593 Digital Publisher
CEIT
ISSN 2588-0705

Tecnología educativa de blockchain para prevenir ciberataques en ITSOEH

Blockchain educational technology to prevent cyberattacks in ITSOEH

Jesús Alberto García-Rojas[1]
Instituto Tecnológico Superior del Occidente del Estado de Hidalgo - México
jgarcia@itsoeh.edu.mx

Teresa de Jesús Vargas-Vega[2]
Instituto Tecnológico Superior del Occidente del Estado de Hidalgo - México
division_gempresarial@itesa.edu.mx

Raquel Rodríguez-Aguilar[3]
Instituto Tecnológico Superior del Occidente del Estado de Hidalgo - México
rrodriguez@itsoeh.edu.mx

Kenia Landeros-Valenzuela[4]
Instituto Tecnológico Superior de los Ríos - México
rrodriguez@itsoeh.edu.mx

doi.org/10.33386/593dp.2023.2-1.1702

V8-N2-1 (mar) 2023, pp. 136-152 | Recibido: 20 de enero de 2023 - Aceptado: 10 de febrero de 2023 (2 ronda rev.)
Edición Especial

1 Ingeniería en Gestión Empresarial
ORCID: https://orcid.org/0000-0002-0292-0789

2 Profesora certificada por la ANFECA. Consultora de las cátedras de Proyectos de Inversión, Análisis Bursátil y Taller de portafolios de inversión en la Universidad Autónoma del Estado de Hidalgo
ORCID: https://orcid.org/0000-0002-6051-7197

3 Ingeniería en Gestión Empresarial

4 Instituto Tecnológico Superior de los Ríos
ORCID: https://orcid.org/0000-0003-4561-0155

Cómo citar este artículo en norma APA:

García-Rojas, J., Vargas-Vega, T., Rodríguez-Aguilar, R., & Landeros-Valenzuela, K., (2023). Tecnología educativa de blockchain para prevenir ciberataques en ITSOEH. 593 Digital Publisher CEIT, 8(2-1), 136-152 https://doi.org/10.33386/593dp.2023.2-1.1702

Descargar para Mendeley y Zotero

RESUMEN

El ciberespacio se ha vuelto es considerado ya un lugar donde las personas pasan la mayor parte de su día a día, lo cual siempre se ve constantemente amenazado por la vulneración de la seguridad cuando se navega por internet, así como la lucha contra los anuncios publicitarios que siempre aparecen en nuestro navegador de internet.

La ciberseguridad que nació o se originó mediante los conocimientos técnicos sobre tecnología de hardware y software que pueden vulnerar la seguridad de los sistemas, se requiere cierto grado de conocimientos en informática para realizar ataques, que como consecuencia borran información, modifican o difunden causando daño al sujeto pasivo que puede ser cualquier persona que navegue en internet, es por ello que la ciberseguridad se ha vuelto un tema de seguridad nacional, pues ahí se realizan diariamente transacciones, compras y negocios en línea que mueven a diario cantidades millonarias, al alcance de solo un clic y una tarjeta de débito o crédito (Fernández, 2018).

Palabras clave: internet; educación; prospectiva; seguridad

ABSTRACT

Cyberspace has become considered a place where people spend most of their day to day, which is always constantly threatened by security breaches when browsing the Internet, as well as the fight against advertisements that always appear in our internet browser.

Cybersecurity that was born or originated through technical knowledge about hardware and software technology that can violate the security of systems, a certain degree of computer knowledge is required to carry out attacks, which as a consequence delete information, modify or spread causing damage to the a taxable person who can be anyone who browses the internet, which is why cybersecurity has become a national security issue, since there are daily transactions, purchases and online businesses that move millions of dollars daily, within the reach of only one click and a debit or credit card (Fernández, 2018).

Key words: internet; education; prospective; security

Introducción

Es por ello que en cuanto a las regulaciones internacionales que tratan el tema de la ciberseguridad y cibercriminalidad se encuentra con el Convenio de Budapest que se llevó a cabo en el 2001.

Asímismo existe aprobación internacional en cuanto a la vigilancia de conductas que pueden manejar los cibercriminales, sobre todo en la trata de personas y en el tráfico de armas, derivando en este acuerdo para evitar lo que se llama la guerra fría, donde se realice la delincuencia y gane el que tenga mejores conocimientos técnicos o informáticos para lograr hacer daño a las naciones (Domínguez, 2014).

El prefijo ciber ha sido muy utilizado desde el año 2000 a la fecha, por lo que siempre que está navegando en internet, o en contacto con una computadora, palabras como ciberbullying, ciberacoso, ciberdelito, ciber espionaje entre muchos otros, donde lamentablemente ya son palabras que han dado la vuelta al mundo donde se conocen virtualmente, hasta llegar a nosotros las personas de carne y hueso, o que además han sido víctimas de los delitos mediante tecnología, como el más común que es un cargo no reconocido en tarjeta de crédito (Flores, 2009).

La palabra ciber que se refiere al mundo virtual, al mundo digital, donde existen recursos valiosos como lo es la información, pero por otro lado también pueden llevar a un mal uso, como realizar actos de terrorismo, espionaje, es aquí a donde nos referimos al termino ciberespacio.

En este punto, cabe mencionar que existe el espacio marítimo, aéreo, terrestre, y demás espacios que existen físicamente, el termino ciberespacio nace de la creación humana donde lo que contienen puede variar en el transcurso del tiempo. Es así que Estados Unidos de América lo nombra como sistema nervioso pues tiene control de infraestructura físicas en cuanto al termino ciberseguridad (Domínguez, 2014).

A final de cuentas el ciberespacio está compuesto físicamente por medios físicos de telecomunicación como son switchs, routers, cable ethernet, cable de fibra óptica, los cuales se interconectan y comunican entre sí, es aquí donde se almacena información importante y de seguridad nacional, que no pueden ser vulnerados, pues se perdería el equilibrio de la nación (Fonseca, 2019).

Internet tiene un papel fundamental, pues es el alma del ciberespacio, donde millones de páginas son albergadas o guardadas, páginas de venta al público, páginas de información, páginas de empresas privadas, páginas de información personal, escuelas en línea, por lo que internet es la manera de poder visitar dicha información, realizar negocios, y muchas operaciones más, un ciudadano puede conectarse desde su smartphone con datos o desde su computadora o cibercafé, desde un aeropuerto, cualquier lugar.

Con la pandemia que hemos vivido o estamos viviendo, no cabe ninguna duda que no hay barreras de tiempo o distancia para acercarnos como personas, ya que con un dispositivo electrónico y conexión a internet se podían hacer conexiones en vivo mediante la plataforma Zoom, Meet, por mencionar algunas.

Escribiendo en términos de tiempo no fue hasta el año de 1999 cuando la OTAN (Organización del Tratado del Atlántico Norte) reconoció lo que es un ciber ataque debido a una operación de las fuerzas aliadas en Kosovo.

