Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VI Número: Edición Especial. Artículo no.:19 Período: Junio, 2019.

TÍTULO: Cultura informática en el entorno geopolítico educativo de la Unidad Educativa INSUTEC.

AUTORES:

1. Máster. Luis Orlando Albarracín Zambrano.

2. Máster. Edmundo José Jalón Arias.

3. Máster. Ítalo Mecías Serrano Quevedo.

RESUMEN: El artículo presenta un análisis sobre la problemática de seguridad en las redes de datos "¿Cómo favorecer los procesos de cultura informática en el entorno geopolítico de INSUTEC Quevedo?", partiendo del uso de métodos científicos de tipo teórico, empírico y matemático, que en conjunto tienen como objetivo el concienciar a la comunidad informática de la utilización de normas y políticas de seguridad. Como resultado en la Unidad Educativa INSUTEC, Quevedo, se reconoce un alto porcentaje de imprudencia informática usando los recursos tecnológicos de interconexión con internet, el porcentaje de usuarios incumplen reglas de seguridad supera el 80%, antecedente que sirve para sugerir medidas básicas de protección informática como punto de inicio para el desarrollo de políticas de seguridad.

PALABRAS CLAVES: Seguridad, Políticas, Internet.

TITLE: Computer culture in the geopolitical educational environment of the INSUTEC Educational Unit.

AUTHORS:

1. Máster. Luis Orlando Albarracín Zambrano.

2. Máster. Edmundo José Jalón Arias.

3. Máster. Ítalo Mecías Serrano Quevedo.

ABSTRACT: The article presents an analysis on the security problem in the data networks "How to favor the processes of computer culture in the geopolitical environment of INSUTEC Quevedo?", Starting from the use of scientific methods of theoretical, empirical and mathematical type, that in the objective of all of them is to make the computer community aware of the use of safety rules and politics. As a result of the INSUTEC, Quevedo, Educational Unit, a high percentage of computer recklessness is recognized using the technological resources of interconnection with the Internet, the percentage of users breaches security rules exceeds 80%, a precedent used to suggest basic measures of computer protection as a point Start for the development of security politics.

KEY WORDS: security, politics, Internet.

INTRODUCCIÓN.

La Internet se ha convertido en una de las herramientas más utilizadas por estudiantes, ejecutivos, secretarias y amas de casa para labores distintas como consulta, búsqueda, comunicación, o simplemente para mantenerse informado, pero también se podrá encontrar en la red personas de mal proceder que actúen como embaucadores, ladrones cibernéticos u otros considerando que los grupos

más vulnerables en las redes informáticas serán siempre los jóvenes. Se realiza la labor investigativa enmarcada en la geolocalización contextual a la Unidad Educativa INSUTEC[1] Quevedo.

En el ambiente sociocultural juvenil analizado en la investigación a través de la aplicación de encuestas realizadas entre los estudiantes de la institución investigada se pudo reconocer diversidad de importantes datos en los hábitos de conectividad en los ámbitos juveniles:

- El universo investigado se mantiene conectado de manera permanente a una red de datos.
- Un elevado 81% ha colocado datos personales en el internet.
- Desconocimiento de normas de seguridad por parte de los cibernautas.

Lo documentado en la investigación de campo lleva el interés de los investigadores a una búsqueda epistemológica y metodológica que logre reconocer las principales falencias en la utilización de recursos tecnológicos a través de métodos empíricos como la observación del universo investigado en los laboratorios de computo, así como en los equipos personales a través de técnicas como la encuesta y la entrevista.

Teniendo como principal interés el centrar la atención en la problemática planteada se consultan diferentes autores reconocidos en el entorno de la informática aplicada a la gestión de procesos de seguridad informática como: Caccuri (2012), De Garay (2008) Ibáñez (2010), Rodríguez (2009), Wallace (2001).

El proceso investigativo revela el Problema de Investigación: ¿Cómo favorecer los procesos de cultura informática en el entorno geopolítico de INSUTEC Quevedo?, presentando además el Objeto de Estudio: *Gestión de seguridad digital*, en consecuencia el Objetivo de la Investigación estará destinado a: *Elaborar un listado de normativas básicas de protección informática*, determinando de

[1] Es la Unidad Educativa privada INSUTEC que anteriormente funcionó como un Instituto por lo que se quedó con ese nombre.

esta manera el Campo de Investigación como: *La dinámica de los procesos de seguridad informática en el entorno geográfico de INSUTEC Quevedo*.

