UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÀLISIS DE RIESGOS DE LA PLATAFORMA WEB TRANSACCIONAL DE LA COOPERATIVA DE AHORRO Y CRÈDITO JARDÌN AZUAYO

LOPEZ QUINDE DIANA CHANENA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

ANÀLISIS DE RIESGOS DE LA PLATAFORMA WEB TRANSACCIONAL DE LA COOPERATIVA DE AHORRO Y CRÈDITO JARDÌN AZUAYO

LOPEZ QUINDE DIANA CHANENA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

ANÀLISIS DE RIESGOS DE LA PLATAFORMA WEB TRANSACCIONAL DE LA COOPERATIVA DE AHORRO Y CRÈDITO JARDÌN AZUAYO

LOPEZ QUINDE DIANA CHANENA
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 04 DE FEBRERO DE 2019

MACHALA
04 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Anàlisis de riesgos de la Plataforma Web Transaccional de la Cooperativa de Ahorro y Crèdito Jardìn Azuayo, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

GONZALEZ SANCHEZ JORGE LUIS
0703333898
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: domingo 03 de febrero de 2019 - 16:28

Urkund Analysis Result

Analysed Document:	CASO PRACTICO SOBRE LA COOPERATIVA JARDIN AZUAYO.docx (D47145969)
Submitted:	1/23/2019 11:45:00 AM
Submitted By:	dclopezq_est@utmachala.edu.ec
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, LOPEZ QUINDE DIANA CHANENA, en calidad de autora del siguiente trabajo escrito titulado Anàlisis de riesgos de la Plataforma Web Transaccional de la Cooperativa de Ahorro y Crèdito Jardìn Azuayo, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 04 de febrero de 2019

Diana Lopez

LOPEZ QUINDE DIANA CHANENA
0705789238

DEDICATORIA

Dedico el presente trabajo con todo mi cariño a:

Mi Dios por permitirme vivir cada día con salud, brindarme la oportunidad de estar junto a los seres que quiero, luego a mis padres María Quinde y Pablo López que son mi pilar fundamental, mi guía, mi mayor motivación en esta vida para luchar por lo que anhelo, siempre están brindándome su apoyo en todo momento, a mi hermano Robinson que es el que me imparte buenos consejos y motiva a seguir a pesar de las adversidades que se presenten, y por supuesto a mis docentes que me impartieron sus conocimientos a través de los distintos semestres que he cursado hasta poder llegar a culminar una meta en mi vida como es ser profesional.

Diana Chanena López Quinde

AGRADECIMIENTO

A Dios que a través de su amor infinito me guía y fortalece para seguir adelante superando cualquier adversidad, a mis padres María Quinde y Pablo López que son un verdadero ejemplo de superación, seres llenos de amor y bondad que me supieron formar como una persona de bien, también a mi hermano Robinson por estar siempre pendiente y apoyándome en todo momento y por supuesto a la Universidad Técnica de Machala por permitir mi formación como un profesional que está capacitado para adaptarse a los diferentes cambios que se dan en la sociedad y sobre todo ser portadora de soluciones ante los diversos problemas que se suscitan a diario.

Diana Chanena López Quinde

RESUMEN

El presente trabajo tiene como propósito analizar el entorno virtual de la Cooperativa de Ahorro y Crédito Jardín Azuayo, aplicando el debido proceso de mejora continua como es el Ciclo de Deming con la ayuda de la Norma ISO 27001, con el fin de implementar acciones que permitan brindar la seguridad necesaria a la información personal/económica de los numerosos usuarios que posee la entidad y que gracias a la ayuda de estas herramientas necesarias, se da paso a la realización de la respectiva matriz en donde se identifica los riesgos, vulnerabilidades y amenazas a los cuales se encuentra expuesto, para luego definir las recomendaciones que se deben de propiciar con el fin de disminuir aquellos daños que están ocasionando un perjuicio enorme a la reputación y estabilidad económica tanto de la entidad como de los usuarios. Ante esta situación nace la necesidad de utilizar como instrumento de investigación la observación directa, ingresando a la Plataforma Web como usuario para realizar las pruebas respectivas; obteniendo como resultado escasos controles de seguridad; afectando con ello significativamente a la entidad financiera. Finalmente en el trabajo se han establecido las medidas de seguridad necesarias para combatir los diferentes riesgos que están al acecho en el uso de la Plataforma.

Palabras Clave: Riesgos, Vulnerabilidades, Amenazas, Entorno virtual, Seguridad

ABSTRACT

The purpose of this work is to analyze the virtual environment of the Jardín Azuayo Savings and Credit Cooperative, applying the due process of continuous improvement, such as the Deming Cycle with the help of the ISO 27001 Standard, in order to implement actions that allow provide the necessary security to the personal / economic information of the numerous users that the entity owns and that thanks to the help of these necessary tools, the respective matrix is made where the risks, vulnerabilities and threats are identified which is exposed, to then define the recommendations that should be promoted in order to reduce those damages that are causing a huge damage to the reputation and economic stability of both the entity and the users. Given this situation the need arose to use direct observation as a research instrument, entering the Web Platform as a user to perform the respective tests; resulting in poor security controls; thereby significantly affecting the financial entity. Finally in the work the necessary security measures have been established to combat the different risks that are lurking in the use of the Platform.

Keywords: risks, vulnerabilities, threats, virtual environment, security

ÍNDICE GENERAL

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

INTRODUCCIÓN

Con el pasar del tiempo y ante las diferentes necesidades que posee el ser humano, la tecnología ha ido avanzando a pasos agigantados, creándose distintas herramientas, que permiten mejorar notablemente la vida de un individuo, otorgándole un nivel de comodidad en las diferentes actividades a realizarse a diario (Guaña, Quinatoa y Pérez, 2017). Ante este contexto el sistema financiero también pasa a adoptar las medidas necesarias para estar a la vanguardia en la operación de los instrumentos financieros y ofrecerles lo mejor a sus usuarios, de la manera más práctica y rápida, lo cual ha dado paso a la creación de las Plataformas Web en las entidades (Hernández, 2015).