En la actualidad, de acuerdo al apartado de Estrategia y gobernanza, de la biblioteca digital del Centro de Excelencia de la Ciberdefensa Cooperativa (CCDCOE Tallin por sus siglas en inglés), centro integrado por 28 países, acreditado por la OTAN y a su servicio, que presenta estrategias de seguridad y defensa nacional, ENCS (Estrategia Nacional de Ciberseguridad), legislaciones nacionales, y declaraciones de derecho internacional vinculadas a la seguridad cibernética, un total de 77 naciones del mundo han creado documentos de ciberseguridad con un enfoque centrado en la seguridad del Estado-Nación, entre las que se incluyen miembros de la OTAN, aliados

Digital Publisher CEIT ISSN 2588-0705

estratégicos de esta alianza, países de África, América Latina, el Caribe, Asía y Oceanía.

En la mayoría de las naciones europeas existen normas similares, y a todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

El derecho penal de los estados interesados en combatir esta nueva delincuencia, contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra sistemas de información perpetrados por particulares. La aproximación del derecho positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que todas las formas de ataque contra los sistemas de información puedan ser objeto de investigaciones mediante técnicas y métodos disponibles en derecho penal.

Los autores de estos delitos deben de ser identificados y llevados a juicio y los tribunales deben disponer de sanciones adecuadas y proporcionadas. Se enviará, así como un claro mensaje disuasivo de ataques contra los sistemas de información. Además, los vacíos jurídicos y las diferencias pueden impedir una cooperación policial y judicial eficaz en caso de ataques contra sistemas de información.

Estos ataques son transnacionales por su propia naturaleza y requieren una cooperación internacional y garantizará que se cumpla la exigencia de doble incriminación (según la cual una actividad debe constituir un delito en los dos países en cuestión para que éstos colaboren a nivel judicial en el marco de una investigación penal).

Desde hace aproximadamente 10 años la mayoría de los países europeos ha hecho todo lo posible para incluir dentro de la ley la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interpretación de mensajes informáticos.

En la mayoría de las naciones occidentales existen similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concentrada.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aun en países como Argentina, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales (Acurio, 2005).

En Argentina aún no existe específica sobre los llamados delitos informáticos. Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la Ley 11.723 de propiedad intelectual gracias al Decreto N° 165/94 del 8 de febrero de 1994. En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran

Bretaña, Holanda, Francia, España, y Chile. Estados Unidos adoptó en 1994 el Acta Federal de Abuso Computacional, que modificó el Acta de Fraude y Abuso Computacional de 1986.

Alemania sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos: a) espionaje de datos; b) Fraude de informático; c) alteración informática.

En Austria, la Ley de reforma del código Penal, promulgada el 22 de diciembre de 1987, en el artículo 148, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de la elaboración automática de datos, a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

Debido a un caso de hacking en 1991, comenzó a regir en Gran Bretaña la Computer Minuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado hasta con cinco años de prisión o multa. Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

En Holanda, en marzo de 1993, entró en vigencia la Ley de Delitos Informáticos, en el cual se penaliza el hacking, el preacking (uso de servicios de telecomunicaciones para evitar el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus, la cual está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

En enero de 1998 Francia dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses de dos años de prisión y multas de 10 mil a 100 mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta internacional y a sabiendas de estar vulnerable los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte, el artículo 462-4 también incluye en su tipo penal una conducta internacional y a sabiendas de vulnerar los derechos de terceros, en forma directa o indirecta, haya suprimido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloroso y pena al mero acose, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento de éste (sabotaje) (Garavilla, 2001).

Por último, el artículo 264-2, del Nuevo Código Penal de España, establece que se aplicará la pena de prisión de uno a tres años y multa…. a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Este código sanciona en forma detallada esta categoría delictiva (violación de secretos/ espionaje/divulgación), aplicando pena de prisión y multa, agravándolas cuando existe intención dolosa y cuando el hecho es cometido por parte de funcionarios públicos se penaliza con inhabilitación, En materia de estafas electrónicas, en su artículo 248 sólo tipifica aquéllas con ánimo de lucro, valiéndose de laguna ,manipulación informática, sin detallar las penas a aplicar en el caso de comisión del delito.

Chile fue el primer país latinoamericano en sancionar una ley contra delitos informáticos,

Digital Publisher CEIT ISSN 2588-0705

la cual entró en vigencia el 7 de junio del 1993. Esta ley se refiere a los siguientes delitos:

La destrucción o inutilización de datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

La ciberseguridad se ha convertido en un aspecto relevante en el mundo pues cada vez se producen más ciberataques que pueden crear grandes problemas a empresas, organismos públicos y particulares, las implicaciones económicas de los ciberataques no son menores, algunos estudios cifran las pérdidas globales por virus maliciosos en 350.000 millones de euros, sobre el particular las Naciones Unidas, la Unión Europea y el G8 han realizado diversas iniciativas destinadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la delincuencia cibernética, en noviembre del 2001 los estados miembros del consejo de Europa firmaron el convenio sobre ciberdelincuencia en Budapest, dicho convenio reconoce la necesidad de cooperación entre los estados y el sector privado en la lucha contra la ciberdelincuencia, así como proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información, actualmente México se encuentra como observador del convenio de budapest y de manera formal ha sido invitado a adherirse al mismo, inclusive el Congreso la Unión ha exhortado en diversas ocasiones a la Secretaria de Relaciones Exteriores iniciar trabajos necesarios para la adhesión de México al convenio, de acuerdo a los datos de la encuesta nacional sobre disponibilidad y uso de tecnologías de la información de los hogares en México, hay más de 84 millones de usuarios de internet actualmente México ocupa los primeros lugares a nivel mundial de los países más afectados por los ciberataques, siendo el año 2020 uno de los más relevantes, pues hackers atacaron la página la Secretaria de Economía, y “anonimous” atacó la página del Banco de México y amenazó a la Secretaría de Hacienda y Crédito Público, así mismo durante ese año el costo por los ciberataques en México creció en 38.4 %, en cuanto a los antecedentes de la ciberseguridad en México encontramos que en 1999 se reformó el Código Penal Federal añadiéndosele el capítulo acceso ilícito a sistemas y equipos de informática que comprendían los artículos 211 bis 1 al 211 bis 7, a partir de dicho antecedente se han dado diversos avances legislativos en materia de ciberseguridad, los más relevantes son los siguientes, el 12 de abril del 2005 se presentó una iniciativa que reforma adiciona y deroga diversas disposiciones del Código Penal Federal del Código Federal de Procedimientos Penales de la Ley Federal contra la delincuencia organizada y de la ley de la Policía Federal Preventiva en materia de delitos cibernéticos y de delitos contra menores, el 28 de marzo de 2012 se presentó un proyecto para reformar y adicionar diversas disposiciones del Código Penal Federal en materia de delitos en contra de medios o sistemas informáticos, el 2 de octubre del 2015 se presentó la iniciativa para expedir la Ley Federal para prevenir y sancionar los delitos informáticos impulsada por el senador Omar Fayad, 19 de marzo el 2019 se presentó una iniciativa impulsada por la senadora Jesús Lucía Trasviña para expedir la Ley de Seguridad Informática, el primero de septiembre del 2020 se presentó la iniciativa para expedir la Ley General de Ciberseguridad impulsada por el senador Miguel Ángel Mancera y el 25 de marzo del 2021 se presentó una iniciativa de la senadora Jesús Lucía Trasviña para expedir la Ley General de Ciberseguridad, en términos de lo previsto en el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos cada una de las entidades federativas a su libre elección y autonomía han legislado sobre diversos temas informáticos digitales y cibernéticos comenzando con equiparar los delitos tradicionales con agravantes por uso la tecnología y medios de comunicación, esto lo encontré en cada uno de

