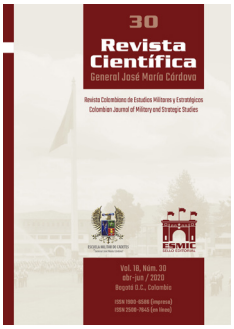

Revista Científica General José María Córdova
(Revista colombiana de estudios militares y estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

Estrategia formativa en defensa digital para adolescentes: experiencia en el Instituto Federal de São Paulo

Felipe Rodrigues Martinez Basile
https://orcid.org/0000-0002-0404-4807
felipe.basile@ifsp.edu.br
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - Campus São Paulo Pirituba, Brasil

Leonardo Juan Ramírez López
https://orcid.org/0000-0002-6473-5685
leonardo.ramirez@unimilitar.edu.co
Universidad Militar Nueva Granada, Colombia

Citación: Basile, F. R. M., & Ramírez López, L. J. (2020). Estrategia formativa en defensa digital para adolescentes: experiencia en el Instituto Federal de São Paulo. *Revista Científica General José María Córdova, 18*(30), 271-287. http://dx.doi.org/10.21830/19006586.579

Publicado en línea: 1.º de abril de 2020

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

ESMIC
SELLO EDITORIAL
Miles Doctus

Revista Científica General José María Córdova
(Revista colombiana de estudios militares y estratégicos)
Bogotá D.C., Colombia

Volumen 18, número 30, abril-junio 2020, pp. 271-287
http://dx.doi.org/10.21830/19006586.579

Estrategia formativa en defensa digital para adolescentes: experiencia en el Instituto Federal de São Paulo

Digital defense training strategy for adolescents: a proposal at the Federal Institute of São Paulo

Felipe Rodrigues Martinez Basile
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - Campus São Paulo Pirituba

Leonardo Juan Ramírez López
Universidad Militar Nueva Granada

Resumen. En una sociedad que se integra a la era de la economía del conocimiento, el aprendizaje en defensa digital para adolescentes es fundamental, en especial para los técnicos de redes informáticas. Este artículo presenta una propuesta formativa desarrollada en el Instituto Federal de São Paulo - Campus São Paulo Pirituba, estructurada en cinco ejes de estudio para la gestión y seguridad de la información, así como los proyectos integradores surgidos en este curso. Participaron 42 estudiantes de educación técnica integrados a la escuela secundaria, quienes presentaron, desde sus intereses personales de indagación, cuatro trabajos sobre temas relacionados con la defensa digital: *malware*, prevención y capacitación, secuestro de datos y ciberacoso. Estos proyectos ponen en práctica los conocimientos aprendidos y su aplicación en investigaciones que forman parte de la educación profesional.

Palabras clave: defensa digital, economía del conocimiento, educación profesional, educación técnica, seguridad de los datos, tecnologías de la información

Abstract. In a society entering the era of the knowledge economy, digital defense learning for adolescents is essential, especially for computer network technicians. This article presents a training proposal conducted at the Pirituba Campus of the Federal Institute of São Paulo and the integrating projects that emerged from this course. The proposal was structured in five information management and security study axes. Forty-two high school students in technical education participated. They presented, from their personal research interests, four works on topics related to digital defense, such as malware, prevention and training, data kidnapping, and cyber-bullying. These projects applied the knowledge obtained and implemented it in the research, which is part of professional education.

Keywords: data security; digital defense; information technologies; knowledge economy; professional education; technical education

Sección: Educación y doctrina • Artículo de investigación científica y tecnológica

Recibido: 5 de enero de 2020 • Aceptado: 18 de marzo de 2020

Contacto: Felipe Rodrigues Martinez Basile ✉ felipe.basile@ifsp.edu.br

Introducción

Educación profesional en el Instituto Federal de São Paulo

Este artículo se propone presentar el proceso de enseñanza y aprendizaje en educación profesional para los técnicos de redes informáticas relacionado con la defensa digital para adolescentes en el Instituto Federal de Educación, Ciencia y Tecnología de São Paulo (IFSP), específicamente en el campus de São Paulo Pirituba (Campus PTB). Allí se está viviendo actualmente un proceso de transformación derivado de la economía del conocimiento, donde la ciencia, la tecnología y la innovación son esenciales para las nuevas carreras laborales.

El campus PTB es parte del plan de expansión de la Red Federal de Educación Profesional y Tecnológica. Se encuentra en la región noroeste del municipio de São Paulo, en el estado de São Paulo, y cubre las regiones de Pirituba, Jaraguá, São Domingos, Freguesia do Ó, Vila Brasilândia, Anhanguera y Perus, que abarcan aproximadamente un millón de habitantes (IFSP-PTB, 2016).

El curso de técnico en redes informáticas del campus PTB está integrado con la escuela secundaria, pero se mantiene en la perspectiva de la educación profesional. Entre sus diversas características, se propone desarrollar habilidades para implementar políticas de seguridad de la información para el acceso a datos y servicios, además de otras acciones relacionadas con la formación profesional de un técnico de redes, que también implica comprender conceptos y reconocer y analizar las normas administrativas relacionadas con los entornos laborales (IFSP-PTB, 2016).

Proyecto integrador

Las estrategias de enseñanza y aprendizaje buscan una visión integral del curso, de modo que los componentes curriculares de la educación básica (portugués, matemáticas, física, química, biología, geografía, historia, filosofía y sociología) confluyan en pro de fortalecer en los estudiantes el desarrollo de amplios conocimientos para el ejercicio de la ciudadanía y la práctica profesional.