En Ecuador las Cooperativa de Ahorro y Crédito para poder competir en el mercado financiero incorporan la Plataforma Web Transaccional, para automatizar los servicios que ofertan y que gestionen sus transacciones desde el hogar u oficina (Sánchez, 2015). Pero así como se desarrolla la tecnología informática en las entidades financieras, también nace como actividad ilícita, penada, el delito informático que es realizado por ciberdelincuentes que se aprovechan de las vulnerabilidades que posee la Plataforma, apoderándose de información personal y económica , todo esto por programas maliciosos, con el objetivo de beneficiarse económicamente (Zambrano, Dueñas y Macías, 2016).

Ante el valor que tiene la temática presentada en el ámbito financiero – informático es preciso realizar la presente investigación que tiene como objetivo: Analizar los riesgos de la Plataforma Web Transaccional de la Cooperativa de Ahorro y Crédito Jardín Azuayo a través de una matriz que permitirá identificarlos plenamente y determinar las causas para proponer las respectivas recomendaciones con la finalidad de eliminar o mitigar el impacto negativo que estos producen a la institución y que la confianza que tienen sus usuarios siga intacta, utilizando como metodología la observación directa y fuentes bibliográficas para poder obtener la información precisa.

1. FUNDAMENTACIÓN TEÓRICA

1.1 Delito Informático

Es aquella actividad ilícita que atenta contra la confidencialidad, integridad y disponibilidad de la base de datos y sistema informático que posee una entidad financiera siendo ejecutada por expertos en burlar las vulnerabilidades que posee el entorno virtual, beneficiándose económicamente a través de la sustracción de información personal y económica de sus usuarios, causando perjuicio a la credibilidad que posee la entidad frente a sus clientes y además sembrando desconfianza (Mayer, 2017).

1.2 Ataque Informático/Ciberataque

Son actos ejecutados por individuos que poseen experiencia y que logran vulnerar las fallas que poseen las Plataformas Web que han incorporado las entidades financieras y de manera anónima y rápida utilizan ordenadores u otro tipo de tecnología informática con el objetivo de causar daño, extorsión física, atacando a los usuarios y principalmente al entorno virtual, perjudicandolos notablemente a través de software maliciosos que controlan de forma remota su funcionamiento para lograr reunir información de carácter confidencial (contraseñas, números de cuenta) y con la misma poder beneficiarse económicamente (Poveda y Torrente, 2016).

1.3 Seguridad Informática/ Ciberseguridad

Es el proceso que se encarga de proteger la integridad de los activos de información que posee una entidad financiera a través de su Plataforma Web, que se ve afectada de manera latente ante numerosas amenazas por ciberdelincuentes (Parada, Flórez y Gómez, 2018).Por esta razón si existe incumplimiento de las políticas o normas con respecto a la seguridad informática esto atraerá perdidas económicas considerables, además los usuarios no tendrán la confianza suficiente en la entidad, lo cual representa un daño significativo a su reputación y el gasto en el que se incurre para la recuperación tienen un costo demasiado elevado (Altamirano y Bayona, 2017).

1.3.1 *La Seguridad Informática en el Ecuador.*

Ecuador no es la excepción pues el avance tecnológico y la necesidad de estar a la vanguardia han hecho que las distintas entidades financieras (Bancos, Cooperativas) opten por llegar a sus clientes ofreciéndoles sus servicios en línea (transacciones electrónicas, pago de servicios básicos, recargas telefónicas, entre otros servicios), logrando así automatizar sus servicios y personalizarlos. Pero de acuerdo a los datos que presenta el Ministerio Coordinador de Seguridad, para el año 2014 las estadísticas revelan que ha habido un mayor porcentaje de violación a la seguridad dentro del sistema financiero, convirtiéndose en un tema preocupante (Vargas, Recalde y Reyes, 2017).

Con un 37% de aumento en el robo a la banca virtual, un 14% con respecto a las tarjetas de crédito y un 46% de robo a los cajeros electrónicos, son cifras que resultan alarmantes para el Gobierno Ecuatoriano, aunque han sido creado varios proyectos tales como: Ecucert, Centro de Operaciones Estratégico Tecnológico, la implementación de las Normas Técnicas Ecuatorianas para la Gestión de la Seguridad de la Información y el Comando de Ciberdefensa dentro de las Fuerzas Armadas, que han aportado pero no han podido concretar un plan estratégico de acción que proteja a las entidades financieras del país de los delitos informáticos (Vargas, Recalde y Reyes, 2017).

1.4 Evaluación de Riesgos

Es un proceso en donde las entidades financieras al contar con su Plataforma Web para ofertar sus servicios personalizados a sus usuarios, implementan herramientas tecnológicas capaces de diagnosticar riesgos, amenazas, con la finalidad de disminuir y hacer frente de manera oportuna los daños y pérdidas que pueden ocasionar y poner en peligro su continuidad dentro del sector financiero, su operatividad, su credibilidad al otorgar los servicios financieros que pone a disposición (Corda, Viñas y Coria, 2017).

1.5 Phishing

Es un acto ilícito que consiste en el envío de correos electrónicos a los distintos usuarios que posee la entidad financiera, en donde le indican qué debe ingresar a un determinado link que es de dudosa procedencia , haciéndoles creer que aquellas página a la cuales va acceder es el portal de la entidad, siendo todo lo contrario, desviándolos a páginas web falsas y logrando sustraerse de esa forma información como: usuario, contraseña, número de cuenta y además realizar transferencias a otras cuentas bancarias (García, 2018).