los códigos penales de las entidades federativas, México es un país con demasiadas instituciones y un gran catálogo de leyes que quizá nadie las conozca en su totalidad, sin embargo en materia federal podemos señalar que estas son las leyes más importantes que contienen ordenamientos en materia de ciberseguridad, para finalizar me gustaría señalar que el espacio cibernético es muy diferente al real, estamos hablando de un mundo inmaterial e intangible, lo cual quiere decir que el modus operandi es totalmente diferente a los delitos tradicionales, por lo cual un delincuente informático en cuestión de segundos podría estar violando las legislaciones de más de 40 países, estos delitos traspasan muros, por lo que crean conflictos y colisiones entre las diversas leyes de los países afectados o implicados en las conductas delictivas, haciendo que cada legislación y convención haga su propia investigación nacional por los mismos hechos, es por eso que debería existir un orden que abarque la totalidad de enjuiciamiento de los hechos cometidos en todas las naciones evitando sentencias contrarias y penas duplicadas (Trasviña, 2019).

Por último, se expide la Ley General de Ciberseguridad donde se derogan varias disposiciones del Código Penal Federal, dicha iniciativa fue propuesta por Jesús En dicha Ley de Ciberseguridad propuestas por Lucía Trasviña Waldenrath, senadora.

Método

La metodología para llevar este proyecto de intervención sobre "Propuesta de ciberseguridad mediante blockchain para evitar los ciberataques en el ITSOEH" fue la deductiva, que se desarrolla de lo general a lo particular, se estuvieron revisando algunos procedimientos para proteger la información, recientemente en ITSOEH se ha lanzado una campaña de respaldos que promueve lo siguiente:

Se utilizó una muestra de 324 de un total de 2600 alumnos, profesores, directivos, en promedio que tiene actualmente el ITSOEH matriculados, para ello se calculó una muestra con respecto a la metodología de investigación cuantitativa. Esta encuesta permitió ver el grado de pertinencia e importancia que tiene el presente proyecto de intervención para la comunidad educativa, la cual tuvo un buen recibimiento, se menciona que se contempló un 99% de nivel de confianza y un 7% en el margen de error, resultando en 300, con lo cual se superó la meta con 324 encuestas aplicadas, y con un fuerte grado de efectividad, del 12.4% de la población total del ITSOEH encuestada (Hernández, 2014).

Figura 1

Cálculo de muestra.

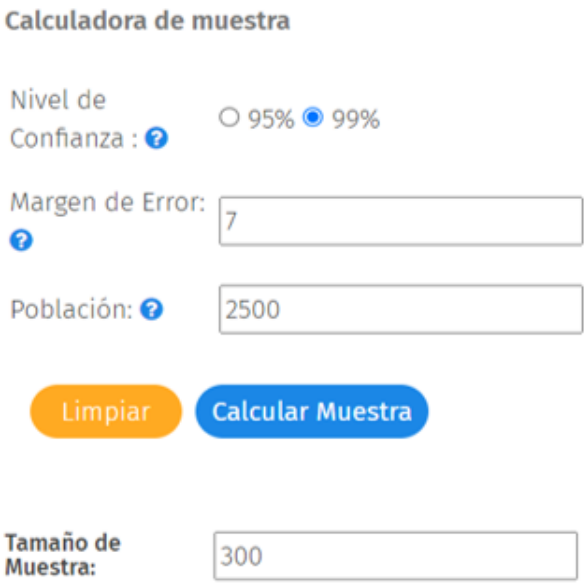
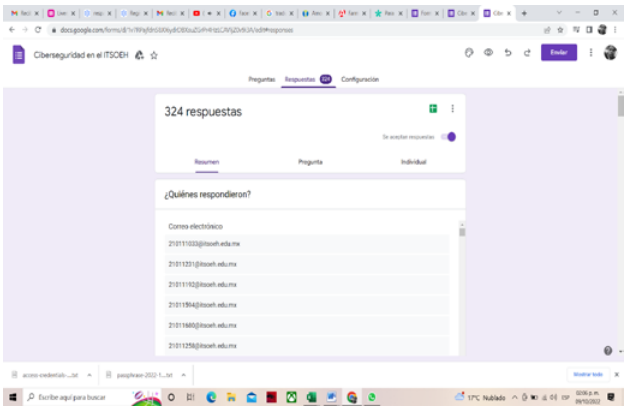


Figura 2

Encuestas contestadas de ciberseguridad en el ITSOEH.



Dentro de la metodología deductiva, se fue trabajando desde información general a lo particular, resultando en el análisis de

593 Digital Publisher CEIT ISSN 2588-0705

diversas lecturas y proyectos que ocupan la tecnología blockchain pero en otras áreas además de la educación, con lo cual se pudo valorar diversas herramientas y experiencias que hicieron resultante optar por la tecnología de Storj, misma que maneja la tecnología de blockchain para proteger la información con alta seguridad a toda la información que se encuentre albergada en ese sitio, con un precio accesible con respecto a la competencia.

Así mismo en las leyes se hizo una revisión de la documentación normas y leyes que regulan los ciberdelitos en el mundo y en México, para poder difundir las posibles sancionen en la que pueden incurrir los ciber delincuentes, por lo que es conveniente capacitar a toda la comunidad educativa.

Desarrollo

Proveedores de blockchain

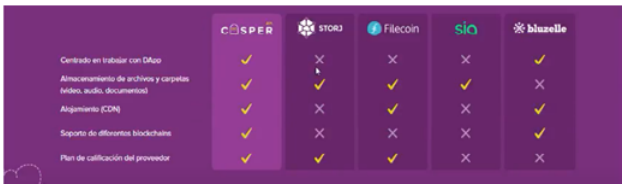
Existen múltiples proveedores de almacenamiento y protecciones basadas en blockchain, en este apartado se mencionarán las bondades de la API o interfaz de usuario, denominado "Casper", que maneja almacenamiento en la nube.

El servicio principal que ofrece "Casper" es el almacenamiento descentralizado de datos, incluyendo la carga, descarga, edición, borrado, gestión de permisos, función de lectura aleatoria de archivos, modificación de datos no cifrados sin sustituirlos, así como la posibilidad de montar su almacenamiento virtual como una unidad externa. El sistema de archivo de datos descentralizado reduce posibles retrasos y aumenta la accesibilidad, lo que significa que todos los datos son accesibles las 24 horas al día y los 7 días a la semana.

La plataforma API de Casper tiene la opción a diferencia de sus competidores como Storj, Filecoin, SIA, bluzelle, de guardar carpetas, videos, audios, documentos, entre muchos otros.

