Desvelando el código: una revisión del conocimiento y concienciación de los estudiantes de ingeniería Informática-UPE-CPF sobre los mecanismos de apropiación digital

María Luisa Hermosilla de Olmedo
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: maluolme31@gmail.com
ORCID: https://orcid.org/0000-0003-4910-6562

Rodolfo Fernando Oliver Ayala
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: rodolfo_oliver@hotmail.com
ORCID: https://orcid.org/0009-0008-4050-420X

Jaqueline Olmedo Hermosilla
Correo electrónico: 990.hermosilla@gmail.com
ORCID: https://orcid.org/0000-0002-4158-1169

Daisy Beatriz Paredes Segovia
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: paredesdaisy82@gmail.com

Victor Ariel Córdoba Bordón
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: victorarielcordobabordon830@gmail.com

Ariel de Jesús Duarte Núñez
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: duartearIel353@gmail.com

Ángel Ramón Servían González
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: angelserviangonzalez@gmail.com

Leandro David Cáceres Ferreira
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: leandrocaceresinformatica570@gmail.com

Salvador Cano Chávez
Facultad de Ciencias de la Informática
Institución: Universidad Privada del Este
Dirección: Ciudad Pdte, Franco, Paraguay
Correo electrónico: 999999.azaazaz@gmail.com

RESUMEN
El estudio investigó el nivel de conocimiento y conciencia de los estudiantes de Ingeniería Informática en la Universidad Privada del Este en lo que respeta a los mecanismos tecnológicos empleados con fines malintencionados para el robo de información. La investigación tuvo un enfoque mixto, de diseño no experimental de tipo descriptivo. Con una población de 258 estudiantes, siendo 174 la cantidad de los elementos de la muestra, que fue escogido con método no probabilístico y técnica por conglomerado. Para la recolección de datos se utilizó el formulario de Google. Los hallazgos revelaron una brecha significativa en su comprensión de estas amenazas cibernéticas, destacando la necesidad urgente de mejorar la educación en ciberseguridad en el currículo. Además, se resaltó la importancia de la concienciación sobre la responsabilidad ética en la gestión de la información y se subrayó la necesidad de colaboración interdisciplinaria en este campo en constante evolución. En conclusión, el estudio pone de manifiesto la importancia de preparar a los futuros profesionales de la informática para abordar los desafíos de seguridad y protección de datos en un entorno digital en constante evolución.

Palabras clave: Seguridad, Informática, Conocimiento, Robo, Información.

1 INTRODUCCIÓN

En el contexto del creciente aumento de los ciberataques, es fundamental que el público esté informado sobre los esquemas y mecanismos que suelen emplearse para el robo de información. Los ciberataques pueden tener consecuencias devastadoras para las víctimas, que pueden sufrir pérdidas económicas, daños a su reputación, o incluso la pérdida de su privacidad. Por ejemplo, una víctima de un ataque de phishing puede perder acceso a su cuenta bancaria o a sus tarjetas de crédito, lo que puede provocar grandes pérdidas financieras. Una víctima de un ataque de malware puede tener su ordenador infectado con un virus que puede robar sus datos personales, como su número de la seguridad social o su dirección de correo electrónico. Y una víctima de un ataque de fuerza bruta puede tener su contraseña comprometida, lo que puede permitir a los ciberdelincuentes acceder a sus cuentas en línea.

Esta investigación se desarrolla con el propósito general, para identificación del conocimiento que tienen los estudiantes de la carrera de Ing. en Informática, sobre los esquemas y mecanismos tecnológicos utilizados con fines maliciosos para el robo de información. Esto responde a que la sociedad moderna se encuentra cada vez más inmersa en un entorno digital, lo que la hace susceptible a diversas amenazas

cibernéticas, como el robo de datos confidenciales, estafas y sobornos, entre otros riesgos. Por tanto, es crucial mantener a las personas informadas y empoderadas frente a estas amenazas, y para ello el profesional debe estar altamente preparado.

Para lograr los objetivos, se llevaron a cabo una serie de investigaciones y análisis exhaustivos que abordaron los siguientes aspectos: Medidas de Protección y Prevención. Encuesta sobre el conocimiento de los estudiantes: Se llevó a cabo una encuesta entre los estudiantes de la carrera de Ing. en Informática de la Universidad Privada del Este, CPF; para revisar su nivel de conocimiento sobre las amenazas de seguridad informática y el robo de información.

La investigación busca contribuir significativamente a la protección de la información personal y confidencial, así como a la preparación de profesionales del área de la informática para hacer frente a las amenazas cibernéticas en la actualidad.

En la era digital, donde la información se ha convertido en un activo invaluable y la ciberseguridad se erige como un tema crítico, es esencial evaluar el grado de conocimiento y comprensión de los estudiantes de Ingeniería Informática de la Universidad Privada del Este, Campus Ciudad Presidente Franco (UPE-CPF), sobre los mecanismos de apropiación digital.

Este planteamiento de problema se basa en la necesidad de abordar los siguientes aspectos: Importancia de la Ciberseguridad: La información digital es un recurso esencial en la sociedad actual, utilizada en actividades cotidianas y profesionales. La falta de comprensión y preparación en ciberseguridad puede dejar expuestas a las personas y organizaciones a riesgos significativos, como la pérdida de datos confidenciales, la interrupción de servicios críticos y el daño a la reputación.

Desafíos Actuales: Los avances tecnológicos y la sofisticación de las amenazas cibernéticas plantean desafíos constantes en la protección de datos y sistemas. La apropiación digital, en sus diversas formas, representa una amenaza latente que debe abordarse de manera proactiva.

Formación Académica: Los estudiantes de Ingeniería Informática en la UPE-CPF son futuros profesionales que jugarán un papel crucial en la seguridad de la información. Revisar su conocimiento actual sobre mecanismos de apropiación digital es fundamental para garantizar una formación adecuada y la preparación de expertos en ciberseguridad.

