Seguridad informática y de la información, articulación y convergencia en el sector financiero y la banca en línea

Computer and information security, articulation and convergence in the financial sector and online banking

Review article

Danilo Antonio Guzmán Parra[1]
ID:https://orcid.org/0009-0006-8833-4807
Wilman Enrique Navarro Mejía[2]
ID: https://orcid.org/0000-0002-8796-7761

Resumen: La seguridad informática y de la información para el sector financiero y bancario, es la temática que abordamos en el presente estudio en el ámbito bancario está experimentando cambios rápidos y el estado de la seguridad y sus esquemas de son variados, tanto desde el punto de vista técnico, como desde el normativo. Por tanto, abordamos varios métodos técnicos, y tres estándares que deben ser tenidos en cuenta en el mundo financiero y bancario en línea, que viabilizan a dichas organizaciones una prestación del servicio con niveles de seguridad para sus clientes de confiabilidad aceptados. Los métodos técnicos los clasificamos en cuatros apartados, que de ninguna manera son definitivos ni excluyentes, pero representan lo más actualizado de la actualidad. Además, realizamos una caracterización de las nuevas tecnologías complementarias para la seguridad, como es lo relacionado con la nube federada y sus componentes más importantes.

Palabras claves: Ciberseguridad, finanzas y banca en línea, estándares de seguridad

Abstract: Computer and information security for the financial and banking sector is the topic addressed in this study. The banking sector is experiencing rapid changes, and the state of security and its frameworks vary both technically and from a regulatory perspective. Therefore, we explore several technical methods and three standards that must be considered in the online financial and banking world, enabling these organizations to provide services with accepted levels of trust and security for their clients. We classify the technical methods into four sections, which are by no means definitive or exclusive but represent the most up-to-date approaches available. Additionally, we provide a characterization of new complementary security technologies, such as federated cloud systems and their key components.

Keywords: Cybersecurity, online banking, security standards

[1] Ingeniero en Redes de Computadores, Director de Servicios en Alliance Enterprice. danilоguzman4@gmail.com>
[2] Ingeniero de Sistemas, Master of Science, Magister en Educación, PhD en Educación. Docente tiempo completo Universidad Distrital Francisco José de Caldas. wnavarro@udistrital.edu.co

1. Introducción

La presente revisión temática, es un estudio acerca de la seguridad informática y de la información y sus aplicaciones en los servicios del sector financiero y la banca en línea, en el cual sintetizamos las formas básicas de los servicios financieros y banca en línea, así como, los métodos de autenticación y autorización más utilizados. Por la rápida evolución de los servicios en línea y el paso a la banca móvil, han dado lugar a generación de nuevos estándares y normas de los que afectan permanentemente a este sector productivo en todas las partes del mundo, por tanto, ha sido un momento ideal y pertinente para la realización del presente estudio. Los cambios en el comportamiento de los usuarios y la constante evolución de equipos informáticos utilizados en la industria financiera y bancaria, afectan directamente a la seguridad informática y de la información en todo su contexto. Es así, como al integrar la banca inteligente en el smartphone, estamos complementándolo con un segundo canal como son los mensajes por SMS, las aplicaciones Web, y los servicios automatizados por la tradicionales; todo lo anterior trae consigo nuevos esquemas de ataques por parte de los ciberdelincuentes.

El objetivo de este artículo, es ofrecer una descripción general de los métodos de autenticación actuales, su relación con los ataques cibernéticos más comunes a los servicios financieros y la banca en línea, y el nivel de protección que pueden proporcionar las organizaciones a sus clientes; para lo cual es necesario siempre estar actualizados con los nuevos requisitos sobre autenticación y autorizaciones que involucran procesos y procedimientos técnicos y de idoneidad, para la prestar servicios de usabilidad y seguridad eficientes y confiables.

Los cambios del sector financiero y bancario se presentan impactados, por la continua evolución digital, a medida que cambian los paradigmas digitales, se presentan nuevas transiciones de la banca presencial a la banca online, y durante el último quinquenio de años presente una fuerte tendencia en la prestación de servicios hacia la banca móvil; lo anterior debido al incremento de la accesibilidad y la conectividad 7/24 de los servicios, y con un entorno así, el contacto físico con el cliente se abandona por completo en favor de la banca digital en línea.

Un estudio de “SwissFinanceCouncil” estima que cerca del 60% de las transacciones bancarias minoristas en todo el mundo se realizan a través de canales móviles y en línea [1], lo anterior concuerda con los informes de otros países como Brasil [2], en donde los canales digitales realizan cerca del 63% de las transacciones bancarias, con aumento sostenido año tras año; mientras que también es evidente en el informe GMCS de Deloitte, que afirma que, según la encuesta del Reino Unido, un teléfono inteligente es el dispositivo preferido para el uso de servicios bancarios por parte de la mayoría de las personas [3].

La creciente masificación de los servicios financieros y bancarios, tiene un gran soporte por ende con el uso de los teléfonos móviles inteligentes, como indica el Pew Research Centre, "hoy en día, la mayoría de las personas que poseen un teléfono móvil poseen un teléfono inteligente" [4].

Por último, uno de los nuevos retos más importantes en la prestación de los servicios en línea, es la verificación confiable de identidad del cliente cuando hace uso de los servicios en línea; lo cual ha obligado a las Organizaciones Financieras y Bancarias, a desarrollar nuevas técnicas de

mitigación de riesgos y gestión de atención de ataques de los ciberdelincuentes. En lo concerniente con la verificación de identidad y operaciones, es claro que la autenticación multifactor con varios factores ha tomado un gran desarrollo y sofisticación. Nuestro artículo ha recabado fuentes amplias y diversas y hemos utilizado técnicas de bibliometría y cienciometría avanzadas, como fue el uso ecuaciones de búsqueda booleanas y el uso VOSviewer.

