2	5	1	5	1	1	5	2,7		
ÍT-22	4	1	3	1	3	2	4	3	3	2	1	1	1	2	1	1	1	1	1	1	1,85	1,95	
ÍT-23	1	1	1	1	2	1	1	3	3	2	1	1	2	2	1	1	2	1	1	1	1,45		
ÍT-24	1	1	1	1	2	1	1	2	3	2	1	1	2	2	1	1	2	1	1	1	1,4		
ÍT-25	1	1	2	1	2	1	1	1	2	2	2	1	1	2	1	1	2	1	1	1	1,35		
ÍT-26	1	2	3	1	1	2	3	2	3	2	2	1	2	1	2	2	1	1	2	1	1,75	1,75	
ÍT-27	1	2	2	1	3	1	3	2	3	2	2	1	2	3	1	1	1	3	2	1	1,85		
ÍT-28	1	1	1	1	3	1	3	2	3	1	2	1	2	3	1	1	3	3	3	1	1,85		
ÍT-29	1	1	1	1	3	1	3	2	2	1	2	1	2	2	1	1	3	4	3	1	1,8		
ÍT-30	1	1	1	1	2	2	1	3	2	2	1	1	2	2	1	2	1	1	2	1	1,5		
ÍT-31	1	1	1	1	1	1	1	3	3	1	1	1	1	1	1	1	1	5	1	1	1,4	1,183	1,5
ÍT-32	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
ÍT-33	1	1	1	1	1	1	1	4	1	1	1	1	1	1	1	1	1	1	1	1	1,15		
ÍT-34	1	1	1	1	1	1	1	1	1	1	2	1	2	2	1	2	1	1	2	1	1,25	1,75	
ÍT-35	3	1	2	3	1	1	4	3	1	2	1	2	3	1	1	3	4	5	3	1	2,25		
ÍT-36	3	1	1	1	3	1	2	1	1	2	1	1	2	1	1	1	1	5	2	1	1,6	1,617	1,5
ÍT-37	3	1	1	1	3	1	2	1	1	1	1	1	2	1	1	2	3	5	3	1	1,75		
ÍT-38	1	1	1	1	2	1	2	1	1	2	1	1	1	1	1	2	1	5	3	1	1,5		
ÍT-39	1	1	1	1	3	1	2	1	1	2	1	3	3	1	1	2	1	1	3	1	1,55	1,45	
ÍT-40	1	1	1	1	3	1	1	1	1	3	1	3	2	1	1	2	2	1	3	1	1,55		
ÍT-41	1	1	1	1	1	1	2	1	1	3	1	3	2	1	1	2	1	1	3	1	1,45		
ÍT-42	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	3	1	1,2		
ÍT-43	1	1	1	1	2	1	3	1	3	1	1	2	1	1	1	1	3	3	1	1	1,5		