Brechas en el Conocimiento: Es necesario identificar las posibles brechas en el conocimiento de los estudiantes, incluyendo la comprensión de las tácticas utilizadas por actores maliciosos en línea, los métodos de prevención y las mejores prácticas en seguridad cibernética.

Repercusiones en la Seguridad Digital: Un conocimiento insuficiente de los mecanismos de apropiación digital puede tener consecuencias graves, tanto a nivel individual como organizacional. La falta de preparación puede dar lugar a vulnerabilidades que son explotadas por atacantes cibernéticos.

Por lo que surge la siguiente pregunta general, ¿Cuál es el conocimiento y concienciación que tienen los estudiantes de Ingeniería Informática de la Universidad Privada del Este sobre los mecanismos tecnológicos que se usan de forma malintencionada para el robo de información? y su respectivo objetivo, determinar el nivel de conocimiento y concienciación de los estudiantes de Ingeniería Informática en la Universidad Privada del Este, Campus Ciudad Pdte. Franco (UPE-CPF), sobre los mecanismos de apropiación digital. Los investigadores se hicieron la siguiente proposición; Hi: El nivel de conocimiento y concienciación de los estudiantes de Ingeniería Informática en la Universidad Privada del Este, Campus Ciudad Pdte. Franco (UPE-CPF), sobre los mecanismos de apropiación digital es alto.

Para probar esta hipótesis, se realizó una encuesta, con el instrumento denominado cuestionario, aplicado a los estudiantes de Ingeniería Informática de la UPE-CPF. La encuesta incluyó preguntas sobre los siguientes aspectos: Definición de apropiación digital, Tipos de apropiación digital, Ejemplos de apropiación digital y Riesgos de la apropiación digital.

2 METODOLOGÍA

2.1 ENFOQUE DE INVESTIGACIÓN

Este trabajo adopta un enfoque multimodal al combinar la recopilación de datos cuantitativos con la caracterización detallada del fenómeno en estudio. Esta metodología nos permite obtener una comprensión más completa y holística del tema de investigación.

2.2 DISEÑO DE INVESTIGACIÓN

Este estudio se caracteriza por su alcance descriptivo, ya que su objetivo principal es recopilar información de manera exhaustiva. Se trata de un diseño no experimental, dado que no se modifica el entorno en el que se lleva a cabo la investigación. Además, adopta un enfoque mixto, ya que el cuestionario planteado proporcionará datos estadísticos, combinando así elementos cuantitativos y cualitativos en el análisis.

2.3 ALCANCES DE INVESTIGACIÓN

Este estudio se caracteriza por su alcance descriptivo, ya que su objetivo principal es recopilar información de manera exhaustiva. Se trata de un diseño no experimental, dado que no se modifica el entorno en el que se lleva a cabo la investigación. Además, adopta un enfoque mixto, ya que el cuestionario planteado proporcionará datos estadísticos, combinando así elementos cuantitativos y cualitativos en el análisis.

2.4 POBLACIÓN Y MUESTRA

El estudio se centrará en los 258 estudiantes de pregrado de la carrera de Ingeniería en Informática de la Universidad Privada del Este, Ciudad Pdte. Franco. De esta población, se seleccionará una muestra que sea representativa, garantizando así la relevancia y aplicabilidad de los resultados obtenidos.

2.5 TÉCNICA DE MUESTREO

La muestra se seleccionará mediante el método no probabilístico con la técnica de selección por conglomerado, en el que se identificará y seleccionará a un subconjunto específico de estudiantes de la Universidad Privada del Este.

2.6 TÉCNICA DE RECOLECCIÓN DE DATOS

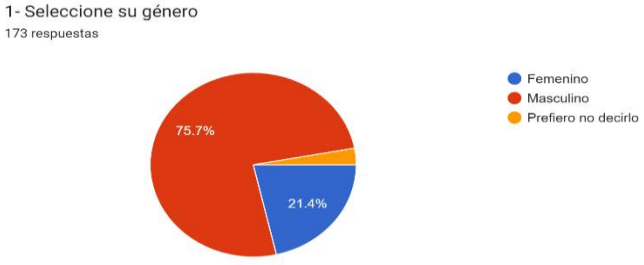
La recopilación de datos se realizará a través de una encuesta, utilizando un cuestionario como instrumento. Este cuestionario estará compuesto por preguntas cerradas con opciones de respuesta, que se implementarán en un formulario de Google. Estas preguntas ayudan a recopilar información valiosa sobre el nivel de conocimiento y concienciación de los estudiantes en relación con la seguridad de la información y los mecanismos de apropiación digital, así como identificar áreas de mejora en su formación académica.

2.7 ANÁLISIS DE DATOS RECOGIDOS

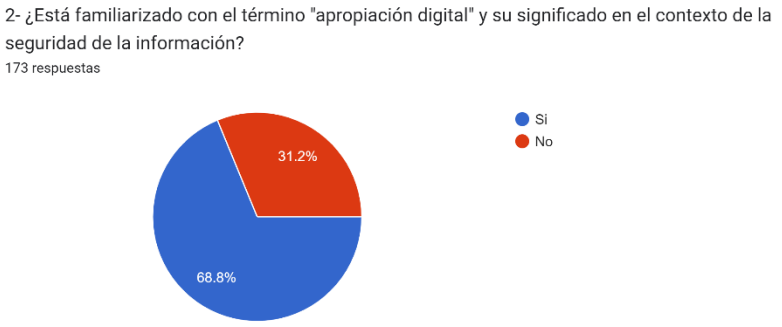
El análisis de los datos recogidos se realizó utilizando un enfoque cuantitativo. Para ello, se utilizó la herramienta Excel para procesar y analizar los datos. Posteriormente, los resultados del análisis se presentaron en forma de gráficos demostrativos para facilitar su interpretación. Se tuvo en cuenta: Limpieza de datos: Este es un paso crucial, es la manera de asegurar de que los datos estén completos, sean consistentes y estén libres de errores.

