MAESTRO y SOCIEDAD e-ISSN 1815-4867

Volumen 20 Número 2 Año 2023
Artículo original

La formación para el manejo seguro de las TIC desde la relación universidad-empresa

The formation for the safe management of ICT from the university-company relationship

MSc. Rubén Font-Hernández*, https://orcid.org/0000-0002-1136-3646
Yoan Silveira-Escalante, https://orcid.org/0000-0002-5370-1121

Universidad de Oriente, Santiago de Cuba, Cuba

*Autor para la correspondencia. email: ruben@uo.edu.cu

Para citar este artículo: Font Hernández, R. y Silveira Escalante, Y. (2023). La formación para el manejo seguro de las TIC desde la relación universidad-empresa. *Maestro y Sociedad*, 20(2), 447-457. https://maestroysociedad.uo.edu.cu

RESUMEN

Introducción: La irrupción de las TIC en los procesos socioproductivos requiere de un capital humano cuyas competencias se desarrollan para fomentar un modo de actuación proactivo ante los aportes de las TIC. Materiales y métodos: Este proceso es concebido a través del aporte bilateral de la relación universidad empresa, sustentado en una propuesta de alternativa de plan de acción que haga posible la tenencia de buenas prácticas en el manejo seguro de dichas tecnologías por el capital humano vinculado al sector empresarial que centró el objetivo trazado en la investigación que se amparó en la dialéctica materialista utilizando de manera especial el análisis y la síntesis, la inducción y la deducción y la unidad de lo lógico y lo histórico. Resultados: Los procesos que hacen posible la preparación del capital humano en función de las buenas prácticas en el manejo de las TIC, convergen en el desarrollo de la competencia básica en infocomunicaciones y de un modo de actuación proactivo ante los aportes de las TIC. Discusión: Las fortalezas del sector empresarial ante la posibilidad de incidente poseen una relación directa con el desarrollo de la competencia básica en infocomunicaciones y el modo de actuación proactiva de su capital humano para manejar de forma segura las TIC en cualquier ámbito. Conclusiones: El crecimiento en la preparación del capital humano desde un proceso formativo en torno al manejo seguro de las TIC desde el vínculo bilateral universidad empresa contribuirá a la mayor eficiencia de los procesos socioproductivos y de formación en la universidad, a partir de la atención a las necesidades de la producción y los servicios en las áreas demandadas, sin perder de vista que la formación del egresado se encamina a una actuación que le permita solucionar situaciones que pueden no estar predeterminadas.

Palabras clave: TIC, competencia básica en infocomunicaciones, capital humano, relación universidad empresa.

ABSTRACT

Introduction: The irruption of ICT in socio-productive processes requires human capital whose skills are developed to promote a proactive mode of action before the contributions of ICT. Materials and methods: This process is conceived through the bilateral contribution of the university-business relationship, supported by a proposal for an alternative action plan that makes possible the possession of good practices in the safe management of said technologies by the human capital linked to the business sector that focused the objective outlined in the investigation that was protected in the materialist dialectic using in a special way the analysis and synthesis, induction and deduction and the unity of the logical and the historical. Results: The processes that make possible the preparation of human capital based on good practices in the management of ICTs, converge in the development of basic competence in infocommunications and a proactive mode of action before the contributions of ICTs. Discussion: The strengths of the business sector in the face of the possibility of an incident have a direct relationship with the development of basic competence in infocommunications and the proactive mode of action of its human capital to safely manage ICT in any field. Conclusions: The growth in the preparation of human capital from a training process around the safe management of ICT from the university-business bilateral link will contribute to the greater efficiency of the socio-productive and training processes in the university, based on the attention to the needs of production and services in the demanded

areas, without losing sight of the fact that the training of the graduate is directed towards an action that allows him to solve situations that may not be predetermined.
Keywords: ICT, basic competence in infocommunications, human capital, university-business relationship.

Recibido: 11/6/2022 Aprobado: 25/10/2022

Introducción

La irrupción de las tecnologías de la información y las comunicaciones (TIC) en la vida social, no excluye a las ciencias de la educación, donde con mucha fuerza ha penetrado en la esfera de la administración y gerencia, en el propio acto de enseñar, y de manera muy especial, en el tratamiento y manejo de la información. Por ello se requiere de un capital humano que pueda operar de manera segura estas tecnologías. El problema no es exclusivo del sector de la educación, pues el impacto de las TIC en la vida social ha dejado su impronta.

La formación en torno a estas tecnologías se ha centrado en enseñar como operar con ellas, soslayando un factor, que se hizo más notorio a partir de los años 90 y ha venido escalando posiciones de importancia entre las materias dentro de las TIC, por el crecimiento de los incidentes relacionados con ella: la seguridad.

A finales de la centuria vigésima, con la tendencia mundial de atender los problemas relacionados con la ciberseguridad en torno al manejo de las TIC se convierte en necesidad la formación con una visión más amplia del capital humano. Esta óptica no solo incluye el conocimiento de determinado software o la operación de un ordenador, sino que también pueda hacerse cualquier operación con estos medios de manera segura, mostrando horizontes cada vez más amplios al desarrollo del hombre común que interactúa con estas tecnologías.