Se registra de esta manera una brecha cultural de conocimiento informático en el entorno sociocultural estudiado considerando una oportuna socialización de normativas que incentivarán a la creación de políticas permanentes de seguridad en redes de datos y comunicación informática.

Se declara como Hipótesis: Con la elaboración y socialización de normativas de uso de redes de comunicación y dispositivos tecnológicos se combatirá el analfabetismo digital logrando la seguridad de datos personales e institucionales.

DESARROLLO.

Fundamentación teórica de la gestión de seguridad digital en redes con fines educativos.

Para iniciar con la información real del problema se debe empezar conociendo: ¿Qué es el internet?; pregunta que debe resolverse sin satanizar a esta herramienta que ha convertido al planeta en el mundo actual que se conoce, ¿Qué sería del mundo sin internet?, otra pregunta que se tratará de disipar, pero para no perder el enfoque en el tema se empieza por analizar la primera interrogante propuesta.

Según Rodríguez (2006), en el libro "Iniciación a la red y el internet" menciona: "Para conceptualizar el internet deberemos empezar indicando que es una red de redes interconectadas entre sí con alcance mundial, pero todas son independientes y autónomas" (pág. 2). En la mayoría de los textos buscados, los conceptos sobre este tema son similares; conceptos muy fríos y en ocasiones demasiado técnicos, y para mejorar el entendimiento únicamente se dirá que el internet es la unión de varios equipos informáticos destinados a compartir información de cualquier tipo.

Basándose únicamente en titulares de los periódicos, alguien que nunca haya entrado a la red podría pensar que Internet está llena de personas con problemas psicológicos, ideas raras y motivaciones dudosas y que la gente normal haría bien en adentrarse en ella con pies de plomo (Wallace, 2001).

En el internet no todo es malo, de hecho es un espacio virtual donde se puede encontrar gran diversidad de cultura, y muy abundante, gente dedicada a compartir sus conocimientos o asesorar en problemas de todo tipo pero al igual que el ying yang existe la contraparte: aquellas personas que los problemas, enojos y molestias de su vida privada los llevan al internet y se desquitan con el primero que se cruce en este trayecto llevando al internet todas sus molestias como si la red fuese un gran botadero de inconvenientes o un lugar para descargar la ira de todo lo vivido en los labores, o su vida cotidiana en lugar de ser creativos y disipar su ira de manera pacífica y relajada.

Un equipo informático puede estar propenso a varios tipos de ataques y entre los más importantes se encuentran las amenazas de software, y las humanas según detallan García-Cervigón & Alegre (2011), en el libro "Seguridad Informática – Sistemas Microinformáticos y redes", las amenazas citadas tienen en común que su método invasivo está basado en la falta de seguridades aplicadas a un equipo informático.

Si bien es cierto que no existe un procedimiento estándar para la protección de información, la Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) presentan en conjunto la ISO/IEC 27001 (2005), en la cual indica que la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) es una decisión estratégica de una organización influenciada por sus necesidades, objetivos, requerimientos de seguridad, los procesos empleados y la estructura de la información en donde ejemplifica que una situación simple requiere un SGSI simple.

Basando una conclusión en el principio básico de la ISO 27001, se podrá indicar con claridad que no existe una forma estándar de protección de equipos; sin embargo, eso no indica que no existan formas apropiadas y básicas de resguardar la información.

Dependiendo de la función que desempeñen, existen varios tipos de seguridad los que pueden clasificarse en preventivos, detectores y correctivos; cada mecanismo ofrece una o más servicios de protección, así lo indica Aguilera (2010) en el libro "Seguridad Informática".