El componente curricular del proyecto integrador fomenta la investigación sobre temas actuales que están directamente relacionados con los contenidos de capacitación profesional, de modo que los estudiantes puedan contemplar una mejora en la vida de su comunidad. Entre los temas sugeridos, los más destacados son tecnología e innovación, entornos virtuales, computación en la nube, desarrollo de sitios web de internet, seguridad de red, tecnologías de asistencia, instalación y mantenimiento de servidores para la aplicación web.

De acuerdo con el Proyecto del Plan Pedagógico (PPC), los estudiantes tienen como objetivo desarrollar el trabajo en grupo, con el fin de que puedan demostrar la integración de los componentes curriculares del nivel básico y el nivel profesional. Esto se logra mediante los siguientes contenidos de capacitación profesional (IFSP-PTB, 2016):

- *Informática y* hardware. Comprensión de las características básicas de los microcomputadores actuales; identificación y especificación de los componentes necesarios para ensamblar y configurar microcomputadores, considerando también las nuevas tecnologías de información y comunicación. Instalación de sistemas operativos en microcomputadores y configuración adecuada, siempre observando las características de procesamiento y usabilidad. Además, se tiene en cuenta el aprendizaje necesario para producir documentos comerciales como textos, hojas de cálculo y presentaciones.
- *Redes.* Clasificación de redes informáticas e identificación de qué tipos de dispositivos de red se están implementando en diferentes entornos. Identificación de topologías y tecnologías relacionadas con redes de área local (LAN). Conocer los mecanismos básicos de los protocolos de comunicación en una red informática, además de expresar conocimientos básicos sobre el modelo OSI, TCP/IP, arquitecturas de red, direccionamiento y equipos.
- *Seguridad de información.* Comprensión de los principios básicos de seguridad de la información, como confidencialidad, integridad, confidencialidad e irrevocabilidad. Tener la disposición de utilizar tecnologías de información y comunicación, enfocados en los procesos de gestión y seguridad, y conocer el ciclo de vida de la información en diferentes tipos de entorno. Además de conocer los problemas de cifrado para la transmisión de datos, con la asociación de herramientas que ayudan a este cometido. Esto también incluye la gestión de riesgos y sus etapas, así como el importante papel de las reglas y políticas que pueden desarrollarse para aumentar el nivel de seguridad, al tiempo que se contemplan los aspectos humanos y la ética de seguridad de la información.
- *Lenguaje de programación.* Conocer los fundamentos de la lógica de programación, desde el punto de vista práctico de identificar un problema del mundo real y desarrollar una solución para este. Ello implica conocer la perspectiva del pensamiento computacional en algoritmos, que describe paso a paso cada una de las soluciones, para que el computador pueda seguir estos pasos en el momento de la traducción a un lenguaje de programación específico. En la composición de algoritmos se usan conceptos de memoria, variables y constantes, incluyendo el uso de estructuras de repetición y decisión que son fundamentales para desarrollar una solución computacional.
- *Administración de sistemas operativos.* Capacidad de poner en acción un sistema operativo con énfasis en la manipulación de comandos entre usuario y computador, considerando la instalación, administración y mantenimiento del sistema operativo. Esto se logra mediante experiencias prácticas en entornos informáticos que permiten el uso de filosofía patentada y *software* libre, lo cual ayuda al proceso de aprendizaje y la resolución de problemas para administrar estos sistemas en el mantenimiento del sistema operativo.

- *Lenguaje de programación web.* Ampliar sitios web utilizando lenguajes de programación como Javascript para la interactividad y validar formularios que pueden incorporarse a las zonas web. Además, los elementos creados o transformados en el sitio web también se pueden agregar a otros sitios web existentes, por lo que también es importante utilizar herramientas de edición.
- *Computación en la nube y virtualización.* Crear y administrar ambientes virtualizados para diversos fines, de modo que pueda utilizar la potencia de procesamiento, principalmente en tareas computacionales que se pueden agregar para la oferta de servicios. Este conocimiento permite almacenar datos fuera de la organización, ahorrar en la obtención de *hardware* y *software*, así como tener un entorno para probar la ejecución de sistemas.

Con este conocimiento técnico, asociado con la educación básica (matemáticas, física, química, biología, filosofía, sociología, lengua portuguesa e inglés), el proyecto integrador se convierte en un componente clave del curso técnico de redes informáticas para la profesionalización de los estudiantes.

Marco teórico y conceptual

Hoy en día, el desarrollo de la ciencia y la tecnología está vinculado a la importancia corporativa para resolver problemas y desarrollar innovaciones. Esto resalta la importancia de asociar las ciencias básicas y las aplicadas. Las transformaciones en la sociedad actual se han modelado gracias a la sustitución de procesos electromecánicos por el uso de la tecnología de la información en varias ramas de los procesos de producción. Lo que se ha demostrado en los últimos años es la organización del trabajo centrada en aumentar la productividad y el control de procesos (Ferreti, 2008).

La educación profesional brasileña ha combinado el conocimiento técnico-científico y tecnología de la información para formar un profesional capaz de satisfacer las demandas de la sociedad basada en la economía del conocimiento. De hecho, con la estructuración de la organización escolar, se destacan los métodos de enseñanza, los materiales de enseñanza y los procesos de evaluación del estudiante (Ferreti, 2008). Dentro de la perspectiva de la economía del conocimiento, la palabra clave de *know-how* se evidencia en la dinámica de flujos de datos e información producida por el poder computacional de las redes informáticas, especialmente mediante el uso de algoritmos de inteligencia artificial. Esto cada vez resulta de más ayuda para la toma de decisiones profesional. Pero eso puede traer muchos problemas delicados relacionados con la protección de datos en un mundo conectado y dinámico. La economía del conocimiento ha modificado la estructura del empleo y el trabajo únicamente vinculado a empresas. Este *conocimiento* se está volviendo importante, porque trae nuevas formas de producción a los trabajadores independientes,

que resuelven problemas sin estar vinculados a trabajos en estructuras formales de una empresa (Guruz, 2011; Gandini, 2016).

