FACULTAD DE CIENCIAS PEDAGÓGICAS

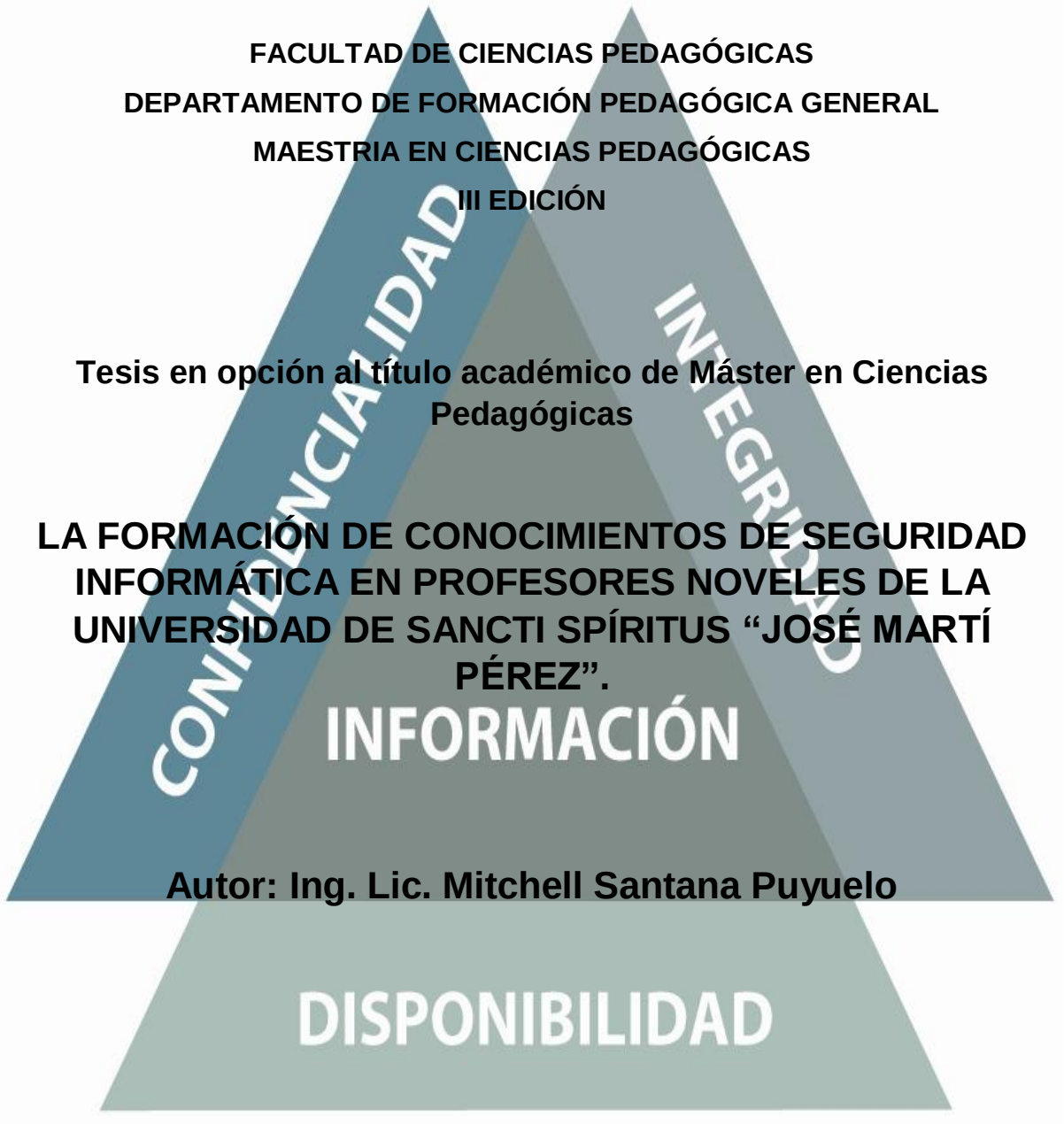
DEPARTAMENTO DE FORMACIÓN PEDAGÓGICA GENERAL

MAESTRIA EN CIENCIAS PEDAGÓGICAS

III EDICIÓN

Tesis en opción al título académico de Máster en Ciencias Pedagógicas

LA FORMACIÓN DE CONOCIMIENTOS DE SEGURIDAD INFORMÁTICA EN PROFESORES NOVELES DE LA UNIVERSIDAD DE SANCTI SPÍRITUS "JOSÉ MARTÍ PÉREZ".



Autor: Ing. Lic. Mitchell Santana Puyuelo

Sancti Spíritus

2018

FACULTAD DE CIENCIAS PEDAGÓGICAS

DEPARTAMENTO DE FORMACIÓN PEDAGÓGICA GENERAL

MAESTRIA EN CIENCIAS PEDAGÓGICAS

III EDICIÓN

Tesis en opción al título académico de Máster en Ciencias Pedagógicas

LA FORMACIÓN DE CONOCIMIENTOS DE SEGURIDAD INFORMÁTICA EN PROFESORES NOVELES DE LA UNIVERSIDAD DE SANCTI SPÍRITUS “JOSÉ MARTÍ PÉREZ”.

Autor: Ing. Lic. Mitchell Santana Puyuelo

Tutor: Dr.C Arlex Valdés González. Profesor Titular

Sancti Spíritus

2018

DEDICATORIA

A la memoria de mi abuelo Hector Puyuelo Consuegra, “Api”.

AGRADECIMIENTOS

Deseo plasmar mi más sincera gratitud a todos los profesores de la Maestría en Ciencias Pedagógicas, III edición, los cuales contribuyeron con su saber para que hoy pueda llevar a feliz término esta investigación.

A la Universidad de Sancti Spíritus “José Martí Pérez”, donde me he formado primero como Ingeniero Agrónomo, luego como Licenciado en Ciencias Informáticas y que hoy me permite defender este proyecto en opción al título de Máster en Ciencias Pedagógicas, lo que me incita a continuar creciendo profesionalmente.

Al DrC. Arlex Valdés González, quién me brindó su apoyo profesional y aportó ideas para la materialización del proyecto que hoy defiendo.

A mi esposa Alena Medina Echevarría, que está en cada uno de mis pensares y es sustento en lo personal y profesional.

A mis padres Aleida Puyuelo Hernández y Martín Santana Sotolongo, que siempre me han apoyado y motivado a alcanzar mis metas.

A mi hermana Mairelys y su hijo Thiago Adam, que son la energía que dinamiza nuestro hogar.

A Carlitos y Yailín, compañeros que siempre me brindaron ideas, ánimo y apoyo para poder concretar este proyecto.

A todas las personas que contribuyeron a la realización de esta investigación.

A todos muchas gracias.

RESUMEN

En la sociedad actual, globalizada y tecnológica, la superación del profesional en temas de seguridad informática es fundamental, más aún si se asocia a instituciones que constantemente producen e intercambian grandes cúmulos de información, como las universidades. La presente investigación fue motivada por un diagnóstico a la seguridad informática en la Universidad de Sancti Spíritus "José Martí Pérez", que determinó carencias en la formación de conocimientos que sobre el tema poseían los usuarios; en relación a lo cual, se propone una estrategia de superación profesional para la formación de seguridad informática en profesores noveles, con el fin de contribuir a su desempeño docente. Para ello se conjugó un sistema de métodos teóricos, empíricos y matemáticos, que posibilitó elaborar, implementar y valorar la propuesta, y arribar a conclusiones. Su instrumentación en la práctica provoca una modificación significativa de la formación de conocimientos sobre seguridad informática en profesores noveles, a partir de las diferencias observadas en la aplicación del pre-experimento pedagógico.

ÍNDICE

INTRODUCCIÓN

El siglo XXI ha trazado veloces retos al avance de las naciones. La globalización del recurso información se ha visto potenciada por el creciente desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), convertidas en piedra angular de procesos económicos, políticos y socioculturales. La informatización acelerada en todos los órdenes de la vida contemporánea, constituye un proceso de vital importancia, que encuentra características singulares en países en vías de desarrollo, con menos presupuesto para invertir en la infraestructura adecuada, en recursos humanos para el diseño de softwares o en la creación de capacidades para el uso de las TIC en una población empobrecida y con altos índices de analfabetismo.

En la región latinoamericana, Cuba resulta un caso singular, cuyo gobierno se ha identificado desde muy temprano con la necesidad de introducir y dominar las TIC en la práctica social: “La informática se convertirá en una poderosísima fuerza científica, económica e incluso política del país” (Castro, F., 2006). El gobierno revolucionario se planteó esta tarea como una prioridad nacional, expresada en los Lineamientos de la política económica y social del Partido y la Revolución (lineamientos 129-139, 2011), no solo como una vía para lograr mayor eficacia y eficiencia en todos los procesos que determinan la producción de riqueza, sino también para aumentar la calidad de vida de los ciudadanos.

En la clausura del Primer Taller Nacional Informatización y Ciberseguridad, celebrada el 20 de febrero del 2015, el Vicepresidente cubano Miguel Díaz-Canel entiende la informatización en Cuba como una meta colectiva: “[…] es un proceso complejo, retador, necesario, que tiene que ser abordado en la multi y la interdisciplinariedad, con visión de país y contando con la participación institucional y ciudadana, el cual debe abarcar transversalmente todos los escenarios y ámbitos de la vida política, económica y social del país, y constituir un imprescindible apoyo y soporte al perfeccionamiento integral de nuestra sociedad socialista, próspera y sostenible”.

A la universidad toca un rol medular en este proceso masivo, en la formación de profesionales competentes y útiles, capaces de enfrentar los retos que la Sociedad de la Información y las Comunicaciones les imponen, capaces de aunar ciencia y tecnología en su labor cotidiana. Pero, aquí la informatización cobra una doble dirección, la difusión de la cultura digital en futuros egresados y, además, el aprovechamiento de los recursos tecnológicos y el acceso y manejo de la información como herramientas útiles al desarrollo de múltiples procesos docentes, científico-investigativos y extensionistas.

Pasados los tiempos medievales en que gremios de profesores y estudiantes (*universitas magistrorum et scholarium*) convergían para la instrucción y difusión de saberes; la universidad moderna ha pasado de la simple reproducción a la creación de conocimiento útil a la sociedad. Se ha transformado en centro productor de cultura, ciencia y tecnología, y para ello, diariamente accede, genera e intercambia grandes volúmenes de información.

En este contexto, la seguridad informática deviene un proceso de vital importancia para garantizar la integridad, disponibilidad y confidencialidad de la información, contra las continuas amenazas y ataques externos e internos a los que se ven sometidas instituciones, empresas y organizaciones por igual, que pueden causar daños irreparables y que resultan totalmente prevenibles.

La seguridad informática es una disciplina cambiante en el marco de las ciencias informáticas, debido al veloz desarrollo de las tecnologías y la informatización de la sociedad, y consecuentemente, al incremento de los delitos y amenazas a los productos y servicios informáticos del mundo entero. Esta dinámica exige la continua superación y actualización de los profesionales de la disciplina, así como la necesidad de orientar y educar a los diferentes usuarios de las redes telemáticas para lograr verdadera competencia en la labor de protección y prevención.

En el plano científico, abunda la investigación en torno a la protección informática de las diversas organizaciones, entre las que priman los gobiernos, las universidades y sobre todo, las empresas, que invierten considerables sumas en

proteger sus datos, actualizar sus softwares y perfeccionar sus mecanismos de protección (Ugas, 2002; Badopi, 2003; González, 2004; Aguirre Murillo, 2005; Viloria, Villegas y Blanco, 2009; Acosta y Negrete, 2012; Alfonso y Arocha, 2012; Ramírez, 2012; Morán, 2016). También, abunda la investigación en torno al desarrollo y actualización de los softwares que monitorean las redes, en busca de vulnerabilidades o brechas a los sistemas informáticos (Stallings, 2003; Trukulo, 2003; Morales, 2006; Lara, 2010). Es de destacar la brecha científica en la carencia de estudios que involucran directamente al usuario y su responsabilidad y aportes a la seguridad informática, que encontramos en la obra del norteamericano Spears (2007; Spears y Barker, 2010).

En Cuba, garantizar la seguridad informática se ha convertido en un aspecto estratégico en la política de todas las organizaciones a lo largo y ancho del país. Con este fin, se han desarrollado diferentes organismos e iniciativas que lideran los procesos de seguridad de la información, regidos por el Ministerio del Interior, el Ministerio de Auditoría y Control y el Ministerio de la Informática y las Comunicaciones: la empresa Segurmática, la Oficina de Seguridad de Redes Informáticas (OSRI) y la Oficina de Seguridad de la Información Clasificada (OSIC), entidades encargadas de la prevención y control.

Dentro de este panorama, el Ministerio de Educación Superior (MES) tiene creada una amplia red informática, que conecta a todas las universidades y Centros Universitarios Municipales (CUM) cubanos. De allí la importancia de considerar la seguridad informática como un proceso de apoyo dentro del Sistema de Gestión de la Calidad que franquea cada uno de los demás procesos estratégicos, claves y de apoyo, desde sus funciones preventivas, educativas, normativas, de control y sanción o retroalimentación. Como entidad que dirige el funcionamiento de las universidades cubanas, el MES se rige por la Resolución 127 (2007) del Ministerio de la Informática y las Comunicaciones (MIC), que plantea el diseño de planes de protección de la información (Plan de Seguridad Informática).

En el plano científico, las investigaciones sobre seguridad informática en Cuba aún son bastante incipientes, representados en la obra de Walter Baluja, director de

seguridad informática del MES y de Raydel Montesino Perurena, vicerrector de la Universidad de las Ciencias Informáticas (UCI) (Montesino, Baluja y Porvén, 2013).

En la Universidad de Sancti Spíritus “José Martí Pérez” (Uniss), un grupo de especialistas vela por la implementación de este Plan, manteniendo relaciones de retroalimentación con todas las áreas de la institución. Entre sus tareas fundamentales, este grupo determina las amenazas y vulnerabilidades de la seguridad informática, a partir de un sistema de supervisión y control que atiende dos dimensiones: lógica (protección de la información digital) y física (protección de los medios tecnológicos tangibles).

El balance de los informes de seguridad informática de la Uniss en los últimos tres años, arroja como resultado que el 90% de las violaciones provienen de la negligencia o la ignorancia de los usuarios de la RedUniss sobre estos temas, tales como: acceso a páginas que no cumplen con el objeto social de la universidad; empleo de la red con fines personales; acceso a sitios que vulneran la seguridad de la red (navegación anónima); transferencia negligente de la identidad del usuario a otra persona; ejecución de dispositivos extraíbles contaminados con virus informáticos sin previo análisis del antivirus; almacenamiento de documentos clasificados (exámenes, actas, informes) en computadoras conectadas a la red sin protección; empleo de un usuario común en una computadora.

Un diagnóstico exploratorio sobre la seguridad informática en la Uniss evidenció otras manifestaciones de la problemática:

- Superficialidad y rutina en el análisis del Código de ética de la RedUniss por los usuarios.

- No se contempla la seguridad informática como requisito o tarea para un buen desempeño laboral, en documentos que legislan, norman o trazan directrices, como contratos de trabajo, políticas científicas, estrategias de comunicación, etc.

- Falta de espacios físicos y digitales para la promoción de la seguridad informática pues, aunque existe una sección dedicada a la temática en la intranet de la Uniss (http//uniss.edu.cu/dirección de informatización/seguridad informática), sus contenidos están desactualizados, y carece de visibilidad y capacidad de interacción con el usuario.

- Baja percepción, por parte de los directivos, del riesgo que genera el mal uso de la RedUniss por los usuarios de sus respectivas áreas.

- No existen líneas, proyectos o grupos de investigación que se ocupen expresamente de la seguridad informática.

- Carencia de programas de posgrado que garanticen la formación o la superación profesional en estos temas.

- No se incluyen contenidos de seguridad informática en la preparación de los profesores noveles, aunque sí reciben adiestramiento en competencias informáticas.

El profesor novel es uno de los usuarios más activos de la RedUniss, con amplias capacidades creadas para el acceso y manejo de la información digital. Como nativo de la Sociedad de la Información y las Comunicaciones, tiene facilidades para adaptarse a los cambios tecnológicos y más inclinación a las fuentes digitales para la obtención de conocimiento docente o científico. Su registro de navegación cuenta con mayor cantidad y variedad de sitios web, con preferencia por las redes sociales, puesto que proviene de otras comunidades académicas o laborales con las cuales mantiene relaciones a distancia a través de la red. Todo lo anterior, paradójicamente, también le convierte en el usuario más vulnerable, dados su escaso conocimiento y experiencia con redes telemáticas.

El novel es uno de los docentes con más influencia sobre el estudiantado, por la cercanía de la edad y la elevada cantidad de horas impartidas (según lo estipulado en la Educación Superior para profesores instructores y asistentes). Suele asumir, además, responsabilidades de tutor de vida o guía de grupo, encabezando

debates o acciones educativas, análisis de reglamentos docentes diversos, como el Código de ética de la RedUniss.

Todo lo anterior permite identificar como **situación problemática** de la presente investigación que los profesores noveles de la Uniss son usuarios vulnerables que carecen de conocimientos sobre seguridad informática, poniendo en peligro la integridad de los recursos y la información que transita por la red, a lo cual responde el siguiente **problema de investigación**: ¿Cómo contribuir a la formación de conocimientos sobre seguridad informática en profesores noveles de la Uniss, desde la superación profesional?

De este modo, se define como **objeto de estudio**: la superación profesional, concretándose como **campo de acción**: la formación de conocimientos sobre seguridad informática en profesores noveles.

En correspondencia con lo anterior el **objetivo general** es: proponer una estrategia de superación profesional que contribuya a la formación de conocimientos sobre seguridad informática en profesores noveles de la Uniss y, en consecuencia, la protección de los servicios y la información que la universidad provee.

Como guía heurística para la solución del problema científico se formularon las siguientes preguntas científicas:

- ¿Cuáles son los fundamentos teórico-metodológicos del proceso de superación profesional y la formación de conocimientos sobre seguridad informática?
- ¿Qué carencias y potencialidades presenta la formación de conocimientos sobre seguridad informática en profesores noveles de la Uniss?
- ¿Qué propuesta permite formar conocimientos sobre seguridad informática en los profesores noveles de la Uniss?

- ¿En qué medida la estrategia de superación profesional contribuye a fortalecer los conocimientos de los profesores noveles de la Uniss sobre seguridad informática?

Como **tareas de investigación** se desarrollaron las siguientes:

- Determinación de los fundamentos teórico-metodológicos de la superación profesional y la formación de conocimientos sobre seguridad informática.
- Identificación de las carencias y potencialidades que presenta la formación de conocimientos sobre seguridad informática en profesores noveles de la Uniss.
- Elaboración de una propuesta que permita formar conocimientos sobre seguridad informática en los profesores noveles de la Uniss.
- Valoración de la contribución de la estrategia de superación profesional para la formación de conocimientos sobre seguridad informática en profesores noveles de la Uniss, a través de la experimentación en la práctica pedagógica.

Variables de la investigación:

- Variable operacional: nivel de formación de conocimientos sobre seguridad informática, la cual se entiende como la apropiación escalonada de conocimientos sobre la temática, de orden teórico, práctico, axiológico y de aplicación en la realidad, los cuales se integran gracias al aprendizaje metacognitivo.
- Variable propuesta: estrategia de superación profesional para la formación de conocimientos sobre seguridad informática en profesores noveles de la Uniss.

En correspondencia con las tareas científicas y desde un fundamento metodológico general dialéctico-materialista, se acude al empleo de métodos y técnicas de investigación. Se emplean como **métodos de la investigación científica, del nivel teórico**:

- Histórico-lógico: permite la sistematización de los principales aportes, progresos y contradicciones que emanan de la construcción teórica y metodológica del objeto de estudio y el campo de acción mediante un proceso crítico de las opiniones autorizadas en cada caso.

- Analítico-Sintético: admite la descomposición del objeto de estudio y el campo de acción en los principales conceptos que lo conforman para facilitar su estudio más exhaustivo y mediante el proceso contrario, la síntesis, integrar las relaciones y características de ambos, de manera que se ofrezca una visión teórica integradora.

- Inductivo-Deductivo: se emplea para conocer las particularidades del problema de investigación y arribar a conclusiones conceptuales sobre la base del movimiento de lo singular a lo general y viceversa.

- Método de tránsito de lo abstracto a lo concreto: permite el conocimiento paulatino de las particularidades del problema científico, a medida que avanza la investigación y se va incrementando el nivel de conocimiento en torno a este.

- Método de Enfoque Sistémico: permite atender a las múltiples relaciones entre el objeto de estudio y el campo de acción y con otros elementos propios de la labor pedagógica. También es útil en la elaboración de la estrategia de superación profesional que se propone, atendiendo a los elementos que la componen, sus relaciones y estructura jerárquica.

Del nivel empírico:

- Análisis de documentos: consiste en la recogida y estudio de documentos de orden legislativo y científico sobre el campo de acción, así como de los informes de seguridad informática de la institución y los planes de superación profesional.

- Observación pedagógica: consiste en la participación no encubierta del investigador en el contexto universitario y se mantuvo durante todo el proceso investigativo un papel activo y una reflexión permanente, siempre atenta a detalles, eventos e interacciones entre los sujetos observados.

- Cuestionario: contribuye a identificar carencias en el conocimiento que los profesores noveles poseen sobre la seguridad informática, su percepción y actitud

frente al problema, la preparación que han podido recibir al respecto, así como sus opiniones sobre las mejores vías para erradicarlas.

- Entrevista semi-estructurada: se emplea para obtener opiniones, conocimientos, juicios y experiencias de especialistas en el tema, técnicos y diseñadores de la RedUniss, mediante la interacción en un contexto de relativa formalidad, pero incentivando el diálogo fluido y espontáneo.

- Experimentación: se empleó en la modalidad de pre-experimento pedagógico. Se introdujo la variable propuesta a partir de la constatación inicial y se evaluaron los cambios en la variable operacional.

- Triangulación: reconoce combinar "distintos métodos en el estudio de un mismo problema, para paliar las limitaciones de cada método" (Alberich, 2000), lo cual permite la comprobación de la validez y fiabilidad de los resultados. Se realiza a través de la síntesis de la información obtenida de diferentes fuentes, a partir de las diferentes técnicas empleadas para luego contrastar los resultados realizando un análisis entre coincidencias y divergencias (triangulación metodológica y triangulación de datos).

Además, se emplean **métodos estadístico-matemáticos** (cálculo porcentual, estadística descriptiva) en el procesamiento de los datos para representar y valorar los resultados de los instrumentos y técnicas aplicadas.

El universo inicial del estudio lo conformaron los 20 profesores noveles que matricularon en el diplomado “Formación básica para la docencia universitaria” durante el curso 2016-2017. De este conjunto, finalmente participaron voluntariamente en el estudio 15 profesores que conformaron la muestra de tipo no probabilístico intencional, siete hombres (46,6%) y ocho mujeres (53,3%) con un rango de edad de entre 23 y 25 años. De acuerdo a su formación profesional, dos Licenciados en Informática y uno en Telecomunicaciones, tres graduados de diversas ciencias sociales y humanísticas, dos ingenieros agrónomos, seis de ciencias pedagógicas y dos licenciados en Cultura Física.

La **novedad científica** de la presente investigación radica en el tratamiento de la seguridad informática, asociándola a la superación profesional específicamente en profesores noveles, una problemática sin antecedentes reconocidos, según los resultados de la indagación teórica al respecto.

El **aporte práctico** lo constituye la estrategia de superación profesional para contribuir a la formación de conocimientos de los profesores noveles sobre la seguridad informática y el diseño de un aula virtual que posibilite la autopreparación e impacte en una conducta comprometida con la seguridad e integridad de la información en la RedUniss.

El cuerpo del documento se organiza conforme a la siguiente estructura: introducción, dos capítulos, conclusiones, recomendaciones, bibliografía y anexos. En el primer capítulo se abordan los fundamentos teórico-metodológicos del proceso de superación profesional y la seguridad informática en profesores noveles, atendiendo a las relaciones de sus principales categorías.