ESTADÍSTICAS PARA EL CÁLCULO DE LA CONFIABILIDAD

P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9	P-10	P-11	P-12	P-13	P-14	P-15	P-16	P-17	P-18	P-19	P-20	suma
3	1	1	1	3	1	1	2	1	1	1	1	1	2	1	1	1	1	2	1	27
1	1	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	3	1	1	25
1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	23
1	1	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	1	2	1	24
1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	2	1	23
1	1	1	1	1	1	1	1	4	1	1	1	3	1	1	4	1	2	1	1	29
1	1	1	1	1	1	1	1	4	1	1	1	3	1	1	4	1	2	1	1	29
1	1	1	1	1	1	1	1	4	1	1	1	3	1	1	4	1	2	1	1	29
1	1	1	1	1	1	2	1	4	1	1	1	1	1	1	4	1	1	1	1	27
3	2	2	1	1	1	2	1	3	1	1	1	1	1	1	4	2	2	1	1	32
3	2	2	3	1	2	2	1	3	2	1	1	2	1	1	4	4	2	2	1	40
1	1	3	2	2	2	1	2	2	2	1	1	3	1	1	1	1	1	2	1	31
1	2	3	1	2	2	2	3	3	1	1	1	3	1	1	2	4	4	2	1	40
1	2	3	1	2	3	2	2	3	2	1	1	3	1	1	2	4	4	2	1	41
1	2	3	1	2	2	3	1	3	1	1	1	2	2	1	4	4	4	2	1	41
4	2	2	1	3	3	4	4	3	2	4	5	2	2	2	4	1	1	4	4	57
1	4	3	5	3	2	5	4	3	2	4	1	3	2	2	4	1	1	4	1	55
2	5	2	1	1	1	2	3	2	3	4	5	3	2	1	4	1	3	4	5	54
3	1	5	5	3	5	2	3	2	3	4	1	3	2	5	4	5	3	4	1	64
4	5	1	1	2	1	2	1	2	3	3	5	2	2	1	4	1	4	4	5	53
1	1	5	5	4	5	1	3	1	1	1	5	1	2	5	1	5	1	1	5	54
4	1	3	1	3	2	4	3	3	2	1	1	1	2	1	1	1	1	1	1	37
1	1	1	1	2	1	1	3	3	2	1	1	2	2	1	1	2	1	1	1	29
1	1	1	1	2	1	1	2	3	2	1	1	2	2	1	1	2	1	1	1	28
1	1	2	1	2	1	1	1	2	2	2	1	1	2	1	1	2	1	1	1	27
1	2	3	1	1	2	3	2	3	2	2	1	2	1	2	2	1	1	2	1	35
1	2	2	1	3	1	3	2	3	2	2	1	2	3	1	1	1	3	2	1	37
1	1	1	1	3	1	3	2	3	1	2	1	2	3	1	1	3	3	3	1	37
1	1	1	1	3	1	3	2	2	1	2	1	2	2	1	1	3	4	3	1	36
1	1	1	1	2	2	1	3	2	2	1	1	2	2	1	2	1	1	2	1	30
1	1	1	1	1	1	1	3	3	1	1	1	1	1	1	1	1	5	1	1	28
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	20
1	1	1	1	1	1	1	4	1	1	1	1	1	1	1	1	1	1	1	1	23
1	1	1	1	1	1	1	1	1	1	2	1	2	2	1	2	1	1	2	1	25
3	1	2	3	1	1	4	3	1	2	1	2	3	1	1	3	4	5	3	1	45
3	1	1	1	3	1	2	1	1	2	1	1	2	1	1	1	1	5	2	1	32
3	1	1	1	3	1	2	1	1	1	1	1	2	1	1	2	3	5	3	1	35
1	1	1	1	2	1	2	1	1	2	1	1	1	1	1	2	1	5	3	1	30
1	1	1	1	3	1	2	1	1	2	1	3	3	1	1	2	1	1	3	1	31
1	1	1	1	3	1	1	1	1	3	1	3	2	1	1	2	2	1	3	1	31
1	1	1	1	1	1	2	1	1	3	1	3	2	1	1	2	1	1	3	1	29
1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	3	1	24
1	1	1	1	2	1	3	1	3	1	1	2	1	1	1	1	3	3	1	1	30
																				112
									0,9					0,09		1,02				10,6

UNIVERSIDAD VALLE DEL MOMBOY

DECANATO DE LA FACULTAD DE INGENIERÍA

INGENIERÍA EN COMPUTACIÓN

CARVAJAL ESTADO TRUJILLO

CONSTANCIA DE VALIDACIÓN

Yo, Claribel Silva, titular de la Cédula de Identidad Nº 12.540.703 certifico que realicé el juicio de experto del instrumento diseñado por YORDY ROMERO VALERA C.I.No. 24.881.868 y YOANIS JESÚS PÉREZ MACHADO C.I.No. 23.775.764 para desarrollar el TRABAJO ESPECIAL DE GRADO, titulado: ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA EN LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO.

En Valera a los veintiséis días del mes de junio de 2018.

Firma

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD VALLE DEL MOMBOY

DECANATO DE LA FACULTAD DE INGENIERÍA

INGENIERÍA EN COMPUTACIÓN

CARVAJAL ESTADO TRUJILLO

CONSTANCIA DE VALIDACIÓN

Yo, Yumary Del Valle Valcellos Barrete, titular de la Cédula de Identidad Nº 14151309, certifico que realicé el juicio de experto del instrumento diseñado por YORDY ROMERO VALERA C.I.No. 24.881.868 y YOANIS JESÚS PÉREZ MACHADO C.I.No. 23.775.764 para desarrollar el TRABAJO ESPECIAL DE GRADO, titulado: ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA EN LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO.

En Carvajal a los 27 días del mes de Junio de 2018.

Yumary Valcellos

Firma

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD VALLE DEL MOMBOY

DECANATO DE LA FACULTAD DE INGENIERÍA

INGENIERÍA EN COMPUTACIÓN

CARVAJAL ESTADO TRUJILLO

CONSTANCIA DE VALIDACIÓN

Yo, Ing. Javier Mazzey, titular de la Cédula de Identidad Nº 11319775, certifico que realicé el juicio de experto del instrumento diseñado por YORDY ROMERO VALERA C.I.No. 24.881.868 y YOANIS JESÚS PÉREZ MACHADO C.I.No. 23.775.764 para desarrollar el TRABAJO ESPECIAL DE GRADO, titulado: ACOSO CIBERNÉTICO EN LA FACULTAD DE INGENIERA EN LA UNIVERSIDAD VALLE DEL MOMBOY, ESTADO TRUJILLO.

En Carvajal a los 27 días del mes de Junio de 2018.

Firma