Abogacía digital para la educación profesional

La seguridad de la información y el desarrollo de estrategias de defensa digital es un tema de gran relevancia y preocupación, dado que se ha evidenciado que pueden ocasionarse daños graves en datos sensibles. Esto ocurre en diferentes sectores de la sociedad, como en el área de la salud, donde la información veraz es esencial para la toma de decisiones clínicas médicas (Basile, 2016, 2019). La ciberseguridad ya es objeto de estudios estratégicos militares y acciones centradas en la seguridad digital destinadas a la eficiencia de las misiones que se llevarán a cabo con robots, programas informáticos y otras tecnologías aplicadas (Espitia et al., 2020).

El caso del nuevo coronavirus ha tenido un efecto devastador, no solo debido a las infecciones fisiológicas, sino también debido a que se ha utilizado para difusión de información de contenido malicioso. En este caso, las computadoras se infectan después de acceder a los enlaces enviados por los atacantes, con la premisa de información que ayuda a prevenir infecciones en entornos del mundo real, a menudo haciéndose pasar por organizaciones de salud (Szafran, 2020). Estas trampas virtuales se producen para obtener datos ilegales, y funcionan debido a la falta de educación en defensa digital entre los millones de usuarios que navegan por la web a diario. En Brasil hay un número creciente de invasiones cibernéticas en dispositivos móviles, principalmente a través de la instalación de aplicaciones (Murdock, 2020).

Las tecnologías de la información se han utilizado ampliamente en los más variados tipos de profesiones para ofrecer servicios, lo que ha aumentado la importancia del estudio de la defensa digital, desde la preparación como ciudadano, pero principalmente cuando existe la necesidad de una educación profesional en la juventud. Estas tecnologías permiten la inserción de nuevas estrategias de enseñanza que involucren a maestros y estudiantes para mejorar los procesos de enseñanza y aprendizaje, centrados en la resolución de problemas (Hermosa, 2015). Así, hay cada vez más desarrollos tecnológicos de apoyo en diferentes áreas, como la salud, la industria, el comercio, pero no hay ninguna preocupación por capacitar a las personas conscientes de sus roles en la llamada economía del conocimiento.

Metodología

La experiencia de enseñar defensa digital para adolescentes se describe en este artículo, haciendo hincapié en el desarrollo del proceso de enseñanza y aprendizaje en 2019. Esta experiencia, inmersa en el laboratorio de computación del campus PTB, se llevó a cabo con 42 estudiantes, entre 14 y 16 años de edad.

Las clases se desarrollaban una vez por semana, con una intensidad de dos horas, para un total de ochenta horas al año. Se realizaron actividades teóricas y prácticas programadas según el plan de acción. Su planificación inicio en febrero y terminó en diciembre del mismo año, considerando el paralelismo de las clases entre el componente obligatorio de la educación básica y los componentes curriculares del área técnica del curso de redes de computadoras.

La gestión y seguridad de la información es el componente elegido en este trabajo para resaltar el proceso de capacitación y la importancia del aprendizaje de habilidades y capacidades para la defensa digital de los adolescentes en la economía del conocimiento. Durante la planificación de este componente, se crearon cinco ejes de estudios que se adaptaron al cronograma de actividades del curso.

Eje 1. Principios de seguridad de la información

Se trabajaron conceptos y definiciones fundamentales para comprender la defensa digital en un contexto en el que observamos la integración entre *hardware*, *software*, entorno y personas. El trípode de seguridad de la información (confidencialidad, integridad y disponibilidad) es lo más destacado de este primer eje. De esta forma, se brinda una explicación de los conceptos, aplicados en diferentes tipos de escenarios del entorno corporativo en el mundo real. Las reflexiones sobre los incidentes actuales y la posterior ruptura del trípode son temas que se discuten semanalmente en clase, de forma que se promueva un pensamiento crítico y libre sobre cuáles serían las actitudes relacionadas con el *conocimiento* para que no haya tal incidente. El ciclo de vida de la información, compuesto por manipulación, almacenamiento, transporte y eliminación (Galvão, 2015), también son temas estudiados en este primer eje. La estructura de la evaluación destaca la actitud profesional al tratar de forma exploratoria los incidentes relacionados con el trípode de seguridad y el análisis de cómo ocurre una violación de seguridad después del análisis del ciclo de vida de la información.

Eje 2. Cifrado y protección perimetral

La comprensión de los algoritmos de cifrado y la necesidad de aumentar el número de barreras a profundidad en la protección del perímetro digital son los temas más recurrentes en el proceso de formación de este eje, para lo cual se trabajan varios elementos de la infraestructura de redes informáticas. Con respecto al aprendizaje de la criptografía, las actividades de laboratorio de computación se centran en el *conocimiento*, desde el uso de algoritmos clásicos asociados con la lógica de programación de Script Bash en GNU/Linux, hasta la visualización de la transmisión de datos en redes. También se trabaja con computadoras que usan claves criptográficas simétricas y asimétricas entre dos puntos en una red local en un entorno aislado, para pruebas de laboratorio. Los grados de secreto se presentan como temas recurrentes en entornos corporativos para el acceso a la informa-

ción en los niveles operativos, tácticos y estratégicos. Además, se lleva a cabo un proyecto de protección del perímetro físico y digital diseñado por los estudiantes, como una evaluación del proceso de aprendizaje del primer y segundo eje.