3 RESULTADOS

3.1 LUEGO DEL ANÁLISIS RESPECTIVO SE PRESENTAN LOS RESULTADOS BAJOS LOS PARADIGMAS CUANTITATIVO Y CUALITATIVO

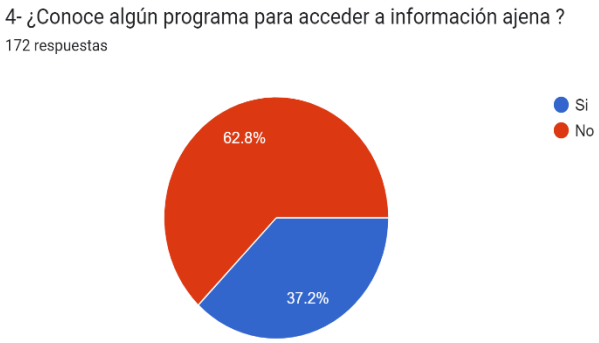


En este caso, 174 personas respondieron a un cuestionario. Responde a la Distribución de género, en el que el 75,7% de los estudiantes de la muestra identifican su género como masculino. El 21,4% de las personas de la muestra identifican su género como femenino. Resto sin preferencia: El "resto" se refiere a las personas que no eligieron identificarse como masculinas ni femeninas. En otras palabras, no revelaron su género en el cuestionario o prefirieron no especificarlo. Para calcular el porcentaje de Estudiantes que no prefirieron decir su género, puedes restablecer la suma de los porcentajes de género conocido (masculino y femenino) del 100%. En este caso: 100% - (75,7% + 21,4%) = 100% - 97,1% = 2,9%. Entonces, el 2,9% de los estudiantes de la muestra no prefirió decir su género.



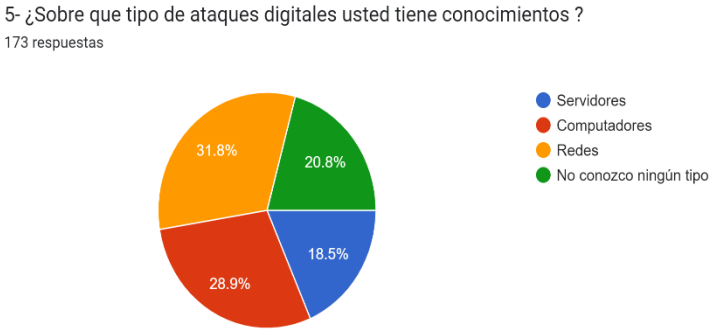
El tamaño de la muestra constituye un grupo de estudiantes y este grupo consiste en un total de 100%. En este caso, la muestra se divide en dos categorías: Personas familiarizadas: El 68,8% de los estudiantes en la muestra están familiarizadas con el término "Apropiación digital". Esto significa que aproximadamente dos tercios de los estudiantes en la muestra lo que significa o han oído hablar de este término. Estudiantes no familiarizadas: El 31,2% de las personas en la muestra no conocen el término "Apropiación digital". Esto implica que alrededor de un tercio de las personas en la muestra no tienen conocimiento de este término o no están familiarizadas con él. Estos porcentajes indican la proporción de personas en la muestra que están o no están familiarizadas con el término "Apropiación digital". Esta información es útil para comprender la difusión o el conocimiento de un concepto o término en un grupo de personas.

Distribución de niveles de conocimiento en informática: El 69,4% de la población tiene un nivel de conocimientos "medio" en informática. Esto significa que la mayoría de los estudiantes en la población tienen un conocimiento de nivel medio en esta área. El 15,6% de la población tiene un nivel "Alto" de conocimientos en informática. Esto indica que una parte significativa, pero menor, de la población tiene un alto nivel de conocimiento en informática. El 15% restante de la población tiene un nivel de conocimientos "Bajo" en informática. Esto significa que un porcentaje relativamente pequeño de la población tiene un nivel de conocimiento bajo en esta área. Estos porcentajes indican cómo se distribuyen los niveles de conocimiento en informática en la población. Es importante tener esta información para comprender el nivel de competencia en informática de la población y para tomar decisiones relacionadas con la educación, la capacitación o la toma de decisiones en proyectos tecnológicos.



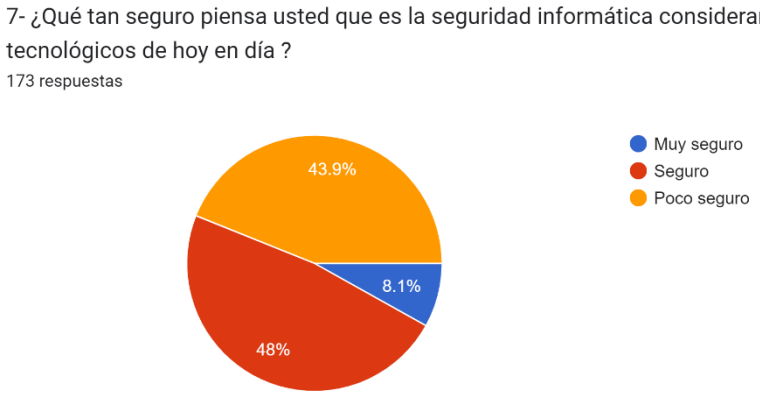
Esta afirmación se refiere a toda la población de interés. Estudiantes con conocimiento: El 62,8% de la población tiene conocimiento de algún programa que se utiliza para acceder a información privada. Esto significa que aproximadamente dos tercios de las personas en la población están al tanto de la existencia de programas diseñados para acceder a información que normalmente debería ser privada. Estudiantes sin conocimiento: El 37,2% restante de la población no tiene conocimiento de estos programas. Esto implica

que alrededor de un tercio de la población no está informada o no sabe acerca de la existencia de tales programas. Esta información se utiliza para entender cuántas personas en la población son conscientes de los riesgos relacionados con la privacidad y la seguridad de la información. Es importante para la toma de decisiones y la educación en temas de seguridad cibernética y privacidad.