El segundo capítulo está dedicado a la interpretación de los resultados del estudio de carencias y potencialidades de la formación de conocimientos sobre seguridad informática en profesores noveles, así como la fundamentación teórica de la propuesta. También se presenta la estrategia de superación profesional concebida y la valoración de los resultados obtenidos tras su implementación.

CAPÍTULO 1. FUNDAMENTOS TEÓRICOS QUE SUSTENTAN LA SUPERACIÓN PROFESIONAL. LA FORMACIÓN DE CONOCIMIENTOS DE SEGURIDAD INFORMÁTICA EN PROFESORES NOVELES.

En este capítulo se fundamenta la superación profesional como proceso esencial de la Educación Superior y su importancia en la formación de conocimientos de seguridad informática entre los usuarios de redes telemáticas para la preservación de la integridad de la información. Luego de este marco teórico-referencial, se presenta un análisis epistemológico de la categoría profesor novel, explicitándose la pertinencia de su superación en temas de seguridad informática.

1.1 Fundamentos epistemológicos de la superación profesional del docente universitario.

La actividad de posgrado tiene sus antecedentes en la Europa medieval, donde las primeras universidades (Bolonia, 1089; Oxford, 1096 y París, 1150) otorgaban los grados de doctor, maestro y profesor que caracterizaban por entonces al hombre culto y capaz en el ámbito de su profesión.

Sin embargo, la actividad no adquiere verdadero carácter científico hasta el advenimiento de la revolución industrial en el siglo XIX. Los avances de la ciencia y la técnica impulsan a las universidades a adaptarse a las nuevas necesidades sociales y productivas, diversificando los contenidos y creando las primeras cátedras de investigación científica. Surge entonces la nueva concepción del posgrado como actividad que interrelaciona la superación profesional con la realidad innovadora, permitiendo a la academia estar a la altura de las exigencias sociales.

Desde muy temprano, la ciencia pedagógica ha enfatizado en la necesidad de la superación de los docentes, una aspiración que se expresa llanamente en la Declaración mundial sobre educación para todos: “El mundo en su conjunto evoluciona tan rápidamente que el personal docente, como los trabajadores de la mayoría de las demás profesiones, deben admitir que su formación inicial no le bastará ya para el resto de su vida” (Unesco, 1990: 170-172).

Pero, la educación de posgrado se orienta de formas muy diversas según las latitudes. En países desarrollados (Estados Unidos y europeos), las instituciones universitarias conciben la superación como forma de elevar el nivel científico-profesional de sus egresados mediante doctorados, maestrías y habilitaciones, conservando la exclusividad y el elitismo que distinguen estas casas de altos estudios. Otras tendencias contemporáneas occidentales son el diseño e implementación de programas que contribuyen al desenvolvimiento de nuevos órdenes epistemológicos, así como la identificación y resolución de problemas profesionales y de la práctica social.

En Latinoamérica, por otra parte, la superación del profesorado adquiere diferente denominación: superación para la administración o para la gerencia educativa. Esta concepción considera la escuela como una empresa, donde el servicio educativo es ofrecido y demandado por el mercado social. La administración de los recursos humanos es una función especializada que desarrollan los gerentes de los centros educativos, y entre sus funciones se encuentran los convenios para la capacitación y actualización de los docentes.

En Cuba, antes de 1959, lo que pudiera llamarse estudios posgraduados estaba limitado a cursos breves de la invocada Escuela de Verano u otros que se brindaban en los Colegios Profesionales y las conferencias especializadas impartidas por las dos únicas universidades del país (Universidad de La Habana, Universidad de Oriente). Tenía una orientación muy exclusivista, que se orientaba a pequeños clanes profesionales, la mayoría de la capital.

Luego del triunfo de la Revolución, el Ministerio de Educación Superior (MES) concibe la superación del personal docente a partir de un modelo descentralizado, donde cada territorio diseña su sistema de superación a partir de las exigencias del desarrollo sociocultural. Desde la década del 60, se crearon instituciones para la impartición de cursos, cursillos, seminarios y otras actividades, destinadas a la superación y el perfeccionamiento del personal docente, técnico y administrativo en ejercicio; pero, no fue hasta el Primer Congreso del Partido Comunista de Cuba (PCC) en 1975 que se emite como resolución sobre política educacional la

necesidad de elevar la calificación de los graduados del nivel superior, a través de cursos especializados de posgrado.

En la educación superior cubana, el posgrado es una de las direcciones principales de trabajo, orientado a promover la educación permanente de los graduados universitarios: “En la educación de posgrado concurren uno o más procesos formativos y de desarrollo, no solo de enseñanza aprendizaje, sino también de investigación, innovación, creación artística y otros, articulados armónicamente en una propuesta docente educativa pertinente a este nivel “(MES, 2004: 2).

La superación profesional de los docentes tiene sus sustentos legales en el Reglamento de la Educación de Posgrado (Resolución 132/2004) del Ministerio de Educación Superior y se ha actualizado en otros documentos como las Normas y procedimientos para la gestión de posgrado (166/2009); las Modificaciones a las Normas de Procedimientos para la Gestión de Posgrado (2013) y otras.

El Reglamento de la Educación de Posgrado, distingue entre las categorías posgrado y superación profesional que suelen usarse como sinónimos en la praxis académica; sin embargo, una contiene a la otra. En la Resolución se aclara que la educación de posgrado tiene dos grandes direcciones: la formación académica de posgrado y la superación profesional.

La primera es el conjunto de procesos de apropiación de capacidades que posibilitan a los graduados de nivel superior alcanzar una alta competitividad científico-técnica y rigor académico. Tiene como formas: la especialidad, la maestría y el doctorado. La segunda dirección abarca los diversos procesos de enseñanza-aprendizaje que permiten la adquisición y perfeccionamiento continuo de conocimientos, aptitudes y habilidades requeridos para un mejor desempeño de sus responsabilidades y funciones laborales.

La superación profesional “tiene como objetivo la formación permanente y la actualización sistemática de los graduados universitarios, el perfeccionamiento del

desempeño de sus actividades profesionales y académicas, así como el enriquecimiento de su acervo cultural" (MES, 2004: 3).

La superación profesional aparece definida en la literatura científica por varios autores y ha adquirido renovado interés en la investigación pedagógica de las últimas décadas.

Añorga (1995) define esta categoría como el conjunto de procesos de enseñanza-aprendizaje que posibilitan a los graduados universitarios la adquisición y el perfeccionamiento continuo de los conocimientos y las habilidades requeridas para un mejor desempeño de sus responsabilidades y funciones laborales. Esta actividad proporciona la superación continua de los profesionales de los diferentes sectores y ramas de la producción, los servicios, la investigación y la docencia, en correspondencia con los avances de la ciencia, la técnica, el arte y las necesidades socio-económicas del país, con el objetivo de contribuir a elevar la productividad y la calidad del trabajo de los egresados de la educación superior.

De acuerdo con este autor, Escudero (1998) define a la superación profesional desde la formación permanente, planteando la necesidad de implicar procesos de aprendizaje diversos, desde el análisis y la reflexión sobre la propia práctica, hasta el acceso significativo y el aprendizaje de nuevos contenidos y habilidades a partir del conocimiento pedagógico disponible y valioso. Este autor compara la educación de posgrado con la de pregrado, concluyendo que en la primera no solo convergen el proceso de enseñanza-aprendizaje, sino también procesos de alto grado de autonomía y creatividad, como la investigación, la innovación, la creación artística y la profesionalización.

Al respecto, Bernaza reflexiona que en la educación de posgrado:

> El proceso de enseñanza, a diferencia de lo que algunos autores plantean, siempre no juega un papel hegemónico, sino que se pone en función de Pagac, que gira alrededor de ellos. La no comprensión de esta diferencia sustancial podría ser la razón de que se transfiera al posgrado prácticas pedagógicas del pregrado donde sí, el proceso de enseñanza es el proceso fundamental y están presente generalmente los componentes académicos, investigativos y laboral, los cuales

> tienen una influencia indiscutible en la formación integral del estudiante universitario, cuya actividad rectora es el estudio profesional (2004: 1).

En tal sentido, este autor enfatiza en el carácter “formativo y de desarrollo en un contexto histórico-cultural concreto” del proceso. Se trata de “un proceso sistemático, de construcción y reconstrucción social del conocimiento a través de la actividad y de la comunicación, transformador no solo del objeto de aprendizaje y su entorno, (…) donde se considera que es posible aprender y desarrollarse a lo largo de la vida, con el fin de alcanzar una cultura general integral” (Bernaza, 2004: 2).

Lo anterior implica que en la superación profesional debe sustentarse en el enfoque histórico-cultural de L.S. Vigotsky, para el diagnóstico de los docentes, así como para la proyección de acciones concretas y eficientes, que lo enseñen a emprender tareas con independencia y creatividad, las que pueden ser enriquecidas con la experiencia personal mediante las interacciones que se producen con los demás.

Centrándose en el profesional docente, García Batista y Addine definen la superación profesional como el “conjunto de procesos de formación, que le posibilitan al graduado de los centros pedagógicos la adquisición y perfeccionamiento continuo de los conocimientos, habilidades básicas y especializadas, así como los valores ético-profesionales requeridos para un mejor desempeño de sus responsabilidades y funciones como docentes con vistas a su desarrollo general e integral” (2001: 17).

Addine refiere que debe ser entendida “[…] como la educación perenne que debe permitir al profesional de la educación formar parte de la dinámica de cambio, para enfrentar los problemas planteados por el adelanto científico y tecnológico; y los imperativos del desarrollo económico, social y político en un contexto dado” (2010: 7).

A las reflexiones de estas autoras se adscribe la presente investigación, por lo completo y abarcador de su concepción, que no circunscribe la superación profesional al ámbito de la formación y actualización de conocimientos sino más

bien de competencias diversas (conocimientos, habilidades, procederes, valores) específicas de la profesión que influyen en un mejor desempeño laboral. Además, sostienen que la superación profesional otorga pertinencia social y científica a la institución educativa, en el accionar reflexivo y transformador de sus docentes.

Josefa Lorences (2003: 36) compila cuatro modelos fundamentales a los que se adscribe la superación profesional del profesorado:

- El modelo de formación academicista, centrado en la actualización de los contenidos, entendidos en su concepción restringida y descontextualizada.
- El modelo de formación utilitaria, que da respuesta a planteamientos técnicos de la enseñanza en el que los docentes tienen la función de aplicar programas y estrategias que han decidido y elaborado expertos externos para la obtención de la máxima eficiencia en el logro de determinados objetivos.
- El modelo de formación centrada en el aula, que impulsa el desarrollo de programas desde el propio diseño y funcionamiento de la escuela, la involucra como organización y facilita su transformación como un todo mediante la creación de condiciones organizativas, de dirección participativa, la promoción del trabajo colectivo orientado hacia la solución de problemas prácticos.
- El modelo de formación descentralizado, en el que se elabora el sistema de superación a partir de las necesidades y exigencias del desarrollo sociocultural de cada territorio en correspondencia con los objetivos generales de la educación, adoptando sus particularidades en dependencia de las cuales se establecen exigencias y niveles de aspiración para el logro de la superación profesional.

Esta clasificación, sin embargo, no logra abarcar toda la complejidad del proceso actual en el ámbito cubano, según considera Nieto (2005): “la estructuración actual de la superación profesional ha demostrado lentitud para ajustarse a los cambios que se producen en la educación actualmente, además de que no reflejan la especificidad del trabajo de superación en el caso de los docentes” (2005: 50-51). Esto ocurre porque se suele partir más de las fortalezas de los centros universitarios en coincidencia con las necesidades de la práctica que de colocar

como elemento generador de la superación a la propia práctica y a las necesidades reales y concretas del contexto donde labora el docente.

Con respecto a la pertinencia del proceso, Mesa y Salvador determinan que "[…] en el caso del personal docente, la superación debe responder a las necesidades, potencialidades, así como a los proyectos de vida de los docentes y a las necesidades del sistema educativo (…), donde evidencie su efectividad en el desempeño alcanzado por los profesores, en formación continua, de sus funciones profesionales, el desarrollo alcanzado en sus modos de actuación profesional; así como en los resultados alcanzados en su objeto de trabajo" (2010: 7).

Mendoza asevera, además, que los sistemas de influencias que ocurren en la superación profesional están definidos por la concepción que se asuma del proceso pedagógico, como: "los procesos conscientes, organizados y dirigidos a la formación de la personalidad, en los que se establecen relaciones sociales activas, recíprocas y multilaterales entre educador, educando y grupo, orientadas al logro de los objetivos planteados por la sociedad, la institución, el grupo y el individuo" (2011: 9).

Los autores anteriores coinciden en que la superación profesional constituye un proceso organizo de forma sistémica, que da continuidad a la formación inicial desde el proceso de enseñanza- aprendizaje, en función de actualizar y perfeccionar el desempeño profesional actual y perspectivo, atender insuficiencias en la formación o completar conocimientos, habilidades, procederes y valores necesarios para un mejor desempeño.

El carácter permanente y la pertinencia social son elementos esenciales en su concepción. Para lograrlos con éxito es importante que al concebirla se tenga en cuenta la participación activa del profesional, en este caso el docente, en la determinación de sus propias necesidades y en la ejecución del proceso. Es importante que se incluyan sus circunstancias, su contexto, así como la creación del compromiso para el cambio y la mejora individual y colectiva.

1.1.2 Formas organizativas principales de la superación profesional

En el Reglamento de la Educación de Posgrado (Resolución 132/2004 del MES) se precisan como formas organizativas principales de la superación profesional: el curso, el entrenamiento y el diplomado, aunque también se incluyen otras como la autopreparación, el adiestramiento, la conferencia especializada, el seminario, el taller y el debate científico, que complementan y posibilitan el estudio y la divulgación de los avances del conocimiento, la ciencia, la tecnología y el arte. Aquí abordaremos algunas de las más importantes.

Añorga define el curso de superación profesional como la "actividad pedagógica dirigida a la satisfacción de necesidades de complementación, actualización y profundización de los conocimientos de los profesionales. Debe enfatizarse su uso en la difusión organizada de los resultados de la ciencia y la técnica ante las limitaciones de bibliografía novedosa y útil" (1995: 10).

Por otra parte, la autopreparación puede ser entendida como las acciones que cotidianamente desarrolla el docente para apropiarse de los conocimientos y habilidades necesarios para desarrollar sus clases, tareas de superación u otras actividades de carácter metodológico o formativo en la institución escolar, o como una forma específica de la superación profesional mediante la que el docente, sigue las orientaciones de un programa y de un conjunto de guías de estudio, y logra vencer una de las etapas del proceso, en la cual se ponen de manifiesto la evaluación, la autoevaluación y autovaloración, de manera planificada por las personas o instituciones encargadas de diseñar la superación.

El taller se define como la forma de la superación profesional "…donde se construye colectivamente el conocimiento con una metodología participativa dinámica, coherente, tolerante frente a las diferencias; donde las decisiones y conclusiones se toman mediante mecanismos colectivos, y donde las ideas comunes se tienen en cuenta" (Añorga, 1995: 34).

Los debates científicos representan un ascenso en el desarrollo de las acciones de superación, lo cual propiciará que los docentes operen con un pensamiento

más crítico, reflexivo y con mayor nivel valorativo, lo que de una forma u otra enriquece el intercambio de ideas, juicios, puntos de vista y opiniones acreditados por trabajos de su propia práctica en relación con procesamiento de la información.

La superación profesional, por tanto, es la vía seleccionada en la presente investigación para contribuir a la formación de conocimientos sobre seguridad informática en los profesores noveles de la Uniss.

1.2 Superación profesional del profesor novel.

El proceso de superación profesional o pedagógica es fundamental para el profesor novel, porque en estos primeros años se forman y se consolidan la mayor parte de los conocimientos, competencias, valores y actitudes inherentes al ejercicio de la profesión.

Etimológicamente el novel es una persona generalmente joven, sin experiencia, que aprende un arte, oficio o facultad o empieza una actividad por primera vez y lo hace con la asistencia y el apoyo de un maestro o una maestra. Entrando en el contexto de la educación, Imberón (1994) define a los profesores noveles como todos aquellos que poseen menos de tres años de experiencia en su quehacer profesional, aunque algunos autores lo prolongan hasta los cinco primeros años.

El profesor novel es el que egresa de las aulas universitarias o institutos pedagógicos, donde se formó durante cinco años o más, con todo lo necesario para ejercer la profesión, con esos métodos de enseñanza, técnicas educativas, psicología educativa, con una práctica pre-profesional como curso al término de los estudios. A este docente joven, “nuevo” en el inicio de su profesión, debemos denominar como profesor novel (Bozu, 2010).

En la Educación Superior en Cuba, el profesor novel proviene de muy diversas especialidades, seleccionados de entre los mejores graduados en sus respectivas ramas, para trasmitir el conocimiento adquirido. Pero, no todos estos jóvenes ostentan una formación que les prepara para ejercer el magisterio, sino que deben adquirirla, en la mayoría de las ocasiones, en la institución en que se desempeñan.

Este período de inserción profesional del profesorado novel se denomina adiestramiento laboral y abarca los tres primeros años de desempeño en la docencia. Este adiestramiento se concibe como un período de aprendizaje y de orientación profesional, el cual tiene como antecedente la formación pedagógica que se desarrolla en el planteamiento curricular de todas las carreras universitarias desde el curso (Torra, 2013).

Durante el adiestramiento laboral, el profesorado novel recibe atención diferenciada de sus profesores, que son docentes experimentados que participan en las actividades del sistema de trabajo metodológico que desarrolla el departamento docente. La institución propone un programa sistemático de apoyo a los profesores durante su adiestramiento, para introducirlos en la profesión y ayudarlos a abordar los problemas, de modo que refuerce su autonomía y facilite su desarrollo en la docencia.

En esta etapa no debe asumir responsabilidades académicas, ni tener alta carga docente para poder dedicar la mayor parte del tiempo a su propia formación profesional docente. No obstante, muchas veces ocurre todo lo contrario, asume responsabilidades académicas, altas cargas docentes y se siente agobiado por la cantidad de tareas que debe cumplir y por la falta de tiempo, que impiden su adecuada preparación para la docencia (Torra, 2013).

Diferentes autores consideran la iniciación a la docencia como una etapa esencial para el futuro desarrollo profesional del novel y también de vulnerabilidad frente a una realidad nueva, ajena y estresante.

Marcelo (2009) comenta que la experiencia adquirida durante el primer año de docencia produce cambios significativos en las actitudes de los profesores, como en el manejo de grupos y en el ámbito disciplinar, adquiriendo conductas más autoritarias y controladas.

Para Bozu (2010), la etapa de iniciación a la docencia es un periodo de suspenso y optimismo a la vez, donde las actitudes y concepciones sobre la enseñanza no cambian de manera radical, pero sí se modifican en la reflexión sobre la formación recibida y la capacidad que se tiene para asumir el nuevo reto.

En esta etapa se produce la socialización profesional del profesorado novel, entendida esta como el proceso de apropiación activa de la cultura de la universidad, la enseñanza y el aprendizaje, es una condición necesaria para el logro de una experiencia profesional docente satisfactoria. Zeicher y Gore (1990, citados en Bozu, 2009) establecen tres etapas en el proceso de socialización o inducción del profesorado novel:

- Socialización primaria: abarca aquellos años que pasó en el aula universitaria, en los cuales se fue formando una visión y unas creencias de lo que era la enseñanza universitaria, cómo debía ser y desarrollarse. Las concepciones y creencias que ya se poseen juegan un papel fundamental en el dibujo de esa visión de la enseñanza universitaria.
- Socialización secundaria: entra en contacto real con la institución, con el estudiantado y colegas del departamento docente. La incorporación a la institución marcará su desarrollo profesional, ya que la estabilidad laboral y las relaciones socio-profesionales sellarán una alianza que se supone larga y duradera y que va a determinar sus modos de actuación futuros. En el ejercicio docente es donde se da la verdadera socialización, cuando se produce el choque con la realidad y se desarrollan estereotipos, ideas, convicciones y creencias sobre el proceso de enseñanza- aprendizaje.
- Socialización terciaria: se refiere al desarrollo del profesorado novel dentro del aula y a sus relaciones con la comunidad universitaria. Si su desarrollo en el aula no es satisfactorio, su crecimiento como profesional se verá afectado, ya que no trabajará con soltura en el aula y verá el estudiantado como algo que le impide su desarrollo profesional. Por otra parte, la presión que ejerce la comunidad universitaria sobre el profesorado universitario novel es de tal magnitud, que puede generar en él unas expectativas inalcanzables, una situación de estrés y un sentimiento de frustración que pueden llevarlo al abandono de la profesión.

Pero, no solo son importantes para el novel la adecuada preparación pedagógica y la socialización exitosa en esta etapa. La Educación Superior en Cuba también exige de sus docentes una serie de competencias que determinan su desempeño profesional integral en el contexto universitario, como la actualización político-

ideológica, la producción y socialización científicas, la autogestión de la información, la preparación profesional continua, el uso seguro y provechoso de las tecnologías en función de su labor, entre otras.

Mitchell y Kerchner (1983), retomados por Imberón (2000: 9), definen diversos estadios de profesionalización del docente:

- El profesor como trabajador: concibe la escuela como un sistema jerárquico del cual es gerente o director quién dice qué, cuándo y cómo debe enseñar el profesor, así las tareas de concepción y planificación están separadas de la ejecución.
- El profesor como artesano: se atribuye una mayor responsabilidad al docente para seleccionar y aplicar las estrategias de enseñanzas. En los programas formativos se prioriza la adquisición de trucos del oficio por encima de la teoría y la reflexión.
- El profesor como artista: se enfatiza la creatividad personal, y se permite el desarrollo de un mayor grado de autonomía docente. La adquisición de la cultura general y profesional está condicionada y tamizada por la institución, personalidad y dinamismo individual.
- El profesor como profesional: el trabajo profesional por naturaleza no es propenso a la mecanización. El docente está comprometido con la autorreflexión y el análisis de las necesidades del estudiantado, y asume importantes cuotas de responsabilidad en las decisiones curriculares que se comparte.

Justamente en el contexto universitario se pueden ver manifestaciones que revelan estos tipos de profesores, pero las intenciones prioritarias contemporáneas buscan un profesor matizado con todas estas características, cuya expresión más acabada es el profesor como profesional, capaz de ejecutar las tareas con gran atención, exactitud y rapidez, sobre la base de una elevada preparación y con pleno dominio de los procederes, actitudes y valores propios de su actividad laboral, independientemente de la formación inicial que haya recibido.

El diseño de programas o cursos de superación profesional en las instituciones de educación, son herramientas necesarias para asegurar la permanencia y la preparación integral del profesorado joven, en un proceso que debe tomar como

referencia al individuo, y que debe revelarse sistemático e ininterrumpido, tanto para la etapa inicial como para etapas posteriores.

Sin embargo, muchas veces el curso puede no resultar suficiente. Hoy, las Tecnologías de la Información y las Comunicaciones (TIC) están desplazando, cada vez más, los modelos tradicionales de superación profesional hacia nuevas estrategias que proponen ventajas novedosas al profesor principiante, basadas en el autoaprendizaje y la preparación permanente.

1.2.1 Las TIC y el profesor novel. Necesidad de su superación en conocimientos de seguridad informática.

Los retos actuales de la Sociedad del Conocimiento proponen una actualización constante del proceso de formación pedagógica, que ha incrementado los niveles de acceso y disponibilidad del conocimiento, lo cual ha determinado una creciente demanda social de habilidades de aprendizaje y de dominio de las TIC como competencias fundamentales del profesorado universitario. De la actualización de estas competencias depende el buen desempeño docente en el aula, lo que determina otra ventaja de asumir nuevas estrategias en el proceso de superación profesional del profesor novel.

La integración de las tecnologías al proceso de enseñanza-aprendizaje ha supuesto, desde sus inicios, un auténtico cambio estructural en todo el ámbito educativo general. Así lo pone de manifiesto la UNESCO con el reconocimiento que da a las TIC, al señalar que “ofrecen un variado espectro de herramientas que pueden ayudar a transformar las clases actuales -centradas en el profesor, aisladas del entorno y limitadas al texto de clase- en entornos de conocimiento ricos, interactivos y centrados en el alumno” (UNESCO, 2004: 20).