Existen varias prácticas que pueden ser implementadas en los planes informáticos para mejorar la gestión tecnológica y sus políticas de seguridad, indica Portainter (2012) en el libro "Seguridad Informática" que en una institución pueden implementarse las mejores prácticas generalmente basándose en normativas de estandarización pero la mayor consideración son los limitados recursos para esta área incluso en las organizaciones más grandes, los recursos tiene un límite, la única diferencia es la cantidad de ceros a la derecha que tienen esos límites.

"Tener la capacidad de asegurar un sistema implica tener el conocimiento y entendimiento de cómo funciona el mismo" fueron las palabras del famoso Hacker Kevin Midnick, explicando que la mayor protección no debe ser únicamente a los sistemas sino a los equipos informáticos done están alojados los mismos.

Diagnóstico de los procesos de seguridad informática en INSUTEC Quevedo.

En un reporte de la Internet World Stats (IWS) al 31 de diciembre de 2011, fueron estimadas 6 mil 930 millones 55 mil 154 personas en el mundo, de las cuales 2 mil 267 millones 233 mil 742 son usuarios de Internet. Con estas cifras, la IWS estimó la penetración mundial de Internet en un 32.7 por ciento. Mientras tanto en Ecuador, datos indicados por el INEC (2012); indican que la población del país tiene un 31% de acceso fijo al internet mientras que cerca del 65% alguna vez han utilizado internet.

La última encuesta del Instituto Nacional de Estadística y Censos (INEC; 2011), sobre el acceso de los ecuatorianos a las Tecnologías de la Información y Comunicación (TIC), realizada en diciembre de 2011, reveló que el 24,7% de los hogares tiene una computadora de escritorio y el 9,8% tiene una

portátil. Esto es, el 35% de los 3 815 000 hogares que existen en el país. El sondeo realizado en 579 centros poblados abarcó una muestra de 21 768 viviendas, según Byron Villacís, director del INEC (2011).

El porcentaje de personas que usó Internet en los últimos 12 meses corresponde a 31,4%; hace cuatro años, esa estadística era del 25,7%, develando un alza de 5,7 puntos porcentuales.

Quienes mayor uso le dieron en 2011 a Internet en el Ecuador fueron los hombres con el 32%, frente al 30,8% para las mujeres. En ambos casos, la cifra subió seis puntos en cuatro años.

En cuanto a las edades, se determinó que seis de cada 10 jóvenes de entre los 16 y 24 años tuvo un uso activo del Internet (59,4%), seguidos por quienes tienen de 25 a 34 años (39,6%). Quienes menos usaron el Internet fluctúan entre los 65 y 74 años (3,3%).

El 57,3% de los usuarios ingresó por lo menos una vez al día; mientras el 36,9% lo hizo en promedio una vez por semana. El principal uso del Internet se enfocó en las comunicaciones con la familia y amigos, y los ingresos a la web se realizaron en su mayoría desde el hogar del usuario.

Pichincha se registró como la provincia con mayor porcentaje de población que usó Internet en 2011, con el 44,5%, seguida por Azuay con el 36,9%, y la que menos lo usó fue Santa Elena, con 18%.

Un elemento que resaltó Villacís es que el quintil más pobre del Ecuador incrementó su hábito del uso de Internet.

En el año 2008, el 7,9% de pobres utilizaba Internet, y ahora llega al 15,5%. De ellos, el 50% lo utilizó para comunicarse y su frecuencia de acceso es del 57,3% al menos una vez al día y el 36,9% mínimo una vez a la semana.

Con este estudio del INEC (2012), se sostiene la idea de que cada vez son más las personas que interactúan en el internet, siendo esta una potente herramienta de comunicación sobre todo con familiares que no comparten la misma locación, incluso en esferas sociales en las cuales se puede

empíricamente decir que no existe contacto con el internet. Este estudio realizado en Ecuador nos demuestra una vez más que el crecimiento de la utilización del internet no depende de situaciones económicas o sociales sino más bien una necesidad natural del ser humano por estas conectado con sus familiares o la simple curiosidad de conocimiento.

En una encuesta realizada a los estudiantes del Colegio INSUTEC de la ciudad de Quevedo a finales del mes de noviembre 2018, los resultados encontrados fueron alarmantes, más aún al notar que el 81% de la población estudiantil poseen acceso a internet de manera permanente todos los días de la semana y tan solo un 3% no acostumbra el acceso a la red, siendo el restante porcentaje cibernautas eventuales, considerando este caso una conexión a la red de manera semanal.