Para el estudio del tema se han tomado en consideración informaciones aparecidas en la prensa digital cubana así como materiales en torno a la formación por competencias considerados vitales como los de Elliot (1993), Bunk (1994) y Forgas (2005) y en lo referido al papel del capital humano en el manejo seguro de las TIC se valoraron los aportes de Mendoza (2016), Foltyn (2017), Herán (2019), Iglesias (2019), Owaida (2021) y Juanes (2021), entre otros.

Tomando en consideración las debilidades que afloran en los estudios que se realizan a escala planetaria, que muestran al factor humano como el responsable de una gran cantidad de incidentes de la seguridad informática y que se hace más notoria en el sector empresarial, se impuso la necesidad de buscar soluciones al problema de cómo contribuir a la formación del capital humano en el sector empresarial desde la relación universidad empresa, siendo este un nexo cuyo fomento solidificaría no solo el proceso productivo, sino la atención a los procesos formativos sustentados desde las necesidades empresariales.

Esto condicionó que se trazara como objetivo la elaboración de un plan de acción para el fomento de las buenas prácticas en el manejo seguro de las TIC en el capital humano a través de la relación bilateral universidad empresa.

Materiales y métodos

Entre los métodos teóricos se utilizaron el análisis y síntesis para arribar a la definición de los unidades iniciales a desarrollar de la competencia básica en infocomunicaciones, al desarrollar la descomposición de las partes del proceso investigado y la obtención de elementos sintetizados y generalizadores para su utilización en el plan de acción y su utilización posterior en el proceso de formación.

La unidad de lo lógico y lo histórico, como parte de la dialéctica materialista en el proceso de búsqueda y ordenamiento desde lo histórico y lo lógico de los procesos vinculados a la definición de las unidades de la competencia básica en infocomunicaciones en el área de seguridad informática y la definición de los antecedentes y la lógica de la investigación. El método de inducción–deducción fue utilizado en la confección del plan de acción a partir de las necesidades de solución adecuadas para cumplir el objetivo.

En el ámbito de lo empírico se utilizó el análisis bibliográfico que propició el estudio de los estándares para las buenas prácticas y los informes de las herramientas para detección de vulnerabilidades que permitan la concepción que sustente la propuesta de plan de acción que ofrece.

Resultados

La aparición de internet en Cuba de manera masiva se produjo con la ampliación de la telefonía móvil y la apertura del mercado de esta a través de las salas de navegación. En Cubadebate esto quedó reflejado de la siguiente manera:

Para mucho usuarios el camino hacia Internet no ha sido tarea fácil, sobre todo, cuando la senda comienza en nuestro país. El primer viaje "masivo" hacia la red de redes ocurrió en 2013, con las salas de navegación para personas naturales (...) Mas, no fue hasta 2015 que se hizo notar la presencia criolla en Internet, con la llegada de la WiFi a diversos territorios del país (Figueredo, 2019).

Un informe presentado por el Ministerio de Comunicaciones de Cuba exponía: "De los 5 millones de personas que acceden a servicios de Internet, el 60 por ciento lo hace desde sus puestos de trabajo y de estudios (…) lo hacen de manera gratuita y lo paga el presupuesto del Estado de esas instituciones" (Cuba. MINCON, s.a.) cuestión esta que incrementa aún más la cifra de personas que acceden a la red de redes.

Esta apertura se amplió mucho más con el servicio Nauta Hogar que en 2017 abrió las puertas a 124 mil nuevos usuarios y ha seguido creciendo. Posteriormente el servicio de internet por datos en los teléfonos móviles, cuyo volumen de servicios con acceso, en diciembre de 2019, sumaba los 3,7 millones, para crecer mucho más en los años siguiente al sobrepasar los 6 millones de líneas de las que acceden a internet regularmente más de 4 millones, según datos aportado por Empresa de Telecomunicaciones de Cuba (ETECSA) en agosto de 2020 (Radio Metropolitana, 2020).

En el mes de diciembre de 2020 ETECSA brindaba el dato de que ya existían en el país 6 millones 300 mil líneas móviles activas y añadía: "Desde febrero a la fecha, el tráfico de datos de internet en Cuba se ha triplicado. Si en el segundo mes del año se consumían 14 Gbps hoy se necesitan 42 Gbps" (Radio Santa Cruz, 2020).

Sin embargo, esta apertura no se hizo acompañar de un incremento de la preparación de las personas para enfrentar la aventura de adentrarse en la red de redes. Si se revisan los planes de estudio y programas de la educación en general se encontrará que se presta atención a desarrollar conocimientos sobre sistemas operativos y ofimática y el tema de la seguridad informática se circunscribe a un breve bosquejo de la existencia de los "virus" informáticos, aunque los contenidos que se proponen, se consideran escasos, para contribuir al desarrollo de una posición preventiva ante esta problemática, por ello, se puede afirmar que no se brinden las herramientas necesarias para el manejo seguro las TIC.

Es común desde la década del 90 de la pasada centuria, el desarrollo de posiciones proactivas para el manejo de las TIC y por ello para la prevención de los incidentes se ha tornado un imperativo la tenencia por quienes utilizan estas tecnologías en el ámbito laboral y social de competencias que les permitan sortear los escollos que encaran en estas acciones. Esto permite demostrar la necesidad de la formación en el capital humano de la competencia básica en infocomunicaciones desde la relación de la universidad empresa como un imperativo para el manejo seguro de las TIC.