2. Caracterización de Nuevas Tecnologías para la Seguridad informática y de la información

La computación en la nube es un nuevo prototipo que proporciona a los usuarios servicios externos bajo demanda y en función del pago por consumo [6]. El mundo digital en constante expansión, definido por la proliferación de servicios en línea, las aplicaciones basadas en datos y el imparable aumento de los contenidos generados por los usuarios, ha dado lugar a una demanda sin precedentes de recursos computacionales en entornos de computación en nube [7]. Los proveedores de servicios en la nube (CSP) se han convertido en la piedra angular de la era digital y ofrecen soluciones de infraestructura como servicio (IaaS) para satisfacer las demandas de almacenamiento, procesamiento y transmisión a altas velocidades, no obstante, a medida que crece el mercado de los servicios en la nube, los CSP se enfrentan a un reto cada vez más complejo, como es, poder cumplir con la calidad del servicio.

Como resultado de la anterior dinámica tecnológica, ha surgido la noción computacional de nube federada, entendida como los servicios en la nube interconectados de diferentes proveedores que se administran como un único entorno informático unificado, lo anterior viabiliza la optimización de recursos y por tanto una mejor prestación de la calidad del servicio ha. En síntesis, los proveedores de servicios en la nube unen sus fuerzas en este enfoque, creando un ecosistema colaborativo en el que ponen en común y comparten sus recursos informáticos no utilizados. La federación resultante, conocida como computación en nube distribuida, presenta una serie de ventajas, entre ellas una mayor disponibilidad y fiabilidad [8]. Este enfoque colaborativo permite a la "federación" superar las restricciones inherentes que experimentan los CSP individuales cuando se trata de mantener la calidad del servicio, especialmente durante periodos de alta demanda de recursos o de bajo uso.

Elegir el mejor proveedor de nube para los servicios, y desplegarlo a un costo acorde a las necesidades de las organizaciones es un trabajo cuidadoso que se debe confiar a profesionales idóneos, por tanto, es importante conocer la capacidad de la computación en nube federada para garantizar un uso eficiente de los recursos informáticos incluso cuando la demanda global es baja [9]. Esta capacidad, única en su género, pone de manifiesto la necesidad de aplicar estrategias adecuadas de gestión de recursos para los servicios IaaS prestados por los CSP federados en la nube. Esas soluciones son fundamentales no sólo para mantener la integridad, disponibilidad y fiabilidad de la calidad del servicio, sino también para liberar el potencial de los recursos informáticos subutilizados [10]. Una de las principales funcionalidades es del broker o pasarela de una nube federada, distribuye las peticiones de los clientes entre los CSP participantes, de forma que se aproveche la infraestructura múltiple de la computación en nube. Esto se consigue teniendo en cuenta varias funciones objetivo, en particular las relacionadas con la multiplexación estadística.

La computación en la nube federada IaaS, se apoya en muchos tipos de centros de datos, los centros de datos de la nube pública gestionados por los principales proveedores de servicios en la nube, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP), son ejemplos comunes de estos centros de datos. También desempeñan un papel importante los centros de datos privados propiedad de organizaciones o empresas individuales, que se encargan de su mantenimiento; así como, las configuraciones de los centros de datos híbridos que incorporan tecnología de nube pública y privada. Los centros de datos interconectados y los centros de datos periféricos situados más cerca de los clientes finales pueden mejorar el rendimiento y la capacidad de respuesta de los servicios de una nube federada. Debido a la variedad de tipos de centros de datos, los sistemas de nube federada pueden proporcionar una amplia gama de servicios y recursos para satisfacer diversas necesidades a los clientes.

No obstante, un entorno de la nube puede enfrentar incapacidad de los proveedores para gestionar los datos de los usuarios, la falta de transparencia y a riesgos de mala gestión, todo lo cual puede tener un impacto negativo significativo en la reputación de los proveedores de la nube [11]. Por ello, es muy necesario generar confianza para que el entorno de la nube sea fiable. En los últimos años, la investigación sobre nubes federadas ha crecido como medio de resolver a gran escala problemas que requieren un uso intensivo de grandes volúmenes de datos y cálculos. Debido a la complejidad de los modelos de prestación de servicios, la gestión de la confianza es una necesidad absoluta para los servicios en nube que funcionan de forma descentralizada. Para garantizar el éxito del despliegue en un entorno de nube federado, abierto, dinámico y lleno de imprevistos [12], es imprescindible establecer una relación de confianza entre usuarios, proveedores de servicios en la nube y proveedores de la nube. Existe una necesidad constante de protocolos y herramientas innovadores que puedan mejorar y evaluar el nivel de seguridad proporcionado por un servicio de computación en nube [13], sus intermediarios o su proveedor de servicios, en general la seguridad de un servicio federado en la nube tiene que abordar una amplia de temas, como la autenticación, la autorización y la protección de datos, entre otros.

Los objetivos de seguridad de la información son fundamentales, y para abordar adecuadamente estas temáticas de seguridad en relación con los servicios en la nube antes de su selección, el entorno de la nube exige el uso de una herramienta que pueda realizar evaluaciones y valoraciones de riesgos. Cuando se trata de conseguir seguridad en la arquitectura, la confianza es un componente que puede evaluarse a cualquier nivel [14], por ejemplo, no es lo mismo compara dos entidades, cuya confianza se determina entre ellas; en cambio, la reputación de una la nube es una evaluación global de la misma. Por lo tanto, en la práctica es vital elegir al proveedor entre una amplia gama de variables, para emitir un juicio de confianza.