La UNESCO identifica también las TIC como una competencia transversal de carácter instrumental que permite la expresión y la comunicación, el acceso a la información, el archivar documentos y datos, la realización de tareas de presentación, así como para el aprendizaje, la investigación y el trabajo cooperativo.

Las tecnologías han abierto un horizonte de propuestas novedosas para apoyar el proceso de enseñanza-aprendizaje, acercándolo al modelo autogestionario y de independencia cognoscitiva a que aspira la educación superior cubana. Esto ha propiciado el surgimiento de la Tecnología Educativa, la disciplina que se centra en la realización de softwares educativos y otras formas tecnológicas, que devienen medios de enseñanza, aprovechando al máximo las posibilidades que ofrecen las TIC en la esfera educativa, lo cual ha producido profundos cambios en el proceso al incorporar algunos medios nuevos y cambiar muchos de los métodos y técnicas para el empleo de los tradicionales.

Pero, así como han impactado todos los órdenes de la vida cotidiana actual, el uso extendido y acelerado de las TIC, ha permeado todos los procesos universitarios, no solo aquellos relacionados con la enseñanza-aprendizaje de pregrado: la comunicación, social y con fines de organización o académicos; la investigación científica, reflejada en la búsqueda de información o en la socialización de resultados obtenidos en el proceso; la divulgación y promoción de actividades de extensión universitaria; los procesos de dirección, entre otros.

El empleo de redes telemáticas que permiten el intenso intercambio de información diversa entre los usuarios, ha venido a transformar y facilitar el funcionamiento de todos estos procesos, por medio del correo electrónico, el acceso a Internet, la creación de sitios propios de cada institución y organismos educacionales (Intranet).

La integración de la TIC a la dinámica universitaria ha sido exitosa, hasta el punto de que hoy es imposible concebir la universidad sin ella. En nuestro país su integración ha tenido particularidades, debido al atraso tecnológico, a la necesidad de capacitar a las personas para el uso efectivo de sus recursos, pero también por la concepción humanista, equitativa y ética en el empleo de la tecnología. Todo ello ha generado diferentes niveles de aceptación entre los usuarios, y aunque se considera una batalla ganada, esa aceptación difiere según la preparación, el tiempo del que dispone el usuario, las metas profesionales y las motivaciones, la edad, etc.

Sin lugar a dudas, las nuevas generaciones han sido más receptivas a la inserción y empleo de las TIC en el escenario universitario. Entre el profesorado, el docente novel se destaca como un usuario activo y receptivo de las TIC que, por su condición de nativo de la Sociedad de la Información y las Comunicaciones, posee capacidades creadas para incorporarlas de forma natural y creativa a su vida cotidiana y a su desempeño profesional.

Además, la universidad estimula e impulsa la superación y el desarrollo científico de sus docentes desde muy temprano, y el novel se encuentra iniciándose en los caminos de la investigación, insertándose en formas de posgrado (cursos, diplomados, maestrías, doctorados) y acogiéndose a proyectos. Con facilidades para adaptarse a los cambios tecnológicos, es un investigador que se decanta por las fuentes digitales para la obtención de conocimiento.

Su registro de navegación revela consultas a mayor cantidad y variedad de sitios web que otros docentes, con preferencia por las redes sociales (Facebook en su mayoría) y el uso frecuente del correo electrónico, puesto que proviene de otras comunidades académicas o laborales con las cuales mantiene relaciones a distancia a través de la red. Es un usuario activo, curioso, explorador y sociable, lo cual representa una fortaleza que impulsa su desarrollo profesional, pero también, constituye una vulnerabilidad, teniendo en cuenta su escaso conocimiento y limitada experiencia con redes telemáticas.

Añadir la seguridad informática como contenido de superación para el docente novel es una de las tareas indispensables para la universidad de estos tiempos. Las nuevas generaciones de maestros traen cada vez más acentuadas estas características, en un contexto educacional de transformación constante por la inserción de las TIC y agravado por el constante desarrollo de amenazas informáticas y la falta de preparación para enfrentarlas.

Otras razones, relacionadas con la organización de los procesos universitarios, avalan esta necesidad, pues el novel es uno de los docentes con más influencia sobre el estudiantado, por la cercanía de la edad que permite la creación de afinidades entre ambos y por la elevada cantidad de horas que comparten en el contexto de la clase (según lo estipulado en la Educación Superior, los profesores

instructores y asistentes tienen elevada carga docente), lo cual le convierte en un paradigma cercano, en un modelo a seguir.

El novel suele asumir, además, responsabilidades de tutor de vida o guía de grupo, encabezando debates o acciones de la estrategia educativa, acompañando a los estudiantes en momentos importantes de su vida en la comunidad universitaria, compartiendo su experiencia, así como el análisis de reglamentos docentes diversos, entre ellos el Código de Ética de la RedUniss.

1.3 La seguridad informática. Acercamientos a su estudio.

La seguridad es una categoría que ha preocupado al hombre desde el principio de los tiempos, pero que ha adquirido una relevancia sin precedentes en la sociedad contemporánea, aplicada a todos los espacios de la vida social. El concepto de seguridad ha evolucionado desde entonces, pasando por la seguridad ciudadana hasta los más complejos mecanismos que aseguran una comunicación fiable y el intercambio de información digital de forma segura.

Manunta (2006: 34) define seguridad como “una necesidad básica que, interesada en la preservación de la vida y las posesiones, es tan antigua como la vida misma. Sus indicios se encuentran plasmados desde el inicio de la escritura”. Este concepto general ya atiende al carácter primario y urgente de la seguridad, un rasgo sobre el que hay consenso entre los teóricos del tema.

Un poco más allá, Morales (2006) identifica la categoría con la psicología humana: “debe ser interpretada como un estado subjetivo que nos permite percibir que nos desplazamos en un espacio exento de riesgos reales o potenciales”.

Sánchez (2003) conviene en que la seguridad es una necesidad de la persona, los diversos grupos humanos y las naciones, al mismo tiempo que constituye un derecho inalienable: “Seguridad proviene del latín *securitas*, que a su vez se deriva del adjetivo *securus*, sin cura, sin temor; implica las nociones de garantía, protección, tranquilidad, confianza, prevención, previsión, preservación, defensa, control, paz y estabilidad de las personas y grupos sociales, frente a amenazas o presiones que atenten contra su existencia, su integridad, sus bienes, el respeto y ejercicio de sus derechos, etc.”.

Por su parte, Olivera (2006) alega que la seguridad es la interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado, enmarcada por la situación global".

Ya aquí se hace patente que la seguridad depende de la continua tensión de contrarios: pérdida-preservación, presencia-ausencia de riesgos o peligros, sobre todo en las sociedades actuales. Según Lara (2006): "La seguridad trae consigo una ausencia de amenazas, situación que en el mundo contemporáneo es muy difícil de sostener, pues las sociedades actuales son crecientemente sociedades de riesgo. El componente riesgo es permanente y da carácter propio a los Estados y sociedades, como tal, la seguridad no puede ser entendida como ausencia de amenazas".

Adscribiéndonos a los criterios anteriores, la seguridad hoy no puede medirse por la ausencia total de amenazas, lo cual constituye una utopía social, sino por la capacidad de esas sociedades para minimizar y prevenir los riesgos posibles, lo cual equivaldría a elevar la tranquilidad, la confianza y la calidad de vida de las personas. Sin embargo, es de destacar que hoy no solo se habla de seguridad asociada a los espacios físicos sino también a las dimensiones virtuales a las que se ha expandido la vida social hoy, gracias al desarrollo de la tecnología digital.

La globalización del conocimiento y la cultura, la ciencia y la tecnología, la economía, la comunicación masiva e interpersonal, se ha desarrollado aceleradamente gracias al avance tecnológico acelerado de las últimas décadas. La creación de Internet, de la telefonía móvil, de las redes sociales, han traído nuevos espacios que conectan los más diversos sistemas (defensivos, financieros, viales, etc.) y enlazan a las comunidades más alejadas del planeta, propiciando el intercambio masivo de información a nivel global.

Pero, el ciberespacio no siempre garantiza el acceso seguro o privado de los usuarios. Existen personas ajenas a la información, conocidas como *hackers* o piratas informáticos, que buscan tener acceso a la red para modificar, sustraer o borrar datos, por beneficio propio o en nombre de otros. Los estudiosos del tema coinciden en que la mayor parte de las violaciones e intrusiones a los recursos informáticos son realizadas por el personal interno (administrativo o de sistemas),

que domina los procesos y metodologías y tiene acceso a información sensible cuya pérdida puede afectar el buen funcionamiento de la organización vulnerada.

La causa fundamental de los delitos informáticos es la seguridad ineficiente de las compañías y organizaciones y la falta de conocimiento relacionado con la protección de los recursos informáticos frente a las actuales amenazas externas e internas, por parte de especialistas y usuarios. De esta forma, la seguridad informática se convierte en una disciplina de primer orden en el mundo globalizado tecnológicamente.

Aunque muy joven, la seguridad informática se fortalece científicamente y explora sus fronteras y sus relaciones interdisciplinarias con celeridad. Morán (2016) la define como un grupo de "técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados". Esta breve definición ya destaca la misión protectora de la seguridad informática, pero pone demasiado énfasis en el hardware como objeto de esta protección.

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware o conjunto de todos los sistemas físicos (CPU, cableado, impresoras, CD-ROM, cintas, componentes de comunicación), el software o conjunto de los elementos lógicos que hacen funcionar al hardware (sistema operativo, aplicaciones, utilidades) y los datos (conjunto de información lógica que manejan el software y el hardware: bases de datos, documentos, archivos).

Todo lo anterior avala la opinión de Rosado, D. et al. (2014), que reconocen la seguridad informática como "[…] un proceso complejo que conlleva tres aspectos: gente, procesos y tecnología. Si estas variables no se evalúan y resuelven como partes de un todo, se obtiene como producto final un potencial o real desastre".

Atendiendo a esta visión de la disciplina como proceso complejo e integrador, en el Decreto-Ley No. 199 (1999) se identifica la seguridad informática como:

> […] un conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que

se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información.

Según este concepto, aunque la seguridad informática se orienta hacia la protección de todos los elementos del sistema informático, la mayoría de los procedimientos para la seguridad se orientan hacia los datos, pues son los más expuestos a todo tipo de riesgos, y también los que más rápidamente se devalúan. Están expuestos a más riesgos, puesto que son accedidos por más personas: usuarios, analistas, programadores, que los restantes bienes y sometidos a las mismas amenazas no intencionadas que los demás (Decreto Ley 199/1999, Capítulo 1, Inciso ñ).

En la sociedad actual, el volumen de datos que es procesado, almacenado y trasmitido es mayor que en épocas anteriores; además, no sólo el volumen sino la importancia de esta información, para el desarrollo económico y social, no tiene precedentes. Hoy en día, la información es considerada un capital invaluable, al que las empresas y otras organizaciones conceden la mayor importancia y no escatiman recursos a la hora de invertir en ella.

La mayoría de los autores (Díaz, 2004; Bradanovic, 2006; Montesino, Baluja y Porvén, 2013; Acosta y Negrete, 2012) coinciden en que la seguridad informática maneja tres conceptos básicos importantes para la seguridad de la información, particularmente en la Internet o en redes de datos. Estos son: confidencialidad, integridad y disponibilidad. Tomando como criterio el punto de vista del usuario, también pudieran manejarse otros como autenticación, autorización, contabilidad y no repudio.

Montesino, Baluja y Porvén (2013) definen confidencialidad o privacidad como el requerimiento de que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. La confidencialidad de la información se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, mediante cifrado.

Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas", la

intercepción o recepción electromagnética no autorizada, o la simple intrusión directa en los equipos donde la información está físicamente almacenada (Bradanovic, 2006).

Acosta y Negrete (2012), por su parte, afirma que la integridad asegura que nadie pueda modificar datos confidenciales, específicamente personas no autorizadas. También evita a quienes tienen privilegios para realizar las modificaciones, o lo hacen sin autorización. La integridad es una cualidad que asegura la consistencia de los datos, es decir, que la información refleje la verdad, que haya sido borrada, reordenada, copiada, o alterada de alguna forma, bien durante el proceso de transmisión o en su propio equipo de origen.

Para Bradanovic (2006), la disponibilidad asegura que la información pueda ser recuperada en el momento que se necesite, esto es evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

La disponibilidad asegura que la información esté a la mano cuando sea necesario en tiempo y espacio, para las personas que la requieren. En otras palabras, la disponibilidad garantiza que los sistemas funcionen cuando se necesitan (Acosta, y Negrete, 2012).

A esta propiedad se asocian otros conceptos básicos, pues para lograr que la información esté disponible al usuario adecuado se utilizan mecanismos de autenticación y autorización. Según la norma ISO 7498-2, la autenticación es un "servicio de seguridad que se puede referir al origen de los datos o a una entidad homóloga. Garantiza que el origen de datos, o entidad homóloga, son quienes afirman ser." Este aspecto requiere una identificación correcta del origen del mensaje, asegurando que la entidad o usuario no sean falsos.

Los sistemas se hacen mucho más seguros si esa autenticación no puede ser refutada después, o sea, si el usuario no puede esquivar ninguna responsabilidad en las acciones que desarrolló dentro de un sistema. Esto se conoce como no repudio de la identidad, una propiedad que ofrece protección a un usuario frente a otro que niegue posteriormente que en realidad se realizó cierta comunicación. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el

mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

Por su parte, la contabilidad se basa en el registro de todas las actividades que ocurren en el sistema. Cada proceso de autenticación y autorización son registrados con un nivel de información acorde a la configuración del sistema, mediante la contabilidad es posible saber cuál y cómo es el uso del sistema; puede conocerse qué preferencias tienen los usuarios y qué infracciones cometen (Montesino, Baluja y Porvén, 2013).

Por consiguiente, la seguridad de los sistemas de información está amenazada por un creciente número de ataques cada día, acciones que podrían ocasionar una violación de la seguridad de la información (confidencialidad, integridad o disponibilidad).

1.3.1 Amenazas o ataques a la seguridad de la información. Formas de enfrentamiento.

Según Aguirre Murillo (2005) existen cuatro categorías generales de amenazas o ataques:

- Interrupción: constituye un ataque contra la disponibilidad pues un recurso del sistema es destruido o se vuelve no disponible. Por ejemplo, cuando se destruye un elemento hardware, se corta una línea de comunicación o se deshabilita el sistema de gestión de archivos.
- Modificación: ataque contra la integridad. Una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo, como cuando se cambian los valores de un archivo de datos, se altera un programa o se modifica el contenido de mensajes transferidos por la red.
- Fabricación: ataque contra la autenticidad. Una entidad no autorizada inserta objetos falsificados en el sistema. Por ejemplo, la inserción de mensajes esporádicos en una red o la adición de registros a un archivo.

Estos ataques se clasifican, a su vez, en pasivos y activos.

- Ataques pasivos: el atacante no altera la comunicación, sino que únicamente la escucha o monitorea, para obtener la información que se trasmite. Sus objetivos son la intercepción de datos y el análisis de tráfico,

una técnica más sutil para obtener información de la comunicación, que resulta muy difícil de detectar, pues no provoca ninguna alteración de los datos.

- Ataques activos: implican algún tipo de modificación del flujo de datos trasmitido o la creación de un falso flujo de datos. Se subdividen en cuatro categorías:
    - Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados reemplazando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
    - Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
    - Modificación de mensajes: una porción del mensaje legítimo es alterada o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
    - Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes esporádicos. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Trukulo (2003) señala dos tipos de atacantes o intrusos, de acuerdo a las motivaciones para el ataque y las acciones realizadas después: hackers y crackers. Los hackers saltan las barreras de seguridad, borran sus huellas y salen sin hacer daño a la empresa o al usuario. Están motivados por aprender sobre seguridad informática, pero sin la intención de causar daño, por eso sólo

modificarán lo necesario para no ser encontrados. Los crackers tienen motivos económicos, son mercenarios destructivos de la información.

Alfonso y Arocha (2012) clasifican a los atacantes siguiendo como criterio el nivel de conocimiento informático que se posee y determina tres tipos: básico, medio y avanzado. Los intrusos de nivel básico son usuarios que poseen un conocimiento limitado, con respecto a determinadas debilidades de los sistemas y el uso de herramientas informáticas, pero que de alguna forma logran tener acceso fácil a determinada información de manera ilícita, estos casos pueden acontecer cuando las personas acceden y navegan por las páginas del Internet y tienden a realizar pruebas de programas informáticos de los cuales no tienen pleno conocimiento acerca de los daños que pueden causar.

Los intrusos de nivel medio ya desarrollan programas de intrusión, conocen cómo detectar el sistema operativo que está usando la víctima, testean y bucean en sus vulnerabilidades, ingresan sin respetar las restricciones de usuarios u contraseñas, pero sus objetivos no están bien establecidos, motivo por el cual los ataques pueden decaer en el intento. En el nivel avanzado se incluyen intrusos con conductas dirigidas a causar daños devastadores de forma especializada. Sus métodos son variados y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección, como el llamado *phishing.*

Badopi (2003) asegura que existen tres factores para afrontar los ataques o intrusiones: la prevención, la detección y la recuperación. La prevención se encarga de preparar el equipo para recibir los ataques, mantener una buena política de seguridad y poder reaccionar instantáneamente, para así evitar el ataque. Medidas de prevención son las copias de seguridad, los cortafuegos o *firewalls*, los sistemas de detección de intrusos (IDS por sus siglas en inglés), etc, que ayudan a evitar el ataque.

La detección consiste en identificar los ataques en el momento en que se realizan, para poder contrarrestarlos debidamente. Una medida para la detección temprana es un IDS bien configurado, que sepa al momento lo que está ocurriendo y avise de inmediato. Por su parte, la recuperación es la parte más crítica, cuando no se

ha logrado evitar el ataque, y consiste en rescatar la información inicial, borrando el ataque para poder continuar con normalidad.

También existen mecanismos de defensa que contribuyen a prevenir y preparar para ataques informáticos. González (2004) señala los más relevantes: autenticación e identificación, encripción, controles de software y hardware, políticas, firma digital, esteganografía, tráfico de relleno, control de encaminamiento y unicidad.

La autenticación e identificación, relacionada con esta propiedad de la seguridad de la información (que referimos más arriba), es el mecanismo que hace posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Se refiere a la determinación de usuarios y contraseñas, con identidades únicas y verificables.

La encripción o criptografía es el arte de escribir en secreto, de transformar un texto simple a un párrafo ilegible con lo que se asegura que el mensaje solo puede ser leído por la persona que tenga permiso. Es aún la herramienta más poderosa para proporcionar seguridad computacional, al hacer que un texto sea ininteligible para el observador externo se logra que se nulifique el valor de una intercepción de los mensajes y la posibilidad de que sean modificados o fabricados.

Los controles de software permiten que los programas sean lo suficientemente seguros para excluir ataques desde afuera. También deben de ser diseñados y mantenidos para que uno pueda tener confianza en su seguridad. Los controles de software pueden incluir lo siguiente controles internos de programa, controles al sistema operativo y controles de desarrollo.

El hardware también puede contribuir al control, pues se han diseñado numerosos dispositivos que asisten en la seguridad computacional, como implementaciones de encripción en el hardware o en *smartcards* para asegurar el acceso limitado, protección al robo o dispositivos que verifican las identidades de los usuarios.

Las políticas son los controles que realiza la administración de una organización o su grupo de expertos para prevenir distintas amenazas que pueden presentarse en los sistemas o recursos de información. Todas las organizaciones asumen e

implementan políticas de seguridad informática, que no solo determinan cómo se realiza el control y qué medidas se toman, sino que también procuran la capacitación y entrenamiento inmediato de sus recursos humanos.

La firma digital implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.

La esteganografía es una técnica consistente en ocultar un texto o cualquier otra información, dentro de un archivo de gráfico o de audio, asegurado con una clave de acceso solo conocida por la persona que creó el archivo, quien también será el encargado de hacerla saber a quién tenga que descubrir el contenido de dicha foto o audio, sin la cual sería casi imposible de obtener.

El tráfico de relleno consiste en enviar información espuria junto con los datos válidos para que el atacante no sepa qué cantidad de datos útiles se está transmitiendo.

El control de encaminamiento permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo, posibilita solicitar otras rutas en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

La unicidad consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación de mensajes.

Estos mecanismos de defensa y formas de enfrentamiento a las amenazas informáticas, ayudan a prevenir y rechazar ataques informáticos, así como identificar, valorar, eliminar, minimizar, manejar y aceptar esos riesgos. Esta es la esencia de la seguridad informática, que no debe asociarse con términos como “limitar”, “restringir” o “prohibir”, aunque estos se hallen implícitos. En conclusión, “la seguridad de la información sirve para abrir puertas, no para cerrarlas, evidentemente, la idea es abrir la puerta sólo a quién se le tiene que abrir” (Pérez, 2006).

Habilitar mecanismos de defensa, pero extender todos los recursos de la información hacia entornos abiertos, disponibles y más seguros. Esta aspiración, claramente, no puede lograrse solo con políticas, softwares especializados o restricciones, porque la seguridad informática es un concepto complejo, en el que se dan la mano numerosos factores técnicos y humanos.

1.3.2 Políticas de seguridad informática en Cuba.

Las nuevas condiciones impuestas por el desarrollo informático han determinado la necesidad de adecuar el ordenamiento jurídico y el funcionamiento de las organizaciones a las peculiaridades de la actividad ciberespacial y el uso de recursos informáticos, dictando principios, procederes y normas legales que contribuyan a regularlas. El Código Penal cubano se ha actualizado respecto al tema, definiendo y sancionando los delitos informáticos en el país; de igual manera, se han legislado decretos y resoluciones de diferentes organismos que orientan las políticas de seguridad de las organizaciones en torno a los procesos informáticos que desarrollan.

La política de seguridad informática atiende a los principios de confidencialidad, integridad y disponibilidad. Estipula una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento. En el contexto cubano, aparece reflejada en los siguientes documentos legales:

- Resolución Ministerial 6/96 del Ministerio del Interior (Minint).
- Decreto Ley 199/99 del Consejo de Estado.
- Resolución Ministerial 127/2009 del Ministerio de la Informática y las Comunicaciones (MIC).
- Resolución Ministerial 176/2009 del SIME.

Los órganos encargados de establecer la política para garantizar una adecuada seguridad informática, han establecido reglas básicas en este sentido. Al respecto, sugieren que esta debe adecuarse a las necesidades y recursos de la enseñanza,

al valor que se le da a estos recursos y a la información que se procese, así como al uso que se hace del sistema en todos los centros del sector. Por otra parte, deben evaluarse los riesgos, el valor del sistema protegido y el costo de atacarlo, además del conocimiento del sistema a proteger y de su entorno. También hacen referencia a la experiencia en la evaluación de riesgos y al establecimiento de medidas de seguridad.

Sobre esa base se elabora el Plan de Seguridad Informática de las organizaciones, basado en la identificación y análisis de riesgos, detectando los aspectos que hacen al sistema informático susceptible de ser atacado o amenazado (vulnerabilidades). Este es el documento básico que establece los principios organizativos y funcionales de la actividad de seguridad informática en un órgano, organismo o entidad, a partir de las políticas y conjunto de medidas aprobadas sobre la base de los resultados obtenidos en el análisis de riesgo previamente realizado.

En el Ministerio de Educación Superior cubano, las medidas de seguridad informática se toman en las instituciones. Es por ello, que en cada una se designa un responsable de velar por la ejecución y el cumplimiento de lo establecido en el Plan de Seguridad Informática. En las universidades es un docente el encargado de realizar esta labor, que tiene entre sus responsabilidades fundamentales:

a) Organizar y controlar las medidas de seguridad informática contempladas en el Plan.
b) Aplicar un sistema informativo que le permita conocer la situación en las entidades subordinadas, basado en auditorías y análisis periódico de las trazas (constancia de los accesos de los usuarios a los diferentes servicios de la red).
c) Informar y asesorar a los directivos en temas de seguridad informática y en la toma de decisiones respecto a las medidas a tomar por violaciones.
d) Asegurar la preparación del personal técnico relacionado con los procesos informáticos en la temática.

El jefe de seguridad informática debe ser un profesional preparado y con voluntad constante de superarse en la materia, para mantenerse actualizado y poder

asesorar y enfrentar cualquier contingencia durante su trayectoria laboral como especialista.