Del grupo, que alguna vez se ha conectado a internet, un elevado 81% ha suministrado datos personales a algún sitio en la red sean estos foros, blogs o sites de registro, sin proteger su equipo de un ataque informático ni mucho menos utilizando políticas de seguridad.

Los porcentajes presentados en la investigación revelan que la sociedad actual permanece conectada la mayor cantidad de tiempo y casi en su totalidad con un elevado 81% compartiendo datos de manera permanente en el internet además de ser usuarios sin cultura informática ya que la dinámica de las encuestas descubre el nulo conocimiento o aplicación de normas de protección y seguridad.

Teniendo ya toda esta información el autor cree extremadamente necesario el compartirla para evitar estos ataques, y la principal forma de precaución deberá ser siempre la desconfianza, incluso de los contactos conocidos, ya que es más probable que el atentado sea cometido por un amigo de red, porque conocerá cierta información que le ayudará a obtener lo que busca.

Sistema de acciones para el desarrollo de procesos de protección de la información en el contexto del Colegio INSUTEC.

Métodos Básicos de protección de Información.

En lo posterior se listan algunos consejos extraídos de la revista SUITE101 que pueden ayudar a mantener seguros nuestros datos en el internet de estos molestos y dedicados hackers y sus ataques con aplicaciones informáticas.

- Evitar hacer clic en enlaces sospechosos a páginas desconocidas recibidos por correo, así el remitente de esos emails sea una persona conocida. A veces los hackers toman los nombres de contactos para tener más credibilidad y también puede darse el caso de que esa persona conocida tenga malas intenciones.
- Ninguna entidad financiera realiza actualizaciones de datos con sus clientes a través del internet en el caso de llegar un correo que parezca del banco pidiendo ese tipo de información, comunicarse inmediatamente con el banco y denunciar esto.
- A pesar de que parecería obvio, existen personas que aun comparten información muy privada en redes sociales o chat, sabiendo que nunca se debe escribir número de tarjetas ni contraseñas por correo, chat o redes sociales, pues podrían ser fácilmente obtenidos por terceros.
- Evitar en lo posible usar cybers para entrar en las cuentas de correo o del banco, ya que los dueños podrían tener programas que simulen estas páginas o que almacenen los datos ingresados de esta manera al digitar su usuario o contraseña bancaria estas se estarían copiando en las bases de datos de estos lugares.
- Las preguntas de seguridad, en caso de olvido de contraseña, no deben ser obvias, tienen que ser cosas que sólo la persona dueña de la cuenta pueda saber. De ser algo obvio, cualquiera que conozca un poco a la persona puede violentar la seguridad mediante la respuesta a dicha pregunta.

- No instalar programas de dudosa procedencia o autorizar la instalación de programas durante la visita a páginas web, ya que estos no tienen procedencia certificada pudiendo contener software corrupto o virus.
- Mantener siempre actualizado el antivirus y hacer análisis periódicos y de preferencia trabajar en nuestros equipos personales con antivirus con licencia y no de manejo de pruebas o licencias gratuitas.
- Siempre tener activo el cortafuegos para que evite el ingreso de programas sospechosos.
- Utilizar contraseñas largas, alfanuméricas, que contengan combinaciones de mayúsculas, minúsculas, números y símbolos; ya que existen programas que obtienen las contraseñas débiles.
- Jamás responder o realizar envíos de correos masivos o cadenas, donde llega un correo en el cual se pide que sea reenviado a todos los contactos. En el caso de decidir continuar con esta cadena por información o motivos personales deberá escribir las direcciones en la casilla de CCO (copia oculta) para que las direcciones de los amigos no sean reveladas.
- No aceptar personas desconocidas en las redes sociales. Podrían ser identidades falsas y con malas intenciones.
- En caso de hacer compras en línea, fijarse en la parte superior de la página, que contenga el protocolo HTTPS, porque la S significa que es una página verificada y por lo tanto segura.
- No hay que revelar datos como nombre completo, número de cedula, direcciones o teléfonos en las cuentas de correo o redes sociales.
- En la actualidad, en la mayoría de los sitios web de acceso público o informativo el visitante es el afortunado visitante 1 millón o tuvo la suerte de ganarse un Ferrari o una cuenta bancaria con mucho dinero en ella, aunque debería ser sentido común no está demás indicar que nunca se debe

hacer clic en estas páginas que indican al visitante como el ganador de algo. En la mayoría de los casos, por no apuntar, la totalidad es una trampa.