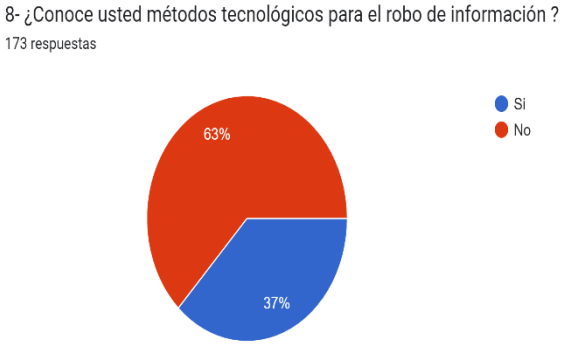


Estudiantes con conocimiento sobre ataques a redes: El 31,8% de la población tiene conocimientos sobre ataques digitales dirigidos a redes. Esto indica que alrededor de un tercio de los estudiantes en la población entienden lo que son y cómo funcionan los ataques a las redes. Estudiantes con conocimiento sobre ataques a computadoras: El 28,9% de la población tiene conocimientos sobre ataques digitales dirigidos a computadoras. Esto implica que un poco menos de un tercio de la población está familiarizado con los ataques cibernéticos dirigidos a sistemas informáticos individuales. Estudiantes que no conocen ningún tipo de ataque informático: El 20,8% de la población no tiene conocimiento sobre ningún tipo de ataque informático. Esto significa que un quinto de la población no está al tanto de los ataques digitales. Estudiantes con conocimiento sobre ataques a servidores: El 18,5% restante de la población tiene conocimientos sobre ataques digitales dirigidos a servidores. Esto indica que una proporción significativa de la población comprende los ataques dirigidos a servidores de información.

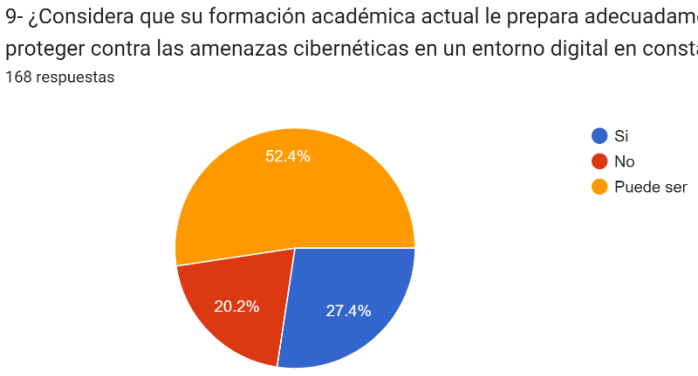
La afirmación describe la distribución del conocimiento de la población en cuanto a los lenguajes de programación utilizados para el robo de información digital. Estudiantes que no conocen ningún lenguaje de programación para el robo de información: El 68% de la población no tiene conocimiento de ningún lenguaje de programación que sea utilizado para el robo de información digital. Esto significa que la mayoría de los estudiantes en la población no están informadas acerca de estos lenguajes. Estudiantes que conocen algún lenguaje de programación para el robo de información: El 32% restante de la población sí tiene conocimiento de al menos un lenguaje de programación utilizado para el robo de información digital. Esto indica que una minoría de la población está al tanto de la existencia de lenguajes de programación utilizados en actividades ilícitas relacionadas con el robo de datos o información digital. Esta información es relevante para entender la conciencia de la población sobre la ciberseguridad y la programación en contextos ilegales. Puede ayudar en la toma de decisiones relacionadas con la educación y la seguridad cibernética.



La afirmación describe las percepciones de la población sobre la seguridad informática actual. Estudiantes que piensan que la seguridad informática es "Segura": El 48% de la población cree que la seguridad informática de hoy en día es "Segura". Esto indica que casi la mitad de la población considera que la seguridad informática es suficiente y que sus datos e información están protegidos. Estudiantes que piensan que la seguridad informática es "Poco segura": El 43,9% de la población piensa que la seguridad informática es "Poco segura". Esto significa que una proporción importante de la población tiene dudas o preocupaciones sobre la seguridad de sus datos en línea. Estudiantes que afirman que la seguridad informática es "Muy segura": El 8,1% de la población opina que la seguridad informática es "Muy segura". Esto indica que una minoría de la población tiene una alta confianza en la seguridad de la tecnología informática actual. Esta información es útil para comprender las percepciones de la población en cuanto a la seguridad informática y puede ser relevante para la planificación de políticas de seguridad cibernética y para la educación del público en temas de seguridad en línea.



Estudiantes que no conocen métodos tecnológicos para el robo de información: El 63% de la población no tiene conocimiento de métodos tecnológicos utilizados para el robo de información. Esto significa que la mayoría de los estudiantes en la población no están al tanto de las técnicas y herramientas que se pueden emplear para el robo de datos o información digital. Estudiantes que conocen métodos para el robo de información: El 37% restante de la población sí tiene conocimiento de métodos tecnológicos utilizados para el robo de información. Esto indica que una minoría de la población está informada sobre las técnicas y herramientas relacionadas con el robo de datos o información digital. Esta información es relevante para comprender cuántos estudiantes s en la población están conscientes de las amenazas a la seguridad informática y la ciberseguridad. Puede ser importante para la toma de decisiones relacionadas con la educación en seguridad cibernética y la prevención de delitos informáticos.