Una función esencial en su quehacer es la auditoría, entendida como el proceso de verificación y control mediante la investigación, análisis, comprobación y dictamen del conjunto de medidas dirigidas a prevenir, detectar, responder acciones que pongan en riesgo la confidencialidad, integridad, disponibilidad de la información que se procese, intercambie, reproduzca y conserve por medio de las tecnologías de información.

De las auditorías y el monitoreo de las trazas se derivan los informes de seguridad informática, que identifican las principales vulnerabilidades de la organización en la seguridad de la información y proponen medidas y estrategias para mejorarla. El perfeccionamiento continuo del proceso, en otras palabras, la gestión de la calidad constituye su esencia.

La política de seguridad informática y los documentos que la norman conceden gran relevancia al usuario en el proceso, a sus necesidades y prioridades derivadas del intercambio de información. Sin embargo, el usuario, que es el agente de los procesos informáticos y que juega un rol medular en la prevención de amenazas y la erradicación de vulnerabilidades, suele ser el gran ausente de los procederes de la seguridad informática en las universidades. Solo existe un documento legal que lo vincula a esos procederes y acuerda su responsabilidad en ellos (Código de ética); ni los contratos laborales, ni las políticas científicas, ni las organizaciones de masas en la universidad definen cuestiones relacionadas. Además, su preparación en el tema no se contempla en los Planes de Seguridad Informática ni entre las funciones que deben cumplir los responsables de ella en la organización.

También es posible constatar un vacío en la ciencia. Entre las investigaciones sobre el tema abundan las que asumen el punto de vista de la implementación de políticas, medidas administrativas, el diseño o implementación de softwares o mecanismos de defensa y prevención, pero poco se ha hablado del factor humano. El usuario contribuye de forma vital a la seguridad informática y puede,

cuando ignora los riesgos y las maneras de protegerse o cuando los conoce, pero es negligente, provocar vulnerabilidades en las organizaciones.

1.3.3 Dimensión ética de la seguridad informática

La seguridad informática no es un asunto solo de administrativos y expertos en la ciencia informática, importa a todos los usuarios, que deben ser preparados para que pueda lograrse un ambiente realmente seguro para el intercambio de información. Hoy se hace cada vez más imprescindible que esa capacitación no incluya solo la simple instrucción sino también la educación en la materia.

Un número creciente de violaciones a la seguridad informática en las organizaciones está relacionado con conflictos de origen ético, como el acceso no autorizado a redes y base de datos o el abuso del correo electrónico, empleado con fines no académicos: divulgación de contenido inadecuado, difusión masiva no autorizada y ataques con objeto de imposibilitar o dificultar el servicio de correo electrónico.

Otra transgresión es el acceso a sitios web con contenido ajeno y contrario a los objetivos y valores que rigen la institución, como pornografía o de ideología contraria al proyecto revolucionario (en su sentido amplio: contrarrevolucionaria, imperialista, pero también elitista, racista, homofóbica, fascista, etc.). Asociado también al uso inseguro de la Internet está la piratería de software (copia ilegal de programas para computadoras), que va en contra de la integridad de la propiedad intelectual, o el diseño y uso de software con fines delictivos (para hurtar o dañar información personal, para cometer fraude).

El documento vinculante que informa al usuario de sus responsabilidades con la seguridad de la información es el Código de ética. Establece, entre otros elementos, los deberes y derechos del usuario con respecto a los servicios que le brinda la red informática a la que se acoge: correo electrónico; navegación nacional e internacional; servicios informativos, de búsqueda y almacenamiento, etc.

El Código se basa en principios éticos fundamentales que se corresponden con la misión y los valores compartidos de la universidad, y es aplicable a situaciones

que caracterizan las actividades con esta tecnología. El Código se centra en la esencia misma de lo que es ser un usuario de Informática. Establece normas de comportamiento que rigen el uso correcto y ético de las tecnologías de la información.

El Código sintetiza la información elemental que debe dominar el usuario final y que contiene el Reglamento interno de la RedUniss que, a su vez, se rige por la Resolución 127/07 del MIC. Es un documento sintético, de fácil comprensión, redactado en lenguaje llano, y susceptible de actualizarse cada cierto tiempo, según la evolución de las tecnologías de la información en nuestro país.

El Código establece que los usuarios finales son los máximos responsables de garantizar que la información a la que accedan o difundan cumpla con los objetivos científico-técnicos de la RedUniss, manteniendo en todo momento una actitud acorde con los principios morales de nuestra sociedad. A partir de esta disposición generalizadora, va dictando una serie de prohibiciones y formas de proceder ante situaciones que ponen en riesgo la seguridad de la información, por ejemplo:

2. Las cuentas de los usuarios no deberán utilizarse con fines lucrativos, ilícitos o de índole personal.

3. Queda prohibida la distribución de información a través de RedUniss no acorde con los principios de la Revolución.

5. Es responsabilidad del usuario informar inmediatamente a su jefe superior, así como a los administradores de la red el recibo de cualquier tipo de mensajes que no sea acorde a la moral y los principios de la Revolución, para definir la procedencia de éste y tomar las medidas pertinentes, evitando su distribución.

6. Es responsabilidad del usuario el chequeo contra virus informáticos de toda la información que reciba y/o envíe por correo, debiendo informar de inmediato la detección de algún virus en cualquier información obtenida por esta vía a su responsable de Seguridad Informática. Además, detendrá el trabajo en la microcomputadora donde se descubra el virus y procederá a su desinfección, elaborando el debido reporte y procediendo como se indica en el reglamento de Seguridad Informática acerca de este tema.

12. Los usuarios deben informar de inmediato cualquier violación del presente código o del Reglamento de la RedUniss a la administración del nivel superior, actuando con celeridad. De la misma forma, deben informar si ocurriera un ataque externo a la RedUniss con información subversiva, proveniente de otro lugar o de alguna organización contrarrevolucionaria.

15. Queda prohibido el uso de Proxy anónimo por parte de los usuarios ya que estos transgreden la seguridad de la información que fluye por nuestra red.

La firma del Código de ética por el usuario establece un compromiso moral con la institución de usar sus recursos de forma segura y como está determinado por las normativas del MES, y otorga a la dirección de la universidad la capacidad de decidir sobre el usuario que rompe con este compromiso. Aunque en el documento no se determinan los tipos de sanciones de acuerdo a las normas infringidas, sí se informa al usuario al respecto que "la Administración Central de la RedUniss se reserva la facultad de sancionar a los usuarios que infrinjan este código y/o el Reglamento" (Código de ética interno de la RedUniss, 2017).

Conclusiones del capítulo

El Código de ética es el único documento que informa la participación directa del usuario en el logro de los objetivos de la seguridad informática, una situación contradictoria si se tiene en cuenta que el usuario es el agente principal del intercambio de información y el uso de los recursos y servicios informáticos. Cada vez se hace más necesario que se le dé el debido protagonismo en la prevención y afrontamiento de los riesgos o amenazas informáticas.

Para ello, es importante brindarle la preparación adecuada para entender esos riesgos, la forma de evitarlos y combatirlos, e incluso, la actualización necesaria en los temas de seguridad informática, constantemente cambiando, de acuerdo a su caracterización como usuario (no es lo mismo para el estudiante que para el docente, para el docente novel que para el experimentado: las motivaciones, habilidades y consumo de recursos o servicios informáticos son diversos).

Sin embargo, no basta solo con adquirir el conocimiento necesario para prevenir situaciones de riesgo, empleando correctamente los recursos y servicios

informáticos, también es importante sensibilizar al respecto, educar en la importancia de asumir actitudes y valores éticos; formar en la responsabilidad individual y el compromiso con la organización a la que se pertenece y con la seguridad de la información que se intercambia en ella.

El docente joven o novel es uno de los que más urgentemente requiere superarse en estos temas, por su caracterización como usuario activo, muy receptivo de las TIC en su desempeño profesional y científico, y a la vez, con escasa experiencia o preparación para el uso de las redes telemáticas.

CAPÍTULO 2. PRESENTACIÓN Y EVALUACIÓN DE LA ESTRATEGIA DE SUPERACIÓN PROFESIONAL PARA LA FORMACIÓN DE CONOCIMIENTOS SOBRE SEGURIDAD INFORMÁTICA EN PROFESORES NOVELES.

En este capítulo se describe y valora la estrategia de superación profesional para fortalecer los conocimientos sobre seguridad informática de los profesores noveles de la Uniss, partiendo de los métodos de investigación y de las técnicas para la recogida de la información, declarados al comienzo. En primera instancia, se presentan los resultados del diagnóstico inicial aplicado a los profesores noveles que constituyen la muestra, lo cual constituyó el punto de partida para definir la variable dependiente y operacionalizarla. Seguidamente se exponen los fundamentos teóricos de la estrategia de superación como instrumento metodológico adecuado para enfrentar la problemática de estudio y se procede a la valoración de los resultados y las regularidades obtenidas durante el periodo de su implementación para lograr los objetivos formulados.

2.1 Concepción de la estrategia de superación profesional

La estrategia, como aporte de significación práctica, tiene como propósito esencial la proyección a mediano y largo plazo de la transformación de un objeto temporal y espacialmente ubicado, mediante la utilización de determinados recursos y medios que responden a líneas directrices específicas. En el contexto concreto de la educación:

> La estrategia establece la dirección inteligente, y desde una perspectiva amplia y global, de las acciones encaminadas a resolver los problemas detectados en un determinado segmento de la actividad humana. Se entienden como problemas las contradicciones o discrepancias entre el estado actual y el deseado, entre lo que es y debería ser, de acuerdo con determinadas expectativas que dimanan de un proyecto social y/o educativo dado. Su diseño implica la articulación dialéctica entre los objetivos (metas perseguidas) y la metodología (vías instrumentadas para alcanzarlas (Armas, Lorences y Perdomo, 2005: 1).

En el caso que nos ocupa, la estrategia de superación profesional se concibe como un conjunto de acciones que, desde la superación profesional en el marco

universitario, permiten cerrar la brecha entre el estado real y el estado deseado, en cuanto a la formación de conocimientos de seguridad informática de los profesores noveles de la Uniss.

Para conformar la estrategia se consultaron múltiples fuentes que analizan el su concepción y estructura, y se asumen los criterios de Armas, Lorences y Perdomo (2005), que consideran que en los marcos del trabajo científico debe considerar los siguientes componentes:

I. Introducción o fundamentación. Se establece el contexto y ubicación de la problemática a resolver, ideas y puntos de partida que fundamentan la estrategia.

II. Diagnóstico. Indica el estado real del objeto y evidencia el problema en torno al cual gira y se desarrolla la estrategia.

III. Planteamiento del objetivo general. Se define el objetivo general y su derivación a otros objetivos que permiten la transformación del objeto.

IV. Planeación estratégica. Se planifican por etapas las acciones con fecha de cumplimiento, lugar de ejecución, métodos y técnicas empleadas, participantes, responsables y los objetivos a los que responden.

V. Evaluación. Definición de los logros y obstáculos que se vencen, valoración de la aproximación lograda al estado deseado.

Fig. 1.1: Diagrama de la Estrategia
Fuente: Elaboración propia

2.1.1 Introducción

La determinación de necesidades de superación de los profesores noveles de la Uniss, relacionadas con la formación de conocimientos sobre seguridad informática permitió que se diseñara y aplicara una estrategia encaminada a su preparación teórico-metodológica, que contribuyera a un mejor desempeño como docente universitario, agente responsable de la integridad de los recursos y el intercambio de la información que transita por la red.

Teniendo en cuenta las características de la problemática estudiada y las necesidades y oportunidades que presentan los sujetos de la investigación respecto a la temática, se asumió la superación profesional como la modalidad de la educación de posgrado que permite afrontar la solución de dichas necesidades, tomando como base los fundamentos teóricos sobre la temática investigada, contenidos en el capítulo anterior.

Atendiendo a las características del Diplomado de Formación básica para la docencia universitaria, se utiliza la variante de superación a tiempo parcial, para la

que se usaron los espacios creados en el sistema de trabajo de la universidad. Esto permitió concretar en la práctica la estrategia propuesta, atendiendo a las exigencias del desempeño docente concreto de los sujetos que conforman la muestra.

La estrategia que se propone está definida por los siguientes rasgos generales o premisas:

- Responde a una contradicción entre el estado actual y el deseado de la realidad educativa en cuestión.
- Estructuración en etapas, descritas a partir de objetivos y acciones que le dan cumplimiento.
- Carácter participativo y didáctico, donde se integra el saber de todos los participantes.
- Carácter dialéctico que le viene dado por la búsqueda del cambio cualitativo que se producirá al implementar la estrategia, por las constantes adecuaciones y readecuaciones que puede sufrir el accionar del docente en el proceso de aprendizaje y sensibilización en el tema de la seguridad informática y por la articulación entre los objetivos y la metodología, entre otras.
- Contextualizada según las prioridades y transformaciones de la universidad, se adecua a las características de su modelo actual. Toma en cuenta las realidades concretas, por lo que sus acciones se articulan con la práctica pedagógica cotidiana y utilizan los espacios creados en el sistema de trabajo para el desarrollo de las acciones de superación y para la aplicación de la propuesta.
- Generalizable como condición de su aplicabilidad y factibilidad en otros contextos semejantes. Su diseño contiene orientaciones factibles de modificación, perfeccionamiento, enriquecimiento y reorganización en nuevas condiciones.

2.1.2 Fundamentos teóricos de la estrategia

Los presupuestos que sirven como base teórica a la estrategia parten de la valoración filosófica, sociológica, pedagógica y psicológica.

Desde lo filosófico, la estrategia se fundamenta en la dialéctica materialista, sobre la cual se estructuran los principios de la ciencia y sus métodos de investigación, apoyados en el materialismo dialéctico.

Se asume que el conocimiento no se encuentra en el objeto mismo, sino en la estrecha relación del sujeto con el objeto, donde es de vital importancia la situación en la cual surge y es utilizado, a través del desarrollo de pensamiento, según la teoría del conocimiento (Lenin, 1964). Así como la concepción del hombre y del aprendizaje humano asumida por Marx y Engels (1955), quienes distinguen:

- Buscar el origen de la psiquis fuera de ella misma, en las relaciones materiales que los hombres establecen entre sí, en la relación social, en sus obras como resultado de su práctica social y en sus relaciones con los otros, como relaciones sociales.
- El concepto de praxis, acción productiva y creadora del hombre sobre la realidad; que le permite transformar el mundo.
- Comprender al hombre como un sujeto activo, capaz de transformar las condiciones en que vive, a partir de su actividad y su propio desarrollo.

Estas concepciones son determinantes en la concepción de la estrategia, donde a partir de los problemas detectados durante el diagnóstico, se busca que el novel se apropie de los conocimientos que contribuyan a su formación y cumpla con la responsabilidad de multiplicar sus conocimientos, considerando en el proceso el ascenso de lo abstracto a lo concreto y de ahí a la práctica como el principio y el fin de la actividad cognoscitiva.

El carácter de sistema se presenta en la estrategia al establecer los nexos y relaciones de cada uno de los elementos, el estudio de la logicidad e historicidad del problema hasta llegar a conclusiones que, como expresión de lo sintético, conducen a una renovación en los mecanismos de adquisición de conocimientos, actitudes y de una actuación pedagógica.

El desarrollo de esta estrategia se fundamenta en la Sociología de la Educación Marxista, que considera la sociedad como condicionante de la educación, en un proceso en el cual el docente se erige uno de los sujetos principales.

En un contexto global de acelerado avance tecnológico que ha alcanzado todas las esferas de la vida, donde las organizaciones diariamente acceden, generan e intercambian grandes volúmenes de información, la formación de capacidades para el manejo de las TIC y la formación de conocimientos en materia de seguridad informática adquieren importancia de primer orden.

La universidad, transformada en centro productor de cultura, ciencia y tecnología, tiene la misión de investigar y de preparar a sus docentes para garantizar la integridad, disponibilidad y confidencialidad de la información, contra las continuas amenazas y ataques externos e internos. Toca al profesorado universitario, responsable de la formación integral de los profesionales de la sociedad, el reto de formarlos y educarlos en estos conocimientos derivados del compromiso con la seguridad de su futuro centro laboral.

Desde los fundamentos psicológicos, la estrategia propuesta se consolida en los presupuestos del enfoque histórico-cultural de Vygotski (1981) y su defensa de la autoformación del sujeto a partir de la mediación cultural, que revoluciona y reorganiza continuamente la actividad subjetiva de los individuos sociales y se manifiesta en una progresiva regulación de sí mismo, evidenciada en el ámbito sociocultural, donde todo proceso psicológico aparece dos veces: primero se aprende en lo interpsicológico como actividad conjunta con otros y solo después se consolida en lo intrapsicológico, como dominio personal o capacidad individual.

Además, se toma en consideración en la presente investigación la noción de Zona de Desarrollo Próximo (ZPD) que plantea las relaciones que se establecen entre aprendizaje y desarrollo, definida por Vygotski como "[…] la distancia entre el nivel real de desarrollo, determinado por la capacidad de resolver independientemente un problema y el nivel de desarrollo potencial, determinado a través de la solución de un problema, bajo la guía del adulto, o en colaboración de un compañero más capaz" (1987: 133).

El diagnóstico como condición de trabajo del docente, unido al autodiagnóstico del estudiante, dirigidos ambos al estudio de las posibilidades y al aseguramiento de las condiciones, que propicien una elevación del estudiante a niveles superiores

mediante la colaboración y la cooperación, logrando de esta manera el dominio independiente de sus funciones.

El alumno constituye el centro de atención, como sujeto consciente, activo y orientado hacia un objetivo, en interacción con otros sujetos, ejecutando acciones sobre el objeto y utilizando los diferentes medios en las condiciones socio-históricas concretas. Se insiste, además, en el carácter transformador, creativo del alumno, en el proceso de apropiación de la experiencia histórico-social, que le convierta en un sujeto que aporta nuevos productos a los ya ofrecidos por la humanidad (Vygotski, 1981).

Estos presupuestos teóricos que sustentan la estrategia también impusieron requisitos para el desarrollo del proceso de enseñanza-aprendizaje:

- Dinámico, donde se entremezclan el trabajo individual y el grupal, se comparten los espacios de aprendizaje, con plena interacción y cooperación, en beneficio de las relaciones interpersonales empáticas que garantizan la efectividad del aprendizaje.
- Participativo, donde el rol protagónico lo asumen los noveles, que deben desarrollar estrategias de aprendizajes metacognitivas para autoevaluar sus conocimientos previos, la adquisición y consolidación de nuevos conocimientos, donde el docente tiene una función orientadora/facilitadora. Se estimula la reflexión para la transformación de la realidad educativa
- Comunicativo por excelencia, donde priman las relaciones horizontales, el diálogo de saberes, el intercambio de experiencias y conocimientos para la construcción colectiva. El uso las TIC como medios para la enseñanza (aula virtual) permite establecer nuevos modelos de comunicación que fortalecen en los profesores noveles su papel como seres activos, emisores pensantes, colaborativos e involucrados en el proceso en el cual participan.
- Comprometido, pues se busca la sensibilización de los noveles para garantizar la seguridad de la información en la Uniss y el reconocimiento de su deber con la multiplicación de los conocimientos adquiridos en todas las esferas de su desempeño docente.

2. 1. 3. Objetivos de la estrategia

Objetivo general

Contribuir a la formación de conocimientos sobre seguridad informática en profesores noveles, de modo que se fortaleza su desempeño como usuario de la RedUniss.

Objetivos a mediano plazo

- Fomentar la incorporación de los conocimientos adquiridos en esta experiencia a todos los espacios de convivencia universitaria en los que interactúa el novel, especialmente en el aula.
- Contribuir al mejor desempeño del novel como docente, investigador, persona social, etc., en el contexto universitario.

Objetivo a largo plazo

- Mejorar la protección de los servicios y el intercambio seguro de información en la Uniss.

2.1.4 Diagnóstico

Este constituye la segunda etapa de la estrategia de superación, en la cual se aplican varios instrumentos para evaluar el estado actual de la problemática en la Uniss, de lo general a lo particular, con énfasis en los conocimientos sobre seguridad informática que dominan los sujetos de la investigación. Para obtener esta información se aplicaron guías de análisis de documentos, entrevistas semiestructuradas y cuestionarios.

Previo al diagnóstico fue imprescindible la definición y operacionalización de la variable formación de conocimientos sobre seguridad informática, de modo que se pudieran ajustar las acciones e instrumentos de la estrategia al cumplimiento de los objetivos trazados. La operacionalización de la variable en dimensiones e indicadores fue posible a partir de la revisión de la literatura científica en torno al tema.

Definición y operacionalización de la variable

A partir del profundo análisis de la bibliografía científica se pudo definir y operacionalizar la variable que se pretende transformar y evaluar en profesores

noveles. Para la determinación de las dimensiones e indicadores de la variable se asume, además, la clasificación de la categoría conocimiento que brinda la Unesco, determinando cuatro pilares fundamentales: “aprender a conocer, es decir, adquirir los instrumentos de la comprensión; aprender a hacer, para poder influir sobre el propio entorno; aprender a vivir juntos, para participar y cooperar con los demás en todas las actividades humanas; por último, aprender a ser, un proceso fundamental que recoge elementos de los tres anteriores” (Delors, 1994).

Partiendo de esta clasificación, se reconoce como Nivel de formación de conocimientos sobre seguridad informática: la apropiación escalonada de conocimientos sobre la temática, de orden teórico, práctico, axiológico y de aplicación en la realidad, los cuales integra gracias al aprendizaje metacognitivo.

Consecuentemente, se operacionalizó para su estudio en cuatro dimensiones: teórica, práctica, axiológica y vivencial (Anexo No.1).

Aplicación del análisis de documentos

Se concibieron y aplicaron guías de análisis a los informes de seguridad informática (Anexo No. 2) y a los planes de superación (Anexo No. 3) de la Uniss en los últimos tres años.

La revisión de los planes de superación de la Universidad de Sancti Spíritus “José Martí Pérez” del 2015 al 2017 permite confirmar que en el periodo no se planificó ninguna acción de superación relacionada con la formación de conocimientos de seguridad informática. Aunque se impartieron cursos que abordaban temáticas asociadas, como cultura informacional, búsqueda y recuperación de la información o comunicación científica, en ninguno se contempla la seguridad informática como parte esencial de sus contenidos u objetivos.

Lo anterior permite afirmar que la superación recibida hasta el momento de iniciarse la presente investigación no satisfacía las necesidades de preparación de los noveles para garantizar la seguridad de la información en su desempeño como docente.

También se revisaron los informes de seguridad informática y de monitoreo de trazas, con carácter mensual y semestral, en el periodo. Se pudo constatar un aumento gradual del número y del tipo de violaciones a la seguridad informática,

relacionadas con actitudes negligentes o ignorantes del usuario de la RedUniss, entre las que destacan, organizadas por el índice de recurrencia:

- Empleo predominante de la red y el servicio de correo con fines personales, para esparcimiento, chat o comunicación interpersonal.
- Acceso a sitios web que vulneran la seguridad de la red, entre ellos destaca la navegación empleando proxys anónimos (proxyninja.com, kproxy.com) para acceder a redes sociales fuera de los horarios determinados por la administración informática.
- Acceso a páginas que no cumplen con el objeto social de la universidad, con alta incidencia en sitios de ocio (Facebook, TWOO) sobre las de contenido académico o científico.
    - También, en menos casos, el acceso a páginas contrarias a los principios morales de la universidad (sitios de contenido sexual).
- Transferencia negligente de la identidad del usuario a otra persona.
- Ejecución de dispositivos extraíbles contaminados con virus informáticos sin previo análisis del antivirus.
- Almacenamiento de documentos clasificados (exámenes, actas, informes), por parte de docentes, en computadoras conectadas a la red sin protección.
- Empleo de un usuario común en las computadoras.

Aunque la mayoría de los usuarios que cometieron infracciones a la seguridad informática fueron estudiantes (56,3 %), un porciento nada desdeñable (43,7%) lo constituían profesores.