En el ámbito empresarial es común que no se reporten los incidentes resultantes de las carencias formativas del personal relacionado con el uso de las TIC, sin embargo, empresas dedicadas a nivel internacional a la ciberseguridad, como ESET (Heran, 2019), han publicado en sus informes anuales sobre tendencias y en diversos artículos que un porcentaje muy alto de los incidentes de seguridad que ocurren son resultado de malas prácticas o deficiencias formativas en el capital humano, que no actúan adecuadamente ante los códigos malignos, no aplican parches de seguridad, son presas fáciles de las trampas de la ingenierías social y junto a ello de la suplantación de identidad, errores en las configuraciones de seguridad de sistemas y servicios, uso de credenciales en lugares públicos que carecen de condiciones elementales de seguridad, entre muchas otras. (Foltyn, 2017)

Es común a escala planetaria que el tratamiento a estos aspectos se realice desde la óptica de las competencias profesionales, descartando el hecho de que las TIC ha impactado todas las esferas de la vida y por ende, las actividades que realiza el hombre fuera de la producción y los servicios, también implican la tenencia de conocimientos, habilidades y valores que son puestos en acción para obtener algún resultado. Una muestra de la afirmación anterior, son las definiciones de competencias profesionales brindadas por autores entre los que se destacan Elliot (1993), Bunk (1994) y Forgas (2005). El primero de ellos refiere:

> *considerar que el conocimiento, la comprensión de la situación, el discernimiento, la discriminación y*

la acción inteligente subyacen en la actuación y en la competencia; en otras palabras, la competencia supone transferencia, respuesta a situaciones nuevas, valores humanos puestos en práctica, conocimiento técnico inteligente y desarrollo de habilidades que sustentan su logro (Elliot, 1993, p. 26).

En esta definición se escurren dos términos que muestran su relación con lo profesional, entre ellos se destacan transferencia y conocimiento técnico. En el caso de las definiciones de Bunk (1994, pp. 8-9) y Forgas Brioso, el término está claramente expuesto.

Para Forgas Brioso, las competencias profesionales son "el resultado de la integración, esencial y generalizada de un complejo conjunto de conocimientos, habilidades y valores profesionales que se manifiestan a través del desempeño profesional eficiente en la solución de problemas de su profesión, pudiendo incluso resolver aquellos no predeterminados" (Forgas, 2015, p. 15). Se adopta la definición del Dr. Forgas Brioso por estar relacionada con las realidades formativas de Cuba y es aplicable, en su concepción general, a las pretensiones de la propuesta que se desarrolla.

El impacto de las TIC en todas las esferas de la vida representa un reto para todos: la posesión de competencias para la interacción con dichas tecnologías, porque de carecer de la preparación no se podrá obtener lo se requiere de las actividades y servicios esenciales de la vida moderna, considerándose un imperativo poseer competencias para el desempeño eficiente con las TIC en cualquier área de la vida social, lo que las convierte en parte del núcleo básico de ellas en todos los individuos con independencia de su relación con los procesos socio-productivos.

En el ámbito de lo formativo la preparación de los individuos se desarrolla de diversas maneras, pero siempre se toman en cuenta conocimientos, habilidades y valores. Por ello, sin importar si se define la formación desde objetivos o por competencias, la tríada antes mencionada será siempre un acicate para quienes tienen la tarea de educar, pues el fin nunca quedará circunscrito al área del conocimiento como demostró Forgas (2005: 16-18).

El manejo de las TIC en cualquier esfera es una realidad, todos los individuos, con independencia de su quehacer profesional, deben poseer conocimientos, habilidades y valores en el manejo de las TIC, de las que una parte, son básicas para su desenvolvimiento en el ámbito social. Visto desde la óptica de las competencias, lo que se llamó inicialmente "competencia básica informática" por el vínculo directo que presentaban las TIC y la informática, evolucionó con el avance vertiginoso de estas tecnologías hasta crear un complejo entramado, en el que la información se crea o se modifica desde medios diversos, que incluyen los teléfonos inteligentes y móviles, que contribuyen a la gestión de la información y las comunicaciones desde diversas tecnologías. Por tal motivo se ha considerado conveniente nombrar este "sector" de las competencias como básica en infocomunicaciones, por ser este último término más abarcador y apropiado en las nuevas condiciones.

Se considera que la competencia básica en infocomunicaciones puede definirse como las cualidades que posibilitan el desempeño eficiente en el manejo de las TIC en cualquier área de la vida social, a partir de nexos existentes entre conocimientos, habilidades y actitudes ético axiológicas, que se manifiestan en su desempeño del individuo, para la solución de problemáticas predeterminadas, o en situaciones cambiantes, desde una posición proactiva ante los aportes de dichas tecnologías.