Eje 3. Informática forense

El pensamiento investigativo que surge de la informática forense se presenta a los estudiantes en escenarios que incluyen el análisis de *hardware*, *software*, entorno y personas. En clase, el profesor analiza los escenarios de solución de incidentes de seguridad de la información, en un intento de construir una narrativa de los hechos que pueda conducir a una mejor visión forense de la información de la computadora, desde el simple juicio de las acciones hasta señalar al culpable de un determinado incidente. Durante la contextualización del tema, semanalmente, se abordan algunos de los casos de filtraciones de datos públicos presentados en los medios, con el objetivo de presentar hechos que representen situaciones que se pueden enfrentar en el entorno corporativo de un trabajo futuro. Los ejercicios de laboratorio abordan la necesidad de establecer estrategias informáticas de investigación forense, asociadas con la recopilación de datos, especialmente en el momento del incidente, para evitar la pérdida de evidencia y señalar las huellas dejadas por los atacantes (Vallim, 2017).

En el proceso se siguen las buenas prácticas de los expertos en seguridad, para que todos los datos recopilados puedan utilizarse para presentar resultados de forma rastreable y siguiendo el principio de mantener evidencia contra posibles cambios (De Santana et al., 2018). Por esta razón, la evaluación del estudiante se hace en *know-how*: el reconocimiento del entorno donde ocurrió el incidente y la recopilación de evidencia, con el examen de esta y de los rastros que pueden analizarse, con el uso de estrategias y herramientas de seguridad.

Eje 4. Normas y reglamento de seguridad de la información

En este eje, los estudiantes comprenden las principales reglas y normas de seguridad de la información que las empresas de tecnología implementan. A partir de este conocimiento aplicado se certifican para trabajar con otras empresas, con la conciencia suficiente acerca de la seguridad. El estudiante debe comprender las recomendaciones ISO/IEC 27000 para la gestión y seguridad de la información en escenarios típicos del entorno empresarial, con énfasis en el manejo del vocabulario de esta norma, analizando las ventajas y desventajas en su aplicación. Luego hay un análisis sobre ISO 27002 —controles de seguridad de la información— e ISO 27005 —gestión de riesgos—, que se puede aplicar en las empresas, incluyendo las instrucciones en el laboratorio de red para crear escenarios donde se puedan utilizar los conceptos aprendidos y discutidos en el aula.

Enfocados en los conceptos principales de la familia ISO 27000, fue posible elaborar con los estudiantes la discusión y propuesta de una política de seguridad de la informa-

ción. Los ejercicios posteriores motivan la creación de una estrategia general con reglas de seguridad de la información, donde las pautas de seguridad para las actividades comerciales son evidentes, considerando un escenario de una clínica médica multiprofesional con diversas especialidades. Dichas políticas deben contemplar temas como el buen uso de la tecnología de la información y comunicación; control de acceso; seguridad de activos, y seguridad que involucra a las personas.

Eje 5. Prevención de incidentes con buenas prácticas digitales

Las buenas prácticas de seguridad de la información se presentan como acciones efectivas para prevenir incidentes durante las rutinas de trabajo en diferentes tipos de sectores. Las investigaciones llevadas a cabo por los estudiantes promueven la adquisición de nuevos conocimientos sobre prácticas realizadas por profesionales especializados en seguridad digital y consultores con certificación en el tema. Los estudiantes se enfrentan al desafío de realizar una lectura juiciosa de los documentos existentes y luego desarrollar ejercicios escritos para crear políticas de seguridad de la información en un entorno corporativo, que pueden variar en este proceso formativo de acuerdo con los incidentes que se presentan en clase semanalmente.

En este proceso de enseñanza y aprendizaje *know-how*, se destaca la estructura de reglas que pueden aplicarse para mejorar la defensa digital de un departamento, una empresa o un lugar de trabajo con pocos trabajadores. En este eje se trabaja en los temas de conciencia y formación tanto para generar oportunidades como para valorar el proceso de educación profesional. Las evaluaciones de aprendizaje se centran en presentar una política de seguridad de la información para un escenario específico de una clínica médica que realiza telemedicina, donde la distancia es un factor relevante para la transmisión de datos y la toma de decisiones en el tratamiento de pacientes.

Los ejercicios consistieron en utilizar conceptos sobre reparación de pérdidas, dentro del tema de incidentes y copias de seguridad, para enfocarse en la continuidad de diversos ejercicios en diferentes escenarios. Los estudiantes discutieron los conceptos de respaldo incremental completo, incremental diferencial y continuo, además de destacar los tipos de respaldo del sitio (frío, cálido, caliente), objetivo de tiempo de recuperación (RTO), objetivo de punto de recuperación (RPO) y reflejo, con el fin de que estos escenarios puedan presentarse en el ejercicio de telemedicina, de modo que se pueda llevar a cabo un plan de recuperación ante desastres y contar con copias de seguridad.

Resultados y discusión

Durante el itinerario formativo de los adolescentes matriculados en el curso técnico sobre redes de computadoras, hay componentes curriculares de la educación básica que son importantes para la formación del estudiante —matemáticas, lengua portuguesa, biología, física, química, geografía, historia, filosofía, sociología y lengua inglesa— y que propor-

cionan los fundamentos para la interpretación de fenómenos, aspectos de lenguaje como la comprensión de textos y de la realidad humana, que tendrán una relación directa con el mundo del trabajo.