CONCLUSIONES.

Este trabajo presenta las siguientes conclusiones:

- Las políticas de seguridad aplicadas en una empresa dependen no solo de la utilidad de la misma sino están supeditadas a los presupuestos empresariales.
- Los resultados de los estudios revelan los crecientes porcentajes de internautas ingenuos en la red acrecentando de esta manera potenciales víctimas de fraudes informáticos y reproductores de virus.
- Es imperioso el manejo de políticas y normas de seguridad en una red sea esta una LAN domiciliaria o extensa de oficina.

REFERENCIAS BIBLIOGRÁFICAS.

1. Aguilera López, P. (2010). Seguridad Informática. España: Editorial Editex.

2. Caccuri, V. (2012). Computación para Docentes. Argentina: Fox Andina.

3. De Garay, J. (2008). Filosofía del Mercado. El mercado como forma de comunicación. España: Plaza y Valz.

4. García-Cervigón Hurtado, A. & Alegre Ramos, M. P. (2011). Seguridad Informática – Sistemas Microinformáticos y Redes,. España: Paraninfo.

5. Ibáñez, N. (2010). Ciberputeadores en Internet. España: Norbooksediciones. Recuperado de: https://www.academia.edu/38398490/CIBERPUTEADORES_EN_INTERNET

6. ISO 27001 (2005) Organización Internacional de Estandarización. Comisión Electrónica Internacional.

7. World Stats, (2011) Internet en cifras. MediaNews Group, Inc. Obtenido de: https://www.excelsiorcalifornia.com/2012/02/14/internet-en-cifras-internet-world-stats-ofrece-datos/

8. INEC, (2011). Instituto Nacional de Estadística y Censos, Tecnología de la información y comunicaciones, Encuesta tecnológica. Obtenido de: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/Resultados_principales_140515.Tic.pdf

9. INEC, (2012). Instituto Nacional de Estadística y Censos, Tecnología de la información y comunicaciones, Encuesta tecnológica. Obtenido de: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2017/Tics%202017_270718.pdf

10. Portantier, F. (2012). Seguridad Informática. Argentina: Primera Edición, Fox Andina. De: http://biblioteca.utsem-morelos.edu.mx/files/tic/14octubre2013/red/Seguridad%20Informatica.PDF

11. Rodríguez Ávila, A. (2006). Iniciación a la Red Internet Concepto, Funcionamiento, Servicios y Aplicaciones de Internet. España: Ideas Propias Editorial.

12. Wallace, P. (2016). The Psychology of the internet. USA: Cambridge University Press. http://assets.cambridge.org/97811070/79137/frontmatter/9781107079137_frontmatter.pdf

DATOS DE LOS AUTORES.

1. **Luís Orlando Albarracín Zambrano.** Licenciado en informática y Ciencias Computacionales, Máster en Informática Empresarial, presidente de la Unidad de Investigación de la Facultad de Sistemas Mercantiles UNIANDES-Quevedo. Correo electrónico: licluisalbarracin76@hotmail.com, uq.luisalbarracin@uniandes.edu.ec

2. **Edmundo José Jalón Arias.** Ingeniero en Sistemas y Máster en Informática Empresarial. Docente titular auxiliar, UNIANDES-QUEVEDO. Correo electrónico: uq.edmunjal@yahoo.com
3. **Ítalo Mecías Serrano Quevedo.** Ingeniero en Sistemas y Máster en Conectividad y Redes; Docente titular auxiliar, UNIANDES-Quevedo. Correo electrónico: uq.italoserrano@uniandes.edu.ec

RECIBIDO: 1 de mayo del 2019. **APROBADO:** 11 de mayo del 2019.