Para formar la competencia básica en infocomunicaciones, a nivel internacional son coincidentes, en línea general, los elementos que forman parte de ella. En los trabajos desarrollados por varios gobiernos locales españoles encabezados por el profesor Jordi Adell, de la Universidad de Jaume, se plantea que el uso de las TIC en cada nivel de enseñanza tiene un objetivo a lograr y ello determina el alcance en la formación de las competencias. Entre las competencias básicas planteadas por el estudio para la enseñanza primaria y la secundaria obligatoria en España está el tratamiento a la información y la competencia digital, que se considera está integrada por los siguientes aspectos (España, 2004, pp. 65-66):

- Búsqueda de información.
- Conocer los componentes básicos de un ordenador.
- Utilizar un tratamiento de textos.
- Encontrar info en Internet siguiendo instrucciones.
- Utilizar recursos digitales para la creación de obras artísticas.
- Fotografía, análisis y tratamiento de imágenes.

- Aplicaciones de diseño y animación.
- Difusión de los trabajos.
- Grabación de música interpretada.
- Comunicarse y colaborar.
- Utilizar medios audiovisuales y recursos informáticos para la creación de piezas musicales.
- Usar distintos soportes digitales.

En Cuba, se plantean en los programas de estudio de la educación general, responden a objetivos generales relacionados que pueden agruparse en la ejecución de procedimientos con los sistemas operativos y de aplicación, especialmente la ofimática. El principio que se plantea es la enseñanza de procedimientos, sin embargo, no siempre se comprende de esta manera y las personas se concentran en aprender cómo usar un determinado software. Esto tiene su base en que la enseñanza de herramientas para el manejo de imágenes y el diseño o de audio, es exclusivo de algunas especializaciones y no de todo el sistema educativo, llegando incluso a definirse que software enseñar. De esta manera se limita el proceso formativo a especializaciones, limitando el desarrollo de un abanico mayor de conocimientos en la formación general.

En los programas educacionales, queda expuesto a la vista de todos, un problema al que no se da tratamiento: la seguridad informática; a pesar de que desde la década de los 90 de la centuria vigésima, ha escalado niveles notables en la atención de los especialistas, por el crecimiento en número y nivel destructivo de los incidentes, lo que ha propiciado la adopción de posiciones proactivas en el manejo de las TIC, lo que da un giro, dejando atrás las posiciones reactivas de actuar luego del incidente.

No es objetivo definir aquí, si el espectro a abarcar es la seguridad informática, de la información o la ciberseguridad; lo esencial es mostrar qué aspectos debe atenderse en la formación, para evitar incidentes que pongan en peligro la información, al ser manejada utilizando las TIC. Como se aprecia en lo expuesto anteriormente, no hay referencias a elementos dentro de esta competencia que contribuyan al desarrollo de lo formativo en seguridad de las TIC. Por esta razón, se considera vital el desarrollo de acciones que contribuyan a desarrollar una unidad de la competencia básica en infocomunicaciones que pudiera nombrarse: modo de actuación proactivo en el manejo seguro de las TIC.

Como es conocido las competencias no son un fenómeno estático, sino que su radio de acción, está determinado por el desarrollo científico técnico en los diversos ámbitos de la vida socio-productiva. Por ello, la formación para el manejo seguro de las TIC, debe partir del abordaje del modo de actuación proactivo en el manejo de las TIC, cuya concepción es necesario analizarla en el sentido estricto, pero también desde una visión amplia. Para quienes que utiliza las TIC en cualquier ámbito de la vida social, es un requerimiento tener definidos los núcleos básicos de conocimientos, habilidades y valores en el uso de dichas tecnologías y por ende los relativos al área de seguridad informática, como se ha apuntado antes.

Estos aspectos debían estar determinados de manera explícita desde la formación básica, en los currículos, pero en los planes de estudio no están expuestos estos elementos de competencia, por lo que es muy importante que las entidades deben comenzar a definir cuales serían estos elementos y que unidades de competencia integran cada uno de los elementos, atendiendo a la obligación que marca el artículo 40 del Decreto 360/19 de la República de Cuba, sobre la preparación de sus trabajadores en el uso seguro de las TIC y el papel que en ello desempeñan las normas ISO de la serie 27000.

Sin embargo, antes de entrar a definir estos aspectos es conveniente la atención al problema desde lo general: el modo de actuación. No se pretende hacer un análisis de todas las aristas que implicaría definir el modo de actuación y sus relaciones con aspectos técnicos, psicológicos o ético axiológicos y que han sido objeto de diversas investigaciones (Font, 2014), el ideal se enmarca en tratar de sacar a la luz una realidad que es necesaria para lograr avances en la seguridad y protección de los sistemas informáticos.

Muchas veces se ha dicho que el factor humano hace posible, en un porcentaje muy elevado, las brechas que se producen en los sistemas informáticos, pero también es cierto, que cuando el capital humano está preparado para solventar los problemas a los que se enfrenta en el quehacer cotidiano con las TIC, se está en presencia de una trinchera de inestimable valor. (Mendoza, 2016, Iglesias, 2019. Owaida, 2021 y Juanes, 2021)

La fortaleza está sustentada en la preparación del individuo, en sus habilidades en el uso de las TIC y también en los aspectos de tipo ético que le permiten discernir entre lo adecuado y lo que no es, o sea, en la tenencia

de competencias básicas para las infocomunicaciones, sin embargo, debe destacarse por encima de esto, la posición de que esta manera de actuar se sustenta en la prevención, considerada desde la década final del siglo XX hasta hoy, la manera adecuada de actuar ante los aportes de las TIC.