En los balances semestrales de monitoreo de las trazas también se identifican los veinte usuarios con mayor actividad en la navegación en Internet y en el uso del correo electrónico (envío y recepción de mensajes). Se pudo constatar que, durante el periodo observado, entre los usuarios más activos de la Uniss primaban los docentes de diferentes departamentos. En la navegación internacional, los docentes más activos eran jóvenes y en el uso de correo electrónico, aquellos con responsabilidades de dirección (decanos, jefes de departamento, etc.).

Los sitios web más visitados fueron www.facebook.com, www.intranet.uniss.edu.cu, www.google.com.cu y www.microsoft.com. Los

dominios desde los que se recibieron más mensajes fueron: la red social Facebook (en formato de notificaciones), uniss.edu.cu y el servidor de correos de google denominado gmail.com.

Aplicación de la entrevista semi-estructurada

La entrevista (Anexo No. 5) se aplicó a siete especialistas o personas vinculadas a la seguridad informática, entre ellos dos miembros del equipo que gestiona el proceso en la Uniss, tres administradores de red de diferentes áreas y dos técnicos de laboratorio. Los sujetos que conforman la muestra entrevistada se seleccionaron intencionadamente, por su participación activa en la prevención e identificación de amenazas a la seguridad de la información o por sus responsabilidades en nodos o laboratorios de computación, que les convierten en puntos de referencia para el usuario común, que acude a ellos por asesoría en materia informática.

La totalidad de los entrevistados domina el concepto de seguridad informática, sus dimensiones físicas y lógicas, y la forma en que se organiza en la Uniss. Se reconoce, de manera general, el papel que juegan el equipo de especialistas de la Sede Central, los administradores de la RedUniss y técnicos de laboratorio, los decanos y otros responsables de Activos Fijos Tangibles (AFT) en las Facultades, Departamentos no docentes y Centros Universitarios Municipales (CUM). Sin embargo, solo tres entrevistados reconocen que el trabajo de la seguridad informática se dirige y supervisa por los más altos niveles de dirección (rectora y vicerrector primero).

Respecto a la pregunta dos de la entrevista, todos los sujetos reconocen el carácter transversal de la seguridad informática:

- “[…] se relaciona con todo lo que se hace en la universidad, porque las TIC se emplean cada vez más: para la docencia, cuando investigamos, para comunicarnos de diferentes maneras”.
- “Todos nosotros trabajamos de forma cada vez más conectada: se crean redes de conocimiento e investigación, la Intranet, el correo, la Internet, que es vital para todo lo que hacemos, y la seguridad informática es la forma de que todo eso se haga sin peligro, sin riesgo, porque cada día salen miles de

virus nuevos a la red y programas para engañar a la gente y robarles la cuenta".

La pregunta tres del cuestionario de la entrevista fue una de las que obtuvo más diversidad de criterios y buenas sugerencias, entre las que se repite la necesidad de que se divulgue más y se impartan preparaciones sobre el tema, no solo a quienes trabajan directamente administrando recursos y servicios informáticos, sino también a directivos, profesores y estudiantes de las diferentes áreas:

- "La seguridad informática se ha vuelto un reto en la Uniss porque nos integramos con el pedagógico, tenemos el doble de usuarios que antes con más ancho de banda y más privilegios, tenemos más servicios informáticos. El equipo de tres personas que supervisamos las trazas, por ejemplo, ya no nos damos abasto. Por eso es tan importante trabajar más con la gente, porque la gente comprenda la importancia de saber sobre el tema para protegerse. Este es un problema de todos."
- "Aunque la dirección de la Uniss ha demostrado un mayor interés en la seguridad informática y se nos da [al equipo de seguridad informática] un punto regularmente en los consejos de dirección, creo que es importante trabajar más con los decanos de las facultades y otros jefes de áreas, el tema de los riesgos que trae el mal uso de la RedUniss y la necesidad de que se tomen medidas serias con aquellos usuarios que reinciden en violaciones a la seguridad informática".
- "La gente conoce poco sobre seguridad informática, lo ven como un concepto abstracto o no ven todo lo que implica y a quienes implican. Yo pienso que puede divulgarse más sobre el tema. Mira, hay un espacio creado en la Intranet sobre la seguridad informática, pero está abandonado, nadie lo actualiza. También pudieran crear un sitio propio o un folleto que divulgue el tema".
- "[…] está un poco decaída en la Uniss y no solo en cuanto a que se visualice mejor como proceso, sino también en materia de investigación. Que yo sepa, no hay creados grupos o proyectos sobre seguridad informática, ni se ve representada en los eventos de la universidad".

Sobre la pregunta cuatro, todos los entrevistados refieren que no tienen conocimiento de ninguna actividad de superación profesional desarrollada en la Uniss, dirigida a formar conocimientos sobre seguridad informática. Al respecto, uno de ellos refiere: "[…] es una disciplina muy nueva, en constante renovación. Hay que estarse informando constantemente para poder estar realmente preparado. Incluso a nivel nacional escasean las preparaciones sobre el tema; se ha hecho algún que otro taller dirigido por la Dirección de Informatización del MES, donde se intercambian softwares, se comparten algunas experiencias, pero nada muy especializado. Si eso es así a nivel nacional, imagínate en la Uniss".

En torno a las preguntas cinco y seis, que indagan sobre la contribución del usuario a la seguridad de la información, los entrevistados coinciden en la necesidad de valorar más esa contribución y ofrecer mejor preparación:

- "Claro, el usuario es fundamental y la mayoría de los usuarios de la Uniss no saben de informática como nosotros, y a veces saben, pero no tienen conciencia de lo importante que es respetar las medidas de seguridad. Eso pasa, por ponerte un ejemplo, con los proxys anónimos. Los usuarios saben que no se puede, porque se lo hemos dicho, pero siguen usándolos para meterse en Facebook".
- "El usuario común, como tú dices, no tiene preparación ninguna. Sabe lo que dice el Código de ética, que no siempre se entiende porque no se analiza con personal especializado o porque ni siquiera se lee y se firma como una formalidad. Luego el desconocimiento de la ley no te exime de la culpa y es cuando se viola la seguridad informática".
- "Nos falta preparación, pero más que eso, nos falta corazón, porque el usuario conoce de forma general lo que puede y no puede hacer, no es un usuario cualquiera: son profesores y estudiantes universitarios, mejor preparados que otros, pero igual se cometen muchas violaciones […] Yo creo que también porque no se están tomando las medidas que se debería con ellos, tampoco la seguridad informática forma parte de su evaluación de profesor o de la integralidad del estudiante".

En torno a la última pregunta, las opiniones fueron muy variadas:

- “Todos los profesores y estudiantes deberían recibir preparación en temas de seguridad informática, no solo los noveles”.
- “Sí, creo que preparar al novel pudiera ser parte de la solución al problema, porque el novel es el profe joven, el que comienza en la universidad. Tiene mucho tiempo para prepararse y está comenzando, le queda toda una vida laboral por delante”.
- “Me parece fundamental, el profesor tiene que prepararse en ese tema desde que es novel, para que pueda aplicarlo en su labor en la universidad e influir en los estudiantes, desde el espacio de la clase”.

Aplicación del cuestionario a profesores noveles.

Se elaboró y aplicó un cuestionario (Anexo No. 4) a profesores noveles con el propósito de diagnosticar los conocimientos formados en materia de seguridad informática e indagar sobre su percepción de la problemática que plantea la investigación. Se buscó, además, conocer sus necesidades de superación en el tema y las formas de organización que consideraban más adecuadas, para adecuar la propuesta a las características reales de los sujetos de la muestra.

Respondieron el cuestionario 15 profesores noveles de los 20 matriculados en el Diplomado de Formación básica para la docencia universitaria en noviembre de 2016. La causa fundamental que motivó la selección de la muestra fue la ausencia de profesores el día de la aplicación del instrumento.

El cuestionario está conformado por 12 incisos que siguen diferentes patrones de pregunta: cerradas de Sí/No, de fundamentación, y una pregunta para autoevaluar los niveles de conocimiento sobre el tema según una escala del 1 al 9. Los resultados de la aplicación de este instrumento se precisan a continuación.

En la pregunta 1 el 100% de los sujetos considera importante la formación de conocimientos sobre seguridad informática para el desempeño del profesional universitario. Fundamentaron su respuesta el 86,7% de los noveles, entre las razones que expresan se encuentran: “el profesional universitario debe estar muy preparado, no solo en los contenidos de sus asignaturas, sino que debe poseer una cultura general integral”; “hoy la Informática es fundamental para el trabajo de

cualquier profesional, más para el universitario. Por tanto, la seguridad informática es muy importante"; "es importante para poder aprender a protegernos de los virus informáticos, que contaminan las memorias y las PC y borran la información con la que trabajamos"; "es importante porque todos somos responsables del uso de las computadoras y los dispositivos en la Uniss y la seguridad informática enseña a defenderlos de cualquier agresión".

En la pregunta 2 sobre la incorporación de los conocimientos de seguridad informática a la docencia, 60% de los noveles refieren no impartir docencia aún, solo un 6,6% marcó la opción Sí, y 33,3% respondieron negativamente. El profesor que respondió afirmativamente alega que desde su asignatura dirigió el análisis y firma del código de ética de la RedUniss.

La pregunta 2.2 se plantea para los sujetos que no respondieron afirmativamente la anterior. El 93,3% de los profesores consideran factible integrar conocimientos de seguridad informática en sus asignaturas, pero solo el 26,7% proponen formas de hacerlo, casi siempre relacionadas con la labor educativa desde la clase: crear conciencia en los estudiantes sobre la necesidad de usar el antivirus para proteger sus dispositivos; fomentar el cuidado de las computadoras de los laboratorios o trabajar desde la clase lo normado en el código de ética.

En la pregunta sobre fuentes de información consultadas para la investigación, el 100% de los noveles señalan Internet, 66,7% identifican la biblioteca, 20% instituciones y centros de estudio y solo 6,6% marcó la opción archivo. Aunque todos responden que toman medidas de seguridad cuando navegan en Internet (pregunta 4), solo 40% de los profesores mencionaron cuáles, entre las que se repiten: evitar sitios de contenido pornográfico o contrarrevolucionario y analizar con el antivirus las memorias cuando se ha recuperado información de origen dudoso.

En la pregunta 5, los profesores señalan como otras actividades de su desempeño que exigen conocimientos de este tipo: la comunicación a través del correo electrónico y redes sociales y la vinculación a cursos de posgrado y maestrías.

Lo anterior demuestra que los noveles reconocen la seguridad informática como un conocimiento relevante para la realización de su labor docente; sin embargo,

ofrecen argumentos muy generales al respecto o relacionan la seguridad informática con la protección de hardware o de la información contra los ataques de virus, lo que sugiere que no hay claridad respecto a la misión de la seguridad informática ni a sus múltiples relaciones con el desempeño del docente.

Consecuentes con las respuestas anteriores, 86,7% de los noveles no se consideran preparados en materia de seguridad informática y solo 13,3% indican que sí.

La tabla de la pregunta 7 cambia los patrones de pregunta, pidiendo al encuestado evaluar sus conocimientos, específicamente aquellos de orden teórico y práctico, sobre el tema. Se les pide usar una escala del 1 (escaso dominio) al 9 (excelente dominio), donde Bajo (1, 2, 3), Medio (4, 5, 6) y Alto (7, 8, 9). Al procesar los datos obtenidos en esta pregunta se concluye que:

- Concepto de seguridad de la información: 53,3% de los sujetos encuestados declaran un valor medio en la escala, 46,6% un valor bajo y solo 6,7% alto.
- Amenazas a la seguridad de la información: 53,3% docentes se evalúan con un valor medio, 33,3% un valor bajo, solo 13,3% alto.
- Formas de enfrentamiento a estas amenazas: 40% de los encuestados indican un valor medio, 53,3% un valor bajo, y solo 6,7% alto.
- Deberes y derechos del usuario: se califican con un valor alto de la escala el 73,3% y 26,7% con valor medio.
- Principales vulnerabilidades de la Uniss: 33,3% señalan un valor medio y 66,7% bajo.
- Actualización periódica del antivirus: 26,7% de los docentes se evalúan de alto, de medio el 13,3% y de bajo el 60%.
- Uso del antivirus para proteger dispositivos de almacenamiento: buen dominio de esta habilidad. Se ubicaron en la escala alta 86,7% de noveles encuestados y en la escala media el 13,3%.
- Realización de salvas de información: 26,7% de los encuestados indican un valor alto, 33,3% un valor medio y 40% bajo.

- Encriptación de información relevante: 86,7% de ellos señalan un valor bajo y solo el 13,3% un valor alto.
- Gestión responsable la cuenta de correo: se consideran con un nivel alto en la escala el 100%.
- Cambio periódico de la contraseña: indican un valor alto el 33,3% de las personas y con valor medio el 66,7%.
- Identificación de páginas académicas y científicas de otras de dudoso contenido: se evalúan con un valor alto el 100% de los encuestados.
- Identificación de páginas con certificación de seguridad: solo el 6,7% indica un valor alto en la escala, 93,3% lo señalan como un valor bajo.
- Uso de proxys anónimos: con valor bajo 93,3% de los noveles, 6,7% con valor medio.

El balance del instrumento arrojó que, de los 14 conocimientos de orden teórico y práctico, los noveles marcaron con valores bajos y medios (escaso y regular dominio) al menos nueve. Solo se marcaron con valores altos (excelente dominio) cinco conocimientos; sin embargo, llaman a la reflexión los resultados del ítem referido a los deberes y derechos del usuario, donde cuatro noveles indican valores medios del único documento normativo y de dominio obligatorio sobre la seguridad informática. Pasa similar con el ítem sobre uso de proxys anónimos, marcado como negativo por constituir una violación a la seguridad informática y que un novel declaró con valores medios. Lo anterior evidencia la necesidad de una estrategia que permita desarrollar una serie de acciones de superación en torno al tema.

En las preguntas 8 y 9, los encuestados reconocieron mayoritariamente (100%) la relación de la seguridad informática con valores y principios éticos, fundamentando su vinculación con la ética que debe acompañar al profesional en esta época. Entre los valores compartidos de la Uniss que avalan la contribución del usuario en este sentido, se reconocen la responsabilidad, la honestidad, la honradez y en menor medida, el patriotismo. Un docente propone, además, el sentido de pertenencia con la universidad.

En la pregunta 10, los encuestados alegan como principales vías de adquisición de conocimientos sobre el tema: el autodidactismo, la consulta al código de ética de la RedUniss y la asesoría de algún amigo o compañero de trabajo. Ninguno marcó la vía de la actividad de superación profesional.

Se identificaron como necesidades de superación a incluir en el curso (pregunta 11): el conocimiento de las amenazas a la seguridad de la información y las formas de enfrentamiento, la actualización y uso del antivirus, los contenidos referidos a la seguridad de la navegación en Internet y la salva y encriptación de la información. Como formas de organización de la superación profesional para abordar el tema (pregunta 12), los noveles prefirieron el curso, el taller, la autopreparación y la conferencia especializada, sin otras sugerencias.

Triangulación de instrumentos

Los distintos instrumentos aplicados (guías de análisis de documentos, entrevista semi-estructurada, cuestionario) permiten afirmar la importancia de preparar mejor al usuario de la Uniss en temas de seguridad informática, para erradicar actitudes negligentes o ignorantes que atentan contra la integridad de los recursos y de la información que transita por la RedUniss.

En este sentido, es importante priorizar al profesor joven y novel que, aunque posee capacidades tecnológicas y una activa vinculación a la red, su formación de conocimientos sobre seguridad informática es escasa y muy general. El novel reconoce el tema como relevante para la realización de su desempeño docente, investigativo y comunicacional, así como la necesidad de prepararse al respecto, todo lo cual evidencia una fortaleza para la presente investigación.

Se constató, por diferentes vías que los planes de superación profesional de la Uniss de años anteriores no satisfacen estas necesidades; por lo tanto, se hace urgente el diseño e implementación de una estrategia que permita dar respuesta a la preparación de los noveles para garantizar la seguridad de la información en su desempeño como docente.

2.1.5 Planeación estratégica

La estrategia propuesta se organiza estratégicamente en cinco etapas, que contienen un plan de acciones encaminado a desarrollarlas. Estas etapas de Motivación, Diagnóstico, Planificación, Implementación y Evaluación, se explicitan a continuación:

Etapa de Motivación: Es una etapa de sensibilización y preparación inicial del desarrollo de la experiencia, en que se busca acceder al grupo de noveles a través de Diplomado de Formación básica para la docencia; coordinar y obtener los permisos y espacios necesarios para la implementación de la propuesta; primeros acercamientos al grupo de noveles para caracterización inicial y promoción de las actividades de superación, creando expectativas y reconocimiento de la importancia de la experiencia.

Objetivos:

- Promover la estrategia y sus actividades de superación.
- Sensibilizar a los sujetos que conforman la muestra con la necesidad de participar en la experiencia.
- Gestionar la infraestructura y los permisos necesarios para implementar las acciones de superación.

Acciones:

1.- Diseñar y promover la convocatoria de las actividades de superación.

2.- Acordar con los coordinadores del diplomado el acercamiento al grupo de noveles y la inserción de la propuesta.

3.- Entrevistarse con el grupo de profesores noveles para conocerlos y propiciar un primer acercamiento al tema, a su importancia y a la necesidad de su participación voluntaria en la experiencia.

4.- Identificar espacios, recursos y horarios para la implementación de las actividades de superación profesional.

Responsables: el investigador

Tiempo de duración de la etapa: noviembre de 2016

Etapa de Diagnóstico: se diagnostican conocimientos sobre seguridad informática que tienen formados los noveles participantes en la experiencia. Se

busca identificar su percepción de la problemática y las necesidades de superación al respecto, para poder adecuar la propuesta a las características e intereses reales de los sujetos y que esta adquiera mayor pertinencia.

Objetivo:

- Diagnosticar conocimientos sobre seguridad informática que tienen formados los noveles.
- Identificar heterogeneidad, motivaciones y necesidades de aprendizaje.

Acciones:

1.- Elaborar los instrumentos científicos para diagnóstico.

2.- Aplicar los instrumentos y procesar la información recogida en ellos.

Responsables: el investigador

Tiempo de duración de la etapa: noviembre-diciembre de 2016

Etapa de Planificación: es una etapa de preparación teórica y metodológica intensa, en la que se determinan los objetivos, contenidos, las formas de organización, bibliografías y sistemas de evaluación. Se diseñan los programas de las actividades de superación profesional y se elaboran los medios de enseñanza.

Objetivos:

1.- Determinación de los objetivos de la formación de conocimientos sobre seguridad informática.

- Formar conocimientos teóricos y prácticos sobre seguridad informática en profesores noveles.
- Sensibilizar en la importancia de conocer sobre seguridad informática, fortaleciendo la formación de valores y principios éticos compartidos por la comunidad universitaria.
- Potenciar la integración de los conocimientos sobre seguridad informática en el desempeño profesional del profesor novel.

Los objetivos están encaminados a lograr transformaciones en los profesores noveles fortaleciendo sus conocimientos y actitudes sobre el tema, de forma que se manifieste en su actuación pedagógica, investigativa, diaria, de forma creadora.

2.- Determinación de los contenidos que contribuyan a la formación de conocimientos sobre seguridad informática.

En este objetivo se tuvieron en cuenta las necesidades de superación de los noveles sobre el tema, su percepción y sugerencias, expresadas en el cuestionario.

- Surgimiento de la seguridad informática como disciplina científica. Conceptos y clasificaciones fundamentales: seguridad; seguridad informática; seguridad de la información; sistema informático.
- Características de la información: integridad, disponibilidad y confidencialidad.
- Conceptos y tipos de vulnerabilidades, amenazas e incidentes informáticos.
- Medidas de prevención, contención y recuperación.
- Acciones que puede realizar el profesor novel para contribuir a la prevención y contención de incidentes y recuperación de la información:
    - Protección y recuperación de información vital. Uso y actualización de softwares antivirus para proteger dispositivos de almacenamiento. Realización de salvas y encriptación de datos. Procedimientos ante incidentes relacionados con la seguridad informática.
    - Gestión responsable del correo electrónico y de la cuenta de dominio. Detección de mensajes spam y phishing. Diseño de una clave de acceso robusta. Cambio periódico y protección de la clave.
    - Navegación segura en Internet. Identificación de páginas con certificación de seguridad (https) y páginas de contenido académico y científico de las que no lo son. El proxy anónimo y los softwares que vulneran la seguridad de la información, riesgos de su uso.
- Ética profesional y formación de valores asociados a la seguridad informática. El Código de ética de la RedUniss.
- Capacidades para la apropiación e integración de los conocimientos sobre seguridad informática en el desempeño del profesor novel con énfasis en la labor pedagógica.

3.- Selección de las formas de organización de la superación.

Para adoptar las formas organizativas de la superación se tuvo en cuenta las características actuales de la educación superior, los resultados del diagnóstico

aplicado a los sujetos de la investigación y lo establecido en el Reglamento de la Educación de Posgrado de la República de Cuba. En su selección se consideró la necesidad de desarrollar el carácter ascendente de las acciones de superación en cuanto a su nivel de complejidad:

- Curso de superación profesional a tiempo parcial. Se empleó con el objetivo de contribuir a la formación de conocimientos teóricos y prácticos sobre seguridad informática en profesores noveles y sensibilizar en la importancia de prepararse desde la asunción de valores y principios éticos.
- Autopreparación. Constituye un peldaño superior al anterior. Se busca profundizar en los contenidos abordados, logrando independencia y autogestión en la dirección del aprendizaje.
- Taller profesional. Asisten los docentes que han logrado cumplir con los objetivos propuestos en las formas anteriores. Su objetivo fundamental es potenciar la integración de los conocimientos sobre seguridad informática al desempeño profesional del profesor novel. En estos talleres se utilizó la autoevaluación, la coevaluación y la heteroevaluación como procedimientos evaluativos, lo que permitió la confrontación de ideas, juicios, opiniones, el ejercicio de la crítica, así como la socialización de los conocimientos adquiridos.

4.- Diseño del sistema de evaluación.

5.- Identificación de bibliografía básica y complementaria.

Acciones

1.- Elaboración de los programas de cada forma de organización propuesta.

- Programa del curso de superación profesional. (Anexo No.7)
- Programa de autopreparación. (Anexo No.8)
- Programa de los talleres profesionales. (Anexo No.9)

2.- Diseño de medios de enseñanza (aula virtual) para apoyar la docencia.

Responsables: el investigador

Tiempo de duración de la etapa: enero-marzo de 2017

Etapa de Implementación: es la más extensa en el tiempo. Es la fase donde se impartirán los cursos diseñados y adaptados al docente novel, según las

necesidades identificadas. Se aplica la observación pedagógica durante toda la etapa con el propósito de valorar la recepción y efectividad de la propuesta, observando la participación y actitudes de los sujetos que conforman la muestra. Esta etapa exige la alerta constante y actitud reflexiva del investigador en cuanto a la asistencia a los cursos, la motivación y tratamiento de la temática por parte del estudiante.

Objetivos:

- Impartir las actividades de superación propuestas.
- Observar comportamientos y actitudes de los noveles durante el proceso.

Acciones:

1.- Impartir las actividades de superación propuestas.

2.- Evaluar el desempeño de los cursantes en cada actividad.

3.- Aplicar la guía de observación pedagógica.

Responsables: profesores de las actividades, noveles.

Tiempo de duración de la etapa: abril-mayo de 2017

Etapa de Evaluación: No por ser la última deja de tener importancia vital y se irá desarrollando durante todo el proceso y retroalimentándose de cada resultado y logro obtenido. Lleva implícito la observación constante con ayuda de la guía y los momentos de intercambio colectivos para medir la temperatura del grupo, necesidades insatisfechas, bienestares, dudas, sugerencias y la evaluación del aprendizaje desde la autoevaluación, la coevaluación y la heteroevaluación, hasta la entrega de certificados de cada actividad.

2.2 Evaluación de la estrategia de superación profesional.

En el epígrafe anterior se presentó la estrategia de superación profesional para la formación de conocimientos sobre seguridad informática en profesores noveles. A continuación, se presentan los resultados de la evaluación de la estrategia, mediante la aplicación de un pre-experimento pedagógico.

Para ello se procedió a definir y operacionalizar la variable: Formación de conocimientos sobre seguridad informática.