Figura 3

Comparación de API para almacenamiento en la nube mediante la tecnología blockchain.

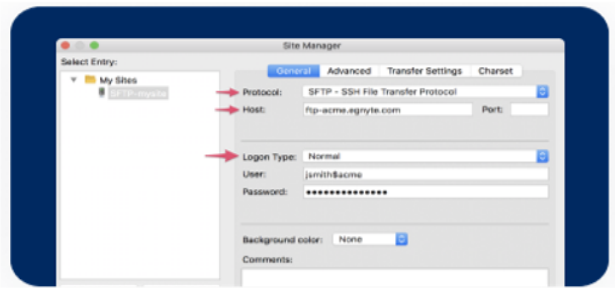


Fuente: (Casperproject, 2022).

Además, servicios como Dropbox, Google Drive y Mega ofrecen almacenamiento gratis hasta una determinada capacidad. Si el usuario requiere una capacidad de almacenamiento mayor a tal límite, debe pagar una cierta tarifa. En el caso de Dropbox, esta plataforma permite almacenar 2 GB de forma gratuita, pero si el usuario requiere 1 TB de almacenamiento, deberá pagar 10 dólares mensuales. En contraste, la blockchain de Sia tiene una tarifa mensual de tan solo $0.31 dólares por 1 Terabyte y si fuera con banda ancha que es mucho más rápido cuesta $7 dólares el mes por terabyte. En este sentido la plataforma de Sia, es la mejor opción pues permite crear respaldos, los beneficios es que con este espacio de un tb=1000 gb, es suficiente espacio, para que todos los departamentos del ITSOEH suban su respaldo, además con la gran ventaja de la interfaz de usuario como es fillezilla, que es un programa que he utilizado para crear páginas web, ahora mediante el protocolo SFPT (Transferencia de archivos con protocolo de seguridad), permite que se tengan respaldos en varios lados del mundo con copias de la información cifrada, con único acceso a visualizarla a sus propietarios, es muy sencillo el uso del programa Filezilla (Figura 2), únicamente se ingresa la dirección del servidor, se arrastra la carpeta que se va a respaldar, no importando el tamaño hacia la carpeta destino y se envía o sube la información, inmediatamente la información se duplica en varios servidores, por si alguno fallara, pueda haber una copia de la información, con esto parece algo sencillo, pero se pueden levantar servidores de correo, de sistemas educativos, financieros, académicos, para que la institución pueda seguir operando.

Figura 4

Interfaz Fillezilla para respaldos SFTP y Sia.

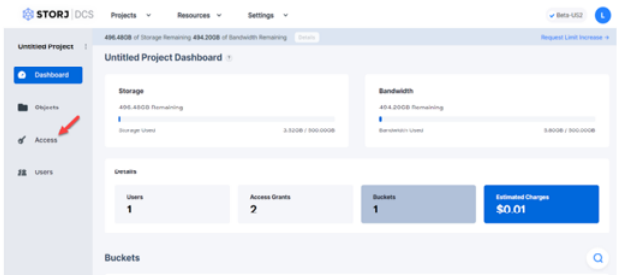


Fuente: (STORJ, 2022).

En conclusión, un administrador en el ITSOEH o varios administradores seleccionan las carpetas que se respaldaran (Figura 3).

Figura 5

Interfaz Sia usuarios activos y espacio disponible.

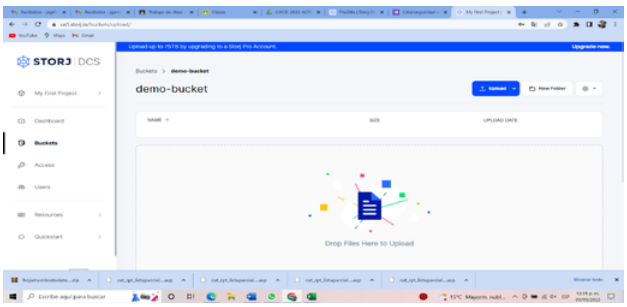


Fuente: (STORJ, 2022)

Cada persona encargada del resguardo o respaldo hace la copia de la información, se puede de 2 formas, una mediante Filezilla o mediante la página web de Sia, en la plataforma Sia igual es sencilla pues marca cuantos gigabytes quedan disponibles para respaldar, únicamente se sube la carpeta con la información y queda respaldada de forma segura (Figura 4).

Figura 6

Subiendo información de respaldo a plataforma web Sia.



Fuente: (STORJ, 2022)

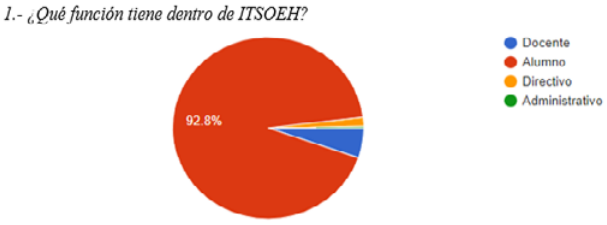
Resultados

Encuesta

Dicha encuesta fue desarrollada mediante la plataforma Google Forms apoyándome de las TIC a personal docente, administrativo y alumnado del ITSOEH.

Figura 7

1.- ¿Qué función tiene dentro de ITSOEH?

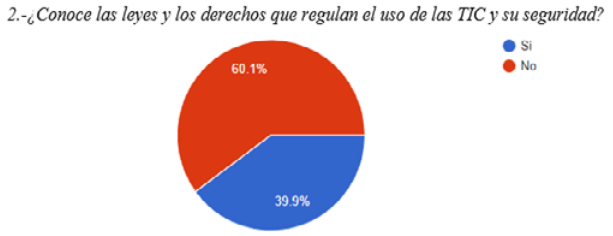


La figura 7 se muestra los resultados obtenidos de la pregunta 1 donde se pregunta sobre que función tiene desarrollando en El Instituto Tecnológico Superior del Occidente del Estado de Hidalgo (ITSOEH), sin embargo un 92.8% representan a los alumnos, un 5.4% representa a los docentes, el 1.6% a los directivos y finalmente el 0% fue el personal administrativo de acuerdo a los resultados arrojados de la encuesta en el plantel, se puede apreciar que gran parte de la comunidad de ITSOEH que respondió a la encuesta fueron alumnos.

593 Digital Publisher CEIT ISSN 2588-0705

Figura 8

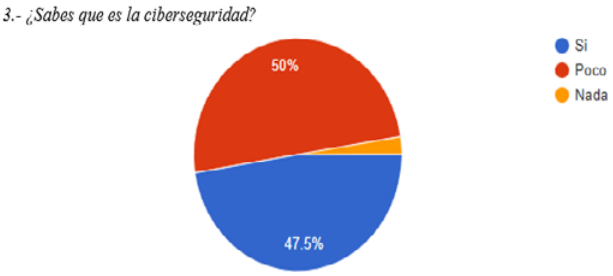
2.-¿Conoce las leyes y los derechos que regulan el uso de las TIC y su seguridad?