La posición de reaccionar o responder con medidas para dar solución a problemas creados por un incidente constituyen ya un aspecto para hacer historia o la forma de actuar para riesgos cuyo estudio mostró que los costos de prevenirlo era mayores que los de reaccionar para la solución, es por eso que se ha tornado en esencia la posición proactiva en el manejo de las TIC, que no es otra cosa que actuar desde la prevención.

El modo de actuación proactivo en el manejo seguro de las TIC es la acción desde la prevención y las buenas prácticas que plantea el uso de dichas tecnologías por el individuo en cualquier contexto y ante las situaciones predeterminadas o no, con la finalidad de solucionar problemáticas impuestas por el quehacer cotidiano.

En nuestra consideración la actuación desde la prevención no es una cuestión estática y por ende las entidades, para la superación de su capital humano, debe fijar las etapas y requisitos a cumplir en cada una de ellas, que desarrollen las competencias de sus empleados, incluyendo de manera especial el uso de las TIC con visión proactiva. Esto redunda en el desempeño, pero también en la eficiencia de la gestión empresarial.

Como punto de partida para cumplir el objetivo propuesto, es necesario establecer que elementos integran la unidad de competencia modo de actuación proactivo en el manejo seguro de las TIC. Se considera que, de manera inicial, la formación debe enfocarse en los siguientes aspectos (Font, 2015, p. 4):

- Desarrollar una actitud ética, abierta, responsable y crítica ante las aportaciones de las nuevas tecnologías.
- Determinar y aplicar los mecanismos básicos que garanticen confidencialidad, integridad y disponibilidad del trabajo con las TIC.
- Determinar cuando la información puede estar comprometida por códigos malignos y actuar de manera efectiva en la neutralización de los mismos.
- Utilizar las redes sociales y la comunicación de manera activa, responsable y segura según el contexto escolar y social.
- Realizar salvas de la información en cualquiera de sus variantes según las condiciones imperantes.

Las etapas posteriores del trabajo de educación de usuarios y los niveles en que se incidirá o se fijarán para ser alcanzados, se determinan por las necesidades del personal y las propias políticas que fije cada entidad en su plan de seguridad de las TIC y se sugiere estén sustentadas en algún estándar internacional.

Con el uso de metodologías para la detección de vulnerabilidades y la realización de pruebas de penetración éticas en los sistemas informáticos, comienzan a aflorar las cuestiones que demuestran la necesidad de la creación de un accionar preventivo desde la formación del capital humano para el manejo seguro de las TIC.

En estudios realizados por los autores en diversos sistemas informáticos con la finalidad de detectar de vulnerabilidades, afloran algunas que se relacionan directamente con el accionar de especialistas en el trabajo con estas tecnologías, entre las que destacan:

1. Sistemas operativos y de aplicación desactualizados y por ende, vulnerables a acciones intrusivas, relacionadas con:

- Configuración inadecuada de las acciones de actualización de las estaciones de trabajo desde el sitio destinado a este fin.
- Obsolescencia tecnológica de estaciones de trabajo, que lleven al uso de sistemas operativos en versiones obsoletas, como por ejemplo: Windows XP y Windows 7 que carecen de soporte técnico del fabricante y por ende de actualizaciones para sus huecos de seguridad conocidos.
- Limitaciones de diversa índole en el enlace al soporte para actualizaciones.
- Uso aplicaciones que son vulnerables o en versiones antiguas.

2. Uso inadecuado o falta de actualización de programas antivirus como consecuencia de:

- Deficiencias con la configuración de la actualización automática de los programas antivirus.
- Errores de configuración para la respuesta a códigos malignos en dichos programas.

- Actualización manual de los antivirus, que deja en manos de una persona esta acción, lo que hace factible una falla.
- Deficiencias en los permisos de administración de los antivirus que posibilitan su manipulación por cualquier usuario.

3. Puertos abiertos sin justificación o con reglas de protección inadecuadas.

A estas vulnerabilidades, se añaden las que propician el accionar del personal no especializado, que están caracterizadas por carencias de formación en el manejo de las TIC. Entre ellas se destacan:

- Uso de medios personales en tareas institucionales, que contienen información personal e institucional, que salen y entran sin un control adecuado del sistema informático conocido como BYOD. (Bring your own device).
- Deficiencias en la cadena de generación y custodia de credenciales de usuarios, se comparten credenciales o se utiliza un usuario único en una estación de trabajo por todas las personas que la utilizan. Se detectan contraseñas guardadas o "recordadas" en navegadores o formularios de autenticación de las estaciones de trabajo.
- Deficiencias en el proceso de respaldo y custodia de la información, que limitan las posibilidades de recuperación ante un incidente.
- Deficiencias en la gestión de incidentes de seguridad, no solo en su información a las entidades estatales dedicadas a su control, sino al personal técnico y dirigente de la entidad, para que se produzcan los análisis y procesos correctivos, que evitan su repitencia. Se carece de una memoria escrita que detalle los incidentes ocurridos.
- Se carece de copias de respaldo de las trazas de los servidores y estaciones de trabajo.
- Debilidad en los mecanismos de control de usuarios en las tecnologías multiusuarios.
- Utilización de cookies en sistemas ofimáticos a pesar de la posibilidad de daño que presentan.