Percepción de la formación académica: La mayoría de los encuestados indican que su formación académica podría prepararlos adecuadamente para identificar y protegerse contra amenazas cibernéticas. Esto implica que la mayoría de los estudiantes encuestados creen que su educación les proporciona al menos una base razonable para lidiar con cuestiones de ciberseguridad, aunque no necesariamente con un alto grado de preparación. El 27% de los encuestados afirma que sí, su formación los prepara adecuadamente.

Esto indica que un poco más de una cuarta parte de los encuestados se siente bien preparado por su formación académica para enfrentar amenazas cibernéticas. El 20% de los encuestados dice que no, su formación no los prepara adecuadamente. Esto significa que una quinta parte de los encuestados no cree que su educación les haya proporcionado una preparación adecuada para lidiar con amenazas cibernéticas. Estas respuestas reflejan las percepciones de los encuestados sobre la eficacia de su formación académica en el ámbito de la ciberseguridad. Puede ser importante tener en cuenta estas opiniones para evaluar la calidad de la educación en seguridad cibernética y considerar mejoras en los programas de formación o concienciación en ciberseguridad.

10- ¿Ha experimentado alguna vez una situación en la que tus datos personales o información confidencial se vieron comprometidos en línea? Si es así, ¿Qué medidas tomaste para abordar la situación? 150 respuestas
Cincuenta de los respondientes indicaron no haber tenido incidentes con la seguridad de sus cuentas en internet. Sin embargo, los demás establecieron estos sucesos, que se detallan a continuación Modificación de contraseñas por otras seguras, encriptación de archivos Tuve una ocasión en mi trabajo, que hubo un intento de robo de datos de usuarios de la empresa por el método Phishing, el cual intervine bloqueando las direcciones de correo atacante en el servidor de anti spam que disponemos Si, busqué soluciones acerca del dicho problema y pidiendo ayuda Contra virus, instalaba antivirus en mi computadora Formateo completo del pc Algo parecido, me quitaron algo de plata, no hice nada, lloré. Cambiar mi contraseña Cambiar contraseña Verificación de dos pasos No logré eliminarla, pero si sobre guardar dichos correos. Si ya me pasó, Pedir ayuda al soporte de esa aplicación Por suerte no eh experimentado esa situación Fue en Facebook, activé la verificación de 2 pasos Contraseñas mucho más largas y de caracteres variados (#$@abc123) Primero que nada, protegí toda mi información Si en varias ocasiones, las medidas que tomé fueron cambiar contraseñas por unas más seguras, activé la verificación en dos pasos. Si, cambiar mis contraseñas y activar métodos de autenticación En esa época, acudí a "recuperar contraseña" y el utilizar un correo auxiliar (ambas a tiempo) reportar No pude realizar ninguna contramedida, puesto que al momento de yo enterarte ya se habían apropiado de cuentas mías, tuve que crear nuevas cuentas. Además de borrar mi información personal, cambié contraseñas y activé la seguridad de dos pasos Intento de hackeo, reforzar la seguridad implementar verificación de 2 pasos y si es posible migrar la información a otra cuenta Si, cambié la contraseña y desvinculé todos los dispositivos de la cuenta Si ya ha sido comprometido, cambiando la contraseña de mis redes sociales. traté de borrar todo y lo que podía cambiar/editar todo lo que se veía de forma pública en internet sobre mi Única experiencia son intentos de robos, por ejemplo, ip loggers que a través de un link camuflado intenta robarte tu información si entras en ellos, jamás caí en uno, pero son muy conocidos y la gente suele caer nunca tuve una experiencia de exposición de información personal, pero si perdí algunas cuentas debido al ataque cibernético, lo primero que suelo ver la raíz/causa del problema que pueden ser aplicaciones de dudosa procedencia o sitios no seguros, luego procedo eliminarlos para luego la limpieza de mi cuenta

Si, intentaron hackear mi Instagram desde otra ciudad lejana (Luque) llego directamente a mi correo y me pidió verificación lo cual solo tuve que cancelar
11- ¿Puede nombrar alguna medida de seguridad básica que las organizaciones suelen implementar para proteger su información contra la apropiación digital?154 respuestas
Diez y siete elementos muestrales indicaron No tener nombres de medidas de seguridad básica utilizada por las organizaciones. Mientras que los demás indicaron esto que se describe seguidamente: Contraseñas El de si eres un robot vpn Las medidas de seguridad básicas que las organizaciones suelen implementar incluyen el uso de firewalls, antivirus y software de seguridad actualizado, políticas de contraseñas fuertes, autenticación de dos factores, capacitación en seguridad para empleados y copias de seguridad regulares de datos. Tener contraseñas seguras, de al menos 12 dígitos, con números, mayúsculas, minúsculas y caracteres. Primeramente, un buen antivirus y servidores de detención de spam Pines, huellas dactilares, escaneos faciales, etc Implementar firewalls de red para controlar y monitorear el tráfico de entrada y salida de la red de la organización y bloquear amenazas potenciales. Autenticación de dos factores Una de las más comunes y que las personas no se toman en serio es sobre las redes sociales, simplemente agregan contraseñas relacionadas con el nombre de su mascota o algo más fácil como: 123456, lo mejor es evitar ese tipo de cosas. Id privada Verificación en dos pasos, por una clave única Verificación de 2 pasos Llamar a un ingeniero que se especializo en esa área Cambio de contraseñas cada cierto tiempo Servidores físicos. Antivirus estándar Copia de seguridad /utilizar contraseñas más difíciles Las contraseñas y demás Seguridad de dos pasos Utilizar antivirus o un navegador seguro Autentificación en dos pasos Número de teléfono Llaves físicas Seguridad de 2 paso y confirmación con el móvil Falcon Strike Hacer una contraseña o copia de seguridad dependiendo de la app que se esté utilizando Una contraseña segura y autenticación en 2 pasos. VPNs y prácticas de seguridad que depende del área de trabajo La medida es que siempre debemos ser discretos con nuestras contraseñas en línea Contratando un paquete de seguridad que contenga antivirus, etc. Encriptación de información. Utilizar contraseña segura Poner una buena contraseña no entrar en cualquier lado o páginas Antivirus Cambio de contraseña No instalar aplicaciones desconocidas De seguridad no, pero de invasión varias una de ellas el Pegasus Contraseñas y keys contraseña Cambiar contraseña Autentificación de dos pasos Protección QoS Contraseña segura Uso de antivirus en los ordenadores, concientización sobre el uso seguro de la computadora Seguro de dos pasos Seguridad en la nube ¿Soporte y respaldo?