2.2.1 Resultados de la aplicación práctica de las acciones de superación profesional.

Para garantizar la validez de los resultados y evaluar los criterios asumidos acerca de la formación de conocimientos de seguridad informática en profesores noveles, se combinan el control inicial, sistemático y final de las dimensiones de la variable operacional.

El diseño experimental que se empleó en la investigación para la implementación de la estrategia en la práctica educativa fue el pre-experimento pedagógico, orientado a comprobar la contribución de la propuesta en el cumplimiento del objetivo general, al comparar los resultados obtenidos en los instrumentos al inicio y al final de la experiencia. El pre-experimento posibilitó la evaluación del estado inicial de la variable, luego se aplicó la estrategia de superación profesional, y finalmente, se volvió a medir, de modo que pudieran realizarse determinadas inferencias acerca de su contribución.

En este sentido, se precisaron las principales direcciones que guiaron la puesta en práctica del pre-experimento:

- Diagnóstico de la problemática relacionada con la formación de conocimientos sobre seguridad informática en profesores noveles en las condiciones de la universidad espirituana.
- Análisis de las dimensiones e indicadores establecidos y su correspondencia con la estrategia propuesta.
- Diagnóstico y evaluación de la variable operacional.
- Implementación de la estrategia diseñada para contribuir a la formación de conocimientos sobre seguridad informática en profesores noveles, lo que permitió la vinculación sistemática de la teoría con la práctica y la reconstrucción permanente de las representaciones subjetivas del profesor novel sobre su futura actividad pedagógica profesional.

La preparación del pre-experimento se efectuó en octubre de 2016. Para realizar la primera predicción se elaboró y procesó el instrumento que conformó el pre-test: el cuestionario a profesores noveles sobre su conocimiento en materia de seguridad informática, diseñado para evaluar los conocimientos sobre seguridad

informática que tienen formados los profesores noveles de la Uniss, de acuerdo a las dimensiones e indicadores descritos, lo que permitió comprobar su nivel de formación inicial.

El diseño del pre-experimento seleccionado presenta determinados inconvenientes que no se deben obviar en su planificación, y que pueden marcar la diferencia entre los resultados alcanzados con el pre-test y los obtenidos con el post-test. Se tomaron un grupo de medidas para minimizar la influencia de posibles variables ajenas: se controló que no hubiera alteraciones en la muestra y de orientó la evaluación de los programas, aplicando los mismos tipos de evaluación para cada tipo de actividad de superación.

Análisis del Pre-test

La constatación inicial en la aplicación del cuestionario a profesores noveles puede leerse en el epígrafe 2.1.4 de este capítulo, los resultados obtenidos con el instrumento se triangularon, además, con los provenientes de las guías de análisis de documentos y la entrevista semi-estructurada, que otorgaban una visión externa y completiva de la problemática en la Uniss.

Después de implementada la estrategia de superación profesional se constatan comparativamente los nuevos resultados, se utiliza el mismo grupo para el control de la variable y el mismo instrumento, controlando las variables ajenas.

Análisis del Post-test

Aplicación del cuestionario a profesores noveles sobre su conocimiento en materia de seguridad informática.

En el análisis del instrumento para la constatación final, se indican específicamente aquellos resultados cualitativos y cuantitativos que indican cambios con respecto a la constatación inicial, con carácter comparativo.

En la pregunta 1, se mantiene que el 100% de los sujetos consideran importante la formación de conocimientos sobre seguridad informática para su desempeño profesional. En esta ocasión todos (100%) fundamentaron su respuesta con argumentos más completos que indican mejor dominio de todos los conceptos y categorías implican la seguridad informática: “es importante porque los profesores trabajamos continuamente con información digital en todo lo que hacemos: cuando

investigamos o publicamos, cuando nos preparamos para impartir las asignaturas, cuando nos superamos, cuando hacemos vida social, etc., y la información hay que protegerla"; "los usuarios tenemos mucha responsabilidad con la seguridad informática y jugamos un papel fundamental en la prevención de ataques informáticos"; "la seguridad informática es un problema de todos, los profesores debemos contribuir mucho, no solo porque somos los que más navegamos en Internet y enviamos correos, también porque somos los que estamos más cerca del estudiante y debemos educarlo en estos conocimientos".

En la pregunta 2 sobre la incorporación de los conocimientos de seguridad informática a la docencia, el 46,7% refieren no impartir docencia aún, otro 46,7% marcaron la opción Sí, y solamente el 6,6% respondió negativamente, aunque todos consideran factible esta integración. Proponen formas muy creativas de hacerlo, fundamentalmente relacionadas con la labor educativa e investigativa de las asignaturas:

- Analizar un principio del código de ética de la RedUniss en cada clase.
- Educar en la protección de la información que se intercambian estudiantes y profesores, usando siempre el software antivirus.
- Socializar en aulas virtuales o laboratorios la actualización semanal del Antivirus NOD-32.
- Incluir como requisito para la redacción de los trabajos de investigación, la consulta a sitios de reconocido contenido académico y científico o con certificación de seguridad.

En la pregunta sobre fuentes de información consultadas para la investigación, la Internet sigue siendo la fuente más consultada (100%). Todos los profesores fueron capaces esta vez de mencionar como medidas de seguridad que toman cuando navegan en Internet, al menos la consulta a sitios reconocidos por la comunidad científica o académica o que posean certificación de seguridad y el análisis con el antivirus de los dispositivos, inmediatamente después de recuperar la información. También señalaron como medida alertar al jefe o a los administradores cuando se ha accedido a información de origen dudoso.

En la pregunta 5, los profesores señalan otras actividades de su desempeño que exigen conocimientos de este tipo, además de las que surgieron en la constatación inicial del instrumento: la publicación científica o docente, la autopreparación, el intercambio con profesores de otras universidades, la dirección u organización de procesos y la divulgación de actividades extensionistas.

El 100% de los noveles se considera preparado en materia de seguridad informática (pregunta 6), lo cual se demuestra en la autoevaluación de sus conocimientos, específicamente aquellos de orden teórico y práctico, sobre el tema (pregunta 7):

- Concepto de seguridad de la información: el 100% de los encuestados declaran valores altos en la escala.
- Amenazas a la seguridad de la información: 60% de los docentes se evalúan con un valor alto y un 33,3% un valor medio y aún el 13,3% bajo.
- Medidas de prevención, contención y recuperación: 46,7% de los encuestados indican un valor alto, 53,3% un valor medio.
- Deberes y derechos del usuario: el 100% se califican con valores altos en la escala.
- Principales vulnerabilidades de la Uniss: señalan un valor medio el 80% de las personas y bajo el 20%.
- Actualización periódica del antivirus: se evalúan de alto el 73,3% de los docentes, de medio el 20% y de bajo el 6,7%.
- Uso del antivirus para proteger dispositivos de almacenamiento: buen dominio de esta habilidad. Se ubicaron en la escala alta el 100% de los encuestados.
- Realización de salvas de información: 53,3% de los encuestados indican un valor alto, 26,7% un valor medio y 20% lo considera bajo.
- Encriptación de información relevante: 60% de los noveles señalan un valor bajo, 26,7% un valor medio y solo 13,3% un valor alto.
- Gestión responsable la cuenta de correo: se consideran con un nivel alto en la escala el 100% de los encuestados.

- Cambio periódico de la contraseña: indican un valor alto el 100% de las personas.
- Identificación de páginas académicas y científicas de otras de dudoso contenido: se evalúan con un valor alto el 100% de los encuestados.
- Identificación de páginas con certificación de seguridad: 66,7% indican un valor alto en la escala, 33,3% señalan un valor bajo.
- Uso de proxys anónimos: con valor bajo el 100% de los noveles.

El balance del instrumento arrojó una elevación considerable de los valores altos y medios en la autoevaluación. Al menos en cinco ítems la valoración alta fue colectiva y en 11 en total predominan los valores altos. Se marcaron dos con valores medios y solo en uno, el referido a la encriptación de información importante, se predominan los valores bajos.

Las respuestas a las preguntas 8 y 9, permanecieron similares, los docentes también proponen la identidad, la integridad y el respeto. En la pregunta 10, los encuestados incluyen ahora la vía de la actividad de superación profesional.

Se identificaron como necesidades de superación en las que profundizar (pregunta 11): el conocimiento de las amenazas a la seguridad de la información y las medidas de prevención, contención y recuperación; la salvaguarda y recuperación de la información y también la actualización sobre los últimos virus y softwares antivirus creados para combatirlos; otros delitos informáticos y programas creados para ello. Como formas de organización de la superación profesional para profundizar en el tema (pregunta 12), los noveles añadieron los debates científicos y las conferencias especializadas.

Análisis de la observación pedagógica

Se empleó la observación pedagógica a las actividades de superación profesional de la estrategia, para valorar la recepción y efectividad de la propuesta observando la participación y las actitudes de los noveles en todo momento. La aplicación del instrumento exigió la atención constante del investigador para recepcionar las experiencias, opiniones y sugerencias en torno al tema y a la implementación de la estrategia. Para ello se determinaron una serie de dimensiones e indicadores a observar (Anexo No.6).

Se observó una buena asistencia a las actividades, por encima del 80% en todos los casos y la puntualidad fue buena, lo cual indica niveles de fiabilidad de los datos obtenidos en el pre-experimento, porque la ausencia repetida podía ser causante de resultados negativos y del fallo de la estrategia.

Esta dimensión se relaciona directamente con la siguiente, la motivación, porque la buena asistencia también implica interés por los cursos y, por lo tanto, permanencia de los implicados en la experiencia. También se constató que la atención hacia todos los que intervenían fue constante, en un marco de respeto, cordialidad e intenciones de compartir vivencias y e ideas originales. La participación fue activa, aunque primó más la participación dirigida por quien impartía el curso que la espontánea, sobre todo en los talleres profesionales que incentivaron el debate por excelencia sobre cómo integrar lo aprendido a la docencia. Se distinguió la formulación de interrogantes por parte de los cursantes, que expresaban dudas y contribuyeron a problematizar en torno al tema en la Uniss.

En la dimensión tratamiento del tema se buscó evidenciar el interés que suscitaba en los asistentes y la manera de abordarlo, que resultó muy satisfactoria. Se observó el surgimiento del debate amistoso y aportador, que permitió que noveles no muy convencidos con la factibilidad de relacionar la seguridad informática con la docencia, al final lograran reconocer la relevancia del tema, la urgencia de influir al respecto en el estudiantado y maneras creativas no forzadas de integrarlas a las asignaturas, de acuerdo a sus características. En torno a esta problemática (la integración de los conocimientos a la labor docente) giraron la mayor cantidad de sugerencias, posibles soluciones y ejemplos de buenas prácticas, en la modalidad de taller profesional.

El logro más significativo giró en torno al objetivo de sensibilización sobre el tema, que permitió crear en los asistentes conciencia de la importancia de mantenerse actualizado sobre seguridad informática y aplicar las medidas de seguridad en todas las esferas de su labor como docente. Se formó, además, el compromiso de promover lo aprendido en todos los espacios posibles de convivencia universitaria, especialmente entre los estudiantes.

De manera general, los noveles expresaron satisfacción con el contenido y la forma en que fue impartido y manifestaron agrado con la misión de contribuir a formar conocimientos sobre seguridad informática en sus futuros estudiantes.

Triangulación de instrumentos del Post-test

Tanto el cuestionario a profesores noveles como la observación pedagógica a las actividades de superación planificadas, arrojaron resultados positivos y que demuestran el éxito de la estrategia propuesta. Los profesores noveles fueron capaces de argumentar mejor y brindar más información sobre las funciones de la seguridad informática y a su importancia en todas las esferas de su desempeño profesional. Se logró la implicación activa de los sujetos que conformaban la muestra, se incentivó el debate, la sugerencia y la comunicación de vivencias relacionadas. Se formó el compromiso con la seguridad informática en la Uniss y la misión de promover los conocimientos adquiridos en diferentes espacios.

En el análisis final acerca de la formación de conocimientos sobre seguridad informática, se pudo inferir que con relación al período inicial los profesores noveles tuvieron un cambio positivo y altamente significativo, si se tienen en cuenta los parámetros establecidos, pues todos los aspectos medidos ascendieron a valores altos y medios.

2.3 Conclusiones del capítulo

La estrategia de superación profesional propuesta tiene carácter dialéctico, participativo y didáctico, es contextualizada y generalizable y se estructura en etapas que orientan su concepción (Motivación, Diagnóstico, Planificación, Implementación y Evaluación). También responde a una contradicción entre el estado actual y el deseado de la realidad educativa evaluada, que se constató empleando el pre-experimento.

La operacionalización de la variable formación de conocimientos sobre seguridad informática, según las dimensiones que establece la Unesco para la categoría conocimiento, permitió orientar la investigación hacia las necesidades reales de los sujetos de la investigación, con una mirada integradora.

En la constatación inicial del problema se identificaron limitaciones en la formación de conocimientos sobre seguridad informática, que precisan la necesidad de preparar a los profesores noveles en los conocimientos esenciales y necesarios que favorezcan su desempeño profesional, empleando la vía de la superación. En la constatación final se evidenciaron cambios favorables y significativos en todas las dimensiones de la variable operacional que permiten evaluar de forma exitosa la propuesta.

CONCLUSIONES GENERALES

El proceso investigativo descrito permite arribar a las siguientes conclusiones como resultado de la revisión teórica y de la experiencia vivida:

La seguridad informática es compleja y transversal a todos los procesos universitarios y el cumplimiento de su misión depende cada día más que se reivindique el rol del usuario como agente activo del intercambio de información. Para ello, es importante brindarle la superación adecuada y educarlo en actitudes y valores éticos, que permitan su compromiso al respecto. El docente novel es un eslabón importante de esta aspiración, por su caracterización como usuario activo y su influencia sobre el estudiantado. Los fundamentos teóricos y metodológicos de la investigación se sustentan en los presupuestos de la seguridad informática como disciplina científica y de la superación profesional, siguiendo las normas y reglamentos del MES.

El diagnóstico de las necesidades de superación de los profesores noveles de la Uniss permite afirmar que, aunque se dominan conocimientos generales sobre seguridad informática y se reconoce la importancia de prepararse en el tema, no hay claridad respecto a la misión y funciones de la seguridad informática ni a sus múltiples relaciones con el desempeño del docente. También se constató el escaso y regular dominio (valores bajos y medios) en diversos conocimientos teóricos y prácticos sobre seguridad informática, que demostró la urgencia del diseño e implementación de la estrategia propuesta.

La estrategia de superación profesional se sustenta en diversos fundamentos pedagógicos, filosóficos, sociológicos y psicológicos, y está concebida sobre la base de una serie de premisas: carácter dialéctico, participativo y didáctico, es contextualizada y generalizable y estructurada en etapas (Motivación, Diagnóstico, Planificación, Implementación y Evaluación) que orientan la dirección inteligente de las acciones encaminadas a resolver los problemas detectados durante el diagnóstico. Está diseñada para desarrollarse en estrecha relación con la labor

profesional que desempeñan los profesores noveles y en ella se emplea la modalidad a tiempo parcial.

La evaluación de la estrategia de superación profesional diseñada, demostró su contribución a la formación de conocimientos sobre seguridad informática, lo cual fue corroborado mediante un pre-experimento pedagógico aplicado a la muestra de profesores noveles. Su instrumentación en la práctica provocó una transformación de la variable operacional, a partir de la significatividad de la diferencia entre los resultados del pre-test y el pos-test. Se logró la implicación activa de los sujetos que conformaban la muestra, se incentivó el debate, la sugerencia y la comunicación de vivencias relacionadas y la aceptación del compromiso con la promoción de la seguridad informática en los diferentes espacios universitarios, particularmente la clase.

RECOMENDACIONES

Sobre la base de los hallazgos de la investigación, se recomienda:

- Incentivar la realización de estudios sobre la seguridad informática en la Uniss de manera general.
- Desarrollar investigaciones sobre la formación de conocimientos sobre seguridad informática en otros usuarios de la Uniss, como directivos o estudiantes, que también constituyen usuarios particularmente activos.

BIBLIOGRAFÍA

Acosta, D. E. y Negrete, E. (2012). La seguridad de la información en las empresas. Disponible en http://www.eumed.net/ce/2012/avnh.html el 16 de diciembre de 2016.

Addine Fernández, F. y otros. (2010). La superación permanente de profesores en Cuba: experiencia renovadora y permanente para la educación superior. La Habana: Universidad de La Habana.

Aguirre Murillo, J. J. (2005). La seguridad es prioritaria para las organizaciones. Disponible en https://www.microsoft.com/latam/technet/articulos/tn/oct05-13.mspx el 16 de diciembre de 2016.

Alfonso, A. y Arocha, H. C. (2012). La seguridad informática es un componente esencial de la Seguridad Nacional. En Revista Mendive, 10 (39).

Álvarez de Zayas, C. M., Fuentes González, H.C. (2007). El posgrado. Cuarto nivel de Educación. La Habana: Editorial IPLAC.

Álvarez, G. y Pérez, P. P. (2004). Seguridad informática para empresas y particulares. Editorial McGraw-Hill.

Añorga, J. (1995). La Educación Avanzada. Una teoría para el mejoramiento profesional y humano. En: Boletín Educación Avanzada Año 1, No.1 (diciembre). CENESEDA-ISPEJV, La Habana, Cuba

Armas Ramírez, Nerelys de Lorences, Josefa & Perdomo, José Manuel. (2003). Caracterización y diseño de los resultados científicos como aportes de la investigación educativa. Evento Internacional Pedagogía. Curso 85.

_____. (2005) Aproximaciones al estudio de las estrategias como resultado científico. CECIP. Instituto Superior Pedagógico “Félix Varela”. Villa Clara. En soporte electrónico.

Badopi, R. (2003). La seguridad de la información en las universidades. Disponible en http://repositorio.utc.edu.ec/bitstream/27000/536/1/T-UTC-1052%281%29.pdf el 16 de diciembre de 2016.

Ban, L. Y. y Heng, G. M. (1995). Computer security issues in small and medium-sized enterprises. Singapore Management Review, 17(1), 15-29.

Bernaza, G. (2004). “Teoría, reflexiones y algunas propuestas desde el enfoque histórico cultural para la educación de posgrado”. La Habana: MES.

Boehm, B. (1991). Software risk management: principles and practices. IEEE Software, 8(1), 32-41.

Bozu, Z. (2009). El profesorado universitario novel y su proceso de inducción profesional. En: Revista Magis, Vol. 1 (2), pp. 317-328.

_____ (2010). El profesorado universitario novel: estudio teórico de su proceso de inducción o socialización profesional. Revista electrónica de investigación y docencia.

Bradanovic, T. (2006). Conceptos Básicos de Seguridad Informática. Disponible en http://www.bradanovic.cl/pcasual/ayuda3.html el 16 de diciembre de 2016.

Castro, F. (2006). La sociedad que no se prepara para el uso de la computación está liquidada”. Discurso pronunciado durante el acto por el aniversario 15 del Palacio Central de Computación. Disponible en: www.voltairenet.org/article136504.html el 16 de diciembre de 2016.

Cela, J. (2014). La experiencia de la Universidad de Lleida en la incorporación de las TIC a la docencia universitaria. En Sangra A. y González, M. (Coords.). La transformación de las universidades a través de las TIC: discursos y prácticas. Barcelona: Editorial UOC.

De Armas, N. et al. (2003). “Aproximaciones al estudio de las estrategias como resultado científico”. Centro de Estudios de Ciencias Pedagógicas. Universidad Pedagógica “Félix Varela”. Manuscrito no publicado.

Decreto-Ley No.199 sobre la seguridad y protección de la información oficial Disponible en: http://www.tic.siteal.iipe.unesco.org/normativa/1436/decreto-ley-no-199-nov99-sobre-la-seguridad-y-proteccion-de-la-informacion-estatal el 16 de diciembre de 2016.

Delors, J. (1994). "Los cuatro pilares de la educación". En La Educación encierra un tesoro. México: El Correo de la UNESCO, pp. 91-103.

Díaz Canel, M. (2015). Discurso pronunciado la clausura del primer Taller Nacional de Informatización y Ciberseguridad. Disponible en: http://www.cubadebate.cu/noticias/2015/02/20/diaz-canel-existe-la-voluntad-

del-partido-y-el-gobierno-de-poner-la-internet-al-servicio-de-todos/#.WlUSBzRrzIU el 16 de diciembre de 2016.

Escudero, T.M. (1998). Consideraciones y propuestas para la formación permanente del profesorado. En Revista Educación No. 317, septiembre-diciembre.

Feixas, M. (2002). El profesorado novel: Estudio de su problemática en la Universitat Autónoma de Barcelona. Revista de Docencia Universitaria, REDU, 2 (1). Disponible en: http://revistas.um.es/red_u/article/view/11821/1140 el 19 de enero de 2017.

Foro Mundial sobre la Educación: Educación para Todos. (2000). Cumplir nuestros compromisos comunes, Dakar, Senegal.

García Batista, G., Addine Fernández, F. (2001). Formación Permanente de profesores. Retos del siglo XXI. (Curso 18). Congreso Internacional Pedagogía. La Habana.

González, M. (2004). El profesorado universitario su concepción y formación como modelo de actuación ética y profesional. Disponible en https://dialnet.unirioja.es/descarga/articulo/3786831.pdf el 18 de noviembre de 2016.

González, C. (2016). Seguridad Informática en Bibliotecas. Disponible en http://files.sld.cu/bmn/files/2016/04/Seguridad-Inform%C3%A1tica-en-Bibliotecas-opt.pdf el 18 de noviembre de 2016.

Gutiérrez. R. (2003). Los componentes del proceso de enseñanza-aprendizaje. Villa Clara: Instituto Superior Pedagógico “Félix Varela”.

Hernández Sampieri, R., Fernández-Collado y Baptista, P. (2006). Metodología de la investigación. 4ta Edición. México: McGraw-Hill/Interamericana Editores, S.A

Imberón, F. (2000). La formación y el desarrollo profesional del profesorado universitario. Hacia una nueva cultura profesional. Barcelona: Editorial Graó.

Jarauta, B. & Bozu, Z. (2013). Portafolio docente y formación pedagógica inicial del profesorado universitario: Un estudio cualitativo en la universidad de

Barcelona. Educación XXI: Revista De La Facultad De Educación, 16(2), 343-361.

Lara, P. (2010). Seguridad en Redes. Disponible en: https://issuu.com/patolara/docs/modulo_de_formacion_seguridad_enredes el 23 de marzo de 2017.

Lenin, V.I. (1964). Cuadernos Filosóficos. Editora política. La Habana.

López, R. (2014). Algunas consideraciones sobre los fundamentos teóricos de la superación profesional en la educación superior cubana. Disponible en http://morfovirtual2014.sld.cu/index.php/Morfovirtual/2014/paper/viewFile/153/86 el 23 de marzo de 2017.

Lorences González, J. (2003). Sistema didáctico para elevar la calidad del proceso docente educativo en la escuela rural. (tesis doctoral). Instituto Superior Pedagógico “Félix Varela. Villa Clara

Manunta, G. Seguridad una Introducción. Revista Seguridad Corporativa. Disponible en http://www.seguridadcorporativa.org el 23 de marzo de 2017.

Marcelo, C. (Coord.). (2009). El profesorado principiante: Inserción a la docencia. Barcelona: Octaedro.

Martín, A., Conde, J. y M, C. (2014). La identidad profesional docente del profesorado novel universitario. En Revista de Docencia Universitaria, Vol. 12 (4), pp.141-160.

Martínez, F. y Prendes, M. (2015). Nuevas tecnologías y educación. Madrid, España: Pearson-Prentice Hall.

Marx, C. & Engels, F. (1960). Obras Escogidas en dos tomos. Ediciones en lenguas extranjeras. Moscú.

Mendoza, C. A. (2011). Modelo teórico metodológico de superación profesional para el mejoramiento del desempeño de la función tutorial en el profesor de la Filial Universitaria municipal. Tesis en opción al Grado científico de Doctor en Ciencias Pedagógicas. Villa Clara: Universidad de Ciencias pedagógicas “Félix Varela”.

Mengual, L. (s/f). Arquitecturas de seguridad. Disponible en: www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf el 23 de marzo de 2017.