Las nubes federadas proporcionan una mayor cantidad de recursos, lo que ayuda a mejorar tanto la rentabilidad como la calidad. Esto incluye mejoras, tanto para el usuario como para el proveedor, como reducción de la cantidad de tiempo necesario para realizar una tarea por un costo determinado, aumentar la cantidad de rendimiento que puede manejar el sistema u optimizar la forma en que se utilizan los recursos [15].

Cuando una nube descubre que su centro de datos está infrautilizado en un momento dado, tiene la opción de decidir si pone sus recursos a disposición de otras nubes. El propio centro de datos no puede desconectarse. Como resultado, existe la oportunidad de compartir los recursos y aumentar el rendimiento. Un cliente de la nube puede evitar fácilmente estar atado a un único proveedor utilizando muchas nubes y manteniendo la capacidad de mover fluidamente las cargas de trabajo entre ellas [16]. También es importante anotar que cuando un proveedor introduce cambios en sus políticas o precios que perjudican a sus clientes, éstos pueden cambiar rápidamente de servicio y gracias a la competencia, otro proveedor de nube puede ofrecer mejores acuerdos de nivel de servicio (SLA) a sus clientes. Garantizar rendimiento con recursos limitados de solo un único proveedor de servicios en la nube, es complejo, porque cuando se presenta un aumento repentino de la carga de trabajo puede provocar un descenso de rendimiento [17]. El rendimiento puede garantizarse utilizando varios proveedores de servicios en nube. La federación de nube es capaz de superar este inconveniente alquilando recursos a proveedores de servicios en nubes internacionales, asegurando así la calidad de servicio acordada previamente. Otro servicio importante es garantizar disponibilidad, un sistema en nube podrá restaurar los servicios federándose con otros proveedores de servicios en nube de forma inafectada en caso de catástrofes naturales imprevistas [18].

2.1. Descripción de Servicios Telemáticos para la Seguridad informática

La creciente actividad y necesidades del mercado informático ha dado lugar a una creciente demanda exponencial de recursos tecnológicos adicionales para satisfacer las necesidades de los clientes en las diferentes esferas de la demanda de servicios, como por ejemplo la seguridad informática y de la información. Ofrecer la calidad de servicio (QoS) prometida, al tiempo que se satisfacen dinámicamente diversas demandas de recursos puede resultar difícil, y riesgosa para el cliente por parte del proveedor cuando no tiene la infraestructura tecnológica necesaria.

Los servicios se seguridad de la información, son paradigmas establecidos por diferentes estándares internacionales y por múltiples fabricantes de tecnologías de comunicaciones de la información, ellos son “partners” colaborativos para agregar recursos no utilizados, lo que se traduce en beneficios financieros y de calidad del servicio. En particular, esta estrategia mejora la disponibilidad y la fiabilidad al tiempo que supera las dificultades de cada estándar para preservar la QoS en medio de fluctuaciones en la demanda de recursos.

Con el nuevo paradigma de la nube federada, se optimizan con éxito los recursos informáticos incluso durante los periodos de baja demanda, lo que exige una estrategia integral de gestión de recursos para la Infraestructura como Servicio (IaaS) dentro de los CSP participantes. Esta estrategia es crucial para preservar la calidad del servicio, garantizar la disponibilidad y la fiabilidad, y optimizar los recursos informáticos subutilizados.

La presente investigación, muestra las novedades de la nube IaaS, revelando una metodología que reorienta los sistemas de nube tradicionales. El marco propuesto para la nube IaaS investiga la migración de máquinas virtuales y la consolidación de recursos, construyendo unos cimientos sólidos basados en los principios de IaaS y haciendo hincapié en el papel crucial de la virtualización. La técnica introduce conceptos pioneros como el Usuario de la Nube (CU) y la Gestión de la Reputación, reforzados por algoritmos específicos que mejoran la seguridad y la confianza en los servicios en la nube. Además, la combinación de los componentes Trust Manager (TM) y Broker Manager (BM) refuerza el control de los SLA y la evaluación de la confianza, alineándose sin problemas con los estándares de IaaS para mejorar la calidad y fiabilidad del servicio.

Para la creación de perfiles de usuario, como son los privados, sociales y corporativos, proporciona una lente independiente para gestionar con éxito a los usuarios de la nube dentro del panorama de IaaS, lo que permite la prestación de servicios personalizados. El SMI y los algoritmos de clasificación de vanguardia, como el algoritmo basado en Deep Q, optimizan la selección y clasificación de proveedores de servicios en la nube, un aspecto importante del IaaS. También el uso del algoritmo Banker y de un plan integral de gestión de acuerdos de nivel de servicio (SLA) proporciona una asignación eficiente de los recursos, reflejando los estándares reconocidos de IaaS.

Este estudio de investigación no sólo arroja luces sobre estas técnicas pioneras, sino que también proporciona lineamientos para el diseño de la nube IaaS y la gestión de recursos, calidad y fiabilidad. La creación de perfiles de usuario, que se clasifica en perfiles privados, sociales y corporativos, proporciona una lente independiente para gestionar con éxito a los usuarios de la nube dentro del panorama de IaaS, lo que permite la prestación de servicios personalizados. El SMI y los algoritmos de clasificación de vanguardia, como el algoritmo basado en Deep Q, optimizan la selección y clasificación de proveedores de servicios en la nube, un aspecto importante del IaaS. El uso del algoritmo Banker y de un plan integral de gestión de acuerdos de nivel de servicio (SLA) proporciona una asignación eficiente de los recursos, reflejando los estándares reconocidos de IaaS. Este estudio de investigación no sólo arroja luz sobre estas técnicas pioneras, sino que también establece un nuevo estándar para el diseño de la nube IaaS y la gestión de recursos, calidad y fiabilidad.