1.6 Pharming

Tipo de fraude informático que utiliza el Internet como base esencial y que por medio de correos no deseados o spam dirige al usuario de la entidad financiera a una página web falsa pero similar a la que utiliza la entidad para ofertar sus servicios o productos financieros a través de su Portal Web, con la finalidad de insertar software maliciosos para que infecten a los ordenadores, específicamente en su sistema operativo y poder apropiarse de la base de datos para luego beneficiarse económicamente (Oxman, 2013).

1.7 Malware

Código malicioso que representa una amenaza latente para el entorno virtual de una entidad financiera, debido a que causa severas molestias en el funcionamiento del sistema informático, esto es porque las personas expertas en utilizarlos, tienen como objetivo obtener la cantidad suficiente de información personal de los distintos usuarios para poder beneficiarse económicamente, manipulando los ordenadores de un lugar distante causando daños económicos y afectando su reputación financiera (Guilabert, 2016).

1.8 Ransomware/ Wannacry

Software dañino que posee la capacidad de encriptar toda la base de datos que posee la entidad financiera a través de su Plataforma Web, para luego pedir una remuneración a cambio de su devolución y desciframiento, aprovechando así las debilidades que posee el sistema informático, sabiendo que si no acceden ante la propuesta, este software pasará a destruir los activos de información y sobre todo se enfrentará ante una gran pérdida económica y desconfianza por parte de sus clientes (Ramos y Gallegos, 2016).

Un claro caso se dio en Ecuador en el año 2017, el 12 de Mayo, en la Provincia de El Oro, exactamente en la ciudad de Pasaje, que es donde se encuentra situada la Cooperativa de Ahorro y Crédito Jardín Azuayo, cuya matriz está ubicada en la ciudad de Cuenca, la misma que se vio afectada por el ataque de un software malicioso denominado Wannacry que colocó en los ordenadores dejando en descubierto su base de datos, archivos, logrando perjudicarla económicamente (Cooperativa de Ahorro y Crédito Jardín Azuayo, 2018).

1.9 Norma ISO/IEC 27001 (Sistemas de Seguridad de la Información)

A mediados de los 90 ante el desarrollo inminente del entorno informático y las entidades financieras que tenían la necesidad de realizar una buena gestión con la seguridad de su información, debido a la presencia de distintas situaciones riesgosas que intentaban poner en peligro tanto la seguridad de los sistemas como la información, surge la presente Norma que es aplicable a las entidades financieras para que proteja la información que se encuentra en la base de datos de su entorno virtual, a través del control del sistema de seguridad de información con sus respectivas recomendaciones idóneas a realizar, para mejorar constantemente en el aspecto de seguridad (Guerra, Meizoso y Roque, 2015).

2. DESARROLLO

2.1 Metodología

Para proceder a realizar la presente investigación acerca de los riesgos, amenazas y vulnerabilidades que la Plataforma Web Transaccional de la Cooperativa posee, y que se encuentran afectando tanto a los usuarios como a la propia entidad, se lo logra en base a la información obtenida a través del método de investigación como es la observación directa, ingresando como un usuario de la entidad financiera para poder analizar y constatar claramente en lo que está fallando la Plataforma y además basándose en fuentes bibliográficas, tales como : revistas científicas, Norma ISO/IEC 27001, para poder conocer sobre el tema y otorgar las respectivas recomendaciones.

Siendo necesario que para realizar la evaluación del entorno virtual de la Plataforma de una entidad financiera para conocer la situación existente y los riesgos que la están afectando y emitir las recomendaciones de mejora, es necesario definir un proceso que guíe y ordene el accionar para establecer la matriz, como es el Ciclo de Deming (PDCA) que es el ciclo de mejora continua, junto a la Norma ISO/IEC 27001, encargándose de gestionar la seguridad de la información (Marìn, Bautista y Garcìa, 2014).

A continuación se detalla el proceso adecuado para realizar el análisis de riesgos a la Plataforma Web Transaccional con la finalidad de obtener un resultado de calidad:

2.1.1 *Análisis del entorno a evaluar.*

Cooperativa de Ahorro y Crédito Jardín Azuayo

La entidad nace en el año de 1996, en el cantón Paute, en Azuay, iniciando con los ahorros iniciales de 120 personas y el capital donado por ONG. Actualmente está laborando en las provincias del Azuay, Cañar, Morona Santiago, Loja y el Oro, a través de 31 oficinas locales y su matriz en Cuenca, además cuenta con más de 200.000 personas como socios y es regulada por la Superintendencia de Compañías (SEPS). Para ofrecerles el mejor servicio financiero a sus usuarios ha optado por la creación de la Plataforma Web Transaccional (https://www.jardinazuayo.fin.ec/coacja/web/) en donde se puede acceder a los distintos servicios financieros que oferta. (Microfides, 2017).

2.1.2 *Definir el alcance y límite de la evaluación a realizar, para poder identificar las posibles fallas que permiten que se den los ataques informáticos.*

Alcance

En el presente trabajo se procederá a analizar e identificar las vulnerabilidades, amenazas o riesgos a los cuales tiende a estar expuesta la Plataforma Web Transaccional de la Cooperativa de Ahorro y Crédito Jardín Azuayo, esta información se la obtendrá accediendo a la plataforma como usuario de la entidad para luego aquella información obtenida ubicarla en una Matriz de Riesgo donde se evaluará el nivel de impacto y la probabilidad de que ocurra, ante este contexto otorgar las recomendaciones pertinentes.

