DETERMINAR LA EFICACIA DE LA PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN ALMACENADA EN EL SOFTWARE DEL INSTITUTO TECNOLÓGICO DEL PUTUMAYO.

Autor(es):
Córdoba Botina, James Estiven [1*], Miranda Barragán, Darien Manuel [2]
[1]estudiante de desarrollo de software, [2]estudiante de desarrollo de software

* stiven.cor2002@gmail.com, darienmiranda72@gmail.com

Resumen.

La seguridad informática, es el proceso que se toma para proteger, conservar datos y garantizar el buen desempeño de los equipos informáticos, evitando ataques de software maliciosos y de cibercriminales. El artículo se desarrolla con el propósito mejorar las condiciones de seguridad informática en el ITP, permitiendo buen funcionamiento operativo en su sistema y protección a la información que se contenga de las personas; según investigaciones realizadas, se recalca la importancia de realizar actualizaciones constantes de los sistemas operativos, las ventajas que se tengan al hacerlo y las desventajas de no hacerlo. Al tomar esta información se analizó el estado de los sistemas operativos en el ITP y como se desempeña su funcionamiento, lo cual demostró las falencias las falencias que presenta y las debidas acciones que se deben tomar, por ejemplo, las actualizaciones de software, limpieza constante de los ordenadores sistemáticos e implementar más seguridad en cuanto al acceso en los sistemas, cuentas y datos personales e institucionales.

Palabras clave: seguridad, redes, Privacidad, protección, información.

DETERMINE THE EFFECTIVENESS OF THE PRIVACY AND PROTECTION OF THE INFORMATION STORED IN THE SOFTWARE OF THE INSTITUTO TECNOLOGICO DEL PUTUMAYO.

Abstract

Computer security is the process that is taken to protect, preserve data and guarantee the good performance of computer equipment, avoiding attacks by malicious software and cybercriminals. The article is developed with the purpose of improving the conditions of computer security in the ITP, allowing good operational functioning in its system and protection of the information that is contained about people; According to research, the importance of constantly updating operating systems, the advantages of doing so, and the disadvantages of not doing so are emphasized. When taking this information, the status of the operating systems in the ITP and how its operation is performing was analyzed, which demonstrated the shortcomings, the shortcomings it presents and the due actions that must be taken, for example, software updates, constant cleaning of systematic computers and implement more security in terms of access to personal and institutional systems, accounts and data.

Keywords: security, networks, privacy, protection, information.

Introducción

El Instituto Tecnológico del Putumayo , como institución de educación superior del estado, tiene bajo su cargo el resguardo de una gran cantidad de información, desde personas en registro, estudiantes, docentes, directivos y contratistas de la institución, por lo tanto está bajo su acción, el poder proveer y brindar un sistema de seguridad informática para la protección de la integridad y privacidad de todos sus miembros, a su vez, garantizar la protección de cuentas, servidores y archivos de importancia para la institución, esto garantiza un servicio óptimo y una apta capacidad de resguardo en el instituto y ofreciendo una imagen positiva como tal para todo el público; a su vez, garantizar el buen funcionamiento en las redes de cobertura de internet, los programas que posean los equipos para la realización de actividades de aprendizaje y laborales en todo el plantel educativo, oficinas de administrativos, salas de cómputo para estudiantes y computadores personales de docentes, puedan desempeñarse con alta eficacia en las actividades y procesos que se utilicen.

Método.

Se realizó un proceso de recolección de información, tanto el personal encargado del área informática y de sistemas del instituto y de artículos y archivos en redes, referente a los procesos y estándares de seguridad informática que maneja el ITP, según la normativa que lo estipula. Para este proceso, se consultaron diferentes bases de datos, desde Scielo, Pubmed, ScienceDirect y entro otros repositorios de instituciones, entre otras fuentes (tuyutechnology, Segurityinformacion, ieee)

En la información citada, se priorizo aquellos documentos que hablaran acerca de la importancia y la eficacia que deben tener los sistemas de seguridad informática de las instituciones que brindan servicio a la comunidad, donde se explicara la forma adecuada para este proceso y la normativa que debe manejarse en este proceso; luego de esto se tomaron los datos más relevantes que hicieran énfasis en el poder entender la importancia de la seguridad informática, los riesgos de un sistema operativo de bajo rendimiento y las alternativas de funcionamiento óptimo para mejorar las condiciones dentro de una institución.

La investigación y recolección de datos realizada en el ITP con el personal encargado de la parte de sistemas y control informático, permitiendo conocer que el instituto no cuenta con un sistema especializado o clasificado para la protección de la información que se maneja, tan solo cuenta con un programa que protege de los correos entrantes la presencia de virus, excepto de defensas sistemáticas para posibles ciberataques y robo de información.