Los componentes curriculares de la formación profesional se distribuyen en un periodo de tres años, como curso técnico en redes de computadoras, que contempla, entre otros temas, introducción a la tecnología de la información y el *hardware*; teleprocesamiento; introducción a la base de datos; diseño de red de computadoras; lenguajes de programación; gestión y seguridad de la información; computación en la nube; infraestructura de red; gestión de redes informáticas; redes inalámbricas, y programación web. Por su parte, el proyecto integrador de los componentes de educación básica y técnica tiene lugar durante dos años, y se considera como el momento más importante de enseñanza y aprendizaje de todo el proceso, dado que implica la integración y preparación de la educación profesional durante este itinerario formativo como técnico de red de computadoras.

Dirección de trabajos integradores

En 2019, los trabajos integrales para estudiantes que asisten al segundo año del curso de red técnica integrada en la escuela secundaria tuvieron como maestros a Felipe Rodrigues Martinez Basile y Ester Kolling Rodrigues. El calendario establecido siguió el plan pedagógico con clases expositivas; prácticas de laboratorio; análisis de situaciones problemáticas para comprender y desarrollar los temas elegidos por los estudiantes, además de la perspectiva de crear informes con el libro de registro; investigación en la web; referencias bibliográficas, datos, documentos, y seminarios que deben presentar periódicamente. Durante el periodo de febrero a diciembre, los maestros organizaron una dinámica de clases semanales con un componente curricular del proyecto integrador, lo que permitió a los estudiantes elegir temas libres. Asimismo, guiaron la comunicación de los estudiantes con otros maestros que pudieran ser consejeros y, en consecuencia, coasesores, con su adhesión a los temas a trabajar durante el año.

Uno de los puntos fundamentales para el desarrollo del trabajo fue el uso de laboratorios de cómputo para llevar a cabo prácticas. Bajo la guía de los docentes, quienes proporcionaron la metodología de investigación y guiaron la realización del proyecto, el proceso de enseñanza y aprendizaje se caracterizó por la producción de documentos, hojas de cálculo e información fundamental para la composición de artefactos que probaron cada etapa del trabajo integrador. Otro aspecto destacado fue la participación de los docentes de educación básica y profesional que contribuyeron en la orientación para cada uno de los trabajos descritos. Para cada trabajo desarrollado, los estudiantes contaron con dos docentes: uno en el área de educación básica y otro en el área técnica, enfocada en desarrollo de ciencia y tecnología con aspectos de innovación.

Los siguientes resultados son el trabajo de los ejes del componente de gestión de información y seguridad, y muestran un formato de proyecto integrador. En estos ejes participaron 42 estudiantes, y 25 tomaron aspectos de su trabajo físico del componente de proyecto integrador. A continuación, se presentan los resultados del trabajo de los estudiantes:

Estudio de la anatomía del malware *como el* spyware

En este trabajo, los estudiantes destacan las amenazas cibernéticas que acceden a diferentes ambientes y que no se pueden evitar, para la defensa digital de sus activos. Realizan un estudio de analogía entre el ciclo de vida de un virus fisiológico que infecta a los humanos y el virus que infecta a las computadoras a través de las tecnologías de la información y la comunicación. Con la comprensión de la estructura interna de estos *malware* fue posible desarrollar variables desde un *keylogger* para capturar datos en una computadora local, con énfasis en la recopilación de datos proporcionados durante el acceso a la web utilizando el navegador. La ingeniería social se estudió para crear escenarios reales de contaminación a los cuales pueden acceder fácilmente los usuarios comunes y avanzados, lo que demuestra que el simple hecho de acceder a la web conectada a internet puede causar un incidente de seguridad de la información. Los estudiantes también consideraron estudios sobre protección del perímetro digital y encriptación en este trabajo.

Aplicación educativa de defensa digital para incidentes cibernéticos

Los estudiantes desarrollaron un método lúdico de capacitación para la educación en defensa digital frente a incidentes cibernéticos, teniendo en cuenta que actualmente hay muchos delitos cibernéticos que pueden afectar a los empleados de empresas de todo el mundo. La aplicación móvil tiene como objetivo crear una interacción con el usuario de la aplicación mediante ilustraciones animadas e interactivas de situaciones de incidentes. Esta interacción humano-computadora tiene como objetivo promover la conciencia y la capacitación para cada uno de los incidentes que se pueden presentar. Inicialmente, los estudiantes trabajaron con *ransomware*. Una diferencia importante del trabajo es la caracterización de un entorno que es muy propicio para el desarrollo de incidentes en dispositivos móviles, incluso más que la gran parte de los usuarios de *home banking* que instalan aplicaciones y acceden a sitios web sin certificados de forma predominante en su tiempo de navegación.

Ciberataques en sistemas financieros: los riesgos de ransomware

Los ataques cibernéticos en los sistemas financieros fueron parte del alcance de este trabajo, destacando la presencia de *ransomware* como un factor importante en el secuestro de datos en computadoras que utilizan transacciones financieras electrónicas. En este trabajo, los estudiantes resaltan que la rutina de acceso a la banca en el hogar ha sido explorada

por atacantes que ya tienen acceso a las computadoras a través de una serie de trampas preparadas por ellos mismos. Los estudiantes también mapean el comercio electrónico como otro entorno de gran amenaza, y muestran que dicha práctica de recopilación de datos y su posterior secuestro ha crecido con los años. Los estudiantes trabajaron sobre una variante del virus *ransomware* e intentaron simular paso a paso desde su infección hasta la situación en la que hay un mensaje de advertencia sobre el secuestro de datos.