Se considera necesario anotar que la mayor parte de las estaciones de trabajo valoradas utilizan el sistema operativo Windows y programas desarrollados para esta plataforma, que al estar sometidos al sistema de licencias y patentes inaccesibles para Cuba, son utilizados a través de subterfugios que hacen más notable la posibilidad de vulnerabilidad o infección por códigos malignos.

Tomando como punto de partida la necesidad de alcanzar la tenencia de un modo de actuación proactivo, se desarrollo como alternativa, el establecimiento de acciones para el fomento en el capital humano de las buenas prácticas en el uso de las TIC en el área de la ciberseguridad. Este accionar propuesto no pueden quedar exclusivamente en un plan de la superación, sino que debe revertirse en necesidades de contenidos educativos propuestos desde la empresa para la formación de los futuros egresados universitarios que va recibir y que serán llevados a vías de hecho por los docentes de las carreras que los forman, de manera que se cuente con el arsenal que cubra las peculiaridades y necesidades de los sistemas informáticos del área empresarial, que a su vez recibirán desde la universidad propuestas para el fortalecimiento de su infraestructura en TIC, que le propicien la supresión de vulnerabilidades.

El plan de acciones diseñado tiene como núcleo duro el fomento de las buenas prácticas en el manejo seguro de las TIC en el sector empresarial. Las etapas previstas son:

I. Formación general en buenas prácticas en TIC

II. Materialización de resultados.

III. Especialización y aporte bilateral.

La etapa I referida a la formación general en buenas prácticas en TIC tiene como objetivo la preparación del capital humano del sector empresarial en la tenencia de buenas prácticas en el manejo seguro de las TIC y tiene definidas inicialmente cinco acciones:

1. Aplicación de instrumentos en entidades seleccionadas del sector empresarial

Objetivo: Caracterizar a través de la aplicación de instrumentos, el desempeño del capital humano del sector empresarial ante los aportes de las TIC en los procesos socio-productivos.

2. Selección de las entidades donde se desarrollarán las intervenciones diseñadas.

Objetivo: Aplicar un sistema de acciones formativas a partir del diagnóstico aplicado en las entidades del sector empresarial para corregir prácticas inadecuadas en el manejo de las TIC.

3. Proceso de inserción y concientización: El núcleo duro de esta acción está en mostrar a los decisores del sector empresarial el contenido del plan de acción a aplicar, que luego de la aprobación, se presenta a los trabajadores que utilizan las TIC en su desempeño.

Objetivo: Demostrar a través de una presentación de los datos recogidos en el diagnóstico la necesidad de acciones formativas de las buenas prácticas en el manejo seguro de las TIC como fortaleza para el desempeño eficiente de la empresa.

4. Proceso formativo del capital humano del sector empresarial en las buenas prácticas en TIC:

Objetivo: Fomentar una cultura de la ciberseguridad y de buenas prácticas en el uso de las TIC en el capital humano de las empresas seleccionadas, atendiendo de manera diferenciada a los colectivos que utilizan las tecnologías en el desempeño de sus funciones. Para cumplimentar esta acción se diseñaron tres cursos de superación o postgrado cuyo requisito es la tenencia de un conocimiento básico en el manejo de las TIC.

a). Ética y seguridad informática (extensivo a todos los trabajadores, aunque la dirección empresarial decide las prioridades, pues esta superación es parte de los procesos de formación continua del capital humano para ponerlo a nivel de las exigencias de la era digital).

b). Buenas prácticas en el uso de las TIC (para los trabajadores que las utilizan en su desempeño en la empresa).

c). Sistema de gestión en ciberseguridad (destinado a los administradores de redes informáticas, especialistas seguridad informática y directivos en el área de las TIC).

5. Servicios científico técnicos:

Objetivo: Fomentar el conocimiento de las buenas prácticas y el modo de actuación proactivo en el uso de las TIC por el capital humano del sector empresarial a partir de la profundización en las acciones para la detección de vulnerabilidades en los sistemas informáticos empresariales.

Seguridad de la Información

Contenido:

1. Evaluación de amenazas y vulnerabilidades en el sistema informático de la empresa para desarrollar las acciones que permitan y faciliten las acciones correctivas con asesoría.

2. Análisis de la base legal sobre ciberseguridad en Cuba con el capital humano de la entidad.

3. Acciones encaminadas a afianzar las buenas prácticas en el manejo de las TIC por los trabajadores de la entidad desde el control sistemático, la superación por vías directas e indirectas.

Análisis de riesgos y Plan de seguridad de las TIC. (PSTIC)

Contenido:

1. Realización de análisis de riesgos del sistema informático de la entidad, para determinar las amenazas, como punto de partida para la elaboración de las políticas, medidas y procedimientos del Plan de seguridad de las TIC (PSTIC), así como su objetivo, alcance, y demás aspectos. Este proceso se sustenta en un acuerdo de confidencialidad y contribuye a establecer el umbral de riesgo de cada entidad.

2. Elaboración del PSTIC sobre la base de la legislación y la metodología vigente desde 2019 en Cuba, para su presentación y aprobación por la dirección de la entidad empresarial. Además el proceso se sustenta en el uso de las normas ISO de la serie 27000 a partir de la obligatoriedad de la tenencia del PSTIC en todas las entidades en el territorio nacional.