La figura 8 se muestra los resultados obtenidos de la pregunta 2 donde se pregunta si tienen algún conocimiento sobre las leyes y los derechos que regulan el uso de las TIC y la seguridad que brinda en donde se puede apreciar que un 60.1% tienen el conocimiento sin embargo el 39.9% no tienen ningún conocimiento alguno sobre las TIC y la seguridad que esta misma da.

Figura 9

3.- ¿Sabes que es la ciberseguridad?



La figura 9 se muestra los resultados obtenidos de la pregunta 3 donde se pregunta si tienen algún conocimiento sobre las leyes y los saben que es la ciberseguridad en donde podemos visualizar que un 50% tienen poco conocimiento sin embargo el 47.5% cuentan con el conocimiento, pero un 2.5% no cuenta con los conocimientos requeridos en base el tema de ciberseguridad, por lo tanto, de esta pregunta se concluye que hay más parte de la comunidad que conocen muy poco sobre el tema.

Figura 10

4.-¿Qué tipo de ciberataque o daño en su equipo de cómputo?

La figura 10 se muestra los resultados obtenidos de la pregunta 4 donde se pregunta sobre qué tipo de ciberataque ha sufrido o algún daño en su equipo de cómputo podemos observar que un 31.3% ha tenido perdida de información, el 27.5% han sido sus contraseña, un 15.3 % ha sido la difusión de datos personales o un uso mal intencionado, el 9.1% han tenido daño físico y/o de hardware, el otro 10% fueron datos del portapapeles y un 5.3% fueron sus capturas de pantallas y grabaciones de pantallas de la webcam y finalmente un 1.6% han tenido otros ataques sin embargo con los resultados arrojados en la encuesta fue el 31.3% que han sufrido la pérdida de información a causa de los ciberataques.

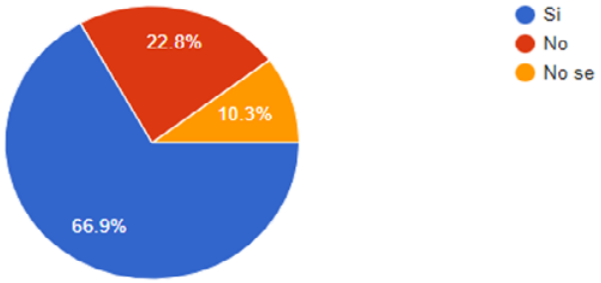
Figura 11

5.- ¿Con que frecuencia sueles actualizar un software antivirus?

En la figura 11 se muestra el resultado de la pregunta 5, donde se pregunta qué frecuencia sueles actualizar un software antivirus de acuerdo con la encuesta en el ITSOEH, el cual es un 37.5% cuando recuerdo, un 18.8% nunca, 35% se le hace actualmente y un 8.8% al menos una vez a la semana, con lo cual la mayor parte suelen actualizar su software antivirus cuando recuerda de acuerdo con las 320 respuestas arrojadas.

Figura 12

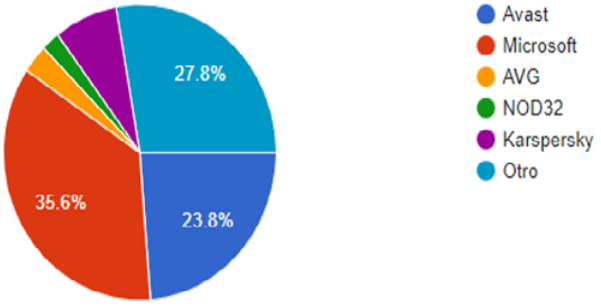
6.- ¿Cuenta con algún software de antivirus instalado en tu computadora?



En la figura 12 se muestra el resultado de la pregunta 6, donde se pregunta ¿Cuenta con algún software de antivirus instalado en tu computadora?, de acuerdo con la encuesta en el ITSOEH, el cual un 66.9 % si tiene, 22.8% no cuenta y un 10.3 no sabe, con la que la mayor de 313 cuenta con una computadora instala con un software de virus.

Figura 13

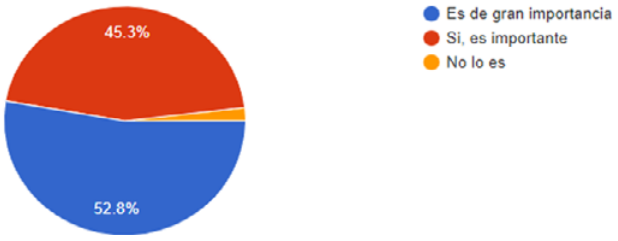
7.-¿Qué software de antivirus sueles utilizar?



En la figura 13 se muestra el resultado de la pregunta 7, donde se pregunta qué software de antivirus suelen utilizar, sin embargo 35.6 % utiliza Microsoft, 23.8 % Avast y un 27.8 % suele utilizar otra aplicación de acuerdo con la encuesta en el ITSOEH, la gran mayoría de estudiantes y docentes suelen utilizar software antivirus Microsoft.

Figura 14

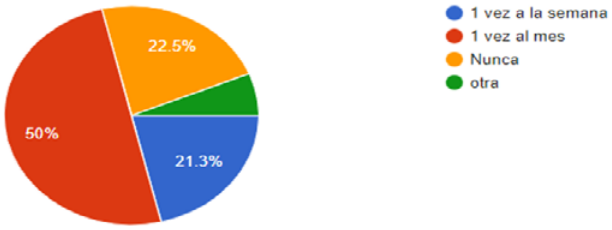
8.-¿Para ti es importante que se aplique ciberseguridad?



En la figura 14 se muestra el resultado de la pregunta 8 donde se pregunta si es importante que se aplique ciberseguridad, sin embargo 52.8% es de gran importancia ,45.3% si, es importante y un 2% no lo es, de acuerdo con la encuesta en el ITSOEH, se puede apreciar que de gran importante que se aplique la ciberseguridad ya que es más asegurable.

Figura 15

9.- *¿Con que regularidad realizas respaldos de información?*

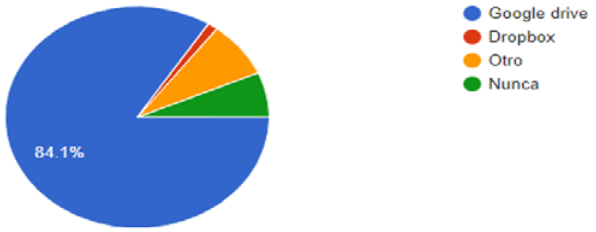


En la figura 15 se muestra el resultado para la pregunta 9, donde se pregunta qué función tiene quien llena la encuesta en el ITSOEH, el cual es un 50% de estudiantes, un 22.5% docentes y un 21.3% directivos, con lo cual se llena en proporción ya que la cantidad de alumnos en el ITSOEH supera los 2800 alumnos, de docentes son 150, y directivos un 2% que son 5 personas de las 50 que dirigen a nivel institucional.