Contraseñas seguras
Verificación de dos pasos
Tener una contraseña, contratar algún paquete de seguridad
Autentificado en dos pasos para la seguridad
No entrar en sitios web desconocido y hacer la copia de seguridad
Copia de seguridad, para guardar datos y protegerlos.
Cookies
Seguridad en la nube
Autenticaciones de dos pasos
Cambio constante de contraseñas, refuerzo en el I.P
Controles de acceso a los datos más estrictos
Patrón y Huella digital
Verificación en 2 pasos
Verificación en dos pasos
Vpn
avat
Antivirus
Contraseñas seguras, antivirus y antimalware y copias de seguridad.
Cambiar la contraseña cada tanto
Encriptación de datos
Método de autenticación de 2 pasos
Cambiar constantemente mis contraseñas y no revelar mucha información.
Cerrar sesión
-Cambiar la contraseña cada 1 mes -Mantener actualizado la cuenta
Seguridad de autenticación de dos pasos
Suelen usar contraseñas de números y letras, patrones y cerraduras con huellas digitales
Correos y contraseñas seguras
Una de las medidas de seguridad más básica sería cambiar la contraseña varias veces
Contratar hackers éticos para detectar las vulnerabilidades y de esa manera corregir los problemas con la seguridad
No entrar en páginas ilegales, ya que tienen anuncios, y capaz algunos de los anuncios son maliciosos, usar un bloqueador de anuncios o no ingresar en la página.
Ningún conocimiento
Trabajar en la nube

12- ¿Puede mencionar al menos tres ejemplos de mecanismos de apropiación digital utilizados para obtener información de forma no autorizada?
146 respuestas

Veinte respondientes No mencionaron ningún ejemplo, indicando no conocerlos.

Mientras que los demás escribieron nombres de los mecanismos apropiados.:
Pishing
incluyen el phishing, malware, ransomware, ataques de fuerza bruta, ingeniería social y ataques de suplantación de identidad.
Phishing - Malware - Ingeniería social
Phishing Spam Malware
Antivirus, softwares de seguridad, planes y pinings
Phishing: Los atacantes envían correos electrónicos falsificados que parecen provenir de fuentes legítimas, como bancos o servicios en línea, con el objetivo de engañar a las personas para que revelen información confidencial Ataques de fuerza bruta: En estos ataques, los ciberdelincuentes intentan adivinar contraseñas probando repetidamente combinaciones diferentes hasta que encuentran la correcta Malware y virus: Los atacantes pueden usar software malicioso, como virus, troyanos o ransomware, para infiltrarse en sistemas informáticos y obtener acceso no autorizado a información confidencial.
Fishing, suplantación de identidad, ingeniería social
Phishing: El phishing es una técnica en la que los atacantes envían correos electrónicos o mensajes falsos que parecen ser de fuentes legítimas, como bancos o empresas conocidas. Ataques de ingeniería social: En los ataques de ingeniería social, los delincuentes manipulan a las personas para que divulguen información confidencial. Malware: El malware es software malicioso que se instala en el dispositivo de una víctima sin su conocimiento o consentimiento.
Redes sociales, asistentes virtuales y plataformas de streaming

Obtención de datos suplantando una web, escaneo de teclas mediante algún virus, mediante programas no oficiales
Pishing, malware, suplantación de identidad
Correos, contraseñas, páginas falsas que te piden completar tus datos
Pishing rico de identidad estafas
Phishing. Maleante. Form grabbing
secuestro de datos (rasomware)
Fhishing
Virus Pishing Daño informático
Nmap, camphish
Pishing, malware, ataque DOS
URLS otros
Páginas de enmascaramiento para robar contraseñas, acceso remoto de escritorio, capturadores de escritura
Keylogger, Pishing y Malware
Podría ser la participación en comunidades en línea, que se pueden relacionar con intereses personales. El aprendizaje en línea, pueden encontrar tutoriales videos y obtener conocimientos o información. Usar hacking de forma no ética para el robo de datos.
No tengo ni la menor idea
Virus informáticos seguimiento de teclado, malwares de seguimiento y espía disfrazados de programas de uso común y virus que sobrecargan los ordenadores con intenciones ilícitas (minería, extorsión, violación de la privacidad, uso de IP a nombre de otra, minería ilegal, etc)
Usar identidad falsa, robar fotos, personificar a otra persona
Firewall, antivirus, cortafuegos
Páginas fake
Hackeo
Por link, por stikes la verdad hay muchas cosas la cual se puede llegar a acceder a tus informaciones
El phising, el troyano, spam por correo electrónico.
Fishing back Door y la utilización de los distintos virus maliciosos utilizados (que son sumamente efectivos)
No tengo idea de cómo hacerlo
hackers, entrar en una página pirata e ingresar tus datos y anotar tus datos e información valiosa en lugar que cualquiera pueda tener accesibilidad
Pishing, ataque doS
-instalación de aplicaciones maliciosas que acceden a la información personal - -
A través de correos no deseados, o de archivos con virus
Ndaikuaai
Obtener informaciones con páginas que roban datos
No, no tengo ejemplos claros
Clonación, kchers y por Red
La vdd nose
Escaneo de qr, link de virus malicioso, inteligencia artificial
Keyloggers, clonaciones de chips, clonaciones de páginas
Puede ser la extorsion, algunas copias de dispositivos
Malware, inyección SQL,Phishing.
Palanca: Un dispositivo rígido que pivota sobre un punto (fulcro) y se utiliza para transmitir fuerza. Polea: Un disco con un agujero o ranura para una cuerda, utilizado para levantar o mover cargas mediante la transmisión de fuerza a través de la cuerda. Engranaje: Conjunto de ruedas dentadas que se engañan entre sí para transmitir movimiento y cambiar la velocidad o dirección de éste.
Por el momento aun no conozco
Links maliciosos
Pishing- Keylover- Ataques a través de redes wifi free
No conosco ninguna
Phishing, key loger
Phishing Malware Ingeniería social
Extorsión, malwares, algún tipo de enlace malicioso.
-scam -spyware -malware
Phishing, key logger
Por medio de enlaces, cookies o llamadas extrañas
-Colocar tu correo y contraseña -Datos personales -Información confidencial
Phishing Keylogger Robo de cookies