Marco teórico

La seguridad informática, **e**s un proceso de protección de datos sensibles, redes y aplicaciones de software contra un posible ataque cibernético (Lopez, 2017).

Los ataques cibernéticos pueden ser considerados como una explotación de recursos, acceso no autorizado a los sistemas, ataques de rescate para encriptar datos y extraer dinero, estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos, como el robo de identidad (M, 2020).

A raíz de la inmensidad de riesgos que entrañan las conexiones a Internet, la seguridad se ha vuelto un concepto que no solo implica la calidad de los sistemas y los servicios, sino también el prestigio de las empresas que los proporcionan, el objetivo es evitar que las comunicaciones estén desprotegidas ante posibles pérdidas o interceptación de datos (Dr., 2019). Actualmente, la práctica totalidad de las organizaciones dependen en mayor o menor medida de sistemas informáticos. Por ello el desarrollo de la seguridad se desempeña de manera constante.

VENTAJAS Y DESVENTAJAS DE LA SEGURIDAD INFORMATICA.

Ventajas:

1. Se encarga de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

2. Crean buenas medidas de seguridad que evitan daños y problemas que pueden ocasionar intrusos.

3. Crea barreras de seguridad que no son más que técnicas, aplicaciones y dispositivos de seguridad que utilizando aplicaciones de protección: cortafuegos, antivirus, anti espías y usos de contraseñas. Protege la información y los equipos de los usuarios (Segurityinformacion, 2017).

4. Capacita a la población general sobre las nuevas tecnologías y las amenazas que pueden traer.

desventajas:

1. En los equipos más desactualizados, un antivirus realmente efectivo puede ser muy pesado, puede hacerlo más lenta, y ocupar mucho espacio en memoria.

2. Los requisitos para su creación de contraseñas son cada vez más complejos. la mayoría de los sitios web requieren inicios de sesión y el cambio de contraseñas con frecuencia se ha vuelto obligatorio en muchos lugares de trabajo. Recordarlas en ocasiones es muy difícil.

NORMATIVA EN COLOMBIA.

ISO/IEC 27001: Especifica los requisitos a cumplir para implantar un SGSI certificable conforme a las normas 27000.

ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información. Define cómo es el SGSI, cómo se gestiona y cuáles son las responsabilidades de los participantes.

Sigue un modelo PDCA (Plan-Do-Check-Act)

Los puntos claves son: Gestión de riesgos y la Mejora continua.

ISO/IEC 27002: Es un código de buenas prácticas para la gestión de la seguridad.

Consiste en: Recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización.

Describe los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especifica los controles recomendados a implantar, es decir, las medidas a tomar.

ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma (Sgc, 2014).

. **Ley 962 DE 2005**: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. • Modelo Estándar de Control Interno

MECI 1000:2005: Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el fin de orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado Colombiano.

Los distintos tipos de seguridad informática.

Seguridad de hardware: hace referencia a la protección de elementos físicos, incluyendo sistemas de alimentación ininterrumpida (SAI), cortafuegos o firewall de hardware, y módulos de seguridad de hardware (HSM) (Bussinesmarketingschool, 2018).

De todos los sistemas de seguridad que pueden existir, es el más adecuado y de mejor calidad ante otros, pues brinda opciones de autenticación a la hora de querer utilizar los ordenadores o equipos personales, alginas de estas son claves, cifrado y autenticación de usuario (AgendaAPD, 2019).

DESVENTAJAS DE HARDWARE

-modelos de producción, no cualquiera puede realizar un hardware.

- Podría ser la incompatibilidad con las nuevas tecnologías. Por ejemplo, si temes de una maquina vieja y quieras adaptarle los de hoy en día, no podes.

- Lo rápido que se vuelve obsoleto.

- La diversidad en la elección, se necesitan cierto hardware para cierto tipo de uso. No es lo mismo el hardware necesario para trabajar con gráficos que el hardware necesario para jugar juegos.

- Los precios. Cada vez es más caro y generalmente hay que esperar a que pase un tiempo para que bajen los precios y cuando ya bajaron, este es obsoleto (Restrepo, 2009).

VENTAJAS DE HARDWARE:

-protege su soberanía, se puede realizar la adaptación de diseños, evita la alianza “trusted computing”

-hardware abierto: es de calidad de estándar abierto y es más económico.

-Compatibilidad: Reconoce la mayoría de otros sistemas operativos en una red.

-Multitarea real: Es posible ejecutar varias aplicaciones y procesos simultáneamente.