Consecuencias psicosociales del ciberacoso en jóvenes y adolescentes

El uso de tecnologías de información y comunicación está transformando el acoso escolar en una variante llamada ciberacoso, por lo cual los estudiantes se interesaron en comprender cómo se produce esta modalidad cibernética. Su preocupación subraya la necesidad de capacitación y conciencia de la sociedad sobre estos hechos serios, que pueden acortar la vida de los jóvenes y adolescentes de acuerdo con la repercusión de la información en el mundo digital y también en el mundo físico en el que viven. En este trabajo, los estudiantes destacan las buenas prácticas y acciones en un entorno digital que ayudan a no promover este tipo de actitud hacia los demás, con acciones preventivas contra cualquier agresión llevada a cabo en el mundo virtual que pueda perpetuarse en el ciberespacio. Se creó un folleto en formato de cómic para sensibilizar a los usuarios sobre las consecuencias psicosociales del acoso cibernético en adolescentes y jóvenes.

Control de acceso biométrico utilizando dispositivos IOT

Actualmente, el mundo físico se ha convertido en un componente cada vez más presente en el acceso a entornos tecnológicos de información y comunicación, de ahí la importancia creciente de los dispositivos caracterizados como IOT (internet de las cosas). Durante esta investigación del tema de defensa digital, los estudiantes experimentaron la autenticación y la irrevocabilidad como características importantes para el registro de perfiles digitales. Como fruto de su aprendizaje, los estudiantes pudieron comprender que la impresión digital, conocida como uno de los tipos de biometría, tiene como punto fundamental la lectura fácil y la individualidad. Por lo tanto, los estudiantes aprendieron cómo usar la autenticación por función biométrica en un sistema de control de acceso simulado. En este trabajo de investigación, los estudiantes asociaron conocimientos informáticos y de *hardware* (a partir de la adquisición, configuración y uso de dispositivos Raspberry), así como conocimientos de administración de sistemas operativos (realización de la instalación y configuración de la distribución GNU/Linux, que proporcionó un entorno de *software* gratis —Raspbian—).

Hay un ambiente informático de placa única para crear un ambiente de control de acceso simulado. Los estudiantes compraron un lector biométrico para recopilar datos de prueba a conexiones con el dispositivo IOT. Con esto, profundizaron los estudios sobre la anatomía y la fisiología de las huellas dactilares del ser humano, y al mismo tiempo

entendieron, a través del desarrollo de este prototipo, que las tecnologías de información y comunicación pueden contribuir a una fácil recopilación de datos, debido a los detalles individuales de las imperfecciones digitales. Todo esto con el fin de promover mayor seguridad de la información y, en consecuencia, ayudar a las empresas y equipos a mitigar amenazas e incidentes.

Desarrollo de juegos educativos: el viaje al conocimiento

Los adolescentes y los jóvenes utilizan actualmente juegos de computadora para el ocio y el entretenimiento, lo que brinda una perspectiva de uso de estos recursos para el aprendizaje escolar. En este sentido, los estudiantes desarrollaron un juego educativo que tiene un guion interactivo, a la vez que permite responder preguntas sobre algunos componentes curriculares específicos. El tema de la defensa digital se abordó una vez más en este tipo de trabajo, con interactividad y la creación de un guion lúdico, que puede proporcionar a través de la inmersión una mayor retención del conocimiento a lo largo de las fases.

En el guion desarrollado por los estudiantes se establecen tres fases, dedicadas a representar respectivamente los siguientes tres temas: geografía de la educación básica; lenguajes de programación, y gestión de la seguridad de la información como parte de la educación profesional. La tercera fase, elaborada por los estudiantes, aborda aspectos de la defensa digital considerando el aprendizaje obtenido a través de la gestión de componentes curriculares y la seguridad de la información. Para ello se destacaron escenarios de juego: una ciudad inteligente con personajes modelo 2D, donde se caracterizaron los enemigos por cámaras de vigilancia y *malware* clasificado como virus que forman parte de una ciudad tecnológica. Otros detalles importantes del modelado y la creación del guion destacaron características de la protección del perímetro digital, como la existencia de paredes para reflejar las llamadas barreras de nivel o alambres de púas en las paredes que representan obstáculos.

Integración entre componentes curriculares

Durante el desarrollo de los trabajos integradores, los estudiantes se reunieron semanalmente con los maestros de orientación del componente del proyecto integrador y mantuvieron reuniones periódicas con los maestros elegidos. Este proceso de iteración y aumento en los artefactos de investigación contribuyó para que el trabajo pudiera integrarse cada vez más con el conocimiento de la educación básica y profesional. Al observar cuidadosamente cada uno de los trabajos en los aspectos más destacados, es posible resaltar lo siguiente:

- *Estudio de anatomía del* malware *como* spyware*:* La integración del conocimiento de las ciencias biológicas a través del estudio de la anatomía del virus biológico asocia sus características del ciclo de vida con características digitales que conforman diferentes tipos de entornos de infección en el mundo digital. Este

trabajo destaca la propagación del virus digital y observa que este puede tener consecuencias desastrosas para mantener la defensa digital de las empresas a nivel mundial.