MES. (2004). Reglamento de la Educación de Posgrado. Resolución Ministerial 132. La Habana.

Mesa, N. y Salvador, R. (2010). El trabajo metodológico en el preuniversitario y su integración con la educación de posgrado y la investigación. Villa Clara: Instituto Superior Pedagógico “Félix Varela”. (Material Inédito).

Montesino, R., Baluja, W. y Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. En: RIELAC Vol. XXXIV (1), pp.40-58.

Morales, G. (2006). Criptografía: Seguridad en la información. Disponible en http://delta.cs.cinvestav.mx/~gmorales/CriptoConf/slicripto.pdf el 23 de marzo de 2017.

Morán, P. E. (2016). Plan de Seguridad Informática en base a parámetros de la norma ISO/IEC 27002 para mejorar la Seguridad de la Información en el Departamento de Tecnologías de Información y Comunicación del Gobierno Autónomo Descentralizado Provincial De Santo Domingo de los Tsáchilas. Tesis de grado previa a la obtención del título de Ingeniero en sistemas e informática. Universidad Regional Autónoma de los Andes. Santo Domingo, Ecuador.

Morant, J.L., Ribagorda, A. y Sancho, J. (1994). Seguridad y protección de la información. Colección de Informática. Madrid: Editorial Centro de Estudios Ramón Areces, S.A.

Olivera, J. (2006). Auditoría Informática y Seguridad Informática. Disponible en https://issuu.com/joseluisalvaradoolivera/docs/auditoriaseguridadinformatica

Partido Comunista de Cuba, PCC (2011). Lineamientos de la Política Económica y Social del Partido y la Revolución. La Habana.

Partido Comunista de Cuba (2016). Actualización de los Lineamientos de la Política Económica y Social del Partido y la Revolución para el período

2016-2021 aprobados en el 7mo Congreso del Partido en abril de 2016 y por la Asamblea Nacional del Poder Popular en julio de 2016.

Pérez, D. (2006). El sistema de información y los mecanismos de seguridad informática. Disponible en https://dialnet.unirioja.es/descarga/articulo/6121657.pdf el

Ramírez, C. A. (2012). Riesgo tecnológico y su efecto para las organizaciones, parte I. Seguridad cultura de prevención para TI. Disponible en: http://revista.seguridad.unam.mx/sites/revista.seguridad. unam.mx/files/revistas/pdf/Seguridad-Num14.pdf el 13 de marzo de 2017.

Reglamento de la Educación de Posgrado de la República de Cuba. Capítulo 1. Artículo1.

Resolución No. 127 /2007 del MIC Reglamento De Seguridad Para Las Tecnologías De La Información. Disponible en: http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf el 17 de diciembre de 2016.

Resolución 6/96 MINNIT. Reglamento sobre Seguridad Informática. Disponible en: http://www.poljgrave.sld.cu/download/R%20127-07.pdf el 17 de diciembre de 2016.

Romero-Moreno, L. M. (2010). La seguridad informática en la seguridad con la plataforma Moodle. En: Revista de Humanidades, No. 17, p. 169 – 190.

Rosado, D. et al. (2014). La Seguridad como una asignatura indispensable para un Ingeniero del Software. Disponible en https://upcommons.upc.edu/bitstream/handle/2099/11778/a25.pdf el 17 de diciembre de 2016.

Solano, O. J., García, D. y Bernal, J. J. (2016). El sistema de información y los mecanismos de seguridad informática en la pyme. En Revista Puntal, Vol. VII (11), pp. 77-98.

Spears, J. L. (2007). End users' contribution to information security policy effectiveness. Ponencia presentada en la 6th Annual Security Conference, Las Vegas, NV. Disponible en

http://www.isy.vcu.edu/~gdhillon/Old2/secconf/secconf07/PDFs/17.pdf el 6 de abril de 2017.

Spears, J. L. y Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522.

Stallings, W. (2003). Fundamentos de seguridad en redes. aplicaciones y estándares. Prentice-Hall Inc.

Trukulo. (2003). Evolución Doméstica Informática. Disponible en http://libertonia.escomposlinux.org/story/2003/1/13/153923/245 el 6 de abril de 2017.

Torra, I. et al. (2013). Retos institucionales de la formación del profesorado universitario. Revista de Docencia Universitaria, Vol.11 (1), pp. 285 – 309.

Torres, R.M. (2009). De la alfabetización al aprendizaje a lo largo de toda la vida. Tendencias, temas y desafíos de la educación de personas jóvenes y adultas en América Latina y el Caribe. 2009. Sexta Conferencia Internacional de Educación de Adultos (CONFINTEA VI, Belém-Pará, Brasil, 19-22 mayo del 2009), organizada por el Instituto de la UNESCO para el Aprendizaje a lo Largo de Toda la Vida (IUAL).

Tünnermann, C. (2003). La universidad latinoamericana ante los retos del siglo XXI, ed. Unión de universidades de América Latina, A.C. Ciudad universitaria. México, D.F.

Tünnermann, C. y Souza, M. d. (2003). Desafíos de la universidad en la sociedad del conocimiento, cinco años después de la Conferencia mundial sobre Educación Superior. Comité Científico Regional para América Latina y el Caribe del Foro de la UNESCO, París. en línea. Acceso desde htpp://unesdoc.unesco.org/images/0013/001344/134422so.pdf.

Ugas, L. J. (2002). Seguridad en organizaciones con tecnologías de información. Disponible en http://publicaciones.urbe.edu/index.php/telematique/article/viewArticle/768/1844 el 6 de abril de 2017.

Unesco (1990). Conferencia Mundial de Educación para Todos: Declaración Mundial sobre Educación para todos y Marco de acción para satisfacer las

necesidades básicas de aprendizaje. Disponible en: http://www.unesco.org/education/pdf/JOMTIE_S.PDF

_____. (1998). Marco de acción prioritaria para el cambio y el desarrollo de la educación superior. Punto 1.6 d; p. 5.

_____. (2008). Marco de acciones de Dakar. Educación para Todos: cumplir nuestros compromisos comunes. Aprobados por el Fondo Mundial sobre Educación de Dakar, Senegal, 26-28 de abril. París.

Valdés, A. (2013). La superación del maestro primario para el uso de la informática en la gestión del diagnóstico del escolar. Tesis presentada en opción al grado científico de Doctor en Ciencias Pedagógicas. Universidad de Ciencias Pedagógicas “Capitán Silverio Blanco Núñez”, Sancti Spíritus.

Vigotsky, L. S. (1987). Historia del desarrollo de las funciones psíquicas superiores. Editorial Científico -Técnica. La Habana.

Vigotsky L.S. (1981). Pensamiento y Lenguaje. La Habana. Editora Revolucionaria.

Viloria, O., Villegas, M. y Blanco, W. (2009). La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional. Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI’2009). Disponible en http://www.laccei.org/LACCEI2009-Venezuela/p162.pdf el 6 de abril de 2017.

Whitman, M. y Mattord, H. (2012). Principles of information security. Boston, USA: Cengage Learning.

ANEXOS

ANEXO # 1. Operacionalización de la variable Formación de conocimientos sobre seguridad informática.

Dimensión teórica (saber qué): conocimientos teóricos generales relacionados con la seguridad informática (definiciones, características, clasificaciones, sistemas categoriales).

Indicadores:

- Conceptos de seguridad de la información, de seguridad informática y otros.
- Principales vulnerabilidades, amenazas e incidentes informáticos.
- Medidas de prevención, contención y recuperación.

Dimensión práctica (saber hacer): acciones que el docente novel, como agente de la gestión de la información y del manejo de los recursos tecnológicos, debe realizar para contribuir a la prevención, contención y recuperación.

Indicadores:

- Uso y actualización de softwares antivirus para proteger dispositivos de almacenamiento.
- Protección y recuperación de información vital.
- Gestión responsable del correo electrónico.
- Navegación segura en Internet.

Dimensión axiológica (saber ser): valores y actitudes éticas que fundamentan la seguridad informática en la universidad.

Indicadores:

- Valores compartidos de la Uniss que se aplican a la seguridad informática (Responsabilidad, Honestidad, Compromiso e Identidad).
- Principios y deberes del usuario comprendidos en el Código de ética de la RedUniss.

Dimensión vivencial (saber convivir): Aprendizajes sobre seguridad informática en el quehacer cotidiano del docente novel.

- Vinculación con la docencia.
- Vinculación con la investigación.
- Vinculación con la superación profesional.
- Vinculación con actividades de socialización.

ANEXO # 2. Guía para el análisis de informes de seguridad informática de la Uniss.

Objetivo: Identificar las principales vulnerabilidades de la seguridad informática en la Uniss durante el periodo 2015-2017.

Indicadores a observar:

- Violaciones más frecuentes a la seguridad informática en la Uniss.
- Actividad del docente (violaciones en las que incurre, características de su navegación en Internet y uso del correo electrónico).

ANEXO # 3. Guía para el análisis de los planes de superación profesional de la Universidad de Sancti Spíritus “José Martí Pérez”.

Objetivo. Identificar el tratamiento de la seguridad informática como tema en los planes de superación profesional de la Uniss durante el periodo 2015-2017.

Indicadores a observar.

1. Cantidad de cursos u otras formas de superación que contribuyen a la formación de conocimientos sobre seguridad informática.

2. Valorar la profundidad en el tratamiento del tema en esas formas de superación.

ANEXO # 4. Cuestionario a profesores noveles sobre su conocimiento en materia de seguridad informática.

Objetivo: Constatar los conocimientos sobre seguridad informática que tienen formados los profesores noveles de la Uniss y su percepción de la problemática que plantea la investigación.

A partir de un proyecto de investigación, en la Uniss se realiza un estudio sobre los conocimientos que sobre seguridad informática poseen los profesores noveles. Sus ideas y sugerencias pueden resultar muy valiosas, por tales razones le invitamos a contestar este cuestionario con sinceridad y precisión. Muchas gracias por su participación.

1.- ¿Considera que la formación de conocimientos sobre seguridad informática es importante para el desempeño del profesional universitario?

Sí _____ No_____

1.1 Fundamente:

_____

_____

2.- ¿La(s) asignatura(s) que imparte incluye(n) la enseñanza y/o formación de conocimientos de seguridad informática?

Sí _____ No_____ No imparto clases aún____

2.1 Si la respuesta es afirmativa, argumente cómo:

_____

_____

2.2 Si la respuesta es negativa o aún no se imparten clases, ¿cree factibles acciones para la formación de conocimientos de seguridad informática en el pregrado?

Sí _____ No_____

2.2.2 ¿Cuáles Ud. implementaría?

_____

_____

3.- En su labor investigativa, ¿a cuáles fuentes de información acude con más frecuencia?

___Biblioteca ___Internet ___Archivo ___Instituciones y centros de estudio

4.- Cuando navega en Internet, ¿toma medidas para garantizar la seguridad de la información?

Sí _____ No_____

4.1 Si la respuesta es afirmativa, mencione algunas:

_____

_____

_____

5.- ¿Qué otras actividades de su desempeño como docente exigen conocimientos sobre seguridad informática?

_____

_____

_____

6.- ¿Se considera preparado en materia de seguridad informática?

Sí _____ No_____

7.- Complete la siguiente tabla sobre sus conocimientos en torno a la seguridad informática. Sírvase indicar su evaluación en cada inciso empleando una escala del 1 (la más baja) al 9 (excelente).

No.	**Conocimientos sobre seguridad informática**	**Valor de la escala**
1	Domino el concepto de seguridad de la información	
2	Puedo mencionar amenazas e incidentes informáticos	
3	Identifico diferentes medidas de prevención, contención y recuperación	
4	Conozco a fondo mis deberes y derechos como usuario,	

	con contenidos en el Código de ética de la RedUNiss	
5	Sé cuáles son las principales vulnerabilidades de la Uniss en este tema	
6	Actualizo periódicamente el antivirus en mi PC, mi tableta, mi móvil, etc.	
7	Uso el antivirus para proteger mis dispositivos de almacenamiento USB	
8	Realizo salvas de la información más importante relacionada con mi trabajo	
9	Sé cómo encriptar información relevante para protegerla.	
10	Gestiono de forma responsable mi cuenta de correo	
11	Cambio periódicamente la contraseña de mi cuenta del dominio Uniss	
12	Cuando navego en Internet, puedo identificar páginas académicas y científicas de otras de dudoso contenido	
13	Cuando navego en Internet, puedo identificar páginas con certificación de seguridad (htttps) de las que no lo tienen (http)	
14	Conozco y uso proxys anónimos para acceder a redes sociales u otros sitios.	

8.- ¿Cree Ud. que la seguridad informática se fundamenta en valores y principios éticos?

Sí _____ No_____

8.1 ¿Por qué?

_____

_____

9.- ¿Qué valores compartidos de la Uniss Ud. conoce que avalan su contribución como usuario a la seguridad informática?

Responsabilidad___ Honradez___ Solidaridad ___ Dignidad___

Honestidad___ Patriotismo___ Antimperialismo___

Otros_____

10.- ¿Cómo ha adquirido los conocimientos que posee sobre seguridad informática?

a) ___A través de actividades de superación

b) ___De forma autodidacta

c) ___Por medio de un compañero de trabajo o un amigo

d) ___Por lo leído en el Código de Ética de la RedUniss

11.- ¿En qué aspectos de la seguridad informática Ud. considera que necesita superarse? En su respuesta puede considerar los contenidos planteados en la pregunta 7.

_____

_____

_____

12.- De las formas de organización concebidas para la superación profesional, ¿cuáles resultarían, a su juicio, más pertinentes para abordar temas de seguridad informática?

___Taller ___Curso ___Diplomado ___Entrenamiento ___ Autopreparación

___Preparación metodológica ___Conferencia especializada ___Debates

___Otras. ¿Cuáles? _____

ANEXO # 5. Entrevista semi-estructurada a especialistas en el tema, técnicos y administradores de la RedUniss

Objetivo: Recoger opiniones, conocimientos, juicios y experiencias sobre el desarrollo de la seguridad informática en la Uniss.

Fecha: Hora: Lugar específico:

Preguntas:

1.- ¿Qué entiende por seguridad informática y cómo se organiza en la Uniss?

2.- ¿Cómo contribuye la seguridad informática a la realización de los procesos universitarios?

3.- ¿Qué aspectos Ud. considera que puede todavía perfeccionar la seguridad informática en nuestra universidad?

4.- ¿Qué cursos de superación profesional, impartidos en los últimos años en la Uniss, contribuyeron a formar conocimientos sobre seguridad informática?

5.- ¿Cómo contribuye el usuario común (docentes, estudiantes, trabajadores no docentes) a lograr la seguridad de los procesos informáticos?

6.- ¿Cree Ud. que los usuarios tienen la preparación adecuada para ello? Fundamente su respuesta.

7.- El novel es el profesor con menos de tres años de experiencia en la Educación Superior, ¿considera Ud. importante que se prepare en temas de seguridad informática? ¿Por qué?

ANEXO # 6. Guía de observación pedagógica a las actividades de superación profesional de la estrategia propuesta.

Objetivo: Valorar la recepción y efectividad de la propuesta observando la participación y actitudes de los docentes noveles que conforman la muestra.

Dimensiones	Indicadores	Se observan	No se observan
1. Asistencia	1.1 Los noveles asisten con regularidad		
	1.2 Los noveles asisten puntualmente		
2. Motivación	2.1 Atención manteniendo la vista de forma permanente a quien hace uso de la palabra		
	2.2 Participación espontánea		
	2.3 Formulación de interrogantes		
	2.4 Permanencia		
3.Tratamiento del tema	3.1 Se produce debate		
	3.2 Se identifican problemáticas y se ofrecen soluciones		
	3.3 Se ofrecen ejemplos de buenas prácticas vivenciales		
	3.4 Se muestra sensibilidad sobre la necesidad de profundizar en la temática		

ANEXO # 7. Programa del curso de superación profesional.

Título: Formación de conocimientos sobre seguridad informática en profesores noveles.

Total de horas. 48 horas.

Autor: Ing. Lic. Mitchell Santana Puyuelo

FUNDAMENTACIÓN

El siglo XXI ha trazado veloces retos al avance de las naciones. La globalización del recurso información se ha visto potenciada por el creciente desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), convertidas en piedra angular de procesos económicos, políticos y socioculturales. La informatización acelerada en todos los órdenes de la vida contemporánea, constituye un proceso de vital importancia, que encuentra características singulares en países en vías de desarrollo, con menos presupuesto para invertir en la infraestructura adecuada, en recursos humanos para el diseño de softwares o en la creación de capacidades para el uso de las TIC en una población empobrecida y con altos índices de analfabetismo.

En la región latinoamericana, Cuba resulta un caso singular, cuyo gobierno se ha identificado desde muy temprano con la necesidad de introducir y dominar las TIC en la práctica social. En la clausura del Primer Taller Nacional Informatización y Ciberseguridad, el Vicepresidente cubano Miguel Díaz-Canel entiende la informatización en Cuba como una meta colectiva: "[…] es un proceso complejo, retador, necesario, que tiene que ser abordado en la multi y la interdisciplinariedad, con visión de país y contando con la participación institucional y ciudadana, el cual debe abarcar transversalmente todos los escenarios y ámbitos de la vida política, económica y social del país, y constituir un imprescindible apoyo y soporte al perfeccionamiento integral de nuestra sociedad socialista, próspera y sostenible" (2015).

A la universidad toca un rol medular en este proceso masivo, en la formación de profesionales competentes y útiles, capaces de enfrentar los retos que la Sociedad

de la Información y las Comunicaciones les imponen, capaces de aunar ciencia y tecnología en su labor cotidiana. Pero, aquí la informatización cobra una doble dirección, la difusión de la cultura digital en futuros egresados y, además, el aprovechamiento de los recursos tecnológicos y el acceso y manejo de la información como herramientas útiles al desarrollo de múltiples procesos docentes, científico-investigativos y extensionistas.

Pasados los tiempos medievales en que gremios de profesores y estudiantes (universitas magistrorum et scholarium) convergían para la instrucción y difusión de saberes; la universidad moderna ha pasado de la simple reproducción a la creación de conocimiento útil a la sociedad. Se ha transformado en centro productor de cultura, ciencia y tecnología, y para ello, diariamente accede, genera e intercambia grandes volúmenes de información.

En este contexto, la seguridad informática deviene un proceso de vital importancia para garantizar la integridad, disponibilidad y confidencialidad de la información, contra las continuas amenazas y ataques externos e internos a los que se ven sometidas instituciones, empresas y organizaciones por igual, que pueden causar daños irreparables y que resultan totalmente prevenibles.

La seguridad informática es una disciplina cambiante en el marco de las ciencias informáticas, debido al veloz desarrollo de las tecnologías y la informatización de la sociedad, y consecuentemente, al incremento de los delitos y amenazas a los productos y servicios informáticos del mundo entero. Esta dinámica exige la continua superación y actualización de los profesionales de la disciplina, así como la necesidad de orientar y educar a los diferentes usuarios de las redes telemáticas para lograr verdadera competencia en la labor de protección y prevención.

En la educación superior cubana, la educación de posgrado es una de las direcciones principales de trabajo y el nivel más alto del sistema de educación superior, orientado a promover la educación permanente de los graduados universitarios. “En la educación de posgrado concurren uno o más procesos formativos y de desarrollo, no solo de enseñanza aprendizaje, sino también de

investigación, innovación, creación artística y otros, articulados armónicamente en una propuesta docente educativa pertinente a este nivel "(MES. (2004). Reglamento de la Educación de Posgrado. Resolución Ministerial 132. La Habana.)

La superación profesional constituye la vía adecuada para contribuir a fortalecer los conocimientos sobre seguridad informática de los usuarios, que actualmente se incluyen escasamente en programas de pregrado de la especialidad u otros de posgrado, y que pueden y deben formarse con urgencia en profesionales de los centros de producción y manejo de información. En las universidades, esta problemática adquiere particular relevancia en el caso de los usuarios jóvenes, y entre los docentes, el novel que, con amplias capacidades creadas para el acceso y manejo de la información digital, constituye uno de los usuarios más activos y vulnerables.

Este curso ofrece respuesta al problema relacionado con la necesidad de que los docentes noveles desarrollen conocimientos varios y conciencia sobre la importancia de la seguridad informática para el desempeño de su labor, formando valores como honestidad, responsabilidad, sentido de la identidad, patriotismo e integridad.

Objetivo General del programa: Formar conocimientos teóricos y prácticos sobre seguridad informática en profesores noveles, sensibilizando sobre su importancia en el contexto universitario.

Sistema de Conocimientos del programa:

Surgimiento de la seguridad informática como disciplina científica. Conceptos y clasificaciones fundamentales: seguridad, seguridad informática, seguridad de la información, sistema informático. Características de la información: integridad, disponibilidad y confidencialidad.

Conceptos y tipos de vulnerabilidades, amenazas e incidentes informáticos. Ética profesional y formación de valores asociados a la seguridad informática. El Código de ética de la RedUniss. Medidas de prevención, contención y recuperación.

Acciones que puede realizar el profesor novel para contribuir a la prevención y contención de incidentes y recuperación de la información:

- Protección y recuperación de información vital. Uso y actualización de softwares antivirus para proteger dispositivos de almacenamiento. Realización de salvas y encriptación de datos. Procedimientos ante incidentes relacionados con la seguridad informática.
- Gestión responsable del correo electrónico y de la cuenta de dominio. Detección de mensajes spam y phishing. Diseño de una clave de acceso robusta. Cambio periódico y protección de la clave.
- Navegación segura en Internet. Identificación de páginas con certificación de seguridad (https) y páginas de contenido académico y científico de las que no lo son. El proxy anónimo y los softwares que vulneran la seguridad de la información, riesgos de su uso.

Sistema de habilidades del programa:

1.- Argumentar el contexto histórico-tendencial y particularidades de la seguridad informática como disciplina científica en la actual Sociedad de la Información y el Conocimiento.

2.- Reconocer y definir su sistema categorial como disciplina.

3.- Identificar tipos de vulnerabilidades, amenazas, incidentes informáticos y medidas de prevención, contención y recuperación.

4.- Valorar la importancia de la seguridad informática en el contexto organizacional actual, asociada a la ética profesional y la formación de valores.

5.- Proteger y recuperar información vital.

6.- Gestionar responsablemente el correo electrónico y la cuenta de dominio.

7.- Identificar medidas de seguridad para la navegación internacional.

Valores a potenciar en este curso:

- Responsabilidad

- Ética profesional
- Integridad
- Identidad con la institución
- Compromiso moral

Estructura de las Unidades Didácticas:

Unidad Didáctica 1: Contexto histórico-tendencial y particularidades de la gestión de información científica en la actual sociedad de la información y del conocimiento.

Objetivos:

1.- Analizar los antecedentes y las particularidades del surgimiento de la seguridad informática, de modo que se comprenda su imbricación e importancia dentro de la Sociedad de la Información y del Conocimiento.

2.- Identificar el sistema categorial de la seguridad informática como disciplina científica, definiendo y caracterizando conceptos fundamentales.

Sistema de conocimientos: Surgimiento de la seguridad informática como disciplina científica. Conceptos y clasificaciones fundamentales: seguridad, seguridad informática, seguridad de la información, sistema informático. Características de la información: integridad, disponibilidad y confidencialidad.

Sistema de acciones a desarrollar: Analizar los antecedentes y las particularidades del surgimiento de la seguridad informática, así como su articulación con el actual escenario histórico-social-económico-tecnológico. Definición de los conceptos de seguridad, seguridad informática, seguridad de la información, sistema informático. Caracterizar la información.

Metodología empleada (métodos, medios, formas de organización):

- Método preponderante: conversación heurística
- Formas: conferencia, consulta y estudio independiente.
- Medios de enseñanza: Diapositivas proyectadas por el computador, materiales y documentos impresos.

Evaluación: La evaluación se realizará de forma oral mediante la participación e intervención de los estudiantes en la reflexión y debate de los temas planteados. Además, se aplicará una evaluación parcial integradora que incluirá la evaluación de esta unidad didáctica.

Unidad Didáctica 2: Modos de actuación de la seguridad informática. Principios y valores éticos que la sustentan

Objetivos:

1.- Clasificar vulnerabilidades, amenazas e incidentes informáticos.