-su seguridad a nivel de servidor podemos encontrar que la seguridad de Hardware es muy buena por sui calidad

- La cantidad de marcas disponibles en el mercado. El no monopolio, hay diversidad para elegir, hay líneas económicas y líneas de alta gama.

- El avance de la tecnología. En 3 o 4 años de paso de trabajar de 1 a 4 núcleos por ejemplo en el caso de los microprocesadores.

- La compatibilidad con todo lo que se podría considerar no informática. Ej: TV, Sistemas de Audio, Estéreos, Mp3, Mp4, etc.

Seguridad de software: se consideraban los menos importantes hasta hace algún tiempo, donde se pudo determinar la importancia de estos mismos, en base a todo el funcionamiento de los ordenadores y el buen rendimiento en los sistemas, el fallo de estos ocasionaría un acceso fácil a cibercriminales y daño irreversible de los sistemas en algunos casos (Obsbussinesschool., 2018).

En cuanto a instituciones y empresas, es mejor optar por sistemas de seguridad más potentes, como:

Cortafuegos (firewall): se trata de una protección para controlar el tráfico de datos en una red. Existen varias técnicas cortafuegos, como Packet Filter, Application Gateway y Proxy Server (Molinetti, 2019).

Software de filtración de contenidos: actúa como un filtro para las personas que tienen acceso a Internet. El contenido online que se puede ver es depurado de acuerdo con las políticas de la organización, favoreciendo la protección contra amenazas como el phishing (Sofecom, 2018).

Al ser desarrollado por las personas, el software presenta vulnerabilidades que deben ser detectadas en el menor tiempo ya que intrusos maliciosos pueden infiltrarse en los sistemas mediante la explotación de algunos de estos defectos de software (Destinonegocios, 2019).

Seguridad de red: protege toda la información que se pueda acceder de internet, por ejemplo, datos, imágenes y documentos, de personas y entidades públicas. En base a esto se han creado herramientas capaces de proteger el software de otros softwares maliciosos que perjudiquen los sistemas y los operadores (Viewnext, 2018).

algunas amenazas son:

- Virus, gusanos y caballos de Troya
- Software espía y publicitario
- Ataques de día cero, también llamados ataques de hora cero
- Ataques de hackers
- Ataques de denegación de servicio
- Intercepción o robo de datos
- Robo de identidad

Hay que entender que no hay un sistema o software que garantice la seguridad de los sistemas y las redes, es por eso que se recomienda la actualización de los ordenadores de

manera constante, para que sean capaces de adaptarse a las nuevas amenazas que se presenten (Universidadviu, 2018). Los componentes de seguridad de red incluyen:

- Antivirus y antispyware
- Cortafuegos, para bloquear el acceso no autorizado a su red
- Sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación, como el día cero o cero horas ataques
- Redes privadas virtuales (VPN), para proporcionar acceso remoto seguro

En un informe (Tuyutechnology, 2017) habla de que no sólo es crucial saber qué es seguridad informática, sino también entender por qué es importante. Los hackers han evolucionado, por lo que las organizaciones y sus empleados deben saber qué es lo que está en riesgo.

La seguridad de los sistemas y de las redes informáticas es esencial en un mundo moderno como el nuestro fuertemente interconectado (de hecho, este período histórico se denomina la “era de la información”) y muchas de nuestras actividades diarias, para llevarse a cabo, usan las redes informáticas (CiC, 2017).

Proteger las redes informáticas, **es** absolutamente crítico y esencial. Es como construir una hermosa casa llena de acabados (servicios por internet) y dejar la puerta de servicio abierta (seguridad). Una idea no inteligente (D´adamo & Toscano, 2018).

Para (Sciencedirect, 2014), el resguardo de la información en centros educativos, técnicos, tecnológicos, universidades, e inclusive entidades de estado, son esenciales para prevenir el robo o alteración que ellos posean tanto de información personal, como de los factores que se involucran en su desarrollo.

Todo lo relacionado con información tantos los estudiantes y docentes en una institución, es blanco de interés para cibercriminales que quieran causar algún daño a estas personas esto fue explicado por “internet Security threat report Symantec” (Onasistems, 2019).

En un artículo de seguridad informática (Arguello, Medina G, & Caiceso E, 2015), explican cuáles son sus vulnerabilidades que presentan los centros educativos, tanto de la educación básica y la superior donde se ven afectados estudiantes, docentes administrativos, empleados y personas de fuera. Todos estos saqueos y robos de información se dan no sólo en computadores de escritorio, sino también en dispositivos de uso personal (tabletas, celulares portátiles entre otros.