No confiar en cualquier aplicación No abrir archivos adjuntos de correos desconocidos Mantener actualizado el sistema operativo
Correos al descuido Contraseñas que jamás se han cambiado Compartir enlaces inadecuados
Por medios de enlaces Las cookies de las páginas
Pishing, acceso a cuentas, estafas.
Chantaje, ingreso sin permiso al ordenador ajeno, algún programa creado que pide los datos del usuario.
Fhishing
Hackeo, malware e ingeniería social
Hacerse pasar por un asistente de Google, hacer falsos premios por Internet con fines de que alguien se registre y ponga cuenta y contraseña, hacerse pasar por soporte de WhatsApp para pedir códigos de verificación de cuenta y robar números de WhatsApp
A través de enlaces no seguros. Malware. Virus
El phinshing El malware Ingeniería social
Links maliciosos y estafadores virtuales
Extorsión o la copia de datos tipo bancarios
Mensajes engañosos o links
redes sociales, estafas y pishing.
Entrar en enlaces desconocidos Compartir contraseña y correo al descuido
Virus, páginas maliciosas
Chantaje, invasión de red, hackeó de información personal
-Instalación de aplicaciones maliciosas - -
Phishing Ingeniería social Ataque de fuerza bruta

4 CONCLUSIÓN Y RECOMENDACIONES

La investigación titulada "Desvelando el Código: Una Revisión del Conocimiento y Conciencia de los Estudiantes de Ingeniería Informática en la UPE-CPF sobre los Mecanismos de Apropiación Digital" proporciona una visión profunda y valiosa sobre la comprensión y la conciencia de los estudiantes de Ingeniería Informática en relación con los mecanismos de apropiación digital. A partir de los hallazgos presentados en este trabajo, se pueden extraer varias conclusiones clave, cumpliendo los distintos objetivos específicos y en relación a la hipótesis de investigación, ésta resultó refutada, ya que los alumnos no tienen nivel alto de conocimiento sobre los mecanismos de apropiación digital:

1. Necesidad de Conciencia: La investigación destaca la importancia de aumentar la conciencia entre los estudiantes de ingeniería informática sobre los mecanismos de apropiación digital. La apropiación digital se ha vuelto esencial en la era actual de la tecnología, y los estudiantes de esta disciplina deben estar preparados para comprenderla y aplicarla de manera efectiva.
2. Brecha en el Conocimiento: También pone de manifiesto que existe una brecha en el conocimiento de los estudiantes en lo que respeta a los mecanismos de apropiación digital. Esto sugiere la necesidad de mejorar la educación y la formación en este campo para garantizar que los futuros profesionales de la informática estén bien informados y puedan abordar los desafíos digitales de manera efectiva.
3. Importancia de la Educación: Los resultados de las respuestas del cuestionario, subrayan la importancia de una educación sólida en Ingeniería Informática que incluya una comprensión sólida

de los aspectos relacionados con la apropiación digital. Los programas educativos deben ser revisados y actualizados para asegurarse de que aborden estas cuestiones de manera adecuada.

4. Desafíos y Oportunidades: La revisión también identifica desafíos y oportunidades en el ámbito de la apropiación digital. Los estudiantes deben estar preparados para enfrentar desafíos como la ciberseguridad, la privacidad de los datos y la ética digital, pero también pueden aprovechar oportunidades para la innovación y el desarrollo de soluciones tecnológicas responsables.

5. Responsabilidad Compartida: Los hallazgos en el trabajo de campo, resaltan que la responsabilidad de mejorar el conocimiento y la conciencia de los mecanismos de apropiación digital no recae únicamente en los estudiantes, sino que también debe ser asumida por las instituciones educativas, los profesores y la industria tecnológica.

En conclusión, "Desvelando el Código" arroja luz sobre la importancia de abordar la apropiación digital en la educación de los estudiantes de Ingeniería Informática y subraya la necesidad de actuar para cerrar la brecha de conocimiento en esta área. Esta revisión sirve como un llamado a la acción para mejorar la preparación de los futuros profesionales de la informática y garantizar que estén equipados para navegar de manera efectiva en un mundo cada vez más digital.