2.- Describir principios y valores éticos que sustentan la seguridad informática.

3.- Identificar medidas de prevención, contención y recuperación.

Sistema de conocimientos: Conceptos y tipos de vulnerabilidades, amenazas e incidentes informáticos. Ética profesional y formación de valores asociados a la seguridad informática. El Código de ética de la RedUniss. Medidas de prevención, contención y recuperación.

Sistema de acciones a desarrollar: Definir y clasificar vulnerabilidades, amenazas e incidentes informáticos. Ejemplificar con la información más actualizada al respecto. Fundamentar la dimensión ética de la seguridad informática. Análisis del Código de Ética de la RedUNiss. Determinar y explicar las medidas de prevención, contención y recuperación en caso de indicentes informáticos.

Metodología empleada (métodos, medios, formas de organización):

- Método preponderante: conversación heurística, método investigativo.
- Formas: conferencias, seminarios, consultas y estudio independiente potenciando el trabajo oral en grupos
- Medios de enseñanza: Diapositivas proyectadas por el computador, materiales y documentos impresos.

Evaluación: La evaluación se realizará de forma oral mediante la realización de un seminario investigativo. Además, se aplicará una evaluación parcial integradora

que incluirá la evaluación de esta unidad didáctica.

Unidad Didáctica 3: Acciones para la prevención y contención de incidentes y recuperación de la información.

Objetivos:

1.- Identificar medidas de protección y recuperación de información vital, en caso de incidentes informáticos.

2.- Determinar acciones para la gestión responsable del correo electrónico y de la cuenta de dominio.

3.- Determinar medidas de seguridad para la navegación internacional.

Sistema de conocimientos: Protección y recuperación de información vital. Gestión responsable del correo electrónico y de la cuenta de dominio. Navegación segura en Internet.

Sistema de acciones a desarrollar: Práctica en el uso y actualización de softwares del antivirus. Realización de salvas y encriptación de datos. Determinar procedimientos ante incidentes relacionados con la seguridad informática. Identificación de mensajes spam y *phishing*. Diseño de una clave de acceso robusta. Medidas de protección de la clave. Identificación de páginas con certificación de seguridad (https) y páginas de contenido académico y científico. Identificación de proxys anónimos y softwares que vulneran la seguridad de la información. Explicar los riesgos de su uso.

Metodología empleada (métodos, medios, formas de organización):

- Método preponderante: conversación heurística, estudio independiente
- Formas de organización: clases prácticas, consultas y estudio independiente, potenciando el trabajo en laboratorios de computación.
- Medios de enseñanza: Diapositivas, materiales y documentos impresos, uso de la red para navegación internacional y uso de correo electrónico.

Evaluación: La evaluación en forma general se realizará mediante la ejercitación

de los contenidos en las clases prácticas a partir de la resolución de diferentes tareas de estudio independiente. Además, se aplicará una evaluación parcial integradora que incluirá la evaluación de esta unidad didáctica.

Integración de métodos, medios y formas del programa

Los métodos básicos a utilizar en todo el programa serán la conversación heurística, el método investigativo, el de trabajo independiente, de forma que el aprendizaje parta, siempre que sea posible de la elaboración colectiva y posea carácter activo, reflexivo e intencional en la realización de las tareas, basado en el uso de los materiales textuales, audiovisuales e informáticos creados para el curso. Se concibieron a partir de las necesidades de aprendizaje de los docentes y en función de sus modos de actuación profesional.

Los medios de enseñanza empleados son Pizarra, PC de los laboratorios, diapositivas, videos, materiales bibliográficos diversos y el aula virtual del curso, montada en la plataforma virtual de aprendizaje Moodle. Las formas que se utilizarán en el ámbito espacial serán: las conferencias, clases prácticas, seminarios y estudio independiente.

El sistema de evaluación de la asignatura tendrá distintos procedimientos, tareas evaluativas y niveles. Desde el punto de vista procedimental se utilizarán la autoevaluación permanente y final, la coevaluación y la heteroevaluación (cada una de estas con sus instrumentos). La evaluación se concibe de manera procesal, cada una de las actividades formativas contempla al menos una herramienta de evaluación, además de las evaluaciones parciales al final de cada unidad temática. La integración de todos los resultados alcanzados conformará la evaluación final del curso.

Bibliografía Básica:

Acosta, D. E. y Negrete, E. (2012). La seguridad de la información en las empresas. Disponible en http://www.eumed.net/ce/2012/avnh.html el 16 de diciembre de 2016.

Alfonso, A. y Arocha, H. C. (2012). La seguridad informática es un componente esencial de la Seguridad Nacional. En Revista Mendive, 10 (39).

Bradanovic, T. (2006). Conceptos Básicos de Seguridad Informática. Disponible en http://www.bradanovic.cl/pcasual/ayuda3.html el 16 de diciembre de 2016.

González, C. (2016). Seguridad Informática en Bibliotecas. Disponible en http://files.sld.cu/bmn/files/2016/04/Seguridad-Inform%C3%A1tica-en-Bibliotecas-opt.pdf el 18 de noviembre de 2016.

Lara, P. (2010). Seguridad en Redes. Disponible en: https://issuu.com/patolara/docs/modulo_de_formacion_seguridad_enredes el 23 de marzo de 2017.

Manunta, G. Seguridad una Introducción. Revista Seguridad Corporativa. Disponible en http://www.seguridadcorporativa.org el 23 de marzo de 2017.

Mengual, L. (s/f). Arquitecturas de seguridad. Disponible en: www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf el 23 de marzo de 2017.

Montesino, R., Baluja, W. y Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. En: RIELAC Vol. XXXIV (1), pp.40-58.

Morales, G. (2006). Criptografía: Seguridad en la información. Disponible en http://delta.cs.cinvestav.mx/~gmorales/CriptoConf/slicripto.pdf el 23 de marzo de 2017.

Morant, J.L., Ribagorda, A. y Sancho, J. (1994). Seguridad y protección de la información. Colección de Informática. Madrid: Editorial Centro de Estudios Ramón Areces, S.A.

Olivera, J. (2006). Auditoría Informática y Seguridad Informática. Disponible en https://issuu.com/joseluisalvaradoolivera/docs/auditoriaseguridadinformatica

Partido Comunista de Cuba (2016). Actualización de los Lineamientos de la Política Económica y Social del Partido y la Revolución para el período 2016-2021 aprobados en el 7mo Congreso del Partido en abril de 2016 y por la Asamblea Nacional del Poder Popular en julio de 2016.

Pérez, D. (2006). El sistema de información y los mecanismos de seguridad informática. Disponible en https://dialnet.unirioja.es/descarga/articulo/6121657.pdf el

Ramírez, C. A. (2012). Riesgo tecnológico y su efecto para las organizaciones, parte I. Seguridad cultura de prevención para TI. Disponible en: http://revista.seguridad.unam.mx/sites/revista.seguridad. unam.mx/files/revistas/pdf/Seguridad-Num14.pdf el 13 de marzo de 2017.

Resolución No. 127 /2007 del MIC Reglamento De Seguridad Para Las Tecnologías De La Información. Disponible en: http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf el 17 de diciembre de 2016.

Romero-Moreno, L. M. (2010). La seguridad informática en la seguridad con la plataforma Moodle. En: Revista de Humanidades, No. 17, p. 169 – 190.

Rosado, D. et al. (2014). La Seguridad como una asignatura indispensable para un Ingeniero del Software. Disponible en https://upcommons.upc.edu/bitstream/handle/2099/11778/a25.pdf el 17 de diciembre de 2016.

Solano, O. J., García, D. y Bernal, J. J. (2016). El sistema de información y los mecanismos de seguridad informática en la pyme. En Revista Puntal, Vol. VII (11), pp. 77-98.

Spears, J. L. y Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522.

Viloria, O., Villegas, M. y Blanco, W. (2009). La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional. Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2009). Disponible en http://www.laccei.org/LACCEI2009-Venezuela/p162.pdf el 6 de abril de 2017.

Whitman, M. y Mattord, H. (2012). Principles of information security. Boston, USA: Cengage Learning.

ANEXO # 8. Programa de autopreparación.

Título: Profundización de conocimientos sobre seguridad informática en profesores noveles.

Total de horas: 48 horas

Autor: Ing. Lic. Mitchell Santana Puyuelo

Fundamentación

La globalización del conocimiento y la cultura, la ciencia y la tecnología, la economía, la comunicación masiva e interpersonal, se ha desarrollado aceleradamente gracias al avance tecnológico acelerado de las últimas décadas. La creación de Internet, de la telefonía móvil, de las redes sociales, han traído nuevos espacios que conectan los más diversos sistemas (defensivos, financieros, viales, etc.) y enlazan a las comunidades más alejadas del planeta, propiciando el intercambio masivo de información a nivel global.

Pero, el ciberespacio no siempre garantiza el acceso seguro o privado de los usuarios, lo que ha contribuido a que en la sociedad actual no se hable de seguridad asociada solo a los espacios físicos sino también a las dimensiones virtuales a las que se ha expandido la vida social. Existen personas ajenas a la información, conocidas como hackers o piratas informáticos, que buscan tener acceso a la red para modificar, sustraer o borrar datos, por beneficio propio o en nombre de otros.

Los estudiosos del tema coinciden en que la mayor parte de las violaciones e intrusiones a los recursos informáticos son realizadas por el personal interno (administrativo o de sistemas), que domina los procesos y metodologías y tiene acceso a información sensible cuya pérdida puede afectar el buen funcionamiento de la organización vulnerada. La causa fundamental de los delitos informáticos es la seguridad ineficiente de las compañías y organizaciones y la falta de conocimiento relacionado con la protección de los recursos informáticos frente a las actuales amenazas externas e internas, por parte de especialistas y usuarios. De esta forma, la seguridad informática se convierte en una disciplina de primer

orden en el mundo globalizado tecnológicamente.

En Cuba, país en vías de desarrollo tecnológico, el formar capacidades para el uso seguro de los recursos tecnológicos y el manejo de información virtual, debe constituir una tarea de primer orden. De ahí la necesidad de concebir planes y programas que tributen a la superación de los profesionales de las organizaciones en esta temática, aún más si estas organizaciones son activas productoras y divulgadoras de información, como es el caso de las universidades.

Sobre la base de estos antecedentes y teniendo en cuenta la situación real que presenta la seguridad informática en la Uniss, se precisa el desarrollo de un grupo importante de actividades encaminadas a la formación de conocimientos sobre el tema en sus usuarios. Este programa se diseña a partir del diagnóstico iniciado a un grupo de profesores noveles, que reveló falta de preparación al respecto.

Por lo tanto, el **objetivo general** de este programa es contribuir a la formación de conocimientos de seguridad informática en profesores noveles, de manera que se fortalezca su desempeño profesional.

Objetivos específicos.

- Fortalecer los conocimientos sobre seguridad informática recibidos en el curso de superación, solucionando posibles deficiencias del proceso de aprendizaje.
- Valorar la importancia de estos conocimientos para el desarrollo del desempeño del docente universitario.

Contenidos

Tema # 1. Recapitulación de los aspectos con deficiencias detectados durante el desarrollo del curso de superación y la aplicación de la prueba pedagógica.

Tema # 2. La seguridad informática, conocimiento esencial del desempeño del docente en la universidad.

Metodología

En el curso se inició la formación de conocimientos sobre seguridad informática y se presentó la metodología, por lo cual los profesores noveles tienen un dominio

elemental de la temática, la metodología a seguir y los medios a emplear. Las acciones de autopreparación se orientan, mediante un conjunto de guías, a la solución de los problemas que aún subsisten. Este programa se orienta a aquellos docentes que vencieron el curso de superación; en este, el aprendizaje tiene al cursante como principal gestor, en los roles de estudiante y evaluador de los avances realizados. La autopreparación se sustenta tecnológicamente en el aula virtual del curso.

Evaluación

Se aplica la autoevaluación sistemática. Como evaluación final se completará una guía de autoevaluación que debe ser contestada por los docentes.

BIBLIOGRAFÍA

Acosta, D. E. y Negrete, E. (2012). La seguridad de la información en las empresas. Disponible en http://www.eumed.net/ce/2012/avnh.html el 16 de diciembre de 2016.

Alfonso, A. y Arocha, H. C. (2012). La seguridad informática es un componente esencial de la Seguridad Nacional. En Revista Mendive, 10 (39).

Bradanovic, T. (2006). Conceptos Básicos de Seguridad Informática. Disponible en http://www.bradanovic.cl/pcasual/ayuda3.html el 16 de diciembre de 2016.

González, C. (2016). Seguridad Informática en Bibliotecas. Disponible en http://files.sld.cu/bmn/files/2016/04/Seguridad-Inform%C3%A1tica-en-Bibliotecas-opt.pdf el 18 de noviembre de 2016.

Lara, P. (2010). Seguridad en Redes. Disponible en: https://issuu.com/patolara/docs/modulo_de_formacion_seguridad_enredes el 23 de marzo de 2017.

Manunta, G. Seguridad una Introducción. Revista Seguridad Corporativa. Disponible en http://www.seguridadcorporativa.org el 23 de marzo de 2017.

Mengual, L. (s/f). Arquitecturas de seguridad. Disponible en: www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf el 23 de marzo de 2017.

Montesino, R., Baluja, W. y Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. En: RIELAC Vol. XXXIV (1), pp.40-58.

Morales, G. (2006). Criptografía: Seguridad en la información. Disponible en http://delta.cs.cinvestav.mx/~gmorales/CriptoConf/slicripto.pdf el 23 de marzo de 2017.

Morant, J.L., Ribagorda, A. y Sancho, J. (1994). Seguridad y protección de la información. Colección de Informática. Madrid: Editorial Centro de Estudios Ramón Areces, S.A.

Olivera, J. (2006). Auditoría Informática y Seguridad Informática. Disponible en https://issuu.com/joseluisalvaradoolivera/docs/auditoriaseguridadinformatica

Partido Comunista de Cuba (2016). Actualización de los Lineamientos de la Política Económica y Social del Partido y la Revolución para el período 2016-2021 aprobados en el 7mo Congreso del Partido en abril de 2016 y por la Asamblea Nacional del Poder Popular en julio de 2016.

Pérez, D. (2006). El sistema de información y los mecanismos de seguridad informática. Disponible en https://dialnet.unirioja.es/descarga/articulo/6121657.pdf el

Ramírez, C. A. (2012). Riesgo tecnológico y su efecto para las organizaciones, parte I. Seguridad cultura de prevención para TI. Disponible en: http://revista.seguridad.unam.mx/sites/revista.seguridad. unam.mx/files/revistas/pdf/Seguridad-Num14.pdf el 13 de marzo de 2017.

Resolución No. 127 /2007 del MIC Reglamento De Seguridad Para Las Tecnologías De La Información. Disponible en: http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf el 17 de diciembre de 2016.

Romero-Moreno, L. M. (2010). La seguridad informática en la seguridad con la plataforma Moodle. En: Revista de Humanidades, No. 17, p. 169 – 190.

Rosado, D. et al. (2014). La Seguridad como una asignatura indispensable para un Ingeniero del Software. Disponible en

https://upcommons.upc.edu/bitstream/handle/2099/11778/a25.pdf el 17 de diciembre de 2016.

Solano, O. J., García, D. y Bernal, J. J. (2016). El sistema de información y los mecanismos de seguridad informática en la pyme. En Revista Puntal, Vol. VII (11), pp. 77-98.

Spears, J. L. y Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522.

Viloria, O., Villegas, M. y Blanco, W. (2009). La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional. Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2009). Disponible en http://www.laccei.org/LACCEI2009-Venezuela/p162.pdf el 6 de abril de 2017.

Whitman, M. y Mattord, H. (2012). Principles of information security. Boston, USA: Cengage Learning.

ANEXO # 9. Guía para la autoevaluación de la autopreparación de los profesores noveles.

Evalúa tu preparación en la temática con una escala de muy alto, (B) bien, (R) regular y (M) mal para cada uno de los siguientes indicadores.

1.- Domino conceptos relacionados con la temática:

a) seguridad _____

b) seguridad informática _____

c) seguridad de la información _____

d) sistemas informáticos _____

e) vulnerabilidad _____

f) incidente informático _____

g) amenaza _____

2.- Sé caracterizar la categoría información _____

3.- Puedo mencionar tipos de amenazas e incidentes informáticos _____

4.- Identifico diferentes medidas:

a) de prevención _____

b) de contención _____

c) de recuperación _____

5.- Reconozco y sé explicar la dimensión ética de la seguridad informática _____

6.- En materia de protección y recuperación de la información:

a) Sé realizar salvas de información _____

b) Sé encriptar información importante _____

c) Sé usar el antivirus para proteger mis dispositivos _____

d) Sé actualizar el software antivirus _____

e) Reconozco los procedimientos a seguir ante incidentes relacionados con la seguridad informática _____

7.- En materia de gestión responsable del correo electrónico y la cuenta de dominio:

a) Puedo identificar mensajes spam y *phishing* _____

b) Sé diseñar de una clave de acceso robusta _____

c) Conozco y ejecuto medidas de protección de mi clave personal _____

8.- En materia de seguridad en la navegación internacional:

a) Identifico y empleo páginas con certificación de seguridad (https) de otras que no tienen (http) _____

b) Identifico y empleo páginas de contenido académico y científico de otras de contenido dudoso _____

d) No empleo proxys anónimos ni softwares que vulneran la seguridad de la información _____

8.- Al término de este programa, reconozco las limitaciones y logros en mi propio aprendizaje sobre el tema _____

ANEXO # 10. Programa de los talleres profesionales

Título: Experiencias en la inserción de los conocimientos sobre seguridad informática en la práctica docente del docente novel.

Total de horas. 48 horas.

Autor: Ing. Lic. Mitchell Santana Puyuelo

Fundamentación

El programa se concibió para darle continuidad a la estrategia de superación de los docentes noveles en función de incentivar la aplicación de los aprehendido en la práctica pedagógica. Para desarrollarlo es necesario que los docentes hayan vencido los aspectos correspondientes al curso de superación profesional y a la autopreparación.

Se planificaron debates en torno a las experiencias de los docentes en el aprendizaje de los conocimientos, buscando el intercambio de ideas, sugerencias y vivencias que permitieran conformar, de forma colectiva, metodologías o procederes para insertar la seguridad informática en su accionar cotidiano, con especificidades en la impartición de docencia. Se busca desarrollar polémica constructiva, creación grupal creativa y reflexión constante sobre la propia práctica. Mediante su aplicación se concibe un incremento del protagonismo de los profesores noveles en la instrumentación de la estrategia de superación profesional.

El **objetivo** del programa es potenciar la integración de los conocimientos más actualizados sobre seguridad informática en el desempeño profesional del profesor novel, específicamente en la práctica pedagógica.

Contenidos

Taller #1. Problemáticas actuales de la seguridad informática en el ámbito internacional y nacional.

Taller # 2. La seguridad informática en el desempeño del docente universitario. Ideas para su inserción en la práctica pedagógica.

Orientaciones para el desarrollo de los talleres

Taller # 1. Problemáticas actuales de la seguridad informática en el ámbito internacional y nacional.

Objetivo: reconocer las problemáticas y la polémica en torno a la seguridad informática, en boga en el panorama internacional y nacional.

Orientaciones.

Debatir sobre las problemáticas y la polémica más actual generada en el panorama internacional y nacional en torno a la seguridad informática, generando comparaciones entre los dos ámbitos. Se busca actualizarse en el tema, continuamente cambiando en esta era globalizada y tecnológica, de modo que el docente pueda llevar a los estudiantes las noticias más novedosas e interesantes.

Taller # 2. La seguridad informática en el desempeño del docente universitario. Ideas para su inserción en la práctica pedagógica.

Objetivo: Exponer las principales ideas y experiencias sobre la integración de los conocimientos aprehendidos al desempeño del docente novel y a su práctica pedagógica.

Orientaciones

Se emplearán el método de elaboración conjunta para determinar ideas rectoras o procederes generales que permitan llevar al aula, aprovechando la heterogeneidad de carreras y asignaturas que imparten o preparan los noveles, los conocimientos sobre seguridad informática aprehendidos en las actividades de superación profesional. Se crearán grupos de trabajo para presentar sus ideas, criterios y experiencias. Se aplicarán la coevaluación y la heteroevaluación para evaluar las propuestas de cada grupo y se escogerán las más completas para formar parte del curso en próximos cursos.

Bibliografía

Acosta, D. E. y Negrete, E. (2012). La seguridad de la información en las empresas. Disponible en http://www.eumed.net/ce/2012/avnh.html el 16 de diciembre de 2016.

Alfonso, A. y Arocha, H. C. (2012). La seguridad informática es un componente esencial de la Seguridad Nacional. En Revista Mendive, 10 (39).

Bradanovic, T. (2006). Conceptos Básicos de Seguridad Informática. Disponible en http://www.bradanovic.cl/pcasual/ayuda3.html el 16 de diciembre de 2016.

González, C. (2016). Seguridad Informática en Bibliotecas. Disponible en http://files.sld.cu/bmn/files/2016/04/Seguridad-Inform%C3%A1tica-en-Bibliotecas-opt.pdf el 18 de noviembre de 2016.

Lara, P. (2010). Seguridad en Redes. Disponible en: https://issuu.com/patolara/docs/modulo_de_formacion_seguridad_enredes el 23 de marzo de 2017.

Manunta, G. Seguridad una Introducción. Revista Seguridad Corporativa. Disponible en http://www.seguridadcorporativa.org el 23 de marzo de 2017.

Mengual, L. (s/f). Arquitecturas de seguridad. Disponible en: www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf el 23 de marzo de 2017.

Montesino, R., Baluja, W. y Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. En: RIELAC Vol. XXXIV (1), pp.40-58.

Morales, G. (2006). Criptografía: Seguridad en la información. Disponible en http://delta.cs.cinvestav.mx/~gmorales/CriptoConf/slicripto.pdf el 23 de marzo de 2017.

Morant, J.L., Ribagorda, A. y Sancho, J. (1994). Seguridad y protección de la información. Colección de Informática. Madrid: Editorial Centro de Estudios Ramón Areces, S.A.

Olivera, J. (2006). Auditoría Informática y Seguridad Informática. Disponible en https://issuu.com/joseluisalvaradoolivera/docs/auditoriaseguridadinformatica

Partido Comunista de Cuba (2016). Actualización de los Lineamientos de la Política Económica y Social del Partido y la Revolución para el período 2016-2021 aprobados en el 7mo Congreso del Partido en abril de 2016 y por la Asamblea Nacional del Poder Popular en julio de 2016.

Pérez, D. (2006). El sistema de información y los mecanismos de seguridad informática. Disponible en https://dialnet.unirioja.es/descarga/articulo/6121657.pdf el

Ramírez, C. A. (2012). Riesgo tecnológico y su efecto para las organizaciones, parte I. Seguridad cultura de prevención para TI. Disponible en: http://revista.seguridad.unam.mx/sites/revista.seguridad. unam.mx/files/revistas/pdf/Seguridad-Num14.pdf el 13 de marzo de 2017.

Resolución No. 127 /2007 del MIC Reglamento De Seguridad Para Las Tecnologías De La Información. Disponible en: http://www.mincom.gob.cu/sites/default/files/marcoregulatorio/1346872659054_R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf el 17 de diciembre de 2016.

Romero-Moreno, L. M. (2010). La seguridad informática en la seguridad con la plataforma Moodle. En: Revista de Humanidades, No. 17, p. 169 – 190.

Rosado, D. et al. (2014). La Seguridad como una asignatura indispensable para un Ingeniero del Software. Disponible en https://upcommons.upc.edu/bitstream/handle/2099/11778/a25.pdf el 17 de diciembre de 2016.

Solano, O. J., García, D. y Bernal, J. J. (2016). El sistema de información y los mecanismos de seguridad informática en la pyme. En Revista Puntal, Vol. VII (11), pp. 77-98.

Spears, J. L. y Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522.

Viloria, O., Villegas, M. y Blanco, W. (2009). La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional. Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology

(LACCEI'2009). Disponible en http://www.laccei.org/LACCEI2009-Venezuela/p162.pdf el 6 de abril de 2017.

Whitman, M. y Mattord, H. (2012). Principles of information security. Boston, USA: Cengage Learning.