593 Digital Publisher CEIT ISSN 2588-0705

Figura 16

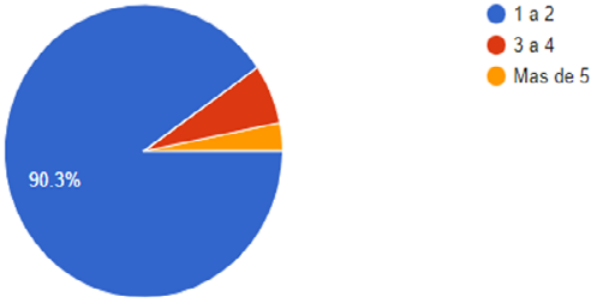
10.- ¿Utilizas algún servidor de almacenamiento en la nube?



En la figura 16 se muestra el resultado para la pregunta 10, donde se pregunta que usted considera que su información de trabajo puede ser susceptible a un ciberataque el cual es un 84.1% de estudiantes, un 25.9% docentes y directivos, con lo cual se llena en proporción ya que la cantidad de alumnos en el ITSOEH supera los 2800 alumnos, de docentes son 150, y directivos un 2% que son 5 personas de las 50 que dirigen a nivel institucional.

Figura 17

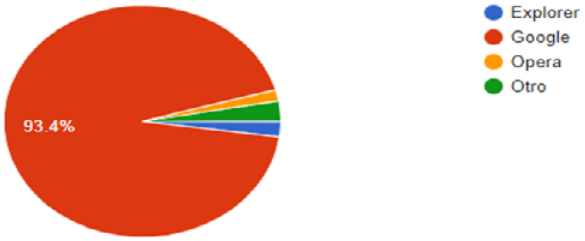
11.- ¿Cuántas veces ha sufrido un ciberataque?



En la figura 17 se muestra el resultado para la pregunta 12, donde se pregunta qué ¿Cuántas veces ha sufrido ciberataque?, el cual es un 90.1% de estudiantes, un 6.7% docentes y un 4% directivos, con lo cual se llena en proporción ya que la cantidad de alumnos en el ITSOEH supera los 2800 alumnos, de docentes son 150.

Figura 18

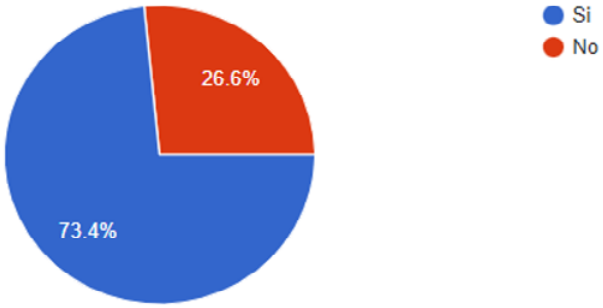
12.- ¿Qué navegador web utilizas normalmente?



En la figura 18 se muestra el resultado para la pregunta 11, donde se pregunta ¿Que navegador web utilizan normalmente? , el cual es un 93,4% de estudiantes y el 2.2% de Explorer y un 1.6% de Opera, y el 2.8% de otro, con lo cual se llena la proporción ya que la cantidad de alumnos es mayor a 2800, docentes son 150, y directivos un 2% que son 5 personas de las 50 que dirigen a nivel institucional.

Figura 19

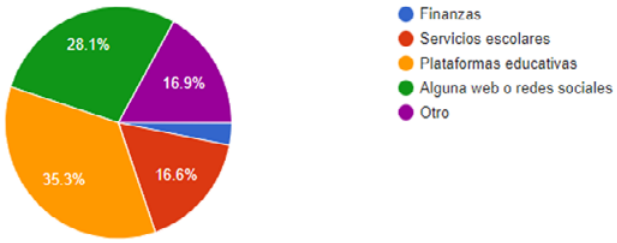
13.- ¿Usted considera que su información de trabajo puede ser susceptible a un ciberataque?



En la figura 19 se muestran los resultados para la pregunta 13,. ¿Usted considera que su información de trabajo puede ser susceptible a un ciberataque?, donde un 73.4% considera que su información si esta vulnerable y puede ser susceptible a un ciberataque, contra un 26.6% que considera que su información está segura, la mayoría de los encuestados considera necesario fortalecer la ciberseguridad de la información en el ITSOEH.

Figura 20

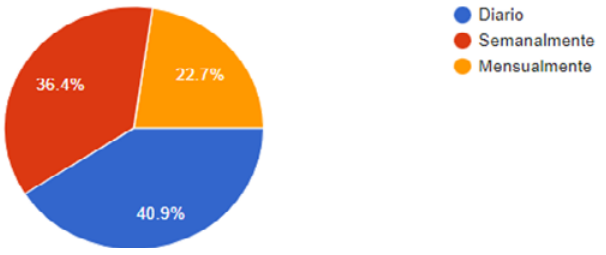
14.-*¿Le ha fallado algún sistema de información escolar?*



En la figura 20 se ve reflejado el resultado para la pregunta 14, donde pregunta si han existido fallas con la información escolar en su sistema del ITSOEH, esto permite visualizar que los encuestados tiene un 35.3% que son los que han tenido fallas en las plataformas educativas, un 28.1% los cuales se les ha encontrado fallas en alguna web o redes sociales, un 16.9% que han tenido fallas en otros, un 16.6% que corresponde a fallas en servicios escolares y un 3.1% lo llegan a tener en las finanzas.

Figura 21

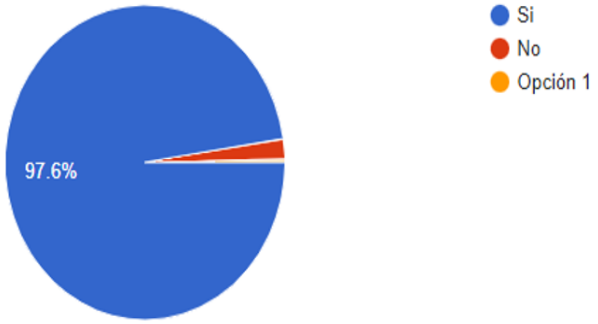
15.- ¿Con que frecuencia le gustaría que su información fuera respaldada?



En la figura 21 se ve reflejado el resultado para la pregunta 15, donde pregunta la frecuencia que les gustaría que su información sea respaldada, esto nos permite visualizar que los encuestados tiene una preferencia del 40.9% que son a los que les gustaría diariamente, un 36.4% lo prefiere semanalmente y un 22,.7% lo desea mensualmente.

Figura 22

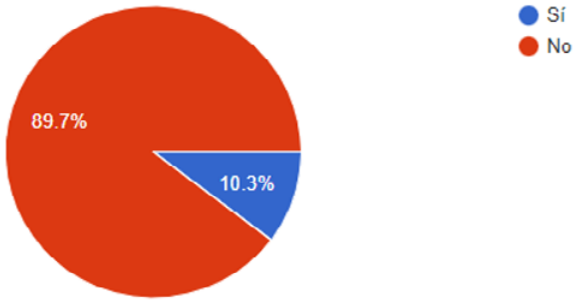
16.-¿Le gustaría que su información fuera respaldada de forma segura con varias copias donde solo tu pudieras acceder a la misma, evitando un ciberataque?