2.2. Clasificación de los Tipos de Ataques a los Sistemas Financieros y Banca en Línea

En el presente aparte presentamos una visión de los ataques más recurrentes a los sistemas financieros y banca en línea y sus tendencias. Se identifican los ataques que están disminuyendo en su uso y los que están surgiendo gracias a los nuevos desarrollos de la tecnología digital, que se utilizan hoy en día y al comportamiento de los usuarios. La seguridad de los sistemas financieros y banca en línea, es un tema de investigación muy conocido y podemos encontrar mucha bibliografía de estudios y artículos científicos, que aportan al mismo en [18, 19, 20, 21, 22, 23], hemos concluido en presentar cuatro grupos de ataque como son, ataques de autenticación y autorización, ataques de comunicación, ataques al sector financiero, y robo de identidad y bancario y

sus correspondientes clases, con base en las referencias anteriores. La clasificación, facilita la orientación en el conocimiento de los ataques a los sistemas financieros y banca en línea, pero de ninguna manera la propuesta es definitiva o excluyente.

Ataques de autenticación y autorización	1. Adivinación de claves (Password guessing)
	2. Búsqueda exhaustiva (Exhaustive search)
	3. Suplantación de identidad (Phishing)
	4. Ataque por canales (Cross chanel)
	5. Software malicioso (malware)
	6. Ingeniería social (Social Engineering)
	7. Inteligencia artificial (Inteligencia artificial)
Ataques de comunicación	1. Manipulación de datos (Data manipulation)
	2. Interceptación clandestina (Eavesdropping)
	3. Por intermediación humana (Man-in-the-middle)
	4. Interceptación humana de navegador (Man-in-the-browser)
Ataques al sector financiero y bancario	1. Secuestro informático (Ransomware)
	2. Internos (Insider)
	3. SWIT (Society for Worldwide Interbank Financial Telecommunications)
	4. Denegación del servicio (Denial-of-service)
	5. A Servidores (Server-side)
Robo de identidad	1. Robo de credenciales físicas (Phisical-credential-stealing)
	2. Accesos no autorizados (Unauthorized-binding)

Tab. Nº 1. Clasificación de los ataques a los sistemas financieros y bancario con base en los tres estándares investigados (Elaboración propia)

2.3. Ataques de autenticación y autorización

El atacante con este tipo de ataque, pretende acceder a credenciales de usuario válidas, como contraseñas, PIN o certificados, entre otros; para un servicio específico.

Imagen[3] Nº 1. Autenticación y autorización.

[3] https://www.google.com/search?sca_esv=c6b59d112dad26b9&sxsrf=ADLYWIKiKYvaY4bpxxika7PAA5v3VSDe2w:1730419746086&q=4.1+Ataques+de+autenticaci%C3%B3n+y+autorizaci%C3

2.3.1. Adivinación de contraseñas (Password guessing)

La adivinación de contraseñas, es un ataque basado que consiste en conseguir "adivinar" sistemáticamente la contraseña de un usuario. Existen múltiples enfoques, como un ataque basado en diccionario, un ataque de fuerza bruta o incluso ataques basados en el uso de redes neuronales [24]. Existen tres métodos principales para los ataques al sector financiero y bancario en línea, los cuales utilizan la misma técnica.

2.3.2. Búsqueda exhaustiva (Exhaustive search)

Conocido también como ataque de fuerza bruta, se basa en probar una gran cantidad (todas) de contraseñas o valores secretos posibles. Este es un enfoque que se utiliza comúnmente en diferentes entornos, entre ellos el financiero, no obstante, los casos de éxitos son limitados por la dificultad de obtener un archivo de contraseñas encriptadas. Sin embargo, es viable descifrar contraseñas de bases de datos de ofrecer una descripción general completa, agregamos la categoría de ataques directamente a credenciales filtradas u otras fuentes y pueden usarlas contra la autenticación financiera y bancaria. La computación distribuida de alto rendimiento se puede utilizar para aumentar la velocidad de ataque [25].

2.3.3. Suplantación de identidad (Phishing)

La suplantación de identidad (phishing), intenta engañar al usuario mediante correos electrónicos o páginas web fraudulentas para robar credenciales u otros datos personales [26]. Considerar al usuario como el eslabón más débil ha demostrado ser una técnica muy peligrosa y exitosa.

2.3.4. Ataques entre canales (Cross Chanel)

Tienen como como objetivo sistemas que utilizan autenticación multifactor (2FA), donde el posible intruso se ve obligado a atacar varios canales simultáneamente, por ejemplo, un ataque simultáneo a la conexión a Internet y a los mensajes SMS. Atacar varios canales suele requerir varios métodos, como una combinación de ingeniería social y piratería.

2.3.5. Malware (Malware)

Son aplicaciones utilizadas para engañar a los sistemas y/o usuarios, el malware especializado diseñado para robar credenciales [27], proviene de las palabras "malicious y software". La clase más común son los troyanos financieros y bancario, que se anuncia como una aplicación útil mientras extrae credenciales o respalda otros ataques en segundo plano. El malware moderno es multipropósito y existe malware tanto para sistemas operativos de computadoras como para dispositivos móviles.

2.3.6. Ingeniería social (Social Engineering)

La ingeniería social es una técnica que generalmente obtiene información de las redes sociales, la cual es utilizada para manipular a las personas, y obligarlas a que entreguen información confidencial, que incluye contraseñas, información bancaria o acceso a una computadora para acceder a información secreta de alto valor, como cuentas bancarias.