Limitaciones

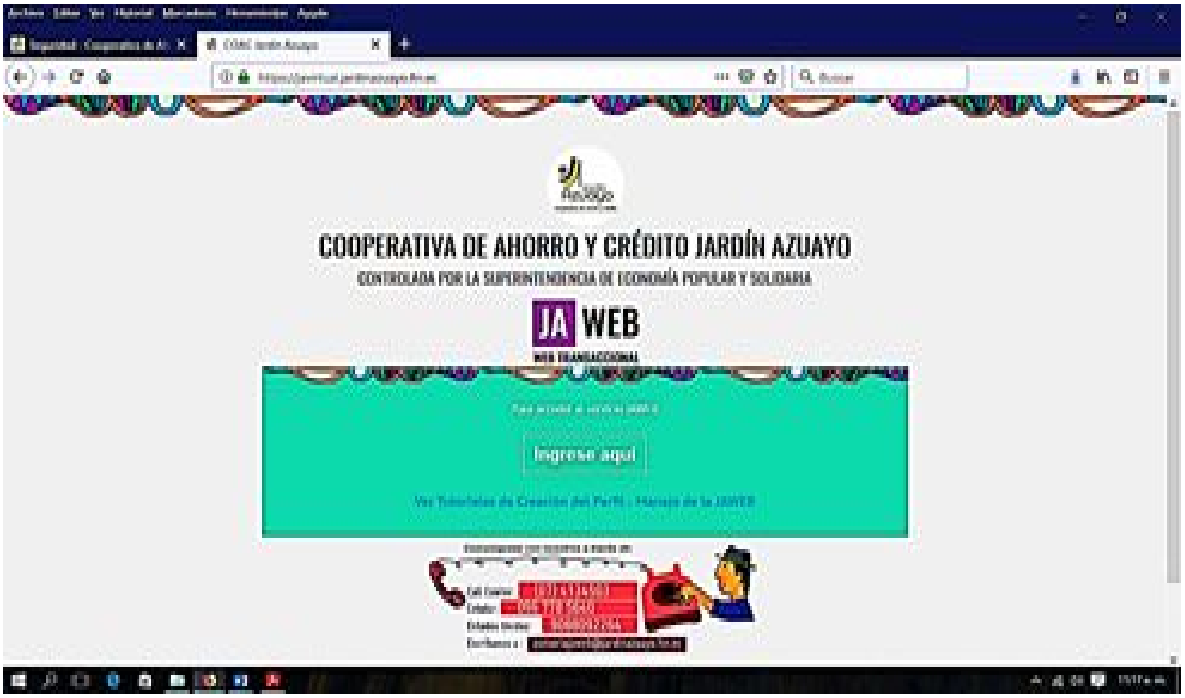
Información incompleta con falta de actualización por parte de la Cooperativa de Ahorro y Crédito Jardín Azuayo.

2.1.3 *Proceder a explorar de manera minuciosa la Plataforma Web de la Cooperativa.*

La Cooperativa Jardín Azuayo cuenta con su Plataforma Web Transaccional (https://javirtual.jardinazuayo.fin.ec/jaweb/jaweb.xhtml) donde al momento de ingresar se puede constatar:

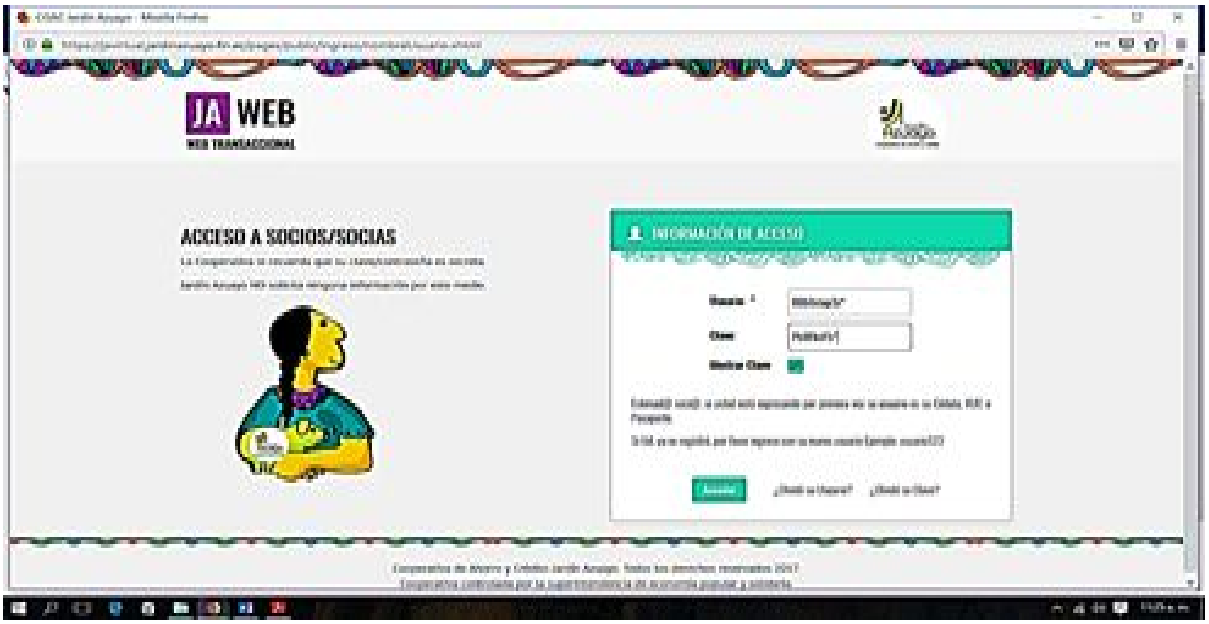
- Se adapta a los diferentes dispositivos tecnológicos (Tablet, celular u ordenador) al momento de querer acceder.
- Posee una interfaz de fácil uso e intuitiva por lo que permite acceder a los distintos servicios que se pueden realizar en la comodidad de su hogar u oficina.
- Cuenta con asistencia técnica ya que a través de operadores pueden despejar la duda que se tenga en cuanto al uso y los beneficios que otorga la Plataforma.

Ilustración 1. Al ingresar al Portal Web Transaccional de la entidad financiera.