3. Desarrollo de un plan de acción para comprensión por el capital humano de la entidad, de la importancia del cumplimiento de las políticas, medidas y procedimientos a partir de la apropiación de las buenas prácticas en el manejo de las TIC.

Escaneo de puertos

Contenido: Utilizando herramientas como el Nmap, se realiza un análisis de los activos del sistema informático de la empresa para determinar puertos abiertos sin justificación, de manera que se realicen los trabajos correctivos para el cierre de vulnerabilidades a partir del informe que se presenta a la dirección de las entidades.

Escaneos de sitios web

Contenido: Con el uso de herramientas especializadas se procede al escaneo a los sitios web de las entidades empresariales para entregar a la dirección de la entidad para la corrección las vulnerabilidades encontradas en los temas, plugins, etc. El informe presentado no solo presenta las debilidades, sino también las vías de solución a cada uno de los señalamientos.

Escaneo de servicios de las redes informáticas

Contenido: Con el uso de herramientas especializadas y siguiendo una metodología de detección de vulnerabilidades que se adecúa a las condiciones de cada entidad, se realiza el escaneo de las redes informáticas de la instituciones del sector empresarial. Estas intervenciones arrojan las vulnerabilidades que presentan cada una de las direcciones IP y por ende todo el sistema informático. En el informe que se entrega al finalizar el proceso se establecen las pautas para la realización del trabajo correctivo que estará en función de supervisar fundamentalmente servicios, servidores, sistemas de hosting, etc. Las penetraciones pueden realizarse siguiendo el principio de caja negra, gris o blanca en correspondencia con la decisión de cada entidad.

Escaneo de estaciones de trabajo

Contenido: Con el uso de herramientas especializadas se procede al escaneo de los activos informáticos de la entidades. Con ellos se detectan las vulnerabilidades que presentan los medios técnicos con IP asignada. En el informe que se compila y se entrega a la dirección de la entidad al finalizar el proceso, están las bases para la realización del trabajo correctivo.

La etapa II de materialización de los resultados centra su objetivo en fomentar desde lo formativo el manejo seguro de las TIC en el nexo bilateral de aporte soporte entre la universidad y la empresa.

- Publicación de boletines, artículos y ponencias de conjunto con el capital humano de las empresas.
- Desarrollo de contenidos conjuntos de ciberseguridad que pudieran servir a las carreras afines en la formación de los especialistas y al personal de la empresa en su formación permanente.
- Utilización del personal de la empresa en el proceso docente a través de su categorización como docentes.
- Creación de web, blogs, etc para la divulgación conjunta de materiales. En este proceso se pueden incluir estudiantes de años terminales como parte de su vinculación a los procesos productivos.
- Trabajo conjunto en la solución de problemas y peculiaridades de las empresas en TIC que serán utilizados en los procesos formativos de la Universidad a partir de la incorporación de los resultados a los programas docentes.

En esta etapa junto al cumplimiento del objetivo, la marcha de los procesos diseñados dan la posibilidad de la medición del impacto de las acciones desarrolladas en la preparación del capital humano empresarial, porque cada una de las acciones que arroje resultados positivos se convierte en un termómetro para valorar hasta que nivel han calado en el modo de actuación las acciones desarrolladas.

La etapa III de especialización y aporte bilateral se materializa en tres grandes acciones:

Objetivo: Formación especializada desde la categorización científica y la especialización del capital humano empresarial como sustento de la relación entre la universidad y la empresa en un mecanismo bilateral de aporte – soporte que contribuya a la elevación de la calidad de los procesos sustantivos vinculados a este nexo.

- Cursos especializados a partir de los intereses de la entidad empresarial sobre temas de ciberseguridad.
- Maestrías y doctorados para elevar la categorización científica del capital humano del sector empresarial en el área de las TIC y ciberseguridad.
- Formación postdoctoral.

La elevación de la especialización y la categorización científica del capital humano en el sector empresarial, que se inició para el fomento de las buenas prácticas en el manejo seguro de las TIC, se torna en si misma,

gestor nuevos procesos que exceden el objetivo inicial y se revierten a los dos extremos de la relación, en nuevas acciones desde el seno de la propia empresa para su desarrollo y para su aplicación en los procesos formativos en las carreras afines, convirtiendo a la vez los centros productivos en laboratorios de investigación que sustenten los procesos productivos seguros desde el uso de las TIC y en emisores de nuevos productos y servicios resultantes de la superación del capital humano.

La formación del personal de las empresas para atender los procesos relacionados con la seguridad de las TIC en las empresas, fortalecen a este sector, porque no solo le permiten el desarrollo de los procesos indicados en el anexo de la resolución 129/2019 de: Planificar, Hacer, Verificar y Actuar que hacen posible el diseño y proyección, junto a la aplicación, el análisis y evaluación de la efectividad de las soluciones que se gestan en torno a las TIC y la corrección de las brechas detectadas, lo que a su vez se revierte en la supresión de erogaciones por esta causa, al poseer el personal para acometer estas acciones en la empresa, a lo que se suma la posibilidad de convertir esta esfera, en un nuevo servicio que puede agregarse a la cartera empresarial de negocios, cuestión que está insertada en los objetivos del Ministerio de Educación Superior, expuestos en su balance anual de 2020.