2.3.7. Ataques con inteligencia artificial

Con la fuerza descomunal como se está utilizando la inteligencia artificial, el sector financiero y bancario no se escapa al mal uso que hacen de ella los delincuentes, para acceder a información confidencial de las organizaciones y sus clientes. Los ataques se especializan exclusivamente en la autenticación biométrica, generalmente en el contexto del proceso "conozca a su cliente" (KYC), como la creación de muestras falsas para engañar a los sistemas de reconocimiento de huellas, voz y rostro. Los atacantes pueden utilizar un algoritmo de clase conocido como red generativa antagónica (GAN), que es una clase de algoritmos de aprendizaje automático diseñados para generar datos artificiales con las mismas estadísticas que el conjunto de entrenamiento [28]. Un ejemplo del uso de GAN es la creación de imágenes de ojos falsos [29].

2.4. Ataques de comunicación

Los ataques a las telecomunicaciones, tienen que ver con el acceso a la infraestructura del hardware, generalmente por medio de programas informáticos que realizan simulaciones o trasplante de usuarios, que escuchan pasivamente la comunicación entre dos partes o participan en ella de forma activa y transparente.

Imagen[4] Nº 2. Estructura de telecomunicación

2.4.1 Manipulación de datos (Data manipulation)

Con la manipulación de datos, el atacante no solo escucha la comunicación, sino que también modifica activamente los mensajes [30, 31], con el objetivo de obtener información relevante o el secuestro de la misma.

2.4.2 Interceptación clandestina (Eavesdropping)

Relacionado con escuchar de forma pasiva alguna comunicación que está sucediendo en una red de cualquier tipo, sin generar ninguna actividad, por ejemplo, ejecutar un software en un

[4] https://www.google.com/search?q=Ataques+ciberteticos+a+las+telecomunicaci%C3

dispositivo de red, que simplemente guarda todos los datos que han pasado a través de él. Los datos recopilados, ya sea cifrados o no, se analizan posteriormente y el atacante puede usarlos posteriormente [32, 33], los esquemas utilizados en todos los sectores de la industria, incluida la académica, por los grandes "beneficios" que se consiguen.

2.4.3. Intermediación humana ((Man-in-the-middle))

Estos esquemas de ataques informáticos conocidos como "Man-in-the-middle", el atacante secuestra todo el canal de comunicación y se posiciona en el medio de la comunicación para obtener acceso a los datos que las partes comunicantes no revelarían voluntariamente [34, 35], en la comunicación cifrada, el adversario crea canales cifrados para ambas partes comunicantes y descifra y vuelve a cifrar todos los mensajes [36], es de los cuidadosos en términos de corrupción, por lo que los procesos de selección de idoneidad debe ir acompañado con un fuerte componente de observancia y respeto por la ética.

2.4.4. Intermediación humana del navegador (Man-in-the-browser)

Los ataques en mención, corresponden a la combinación del tipo "Man-in-the-Browser" con uno del tipo "Man-in-the-middle", pero en este caso, el malware atacante está incrustado dentro de un navegador web [38], es decir, que los hace más complejo de neutralizar o mitigar, por es una trasposición de los dos tipos.

2.5. Ataques propios al sector financiero y bancario

Relacionados con los ataques dirigidos a organizaciones financieras y bancarias, en los cuales los ciberdelincuentes tienen el conocimiento de los procesos y procedimientos para el manejo de tecnología que realizan las organizaciones financieras y bancarias, y a partir de ese conocimiento realizan los diversos ataques con el objetivo robar o violar de datos, y realizar interrupciones o espionaje.

Imagen[5] Nº 3. Acceso fraudulento a servicios bancarios digitales

4.5.1. Secuestro Informático (Ransomware)

El secuestro informático (ransomware), es una categoría de malware capaz de cifrar los datos del usuario e impedir que este acceda a ellos, atacando así la disponibilidad y provocando un ataque

[5] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/tendencias-en-ciberseguridad-en-el-sector-financiero-85912

de denegación de servicio [38], posteriormente, el atacante exige un rescate a la víctima para restablecer el acceso a los datos al momento del pago o transacciones en línea.

2.5.2 Ataques internos (Insider)

Una amenaza interna es un riesgo de seguridad que se origina dentro de la organización atacada. Esto no significa que el actor deba ser un empleado o funcionario actual de la organización. Puede ser alguien externo que se posicionó dentro de la infraestructura de una organización [39].

4.5.3. Ataques SWIFT

Internacionalmente existen varias plataformas que prestan servicios para transacciones financieras y bancarias, pero la más utilizada es, SWIFT (Society for Worldwide Interbank Financial Telecommunications), la cual es un sistema de mensajería electrónica entre bancos, que constituye el principal medio de comunicación para transferencias bancarias internacionales, por cubrimiento y niveles de seguridad, lo cual la hace objeto multiplex e incontables ataques a nivel global.

Estos ataques intentan aprovechar posibles vulnerabilidades en el sistema de interfaz SWIFT, que facilite a los ciberdelincuentes obtener credenciales SWIFT legítimas o de los dispositivos de los bancos. Esto lleva al envío de solicitudes falsas de transferencia de fondos SWIFT a otros bancos [40].

2.5.4. Denegación de servicio (DoS)

Los ataques del tipo denegación del servicio “DoS”, enviará múltiples solicitudes al recurso web atacado para exceder la capacidad del sitio web de manejar múltiples solicitudes y evitar que el sitio web funcione correctamente [41, 42], en algunos casos pueden ser cíclicos convirtiéndolos en recurrentes en intervalos de tiempos aleatorios.