Tomar el control en el ingreso a sitios web las configuraciones de los computadores y bloquear ventanas emergentes debe ser prioridad para poder garantizar el buen funcionamiento de los sistemas informáticos (Bmobile, 2019). El bloqueo de sitios de entretenimiento, redes sociales y sitios inapropiados, disminuye la distracción en las personas (Safedns, 2018).

QUÉ ASPECTOS BUSCA MEJORAR LA INSTITUCION.

Bajo rendimiento del internet: la ocupación o saturación de red, es uno de los problemas más frecuentes en los centros educativos y dificultad el buen procesamiento de los ordenadores y los sistemas (Gomar, 2019).

La vulnerabilidad en el sistema, permite tomar control de los antivirus: al no contar con un software apto para el bloqueo, contención y eliminación de los virus, los sistemas están en riesgo de daño o mal funcionamiento (Onaadmin, 2017).

Gestión de accesos: toda entidad pública y educativa debe tener control de quienes pueden acceder sacar información o modificar la misma, es decir, manejar registración de acceso, roles de seguridad y controlar los permisos, para la seguridad de su información (Oracle, 2012).

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades (Romero C, y otros, 2018). Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones (Tarazona, 2007).

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene (Incibe, 2017). Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan (Mintic, 2016).

TIPOS DE AMENAZAS

Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y; Actos maliciosos o malintencionados.

algunas de estas amenazas son: Virus informáticos o código malicioso, Uso no autorizado de Sistemas Informáticos, Robo de Información, Fraudes basados en el uso de

computadores, Suplantación de identidad, Denegación de Servicios (DoS), Ataques de Fuerza Bruta, Alteración de la Información, Divulgación de Información, Desastres Naturales, Sabotaje, vandalismo, Espionaje (Ieee, 2010).

El término “cibercrimen” se ha señalado que describe “el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (Hernandes, 2008).

Seguridad informática para colegios, instituciones públicas y privadas, trabaja con Ona Systems para implantar una solución en su institución de fácil implementación, y administración que lo ayuda a cumplir los principales problemas de cumplimiento de las normativas legales de ciberseguridad. Protección para endpoint, protección para servidores, protección para móviles, auditoría de seguridad y otras soluciones.

Resultados y discusión

Con base a lo anterior investigado, se puede deducir la calidad de la seguridad informática en el ITP, las falencias que posee y las posibles soluciones que se pueden implementar para mejorar la calidad de este. Según un artículo de políticas de seguridad informática en el ITP, se puede conocer cuáles son las estrategias y planes de control que deban implementarse, pero que hasta el momento no se han desarrollado ni llevado a cabo su implementación de manera óptima y completa, esto puede ocasionar el fácil acceso de terceros, a la información que se contenga en la base de datos.

La seguridad informática debe ser uno de los puntos claves a priorizar en un instituto de aprendizaje y prestador de servicios al público y del estado, pues su base de datos, contiene un gran número de información la cual es deseada obtener por personas y otras entidades, que quieran un beneficio o aprovechamiento de recursos datos personales y procesos que lleve el instituto, con la finalidad de extorsión, alteración o posibles destrucción o desvío de los mismos.

El poder brindar protección no solo a correos entrantes, es de gran importancia para el instituto; como medidas preventivas se deben implementar en cuanto a las redes son programas que garantizan el resguardo y protección de las contraseñas de los usuarios ante posibles robos de identidad, programas como bastpass, logdop, HTTPS everywhere, AVG privacyfix y digo.me (ante social safe), son buenas alternativas para estas acciones de resguardo y protección de los usuarios (Raimkhanov, 2016).

En cuanto a la protección de los ordenadores y los distintos programas que se contengan incluidos su base de datos, se hacer mencionar algunos de los cuales el ITP, mediante un análisis, pueda implementar en todos los ordenadores en el instituto, algunos de los cuales pueden ser: Windows defender Advance threat protection, enhanced mitigation experience toolkit, hitman pro y McAfee security scan plus, todos estos mencionados anteriormente, son capaces de crear barreras que impiden el fácil acceso a personal no autorizado además de troyanos, virus, software espías entre otros programas publicitario (Barbero, 2016).

Referencias bibliográficas

AgendaAPD. (2019). Tipos de seguridad informática: ¿Cuáles son y qué importancia tienen? *agendaAPD.*

recuperado de: https://bit.ly/335lLpo.

Arguello, J. D., Medina G, L., & Caiceso E, A. (2015). riesgos asociados a internet. *sites.* *recuperado de: https://bit.ly/35OtNDW*.

Barbero, I. M. (2016). Los cinco mejores programas para proteger tu ordenador. *betech.* *recuperado de: https://bit.ly/374Vryp*.