REFERENCIAS

Aguilerra López, P. Editerc. (s.f.) Troyanos. Informática y comunicación. https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=que+es+un+Adwares+&ots=PrppWzCHR2&sig=o8MWjP4HZDqnhkfYvGxZwaX8hr4#v=onepage&q=troy

Adwares. https://books.google.com.py/books?id=WHCUYnQ2hz0C&pg=PA9&dq=que+es+un+Adware&hl=es&sa=X&ved=2ahUKEwi33dqt3_z6AhUZjZUCHZ8mBmkQ6AF6BAgKEAI#v=onepage&q=que%20es%20un%20Adware&f=false

Castañeda Meza, L. R. (2021). Revisión sistemática de literatura sobre competencias de uso y apropiación de las TIC en estudiantes virtuales de posgrado (Doctoral dissertation, Corporación Universitaria Minuto de Dios). https://repository.uniminuto.edu/handle/10656/14037

Cerra, M. (2010). Spyware. Seguridad. USERS. https://books.google.com.py/books?id=WHCUYnQ2hz0C&pg=PA102&dq=que+es+el+Spyware&hl=es&sa=X&ved=2ahUKEwj2qdj73_z6AhUIr5UCHd_7D1EQ6AF6BAgIEAI#v=onepage&q=que%20es%20el%20Spyware&f=false

de Luna, E. L. B., García, S. M. A., & de Dios Naranjo, M. E. P. ESTADO DEL ARTE DE LAS COMPETENCIAS DIGITALES PARA LA INNOVACIÓN DOCENTE EN EL ÁMBITO UNIVERSITARIO. PRÁCTICAS SOCIOEDUCATIVAS EN INVESTIGACIÓN, 59. https://ri.ujat.mx/bitstream/20.500.12107/3595/1/4.pdf#page=59

de Cali, S. (2022). PROYECTO EDUCATIVO DEL PROGRAMA DE INGENIERÍA INFORMÁTICA. https://www.uao.edu.co/wp-content/uploads/2023/09/PEP-Ingenier%C3%ADa-Inform%C3%A1tica.pdf

Ferreres Franco, C. (2011). La integración de las tecnologías de la información y de la comunicación en el área de la educación física de secundaria: análisis sobre el uso, nivel de conocimientos y actitudes hacia las TIC y de sus posibles aplicaciones educativas. https://www.tdx.cat/handle/10803/52837

Giraldo Gómez, L. Y. (2014). Competencias mínimas en pensamiento computacional que debe tener un estudiante aspirante a la media técnica para mejorar su desempeño en la media técnica de las instituciones educativas de la alianza futuro digital Medellín (Doctoral dissertation, Universidad EAFIT). https://repository.eafit.edu.co/handle/10784/4488?locale-attribute=es

Herrera Leyva, R. Y. (2018). Nivel de conocimiento que tienen estudiantes de pregrado de Lima sobre mecanismos para el robo de información digital. https://repositorio.usil.edu.pe/items/62895322-f1a3-4e41-923b-d0567c0bf021

Jara Delgado, C. J. (2017). Relación entre el nivel de conocimiento y el uso de las Tecnologías de Información y Comunicación en la formación académica de los estudiantes de Estomatología del Octavo y Noveno Ciclo en el año 2017. https://repositorio.uap.edu.pe/handle/20.500.12990/1417

Luz, C. G. M. (2018). Educación y tecnología: estrategias didácticas para la integración de las TIC. Editorial UNED. https://books.google.es/books?hl=es&lr=&id=KG5aDwAAQBAJ&oi=fnd&pg=PT5&dq=REVISI%C3%93N+DEL+CONOCIMIENTO+Y+CONCIENCIACI%C3%93N+DE+LOS+ESTUDIANTES+DE+INGENIER%C3%8DA+INFORM%C3%81TICA+SOBRE+LOS+MECANISMOS+DE+APROPIACI%C3%93N+DIGITAL&ots=Ov-QKzboMy&sig=O--KaqVeosQ8CKtHCn0dcYZrJDQ#v=onepage&q&f=false

Quintana-Nevárez, A. Robo de información, mas común de lo que todos creen. https://www.researchgate.net/profile/Alberto-Quintana-Nevarez/publication/314772203_Robo_de_informacion_mas_comun_de_lo_que_todos_creen/links/58c5e88fa6fdcce648e8b804/Robo-de-informacion-mas-comun-de-lo-que-todos-creen.pdf Robo de información, más común de lo que todos creen.

Quintana Narvaez, A. (2017). Robo de información, mas común de lo que todos creen. /links/58c5e88fa6fdcce648e8b804/Robo-de-informacion-mas-comun-de-lo-que-todos-creen.pdf

Rivera, F. C., Hermosilla, P., Delgadillo, J., & Echeverría, D. (2021). Propuesta de construcción de competencias de innovación en la formación de ingenieros en el contexto de la industria 4.0 y los objetivos de desarrollo sostenible (ODS). Formación universitaria, 14(2), 75-84. https://www.scielo.cl/scielo.php?pid=S0718-50062021000200075&script=sci_arttext&tlng=en

Rootkit

https://books.google.com.py/books?id=ZqHDDwAAQBAJ&pg=PT143&dq=que+es+es+un+Rootkit&hl=es&sa=X&ved=2ahUKEwjF1_iU3_z6AhURiJUCHZU4D-IQ6AF6BAgNEAI#v=onepage&q=que%20es%20es%20un%20Rootkit&f=false

Spam de Correos

https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=que+es+un+Adwares+&ots=PrppWzCHR2&sig=o8MWjP4HZDqnhkfYvGxZwaX8hr4#v=snippet&q=Spam&f=false

Torres, M. I. (2021). Aportes para una apropiación crítica de conocimientos y usos de hardware y software de programación y robótica en la educación para la primera infancia de Argentina (Master's thesis). https://rdu.unc.edu.ar/handle/11086/23970

Postigo Palacios, A. (20220) Smishing. Sistemas microinformáticos y redes. Paraninfo. Gráfica Summa. España. https://books.google.com.py/books?id=UCjnDwAAQBAJ&pg=PA126&dq=que+smishing&hl=es&sa=X&ved=2ahUKEwiNmNLL3vz6AhVmI7kGHQXbBwsQ6AF6BAgNEAI#v=onepage&q=que%20smishing&f=false