2.5.5 Ataques a servidores (Server-side)

Son ataques lanzados directamente por un ciberdelincuente a un servicio que escucha. Los ataques a aplicaciones web son dominantes en estos días, como lo describe OWASP [43], como inyección SQL, secuencias de comandos entre sitios, autenticación y administración de sesiones defectuosas, etc. [44].

2.6. Robo de identidad

Mediante el robo de identidad, el atacante se apodera de la identidad de alguien para realizar diversos actos fraudulentos o comportamientos delictivos.

Imagen[6] Nº 4. Riesgos de robo de identidad

2.6.1 Robo de credenciales físicas (Phisical-credential-stealing)

Con el robo real de tarjetas de identificación y/o transaccionales físicas o digitales, se pueden crear documentos falsos de alto valor, como pasaportes, licencias de conducir, tarjetas de crédito, extractos bancarios, declaraciones de impuestos, entre otros.

2.6.2. Accesos no autorizados (Unauthorized-binding)

La vinculación no autorizada, es una clase de ataque que tiene por objetivo vincular un dispositivo de autenticación personal (como un token HW, una tarjeta SIM o una clave privada) a la cuenta de la víctima. Debido al uso común de códigos SMS como un segundo factor fuera de banda, los ataques más relevantes están dirigidos a los operadores de telecomunicaciones.

Un ejemplo son ataques de intercambio de SIM, así como, los ataques SS7, el intercambio de SIM es una técnica para desviar los servicios de telecomunicaciones incluidas las llamadas y los SMS de la cuenta del operador móvil de la víctima y transferirlo a una nueva tarjeta SIM controlada por un atacante [45], de igual forma, los ataques SS7 desvían los servicios de telecomunicaciones a un atacante, pero esos ataques siguen el esquema "Man-in-the-middle" y violan los protocolos del Sistema de Señalización 7 (SS7) utilizados para llamadas telefónicas públicas [46], en síntesis los esquemas de ataques utilizan el patrón de intrusión.

3. Estándares de seguridad de la información

3.1. Estándar "NIST" Instituto Nacional de Estándares y Tecnología

El estándar "NIST" (National institute of standards and Technology), es un conjunto de productos estrechamente integrados que permite a los equipos de seguridad de cualquier tamaño detectar, investigar y responder rápidamente a las amenazas en toda la empresa, y se fundamenta en un procedimiento de tres etapas: valoración del riesgo; reducción del riesgo; y evaluación y análisis. Estas

[6] https://elceo.com/tecnologia/bancos-casi-listos-para-solicitar-biometricos-a-clientes-podran-disminuir-el-robo-de-identidad/

categorías incluyen la administración de identidad y el control de acceso, la sensibilización y formación, la protección de datos, los procedimientos y procesos de salvaguarda de la información, el mantenimiento y la tecnología de protección.

También se encarga de impulsar la innovación y competitividad industrial de los Estados Unidos al impulsar la ciencia, los estándares y la tecnología de medición de formas que incrementan la seguridad económica y la calidad de vida; además salvaguardan la privacidad, la integridad y la disponibilidad del sistema y asisten en la administración de los peligros para la protección de los datos. El grupo de controles de los requisitos de privacidad del NIST abarca las protecciones administrativas, técnicas y físicas que asisten en la administración de los riesgos de privacidad y en la observancia de las regulaciones, los controles de seguridad del NIST, se presentan en la tabla número 2.

Identificación	Control
CCS11	Inventario de Dispositivos Autorizados y no Autorizados
CCS2	Inventario de Software Autorizado y no Autorizado
CCS3	Configuraciones Seguras de Software y Hardware para Dispositivos Móviles, Portátiles, Equipos de Escritorio y Servidores
CCS4	Proceso Continuo de Identificación Y Remediación de Vulnerabilidades
CCS5	Control sobre Privilegios Administrativos
CCS6	Mantenimiento, Monitorización y Análisis de LOGs de Auditoría
CCS7	Protección del Correo Electrónico y del Navegador
CCS8	Defensas Contra el Malware Avanzado de Correo Electrónico y del Navegador
CCS9	Limitar y Controlar los Puertos de Red, Protocolos y Servicios
CCS10	Capacidad de Recuperación de Datos
CCS11	Configuraciones Seguras de Dispositivos de Red (Firewalls, Routers y Switches)
CCS12	Defensa Perimetral
CCS13	Protección de los Datos
CCS14	Acceso Basado en la Necesidad de Conocer (Need to Know)
CCS15	Control de Acceso Wireless
CCS16	Control y Monitorización de Cuentas de Sistema
CCS17	Verificación de las Habilidades de Seguridad y Formación Adecuada
CCS18	Seguridad en el Ciclo de Vida de las Aplicaciones
CCS19	Gestión y Respuesta a Incidentes
CCS20	Realizar Test de Penetración y Ejercicios de Ataque

Tabla Nº 2. Controles de seguridad clasificados con base en el "**NIST"**

3.2 Estándar ISO-IEC 27002 de 2013.

SO/IEC 27002 es un estándar internacional utilizado como referencia para los controles al implementar un Sistema de Gestión de Seguridad de la Información, incorporando controles de acceso a datos, control criptográfico de datos confidenciales y administración de claves [47]. La versión del 2013 contiene 14 dominios, 35 objetivos y 114 controles; puede mitigar las multas de incumplimiento de los requisitos de protección de datos y, a su vez, previene las pérdidas financieras de violaciones de datos; esta fundamentada en el ciclo de Planificación-Ejecución-Verificación-Actuar (PDCA), también denominado rueda de Deming o ciclo de Shewhart. El ciclo PDCA puede ser implementado no solo en todo el sistema de administración, sino también en cada componente individual para asegurar un

enfoque constante en la mejora constante de cual tipo de organización en lo referente a la gestión de la tecnología.