Bmobile. (2019). importancia de la seguridad informatica. *bmobile.*

recuperado de: https://bit.ly/324tPq6.

Bussinesmarketingschool. (2018). Tipos de seguridad informática, ¿cuáles existen? *bussinesmarketingschool.*

recuperado de: https://bit.ly/3fgjxIR.

CiC. (2017). La importancia de la Seguridad Informática en tu empresa. *cic.*

recuperado de: https://bit.ly/2HViUYL.

D´adamo, L., & Toscano, F. (2018). La seguridad de los sistemas y de la redes informáticas. *consulthink.*

recuperado de: https://bit.ly/3kDX75Z.

Destinonegocios. (2019). 3 tipos de seguridad informática que debes conocer al proteger tu empresa. *destinonegocios.*

recuperado de: https://bit.ly/3lVzIOo.

Dr., H. (2019). tipos de seguridad informatica: ¿cuales son y que importancia tienen? *hard2bit.*

recuperado de: https://bit.ly/35GYk6r.

Gomar, J. (2019). ¿internet lento?, las causas mas habituales. *tuexperto.*

recuperado de: https://bit.ly/321qEPV.

Hernandes, L. (2008). el delito informatico. *ehu.*

recuperado de: https://bit.ly/3kPGhBd.

Ieee. (2010). ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. *ieee.*

recuperado de: https://bit.ly/3egiyro.

Incibe. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? *incibe.* *recuperado de: https://bit.ly/2TJDkGM*.

Lopez, A. (2017). Seguridad informática: qué es y por qué es importante. *aitana.* *recuperado de: https://bit.ly/34Kzgfq*.

M, L. (2020). ¿que es seguridad informatica? *bitdegree.*

recuperado de: https://bit.ly/2Ga73Fy.

Mintic. (2016). Guía para la Implementación de seguridad de la informacion. *mintic.*

recuperado de: https://bit.ly/3jNRTDx.

Molinetti, S. (2019). Principales tipos de seguridad informática en las empresas. *ThinkBigEmpresas.*

recuperado de: https://bit.ly/2Hnotz6.

Obsbussinesschool. (2018). Tipos de seguridad informática más importantes a conocer y tener en cuenta. *obsbussinesschool.*

recuperado de: https://bit.ly/2IU8Uj8.

Onaadmin. (2017). la vulnerabilidad de los sistemas, permite tomar los antivirus. *onasystems.*

recuperado de: https://bit.ly/2JjI6Zj.

Onasistems. (2019). estrategias de ciberseguridad en instituciones. *onasystems.*

recuperado de: https://bit.ly/3mFgKv5.

Oracle. (2012). Guía de administración del sistema: servicios de seguridad. *oracle.* .

Raimkhanov, M. (2016). Cinco herramientas para proteger tus cuentas en las redes sociales. *ijnet.*

recuperado de: https://bit.ly/2JREApR.

Restrepo, S. A. (2009). HARDWARE 40115.

recuperado de: https://bit.ly/3kTrTqN. *hardware.*

Romero C, M., Figueroa M, G., Vera N, D., Alava C, J., Parrales , G., Alava, C., . . . Castillo M, m. (2018). introduccion a la seguridad informatica y el analisis de vulnerabilidades. *3ciencias.*

recuperado de: https://bit.ly/3mHAWfR.

Safedns. (2018). internet seguro para las instituciones y bibliotecas. *safedns.* *https://bit.ly/3oHHRHP*.

Sciencedirect. (2014). Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Sciencedirect.* *recuperado de: https://bit.ly/3jMqvWw*.

Securityinformacion. (2017). ventajas y desventajas de la seguridad informatica. *Securityinformacion.*

recuperado de: https://bit.ly/36PimMC.

Sgc. (2014). Manual de Normas y Políticas de Seguridad Informática . *sgc.* , 2.

Sofecom. (2018). Tipos de seguridad informática: Todo lo que necesitas saber. *sofecom.* *recuperado de: https://bit.ly/392j8Ze*.

Tarazona, C. (2007). amenazas informaticas y seguridad de la informacion. *Uexternado.* *recuperado de: https://bit.ly/3mI5CxH*.

Tuyutechnology. (2017). ¿por que es tan importante la seguridad informatica ? *tuyutechnology.*

recuperado de: https://bit.ly/3mJlMH3.

Universidadviu. (2018). Tres tipos de seguridad informática que debes conocer. *universidad internacional de valencia.*

recuperado de: https://bit.ly/3pQdaB0.

Viewnext. (2018). tipos de seguridad informatica. *viewnext.*

recuperado de: https://bit.ly/3lQvG9J.