Conclusiones

Los procesos que hacen posible la preparación del capital humano en función de las buenas prácticas en el manejo de las TIC, convergen en el desarrollo de la competencia básica en infocomunicaciones y de un modo de actuación proactivo ante los aportes de las TIC.

Las fortalezas del sector empresarial ante la posibilidad de incidente poseen una relación directa con el desarrollo de la competencia básica en infocomunicaciones y el modo de actuación proactiva de su capital humano para manejar de forma segura las TIC en cualquier ámbito.El crecimiento en la preparación del capital humano desde un proceso formativo en torno al manejo seguro de las TIC desde el vínculo bilateral universidad empresa contribuirá a la mayor eficiencia de los procesos socioproductivos y de formación en la universidad, a partir de la atención a las necesidades de la producción y los servicios en las áreas demandadas, sin perder de vista que la formación del egresado se encamina a una actuación que le permita solucionar situaciones que pueden no estar predeterminadas. Estos procesos encuentran una alternativa en el plan de acción para el desarrollo del capital humano en el manejo seguro de las TIC y el desarrollo de un modo de actuación proactiva.

Referencias bibliográficas

1. Bunk, O. P. (1994). La transmisión de las competencias en la formación y perfeccionamiento profesionales de la RFA. Formación Profesional. Revista Europea.

2. Bursztein, S. (2014). Factor humano:el talón de Aquiles de la seguridad I. https://www.magazcitum.com.mx/index.php/archivos/2735

3. Elliot, J. (1993). El cambio educativo desde la investigación-acción. Ediciones Morata.

4. España. (2004). Gobierno de Canarias. Consejería de educación, Cultura y Deportes. Competencias básicas en las tecnologías de la información y la comunicación (TIC). Evaluación e investigación educativa. http://www.redes-cepalcala.org/inspector/DOCUMENTOS%20Y%20LIBROS/COMPETENCIAS/COMPETENCIAS%20BASICAS%20EN%20TIC.pdf.

5. Figueredo Reinaldo, O. et al. (2019). Cuba en Datos: A un año del Internet por el móvil. http://www.cubadebate.cu/especiales/2019/12/06/cuba-en-datos-a-un-ano-del-internet-por-el-movil/

6. Forgas Brioso, J. A. et al. (2005) Las competencias profesionales. Un nuevo enfoque. SWISSCONTACT.

7. Font Hernández, R. (2015): La dimensión seguridad y sus elementos esenciales para la Competencia Básica en Infocomunicaciones y su inserción en el currículo de las carreras pedagógicas. Maestro y Sociedad, 12(2). https://maestroysociedad.uo.edu.cu/index.php/MyS/article/view/1306/.

8. Font, R. (2014). Lo ético axiológico en los elementos esenciales de la seguridad informática en la competencia básica en infocomunicaciones. Universidad de Ciencias Pedagógicas “Frank País García”.

9. Herán, J. M. (2019): 5 ideas para establecer una dinámica de capacitación en una empresa. https://www.welivesecurity.com/la-es/2019/11/04/ideas-establecer-dinamica-capacitacion-seguridad-empresa/

10. Iglesias Fraga, A. El factor humano, causa y solución de la ciberseguridad. En TICbeat. 17 de febrero de 2019. Recuperado de https://www.ticbeat.com/seguridad/el-factor-humano-causa-y-solucion-de-la-ciberseguridad/

11. Iniseg. Factor humano y ciberseguridad. Un riesgo en crecimiento. En Ciberseguridad al dia. 14 de enero 2020. Recuperado de https://www.iniseg.es/blog/ciberseguridad/factor-humano-y-ciberseguridad/

12. Juanes Fernández, D. El factor humano y su importancia en la ciberseguridad. en Atalayar. 15 de abril de 2021. Recuperado de https://atalayar.com/blog/el-factor-humano-y-su-importancia-en-la-ciberseguridad

13. Mendoza, M. A. Ética, el factor humano más importante en el ámbito de la ciberseguridad. En En Welivesecurity ESET. 20 de septiembre de 2016. Recuperado de:https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

14. Owaida, Amer. Ciberseguridad en la industria financiera: riesgos y desafíos. En Welivesecurity ESET. 24 de marzo de 2021. Recuperado de: https://www.welivesecurity.com/la-es/2021/03/24/ciberseguridad-industria-financiera-riesgos-desafios/

15. Pérez, A. El éxito de los ciberataques depende del factor humano. En Directivos y Empresas. 17 de mayo de 2019. Recuperado de https://www.directivosyempresas.com/internet/tecnologia/ciberseguridad-factor-humano/

16. Radio Metropolitana: Cuatro millones de cubanos acceden a Internet desde sus celulares. 14 de agosto de 2020. Recuperado de: https://www.radiometropolitana.icrt.cu/2020/08/14/cuatro-millones-de-cubanos-acceden-a-internet-desde-sus-celulares/

17. Radio Santa Cruz: Etecsa con ofertas de activación de líneas y un nuevo Nauta Hogar este diciembre. 7 de diciembre de 2020. Recuperado de: https://www.radiosantacruz.icrt.cu/etecsa-con-ofertas-de-activacion-de-lineas-y-un-nuevo-nauta-hogar-este-diciembre/

Conflicto de intereses

Los autores declaran no tener ningún conflicto de intereses.