Cuando vemos que, la norma ISO 27002, titulada "Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información" proporciona una lista de controles y buenas prácticas que pueden utilizarse como guías al seleccionar e implementar medidas para lograr la seguridad de la información [48], nos acercamos a una posible convergencia con otros estándares internacionales, cuya utilización es de un valor sustantivo en muchos sectores, incluyendo el financiero, que es el fin del presente artículo.

3.3. Norma seguridad de datos PCI-DSS 3.2.1

La norma de seguridad de datos "PCI-DSS 3.2.1", La PCI DSS comprende un conjunto mínimo de requisitos para proteger los datos de cuentas y se puede mejorar por medio de controles y prácticas adicionales a fin de mitigar los riesgos, así como leyes y regulaciones locales, regionales y sectoriales. Además, los requisitos de la legislación o las regulaciones pueden requerir la protección específica de la información de identificación personal u otros elementos de datos (por ejemplo, el nombre del titular de tarjeta). Las PCI DSS no sustituyen las leyes locales ni regionales, las regulaciones gubernamentales ni otros requisitos legales [49].

La norma en cuestión, se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen las comerciales, procesadores, adquirentes, entidades emisoras y proveedores de servicios. La PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta y/o datos confidenciales de autenticación [50], al ser una cuyo cumplimiento es obligatorio para las organizaciones del sector financiero, a línea con la investigación del presente estudio, y complemento la posibilidad de la convergencia.

4. Tendencias generales del sector financiero y bancario en términos de seguridad

a) Las empresas de servicios financieros son víctimas de ataques de ciberseguridad 300 veces más frecuentemente que las empresas de otras industrias, el número de incidentes de seguridad en este sector se ha triplicado en último lustro, la denegación de servicio, la ingeniería social, las descargas automáticas y el phishing para difundir troyanos bancarios y personas malintencionadas siguen siendo las estrategias de ataque más frecuentes [19].

b) Los ataques a este sector representaron el 17 por ciento de todos los ataques en las 10 industrias más atacadas [51].

c) La ingeniería social sigue siendo la amenaza número uno para vulnerar las defensas de la seguridad, independientemente de la madurez y frecuencia de las campañas de concienciación sobre seguridad [52].

d) Una de las razones del aumento de la cantidad de ataques es su disponibilidad y accesibilidad, incluso para personas sin conocimientos profundos. Muchas herramientas de ataque, especialmente malware, (incluso exploits de día cero) y kits de phishing, están disponibles para su compra en mercados de la web oscura [53, 54,55].

e) El uso creciente de la Inteligencia Artificial (IA) tanto en sistemas de producción como en herramientas de ataque introduce nuevas posibilidades de ataques. Aunque las superficies de ataque de la IA están apenas surgiendo, Accenture advierte que las estrategias de seguridad deben centrarse en fortalecer sus modelos críticos de IA. Esos modelos se están volviendo cada vez más complejos, lo que aumenta el riesgo de que un adversario descubra un comportamiento particular del modelo que conduzca a su explotación [56].

f) El desarrollo de malware nuevo no cesa, y su detección y mitigación es un proceso interminable, podemos observar que recientemente los troyanos de tipo financieros y bancarios y el ransomware han ganado popularidad y, por lo tanto, el desarrollo de malware de esas categorías está en aumento. Debido a la popularidad y apertura del sistema operativo Android, se convirtió en un objetivo importante del malware móvil.

5. CONCLUSIONES

La principal contribución de este artículo radica en la revisión y evaluación de la seguridad de los esquemas de autenticación compuestos por combinaciones viables de métodos de autenticación en relación con los estándares concurrentes, principalmente la directiva. Para realizar dicha, hicimos la clasificación descrita en el numeral 4, de igual forma describimos la caracterización de los tres estándares que son susceptibles de convergencia en el sector bancario por ende de implementación en el numeral 5. Por tanto, las organizaciones financieras y bancarias deberían tener en cuenta que:

a. Los ataques a la banca electrónica compatible con las amenazas autenticadoras de las Directrices de identidad digital del NIST, pero con un mayor nivel de detalle con respecto al área de la banca electrónica tradicional.

b. Los métodos de autenticación actuales y sus propiedades en el contexto de los estándares internacionales.

c. Posibilidad de combinaciones de los esquemas de autenticación multifactor compuestos por los métodos de autenticación actuales y su cumplimiento convergente con el NIST, ISO 27002 y PCI-DSS 3.2.1.

d. El marco propuesto para la nube IaaS investiga la migración de máquinas virtuales y la consolidación de recursos, construyendo una base sólida fundamentada en los principios de IaaS y haciendo hincapié en el papel crucial de la virtualización.

e. Los componentes de usuario en la nube (CU) y la gestión de reputación, reforzados con algoritmos específicos, aumentan enormemente la seguridad y la confianza en los servicios en nube; y la adición de los componentes Trust Manager (TM) y Bróker Manager (BM), mejora la supervisión de los SLA y los métodos de evaluación de la confianza, al tiempo que se ajusta a los estándares IaaS para aumentar la calidad y fiabilidad del servicio en la nube.

En síntesis, brindamos una visión actualizada y completa acerca de la seguridad informática y de la información para las organizaciones financieras y bancaria en línea, lo que permite al lector tener una descripción general de las opciones disponibles y sus ventajas y desventajas en el contexto de las regulaciones nacionales e internacionales.