- *Aplicación de la defensa digital para incidentes cibernéticos:* La integración de elementos importantes del componente curricular de arte para combinar colores y tipos de presentación del diseño computacional contribuye a la producción de interacción humano-computadora. Así, la escritura de guiones, la aplicación educativa y la defensa digital pasan por la capacitación y conciencia en *know-how* para el entorno corporativo, sea cual sea el sector de trabajo.
- *Ciberataques en el sistema financiero y los riesgos de* ransomware*:* Se da la integración entre conceptos e investigación sobre la geografía de los sistemas financieros en el mundo, mapeando en diferentes regiones los tipos de ciberataques que han tenido consecuencias catastróficas con la aparición de *ransomware*. Se reconoce la importancia de comprender el funcionamiento del *malware*, caracterizado por la identificación de la estructura de programación, mediante la asociación de la lectura mejorada de las versiones de los códigos, que se basan en clases de lenguaje de programación, y la visión misma con que los bancos y otras instituciones deben alinearse y sensibilizarse en defensa digital
- *Consecuencias psicosociales para los jóvenes y adolescentes:* La integración de conceptos sociológicos que abordan aspectos de la experiencia, la ética y las relaciones sociales evidencia la transformación del acoso escolar en ciberacoso, lo que demuestra la importancia de comprender los procesos de transformación social a través del uso intensivo de nuevas tecnologías de información y comunicación. La producción de un folleto de concientización refuerza el mensaje acerca de la información, concientización y capacitación, que se discutió en el aula dentro del componente curricular de la gestión y seguridad de la información.
- *Control de acceso por biometría utilizando dispositivos IOT:* Se integró el conocimiento de las ciencias biológicas para el estudio de la biometría en el aspecto anatómico y fisiológico, asociado a las áreas de lectura digital a través de dispositivos, que se estudiaron en el componente de introducción a la informática y el *hardware*. Asimismo, se detallaron los pasos de montaje y configuración de dispositivos IOT, que demostraron conocimiento en *hardware* y administración de sistemas operativos. La presentación del prototipo de sistema de control de acceso proporcionó una visión de la importancia de la biometría digital en la vida de las personas en diferentes entornos.
- *Desarrollo de un juego educativo:* El proceso integró el conocimiento del área de arte con la composición de personajes a través del modelado 2D combinando colores, texturas, tamaño y secuencias de comandos de las fases del juego. También se dio la integración de componentes curriculares con preguntas y respuestas sobre geografía, lenguajes de programación, gestión de la informa-

ción y seguridad, para que la interactividad del juego permitiera observar problemas matemáticos y físicos a través del movimiento de los personajes, así como los personajes caracterizados como enemigos. Esto se convirtió en un verdadero viaje a través del conocimiento, con elementos significativos para aprender defensa digital. El juego educativo en formato de aplicación utiliza la misma perspectiva adoptada con entornos simulados, como los de la guerra militar (Garay & Reyes, 2012), en los que la simulación de ciertos escenarios puede brindar lecciones importantes para los usuarios frente a situaciones del mundo real.

Evaluación de la integración de obras con contenidos de defensa digital

Al final del plan de estudios del proyecto integrador, se realizó la evaluación de estos trabajos de integración de los grupos de estudiantes de acuerdo con el PPC del curso técnico, según lo dispuesto en la Resolución IFSP n.º 859 del 7 de mayo de 2013. Para ello, se requirió la preparación de un informe final de los detalles del desarrollo de las obras que contienen los modos de ejecución (IFSP-PTB, 2016). Con la finalidad de difundir algunos de los trabajos integradores en la comunidad, especialmente aquellos que se ocupan de la defensa digital, se eligió como ocasión la Semana Nacional de Ciencia y Tecnología (SNCT) entre el 21 y el 26 de octubre de 2019.

Las presentaciones de los estudiantes durante la SNCT se realizaron a través de la creación, elaboración e impresión de los contenidos en formato póster, enfatizando los detalles de las etapas del proyecto llevado a cabo durante el 2019. En este sentido, hubo una evaluación por parte de los docentes del área y de aquellos que formaron parte del componente curricular, del proyecto integrador y asesores, así como una evaluación propedéutica (que representó el 40 % de la calificación final del cuarto bimestre).

Se solicitó elaborar el informe final (con modelo de informe adaptado) para componer la calificación final del trabajo integrador, de modo que se pudiera contemplar la verificación del proceso de enseñanza y aprendizaje en cuanto a las etapas de planificación y también sus modos de ejecución de trabajo. Asimismo, se pudieron valorar las prácticas profesionales de desarrollo técnico y el contenido de información (recopilación de datos e investigación realizada). Con esto, el informe final se caracteriza por la expresión de la producción académica y técnico-científica (que representa el 60 % de la calificación final del cuarto trimestre).

Los estudiantes tenían a mano el modelo de redacción del informe final, donde hay una descripción de los ítems de evaluación junto con las características solicitadas en las prácticas de evaluación escrita, constituidas fundamentalmente por la preparación del informe final y la presentación a la comunidad en la SNCT. Esto permitió integrar los conocimientos de educación básica (en particular, de ciencias humanas, idiomas, ciencias naturales y matemáticas) con el *know-how* de competencias y habilidades que se desarro-

llaron durante el segundo año de formación del curso. Con esto, el curso en el campus PTB se centró en temas actuales de relevancia para la formación de un profesional atento a la importancia de la defensa digital en su currículum laboral.