En la figura 22 se ve reflejado el resultado para la pregunta 16, donde pregunta si les gustaría que su información fuera respaldada de forma segura con varias copias donde solo tú pudieras acceder a la misma, evitando un ciberataque, esto nos permite visualizar que los encuestados tiene una preferencia del 97.6% a qué si les gustaría y un 2.4% que no les gustaría.

Figura 23

17.- ¿Ha escuchado acerca de la tecnología blockchain?



En la figura 23 se ve reflejado el resultado para la pregunta 17, donde pregunta si han escuchado acerca de la tecnología blockchain, esto nos permite visualizar que los encuestados tienen un 89.7% los cuales si han escuchado dicha tecnología y un 10.3% lo que corresponde a los que no la han escuchado.

En la pregunta 18, ¿Ha sufrido algún tipo de ciber amenaza? *Coméntenos su situación, fue una pregunta abierta, donde de

593 Digital Publisher CEIT ISSN 2588-0705

las 320 respuestas, 2.5% robo de información, 2.5% hackeo en sistemas o redes sociales, 95% de la población, donde el porcentaje es minimo, pero con el crecimiento del uso de computadoras en el sector academico o estudiantil, estaran en crecimiento en el futuro, por lo que es necesario prevenir fortaleciendo los mecanismos de ciberseguridad en el ITSOEH.

Conclusiones

Es contundente pensar en este tipo de proyectos, pues al observar el desarrollo, legalidad y utilidad, en pleno crecimiento del tamaño de la información que se maneja diariamente, y no solo pensando como institución, sino como cualquier ciudadano, todos manejan gran cantidad de información y no nos damos cuenta que tan vulnerables somos, en las darknet redes al mero estilo del mercado negro, donde se trafican drogas, personas, órganos, datos bancarios, cuentas de video entre mil cosas más, por lo cual es prioritario velar la seguridad de la información que manejamos día a día, por lo que es necesario prestar atención, asegurar que nuestros datos estén completos, no están difundidos en sitios que puedan vulnerarlos, la cuestión más simple de protección sería un antivirus, configurar un firewall, tener un software para evitar el spyware, un software anti spam o correos basura, ya que por estos medios y muchos otros más donde los ciberdelincuentes con inteligencia y manejo de las TIC quieren aprovecharse de personas que no tienen los conocimientos técnicos, o que simplemente no les gusta la computación, es por ello preponderante capacitar a todo el personal del ITSOEH incluido alumnos, para poder garantizar un tráfico seguro, que permita dar un mejor servicio con calidad educativa.

El hueco que queda afrontar es el de la seguridad de los sistemas informáticos, pues el respaldar la información en la nube no garantiza la privacidad de la información, así como su posible perdida, ya que estos sitios de almacenamiento en la nube, son limitados en su versión gratuita hasta 15 gb que permiten guardar, pero en cantidades mayores habría que comprar almacenamiento, y aunque el recurso económico sea limitado, no es la mejor opción pues blockchain tiene una mejor seguridad debido a que es una red de confianza entre los integrantes, mismos que deben validar cualquier cambio a la información, más aparte el respaldo de la información se encripta, pero sobre todo el mayor valor radica en que el almacenamiento de la información se guardar de forma descentralizada en varios puntos geográficos en el mundo, mas aparte quien alberga la información no podrá visualizarla sino tiene las credenciales pertinentes, con lo cual es la mejor opción en el mercado hoy en día, y muchas instituciones privadas y públicas y de cualquier giro están cambiando a esta medida de ciberseguridad para hacer frente a los ciberdelincuentes.

Quién hoy en día no ha sufrido un ataque informático, el cual daña los equipos de cómputo, estropeando su funcionamiento, perdiendo información, perdiendo tiempo de trabajo el cual nos resta productividad, y es tiempo muerto y perdido que no regresa, no se debe esperar a que pasen cosas desagradables con la información, sino actuar, este modelo de seguridad es una innovación en el ámbito educativo que bien tendría cabida en ITSOEH y en cualquier institución educativa de México, siempre respetando el marco legal que puede entrar en acción en caso de violación de la información, no cabe duda que en México existe un largo camino que recorrer.

Resulto contundente la tendencia en la comunidad educativa, docentes, alumnos, directivos, en el cual tuvo gran aceptación para poder implementar la tecnología de blockchain para poder prevenir violaciones a la red del ITSOEH en cuanto a la ciberseguridad, ya que la mayoría que ha sufrido intrusiones por virus en sus equipos, incluso perdiendo la información, o el funcionamiento adecuado en cuanto a hardware por lo que la hipótesis se acepta “una propuesta de ciberseguridad mediante blockchain impactaría en la evasión de los ciberataques en el ITSOEH”, dado las bondades de blockchain en cuanto a criptografía, respeto a la privacidad y respaldo descentralizado, se impactaría drásticamente en la reducción de ciberataques para la protección de servidores y equipos informáticos de toda la comunidad educativa del ITSOEH, en el sentido legal se hizo una revisión de las leyes que aplican

para sancionar a ciberdelincuentes a nivel internacional y nacional, por lo que comparando a México con países europeos, se tiene un retraso impactante, así como países latinoamericanos, en cuanto a la vulnerabilidad, se tiene un gran trabajo ya que todas las áreas operativas del ITSOEH corren el riesgo de ser atacadas, ya que existen múltiples maneras, si la red institucional tiene puertos abiertos o huecos de seguridad que es por donde entran los ciberataques, en cuanto a las tecnologías se revisó que blockchain tiene un gran auge en la actualidad y muchas instituciones a nivel internacional están adoptando esta tecnología, por lo que es recomendable también sugerir capacitación en cuanto a ciberseguridad y blockchain en toda la comunidad educativa, una difusión permanente y personal dedicado a esta importante labor, como lo es la seguridad, ya que la información es el activo más importante del ITSOEH y por esa simple razón vale la pena invertir tiempo de configuración y recurso económico, legalmente y operativamente es funcional para la mejora sustantiva de la ciberseguridad en el ITSOEH.

Por ultimo haciendo un ejercicio económico como si fuera el pago de un seguro por tener la información integra por año se pagarían en la cuenta de banda ancha o rápida el total $84 dólares por año, dando un promedio de $2000 pesos mexicanos en promedio de pago por tener la información segura es una ganga, para hacer permanente el uso de esta plataforma como es Storj, donde se puedan prevenir ciberataques, la hipótesis se acepta, la integración de blockchain para poder prevenir ciberataques, ya que al tener información descentralizada, triplicada, y encriptada a buen costo, puede ayudar significativamente a dar un servicio de calidad a la comunidad educativa, así como en las encuesta se puedo constatar la gran pertinencia del proyecto, habiendo afectados por ciberataques. En cuanto a la viabilidad técnica que concluye este proyecto de intervención denota que es factible implementar el proyecto de prevención para protegerse contra posibles ciberataques con la tecnología blockchain, pues esta tecnología es de bajo costo, y sobre todo es de fácil operación, donde básicamente se tienen que subir los archivos a plataforma en línea, con esto los sistemas de información, bases de datos, documentos importantes o académicos no van a poder ser atacados por la ciberseguridad en red y descentralizada y de confianza que maneja blockchain, es lo que se busca pues en una pérdida de información de se puede recuperar rápidamente, en el ataque hacia una computadora también, pues se puede formatear una pc por la existencia de virus, pero la información estará intacta, lo cual ayuda a garantizar un mejor servicio educativo, pues toda la comunidad educativa como docentes, alumnos, padres, autoridades, empresarios y directivos tendrán la información de manera íntegra para cuando quieran solicitarla, siendo una de las universidades del mundo que se preocupa por la información, pues este es el recurso más importante, ya que se tienen proyectos de investigación, calificaciones, recurso económico, y demás informaciones que son importantes para la operación diaria del ITSOEH.