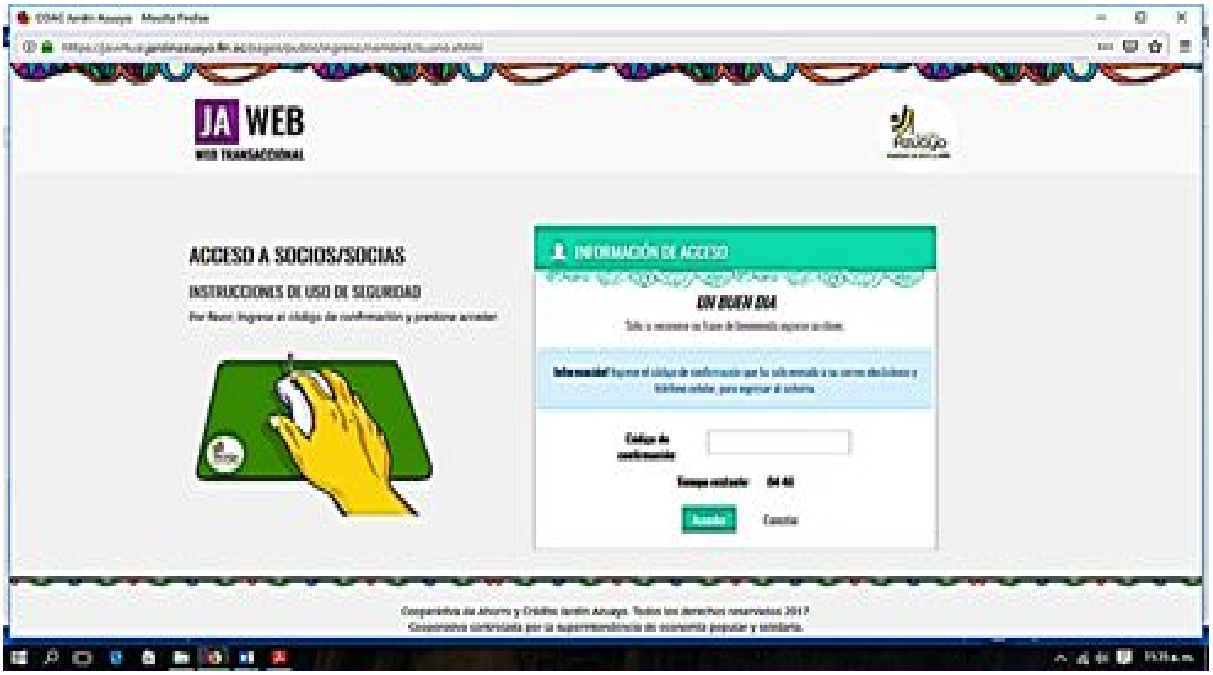
Fuente: Cooperativa de Ahorro y Crédito Jardín Azuayo

Ilustración 2. Para poder ingresar a acceder a los distintos servicios que ofrece la entidad, requiere usuario y contraseña.



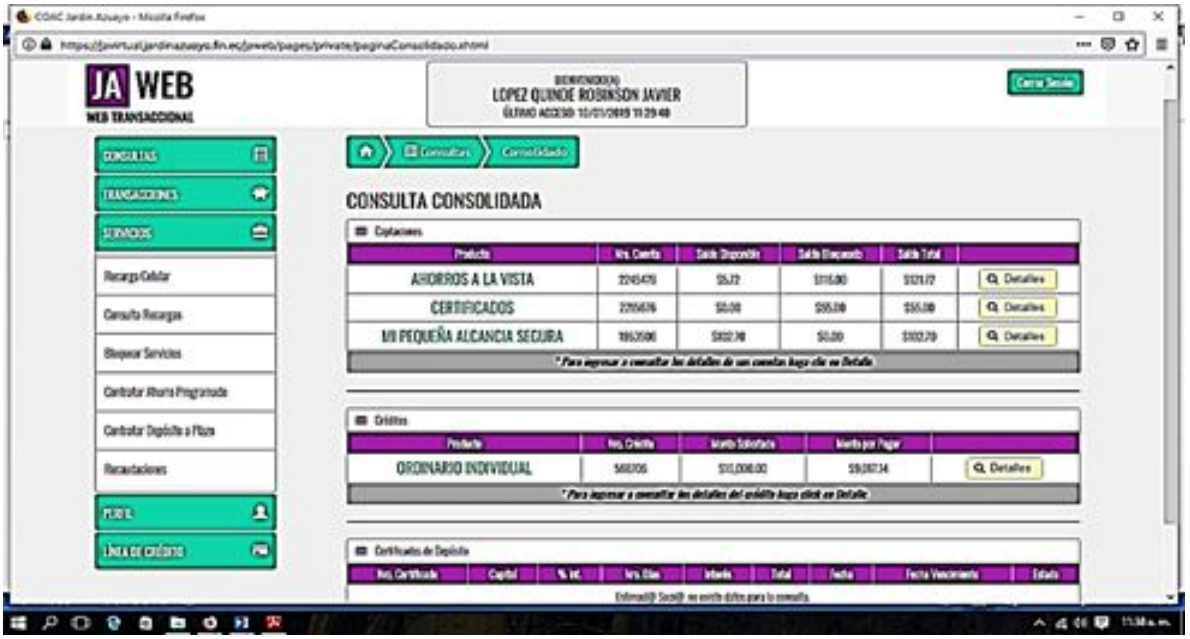
Fuente: Cooperativa de Ahorro y Crédito Jardín Azuayo

Ilustración 3. Envío de Código de confirmación al correo electrónico y por medio de mensaje al celular como última medida de seguridad para el usuario.



Fuente: Cooperativa de Ahorro y Crédito Jardín Azuayo

Ilustración 4. Al ingresar a la Plataforma se puede divisar los diferentes servicios que ofrece la entidad a sus usuarios.