Conclusión

La educación profesional de un técnico de redes informáticas en la economía del conocimiento aporta fortalezas para el *know-how* en el espectro de la defensa digital. El componente curricular de la gestión y la seguridad de la información actualmente es esencial para la formación básica de los ciudadanos, pero lo es especialmente en la educación profesional, donde es necesario mantener un ciclo de vida con la información de los activos de una empresa protegida, en confidencialidad, integridad y disponibilidad, en cualquier sector de la economía. Debe mantenerse asegurado el perímetro físico y digital de esta información. Los trabajos desarrollados después del proceso de la enseñanza de la defensa digital se presentaron en un componente curricular de proyecto integrador, en el cual los estudiantes demostraron el deseo de mejorar y utilizar sus conocimientos en un futuro empleo en el mercado laboral.

Agradecimientos

Los autores agradecen el apoyo brindado por las instituciones que trabajan en proporcionar a los estudiantes oportunidades de desarrollo en la educación profesional, especialmente al Instituto Federal de Educación, Ciencia y Tecnología de São Paulo - Campus São Paulo Pirituba, por facilitar la infraestructura para este proyecto. También a la Universidad Militar Nueva Granada por su apoyo en la celebración de reuniones en línea entre Brasil y Colombia. Un especial agradecimiento a los maestros Alex Sandro Rodrígues Ancioto, Danilo Marcondes de Alcântara, Joyce Martins Mendes, Ivan Miletovic Mozol y Renato Montanher, quienes guiaron y coguiaron los trabajos integradores, y apoyaron con su conocimiento el desarrollo de los artefactos producidos por los estudiantes. Asimismo, un reconocimiento al importante y significativo trabajo del profesor Ester Kolling Rodrigues para guiar la elaboración y producción de diarios, trabajos escritos e informes finales entregados de acuerdo con el cronograma de ejecución.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre los autores

Felipe Rodrigues Martinez Basile es ingeniero en sistemas de información, magíster y doctor en ingeniería biomédica de la Universidad de Mogi das Cruzes. Es especialista en seguridad de la información. Es profesor e investigador en arquitectura de redes informáticas en el IFSP - Campus PTB. Realiza investigaciones multicéntricas sobre seguridad de la información en Suramérica.
https://orcid.org/0000-0002-0404-4807 - Contacto: felipe.basile@ifsp.edu.br

Leonardo Juan Ramírez López es ingeniero electrónico y especialista en instrumentación electrónica, magíster en ingeniería de sistemas de la Universidad Nacional de Colombia y doctor en ingeniería biomédica de la Universidad de Mogi das Cruzes de São Paulo (Brasil). Profesor e investigador senior de la Universidad Militar Nueva Granada, Bogotá, Colombia.
https://orcid.org/0000-0002-6473-5685 - Contacto: leonardo.ramirez@unimilitar.edu.co

Referencias

Basile, F. R., López, L. J., & Amate, F. C. (2019). Método para realizar copias de seguridad de imágenes médicas basado en tareas automatizadas. *JINT. Journal of Industrial Neo-Technologies, 6*(1), 26-33.

Basile, F. R., Thomé, M., Amate, F. C., Rodrigues, R., Bastos, S., & Goroso, D. G. (2016). Segurança de transferência de dados em Telessaúde e Telemedicina. En *Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética* (pp. 279-298). Instituto de Saúde.

De Santana, K. G., De Oliveira, P. R., & Ramos, D. S. (2018). Perícia cibernética: A evolução do trabalho científico pericial informatizado ante aos desafios tecnológicos de ataques virtuais nos sistemas de segurança. *Dat@ Venia, 9*(1), 101-111. http://dx.doi.org/10.20887/rdtv.ccj.2017.V9i1p101-111

Espitia C., A., Agudelo C., J., & Buitrago S., Ó. (2020). Innovaciones tecnológicas en las fuerzas militares de los países del mundo. *Revista Científica General José María Córdova, 18*(29), 213-235. https://doi.org/10.21830/19006586.537

Ferretti, C. J. (2008). Sociedade do conhecimento e educação profissional de nível técnico no Brasil. *Cadernos de Pesquisa, 38*(135), 637-656. https://doi.org/10.1590/S0100-15742008000300005

Galvão, M. D. C. (2015). *Fundamentos em segurança da informação*. Pearson.

Gandini, A. (2016). Digital work: Self-branding and social capital in the freelance knowledge economy. *Marketing Theory, 16*(1), 123-141. https://doi.org/10.1177/1470593115607942

Garay A., C. P., & Reyes G., D. (2012). Juegos de simulación como método de defensa en la guerra. *Revista Científica General José María Córdova, 10*(10), 237-255. https://doi.org/10.21830/19006586.236

Guruz, K. (2011). *Higher education and international student mobility in the global knowledge economy* (revised and updated 2nd ed.). Suny Press.

Hermosa del V., P. (2015). Influencia de las tecnologías de información y comunicación (TIC) en el proceso enseñanza-aprendizaje: una mejora de las competencias digitales. *Revista Científica General José María Córdova, 13*(16), 121-132. https://doi.org/10.21830/19006586.34

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - Campus São Paulo Pirituba (2016, Outubro). Projeto pedagógico do curso técnico em redes de computadores integrado ao ensino médio. https://bit.ly/39JHNiM

Murdock, J. (2020, February 5). Malware poising as new corona virus information spreads online, exploiting fears about global outbreak. https://bit.ly/2Q3n4Pm

Szafran, V. (2020, Janeiro 30). *Brasil teve 23 milhões de celulares infectados por malwares em 2019*. Olhar Digital. https://bit.ly/38CaRYd

Vallim, A. P. (2017). *Forense computacional e criptografia*. Senac São Paulo.