Discusión

Contrastando los mencionado en el presente artículo, no es más que una prueba tangible del gran riesgo que corren a diario nuestras instituciones, ya que siempre se está expuesto a un ciberataque, por lo que más que las leyes protejan a la víctima, lo mínimo que se puede hacer es interponer una demanda por el robo de información o violación de acceso a un sistema, solo por mencionar algún ejemplo, finalmente no queda más que invertir una cantidad de recurso, como en este caso lo maneja el proveedor de tecnología blockchain como es Storj, el cual maneja respaldo anónimo de la información, que se levanta de forma inmediata en caso de pérdida, así como acceso único a las carpetas que se respalden, lo cual en costos supera a una gran diversidad de proveedores de servicio, es importante hacer esta tarea, pues más en el caso de universidades o instituciones públicas o privadas que manejan información o que la información es lo más valioso, vale mucho la pena, garantizar la integridad de los datos, pues la información crece de forma tremenda cada día, por lo tanto crecen los riesgos de ser víctima de un ciberataque.

593 Digital Publisher CEIT ISSN 2588-0705

Conocer las leyes también dan pauta a poder exigir la reparación del daño, o el pago de una multa, o en dado caso llevar acabo un juicio para poder asignar una condena al agresor, hoy en día en México pocas personas son las que llevan a cabo una demanda, pues a veces por desconocimiento, o falta de voluntad, o porque son procesos donde se gasta tiempo, recursos, o evitar el conflicto con la contraparte o agresor, hacen que la víctima desista de demandar.

Es importante capacitarse en cuanto a los derechos y obligaciones que tenemos como ciudadanos, pues siempre se habla de los ciberataques, por lo que se deben tomar medidas para garantizar un uso correcto de los equipos informáticos.

No cabe duda de que se debe seguir innovando en el área de las tecnologías de la información, las leyes y la educación, pues si estas maduran podrán rápidamente crecer, ya que los alumnos incrementan en cada año que pasa, por lo tanto la información crece del mismo modo, y se deben buscar los mejores mecanismos para proteger a los sistemas de información.

El recurso que se invierte en este tecnología será bien recibido en la comunidad educativa, pues ellos mismos comentan que han sufrido ciberataques, han perdido información y no se diga de los sucesos que pueden pasar en el ITSOEH, por ello es importante difundir la forma de operación de Storj y de los beneficios que puede traer consigo.

Se debe reforzar la campaña de medidas de protección y ciberseguridad, para con ello ir disminuyendo el riesgo de ciberataque.

Cada vez son más las instituciones privadas y públicas a nivel mundial las que están incorporando tecnologías como la de blockchain para poder proteger sus bienes intelectuales. En un día normal se pueden perder los correos electrónicos de una escuela, la información de alumnos, calificaciones, convenios, patentes, proyectos de investigación, lo cual sería un golpe terrible para cualquier institución y del dinero ni hablar, pues es el área con mayor prioridad en un ciberataque.

No queda más que difundir esta información, ya que al hacer uso de internet que es un derecho, tiene su lado positivo y su lado de vulnerabilidad, porque se deben siempre tomar medidas, pues es normal ver a un estudiante que tuvo un ciberataque y su información se perdió, lo que concuerdan los autores, es que lo físico o hardware se puede recuperar, aunque con muchos recortes a la educación no es tan posible, pero por otro lado la información es poder, y sin ella no se prospera, pues en el conocimiento esta la luz para una vida en sociedad en forma sustentable en el día a día.

No cabe duda de que operar esta tecnología en el ITSOEH se mejorara la productividad, al no tener que preocuparse por el riesgo de un ciberataque, por lo tanto el personal y alumnos se sentirán más tranquilos mientras utilizan su equipo de cómputo, y por lo tanto podrán realizar un mayor número de investigaciones dentro y fuera del aula, así como profesores y directivos podrán trabajar de una forma más tranquila con lo cual puedan impartir mejores clases al tener más tiempo libre, así como mejorar su productividad académica y por ende crecerá su competitividad obteniendo mejores resultados, sobre todo siendo una institución pionera en el uso de la tecnología blockchain en una escuela pública en el estado de Hidalgo en el nivel superior, con la encomienda de poder difundir este trabajo de investigación para poder llegar a mas universidades a nivel estatal o nacional, mejorando con ello el servicio educativo, formando mejores profesionistas, con transparencia y seguridad en el manejo y operación de los sistemas de información que diariamente son usados por el ITSOEH.

Referencias bibliográficas

Acurio, S. (2005). *Delitos Informáticos: Generalidades.* Recuperado de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aguirre, J. P. (2022). *Ciberseguridad, desafío para México y trabajo legislativo.* :

Bartolomé, A. R. (2020). *Cambiando el futuro: "blockchain" y Educación.* Pixel-Bit. Recuperado de:

Casperproject. (2022). *Proyecto Casper.* Recuperado de: https://casper.network/en-us/

Carrizo, A. (2021). *Ventajas competitivas del uso de Tecnología Blockchain en el sector Telecomunicaciones de Argentina para el período 2021-2025 (Master's thesis).* Recuperado de:

Congreso de la Unión (2022). *Código Penal Federal*. Recuperado de:

Delgado, P. (2019). *¿Qué es Blockchain y cómo se puede aplicar a la educación?*. Recuperado de:

D E E L . (2 0 1 0) . *usuario de Dell™ OptiPlex™ 755.* Recuperado de:

Domínguez, J. (2014). *La ciberseguridad: aspectos jurídicos internacionales.* Recuperado de:

EthicsGlobal. (2022). *Legislación en CiberseguridadMéxico*.Recuperadode:

Fernández, D. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia* (pp. 1-236). Thomson Reuters Aranzadi.

Ficarra F. (2002). *Los virus informáticos.* Recuperado de:

Flores, L. (2009). *Derecho informático*. Ciudad de México. Grupo editorial Patria.

Fonseca, J. (2019). *Ciberseguridad y vigilancia tecnológica: un reto para la protección de datos personales en los archivos.* Tlatemoani: revista académica de investigación, 10(31), 218-246.

Garavilla, M. (2001). *Delitos informáticos.* Recuperado de: https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

Gobierno del Estado de Hidalgo. (2006). *Ley de transparencia y acceso a la información del Estado de Hidalgo.*

Gobierno Estado de México. (2020). *Gobierno digital en México.*

Gobierno de México (2021). *Campaña Nacional Antifraude Cibernético*.