Fuente: Cooperativa de Ahorro y Crédito Jardín Azuayo

Ilustración 5. Detalle de las consultas que puede realizar el usuario en la Plataforma.

Fuente: Cooperativa de Ahorro y Crédito Jardín Azuayo

2.1.4 *Identificar riesgos, amenazas y vulnerabilidades que se están presentando y ocasionando el caos a la institución para proceder a plasmar en la matriz de riesgos, detallando las novedades encontradas.*

Tabla 1. Matriz de riesgos de la Plataforma Web Transaccional de la Cooperativa de Ahorro y Crédito Jardín Azuayo

Matriz de Riesgo									
N	Factores de Riesgo	Impacto			Probabilidad			Nivel de Riesgo	Causa	Recomendación
		A	M	B	A	M	B			
Seguridad										
1	Inexperiencia en el uso de la Plataforma Web Transaccional por parte de los usuarios.	X			X			Alto	Ausencia de capacitaciones sobre el uso correcto de todas las opciones que ofrece la Plataforma Web a sus usuarios por parte del personal informático encargado.	Que el personal encargado de la Plataforma Web Transaccional frecuentemente realice capacitaciones entorno a su uso y sobre las consecuencias que traen su desconocimiento y con horarios admisibles para que `puedan asistir los usuarios.
2	Carencia de actualización de instrumentos de resguardo (software, antivirus, antimalware y parches de seguridad). Fuente: (Cooperativa de Ahorro y Crédito Jardín Azuayo, 2018)	X			X			Alto	Descuido del personal encargado de velar que la Plataforma Web sea confiable y otorgue la seguridad necesaria al usuario.	Actualizar aquellas medidas de resguardo cada cierto tiempo considerable y realizar las pruebas necesarias con el fin de mitigar cualquier daño que pueda ocasionar.
3	Falta de socialización de políticas o normas de seguridad a los usuarios a través de medios electrónicos.		X			X		Medio	Despreocupación del personal informático sobre la socialización en el aspecto de seguridad.	Implementar a través de las herramientas de comunicación como lo son los teléfonos móviles o al correo electrónico de cada usuario, mensajes que contengan las políticas o normas que debe conocer para evitar cualquier situación desfavorable.
4	Inexistencia de bloqueo de seguridad a partir del cuarto intento de ingreso fallido a la Plataforma Web.		X			X		Medio	Descuido por parte del profesional en informática encargado en ir modificando ciertas características de la plataforma web que desfavorecen al usuario.	Implementar la restricción del número de veces en que se puede intentar ingresar a la Plataforma Web Transaccional, como usuario.

Elaborado por: El Autor

2.1.5 Analizar los riesgos encontrados con la ayuda de la Norma ISO/IEC 27001(Sistema de Gestión de Seguridad de la Información), para puntualizar las recomendaciones a otorgar con la finalidad de disminuir la probabilidad de ocurrencia de los riesgos en la Plataforma de la Cooperativa.

A través de la presente matriz se puede notar los riesgos a los que se encuentra expuesto la Plataforma Web Transaccional de la Cooperativa Jardín Azuayo, siendo estos factores importantes que se deben de considerar e implementar las medidas que otorguen la solución pertinente al impacto negativo que están ocasionando a diario, porque con el paso del tiempo logran afectar a los usuarios, causando que tomen la decisión de retirar sus fondos inmediatamente y no confiar debido a que no ofrece las garantías que se requieren.

Aunque la Cooperativa en su ardua labor de ofrecerle lo mejor en seguridad en cuanto a las transacciones que realicen los usuarios utilizando la plataforma e intentando estar a la vanguardia, hay ciertos aspectos que no han sido tomados en cuenta por lo que se ve necesario mencionarlos a continuación detalladamente e indicar las acciones correctivas pertinentes que se deben llevar a cabo para poder contrarrestar los efectos perjudiciales que está ocasionando:

- **Inexperiencia en el uso de la Plataforma Web Transaccional por parte de los usuarios.**

Es de vital importancia que se le dé un buen uso a la plataforma web transaccional, esto se dará si el usuario cuenta con los conocimientos pertinentes para que pueda utilizar de manera correcta todas las opciones que contenga la plataforma en base a los distintos movimientos financieros que pretenda realizar, además para prevenir que:

- Terceras personas por prestar ayuda para poder ingresar a la plataforma y hacer uso de ella, logren saber datos personales, contraseña, número de cuenta, logrando con esto acceder a la plataforma y realizar las transacciones bancarias a su favor.
- Al dejar colocado la contraseña y usuario en ordenadores ajenos (Cyber) se aprovechen indebidamente de estos datos para perjudicar tanto a la institución como al usuario.

- Un ataque Phishing aproveche el momento en que el usuario ingrese a la plataforma a realizar alguna transferencia y al desconocer su uso o medidas que debe adoptar para poder realizarla con éxito, ingrese a correos electrónicos (spam) que contienen enlaces que al acceder a ellos lo envían a páginas web de procedencia dudosa, o bien a través de llamadas telefónicas que solicita que confirme determinada información para sacar provecho de esta situación.

Ante esta situación la probabilidad de ocurrencia es alta debido a la carencia de capacitaciones sobre la adecuada utilización de la Plataforma Web por parte del personal de Informática encargado, que les permita al usuario estar al tanto de todas las modalidades de ataques informáticos que suelen darse por la mala manipulación del entorno virtual. En cuanto a la probabilidad de impacto es alto, debido a que si hay personas perjudicadas por aquellos ataques informáticos al hacer uso de la Plataforma, recaería la culpa en la institución ya que no ofrece seguridad financiera, entonces perdería credibilidad, los usuarios se retirarían de la entidad, y habría perjuicio económico para la entidad y para el usuario.

Por lo que se recomienda y que se tome bastante en consideración, es que frecuentemente se dé capacitaciones con respecto al buen uso que se le debe de otorgar a la Plataforma, en horarios admisibles para que el usuario pueda acercarse y ser partícipe de estas, haciéndoles entender las consecuencias negativas que se derivan por el desconocimiento y que al existir estos casos perjudicarán tanto al usuario como a la entidad, por lo que para evitar estos inconvenientes es mejor saber completamente sobre el uso del entorno virtual.

- **Carencia en la actualización de instrumentos de resguardo (software, antivirus, antimalware, parches de seguridad y copia de seguridad)**

La característica esencial que debe predominar en la Plataforma Web, es su seguridad, por lo que resulta primordial ofrecer esa garantía al usuario, pero existe descuido por parte del personal encargado de monitorear cada determinado tiempo si la plataforma cumple o no completamente en el aspecto de seguridad, y si cuenta con las respectivas actualizaciones de los instrumentos de resguardo, tales como:

- **Software, parches de seguridad.-** siendo prioridad proceder a actualizarlos e incorporarlos a los distintos ordenadores, con la finalidad de evitar que se dé la sustracción de información personal de los usuarios y detener a software maliciosos que afectan a todo el equipo.
- **Antivirus – Antimalware.-** Su debida actualización facilitará la detección e inmediata eliminación de ataques informáticos por parte de software dañinos en especial la de tipo ransomware "WannaCry".

Ante esta situación la probabilidad de ocurrencia es alta, debido a la carencia de monitoreo por parte del personal encargado de verificar si la Plataforma Web cumple con los parámetros de seguridad, tales como: la actualización de software, los respectivos parches de seguridad y la colocación de antivirus que avale una navegación segura al momento de gestionar sus transacciones. En cuanto a la probabilidad de impacto es alto, debido a que si la entidad no toma las medidas correctivas necesarias en cuanto a seguridad se constatará en determinado tiempo que la Plataforma no cubrirá las expectativas del usuario, provocando la pérdida de credibilidad de sus usuarios y sobre todo acarreará pérdidas económicas considerables.

Por lo que se recomienda que de manera periódica se de una revisión exhaustiva en lo que se refiere a seguridad en torno al uso de la Plataforma Web en conjunto con los ordenadores que posee la entidad, ya que resulta primordial que se mantenga actualizado el software, los parches de seguridad y el respectivo antivirus que permitirá el bloqueo de acciones maliciosas que quieran apoderarse de la base datos que posee la entidad financiera para luego beneficiarse del daño por el que llegue atravesar la misma.

- **Falta de socialización de políticas o normas de seguridad a los usuarios a través de medios electrónicos.**

Esto es debido a la despreocupación del personal de informática encargado, el cual no se percata que es importante que la entidad financiera adopte medidas drásticas de seguridad para proteger al usuario de actos delictivos realizados por ciberdelincuentes que se encuentran atentos ante la aparición de cualquier vulnerabilidad que pueda presentar la Plataforma Web de la institución y sacar beneficio propio a causa de la inestabilidad en el entorno financiero y además atraerle pérdidas económicas considerables.

Ante esta situación la probabilidad de ocurrencia es media por que existe indiferencia por parte del personal encargado de la institución financiera, en incorporar boletines de comunicación o mensajes con contenidos de seguridad de manera periódica y que logre llegar sea al teléfono celular o bien al correo electrónico que haya dado en sus datos el usuario, para que esté al tanto de las novedades en aspecto de seguridad que le ofrece la entidad para protegerlo de actividades ilícitas en el uso del entorno virtual.

En cuanto a la probabilidad de impacto es medio, debido a que las personas tratan de poner su mayor esfuerzo al momento de hacer uso de la Plataforma, aun desconociendo los aspectos de seguridad que debe de considerar, pero no hay que dejar de lado que este desconocimiento hace que las personas expertas en burlar estas debilidades que posee el usuario al realizar sus transacciones en el entorno virtual, se aproveche, atrayendo pérdidas económicas para la entidad como el cliente y pérdida de credibilidad en el sector financiero.

Por lo cual se recomienda implementar las herramientas de comunicación como es la telefonía móvil y correos electrónicos de cada usuario para que a través de mensajes de carácter informativo estén enterados periódicamente sobre las políticas o normas de seguridad que se están incorporando con la finalidad de hacer frente a los distintos ataques de los cuales pueden llegar a ser víctimas al momento de utilizar el entorno virtual de la entidad y poder contrarrestar los impactos negativos que estos atraerán.

- **Inexistencia de bloqueo de seguridad a partir del cuarto intento de ingreso fallido a la Plataforma Web.**

Existe un deficiente control para acceder a la Plataforma Web, debido al descuido por parte del profesional de informática encargado en ir detectando y modificando determinadas características de la misma, lo que hace que el entorno virtual sea más accesible para el ingreso de terceras personas con intenciones de obtener información personal y financiera, para sacar provecho de esta vulnerabilidad, debido a que no limita el número de intentos de ingreso y esto provoca que de tantas veces tratar de ingresar, logren lo que desean.

Ante esta situación la probabilidad de ocurrencia es media, debido al descuido que existe por parte del personal en informática encargado en ir constatando que modificaciones se deben realizar en el entorno virtual para ofrecerle un servicio personalizado y seguro a sus clientes, sobre todo al momento de acceder a la Plataforma. En cuanto a la probabilidad de impacto es media, porque al no incorporar la respectiva restricción para ingresar al entorno virtual atraería que tanto el usuario como la entidad se vea perjudicado económicamente.

Por lo que se recomienda que se debe de implementar como método de seguridad para los usuarios y para proteger también a la misma entidad, la restricción del número de veces que se puede intentar ingresar usuario y contraseña, y que al tercer intento que se realice se bloquee inmediatamente esa opción para que el usuario se acerque a las oficinas.

3. CONCLUSIONES

- Del proceso de análisis llevado a cabo mediante la Matriz de Riesgo al entorno virtual de la Cooperativa de Ahorro y Crédito Jardín Azuayo, se determina que posee falencias en el aspecto de seguridad, pero este desatino recae en el usuario que posee la entidad, debido a que no cuenta con el suficiente conocimiento de cómo darle el uso pertinente a los distintos servicios que ofrece la Plataforma, por lo que desconoce políticas o normas de seguridad y la oportuna actualización de los instrumentos de resguardo que se requieren, lo cual produce que tanto la entidad como el propio usuario se vean perjudicados económicamente, con daño a su reputación, perdiendo credibilidad dentro del sector financiero.

- Además es necesario destacar que la entidad financiera no debe defraudar a sus usuarios, más bien debe de incorporar medidas y acciones de seguridad a realizar para que actué en contra de aquellos ataques informáticos de los que puede llegar a ser víctima, por lo que tendría que asignar al personal idóneo para que realice capacitaciones a los usuarios sobre el correcto uso de la Plataforma con horarios admisibles para que puedan asistir, dándole a conocer todos los detalles, normas, políticas, medidas de seguridad a tomar para que contrarresten las consecuencias negativas que atrae estos ataque informáticos que perjudica notablemente al usuario porque sustrae su información personal, económica y sobre todo provoca que la entidad difícilmente salga de la situación caótica a la que puede llegar.

BIBLIOGRAFÍA

Altamirano, Y., & Bayona, O. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que explican su cumplimiento. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informacao(25), 112-134. doi:10.17013/risti.25.112-134

Corda, M., Viñas, M., & Coria, M. (Octubre de 2017). Gestión del riesgo tecnológico y bibliotecas:una mirada transdisciplinar para su abordaje. VII(1), 206-2015. Obtenido de http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1853-99122017000200007&lng=es&tlng=es.

García, G. (Enero de 2018). El Phishing como delito de estafa informática.Comentario a la SAP de Valencia 37/2017 de 25 de Enero(rec. 1402/2016). Iuris Tantum Revista Boliviana de Derecho(25), 650-659. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100025

Guaña, M., Quinatoa, A., & Pérez, F. (Abril-Junio de 2017). Tendencias del uso de las tecnologías y conducta del consumidor tecnológico. Ciencias Holguín, XXIII(2), 1-17. Obtenido de https://www.redalyc.org/pdf/1815/181550959002.pdf

Guerra, B., Meizoso, V. d., & Roque, G. R. (Julio-Agosto de 2015). Normalización y aplicación de los principios de gestión de la calidad en la actividad archivística. Revista Habanera de Ciencias Médicas, XIV(4), 527-535. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1729-519X2015000400016

Guilabert, G. (Junio de 2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. IDP. Revista de Internet,Derecho y Política(22), 48-61. Obtenido de https://www.redalyc.org/articulo.oa?id=78846481005

Hernández, M. (Julio-Diciembre de 2015). El papel del desarrollo financiero como fuente del crecimiento económico. Finanzas y Política Económica, VII(2), 235-256. doi:10.14718/revfinanzpolitecon.2015.7.2.2

Marìn, G., Bautista, P., & Garcìa, S. (Septiembre - Diciembre de 2014). Etapas en la evoluciòn de la mejora continua:Estudio multicaso. (I. Capital, Ed.) Intangible Capital, X(3), 584-618. doi:10.3926/425

Mayer, L. (Abril de 2017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. Revista Chilena de Derecho, XXXXIV(1), 235-260. doi:10.4067/S0718-34372017000100011

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso(41), 211-262. doi:10.4067/S0718-68512013000200007

Parada, D., Flórez, A., & Gómez, U. (Febrero de 2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. Información Tecnólogica, XXIX(1), 27-38. doi:10.4067/S0718-07642018000100027

Poveda, C., & Torrente, B. (2016). Redes Sociales y Ciberterrorismo.Las TIC como herramienta terrorista. Institutional Institute of Security Study (IISS), XXXII(8), 509-518. Obtenido de https://dialnet.unirioja.es/descarga/articulo/5901105.pdf.

Ramos, M., & Gallegos, M. (Diciembre- Marzo de 2016). INFECCIÓN CON EL RANSOMWARE EN EL SERVIDOR DE BASE DE DATOS DEL SISTEMA ONSYSTEC ERP. 3C Tecnología, V(4), 56-76. doi:10.17993/3ctecno.2016.v5n4e20.56-76

Sánchez, B. (2015). Sistemas de crédito cooperativo: defensa del modelo. Boletín de la Asociación Internacional de Derecho Cooperativo(49), 31-48. doi:10.18543/BAIDC

Vargas, B., Recalde, H., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual:modelo ecuatoriano de gobernanza en ciberdefensa. URVIO,Revista Latinoamericana de Estudios de Seguridad(20), 31-45. doi:10.17141/urvio.20.2017.2571

Zambrano, M., Dueñas, Z., & Macías, O. (Agosto de 2016). Delito Informático.Procedimiento Penal en Ecuador. Dominio de las Ciencias, II, 204-215. doi:10.23857/pocaip

WEBGRAFÍA

Cooperativa de Ahorro y Crédito Jardín Azuayo. (2018). Obtenido de https://www.jardinazuayo.fin.ec/coacja/web/seccion/detalle?data=c2VjY2lvbklkPTI5MA%3D%3D

Cooperativa de Ahorro y Crédito Jardín Azuayo. (2018). Cooperativa de Ahorro y Crédito Jardín Azuayo. Recuperado el 27 de Diciembre de 2018, de Cooperativa de Ahorro y Crédito Jardín Azuayo: https://www.jardinazuayo.fin.ec/coacja/web/seccion/detalle?data=c2VjY2lvbklkPTI5MA%3D%3D

Microfides, F. y. (2017). Recuperado el 27 de Diciembre de 2018, de https://microfides.com/jardin-azuayo-ecuador/