Referencias

[1] Swiss Finance Council. (2020). "*Getting Ready for the '20s-Technology and the Future of Global Banking"*. abril. 15, 2024. https://www.swiss_nancecouncil.org/images/ SFC_Discussion_Paper_2020.pdf

[2] Deloitte. (Aug. 2020). FEBRABAN Banking Technology Survey. Accessed: Abril. 17, 2024. https: //www2.deloitte.com/content/dam/Deloitte/br/Documents/_nancialservices/2020%20FEBRABAN%2 0Banking%20Technology%20Survey.pdf

[3] Deloitte. (2019). Global Mobile Consumer Survey: UK Cut.Accessed: Abril 18, 2024. https://www2. deloitte.com/content/dam/Deloitte/uk/Documents/technology-mediatelecommunications/deloitte-uk-plateauing-at-the-peak-the-state-of-thesmartphone.pdf

[5] Pew Research Center. (Feb. 2019). Smartphone Ownership is Growing Rapidly Around the World, but Not Always Equally. abril 20, 2024. https://www.pewresearch.org/global/wp-content/uploads/sites/2/2019/02/Pew-Research-Center_Global-Technology-Use 2018_2019-02-05.pdf

[6] https://www.ucm.es/otri/complutransfer-agentes-software

[7] Kwang, Mong Sing. Computación en la nube basada en agentes. IEEE Trans. Serv. Computación 5 (4) (2011) 564-577.

[8]https://www.researchgate.net/publication/275041433_Global_Trust_A_Trust_Model_for_Cloud_S ervice_Selection

[9] J. Liu, Y. Chen, Una QoS personalizada basada en clústeres y confiable basada en la confianza. Enfoque de predicción para la recomendación de servicios en la nube en la fabricación en la nube. Knowl. -Sistema basado. (2019), https://doi.org/10.1016/j.knosys

[10] A. Asuan, "Transaksi perbankan melalui internet banking," Solusi, vol. 17, no. 3, pp. 317–335, 2019.10.36546/solusi.v17i3.220.

[11]R. Lai, T. Wang y YZ Chen, "Uso de cifrado simétrico de cuadrícula para la protección de la privacidad de la ubicación", J. Commun., vol. 13, núm. 11, págs. Apocalipsis 673–678.

[12]D. Prokopowicz, S. Gwozdziewicz, J. Grzegorek y M.Matosek, "Determinantes de la seguridad d e la transferencia electrónica diaria en el contexto de las tendencias globales en el desarrollod e la banca móvil en Internet", Int. JN Economía. Soc. Ciencia, vol. 7, núm. 1, págs. Apocalipsis 18 8–201

[13]M. Negnevitsky, “Identificación de bancos en quiebra mediante agrupacióncon redes neuronales autoorganizadas”, Procedia Comput. Ciencia, vol. 108, págs. 101-1 1327-1333

[14] F. Buccafurri and G. Lax, "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, vol. 11, pp. 271-296, 2011

[15] A. Braeken, "Public key versus symmetric key cryptography in client–server authentication protocols," International Journal of Information Security, vol. 21, pp. 103-114, 2022

[16] R.Naresh, AyonGupta, Sanghamitra, “Malicious Url Detection System Using Combined Svm And Logistic Regression Model”, International Journal of Advanced Research in Engineering and Technology, vol. 10, Nº. 4, pp. 63-73, 2020.

[17] Gautam Srivastava, C.N.S. Vinoth Kumar, V Kavitha, N Parthiban, Revathi Venkataraman, “Two-Stage Data Encryption using Chaotic Neural Networks”, Journal of Intelligent and Fuzzy Systems, vol. 38, no. 3, pp. 2561-2568, 2020.

[18] R. Mugesh, “A Survey on Security Risks in Internet of Things (IoT) Environment,” Journal of Computational Science and Intelligent Technologies, vol. 1, no. 2 pp. 01-08, 2020. https://doi.org/ 10.53409/mnaa.jcsit20201201

[19] L. Pascu. (2018). Top Security Challenges for the Financial Services Industry in 2018. Bitdefender. accessed: Mayo 10 2024. https://www.bitdefender.com/_les/News/CaseStudies/study/240/Bitdefender-Top-Security Challenges-for-the-Financial-WhitepaperEN-interactive.pdf

[20] F-Secure. Threat Analysis: SWIFT Systems and the SWIFT Customer Security Program. Accessed: Mayo 11, 2024. https://wwwsecure.com/content/dam/f-secure/en/business/common/collaterals/fsecure-threat-analysis-swift.pdf

[21] M. A. Kazi, S. Woodhead, and D. Gan, “A contemporary taxonomy of banking malware,” in Proc. Int. Conf. Sci. Comput. Cryptogr., Dec. 2018, p. 7. https://www.researchgate.net/publication/344017237_A_Contempory_Taxonomy_of_Banking_Malware

[22] P. Black, I. Gondal, and R. Layton, “A survey of similarities in banking malware behaviours”, Comput. Secur., vol. 77, pp. 756_772, Aug. 2018.

[23] A. F. A. Kadir, N. Stakhanova, and A. A. Ghorbani, “Understanding Android _nancial malware attacks: Taxonomy, characterization, and challenges”, J. Cyber Secur. Mobility, vol. 7, no. 3, pp. 1_52, Jul. 2018.

[24] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, “Fast, lean, and accurate: Modeling password guessability using neural networks”, in Proc. 25th USENIX Conf. Secur. Symp. Berkeley, CA, USA: USENIX Association, 2016, pp. 175_191.

[25] R Hranický, L Zobal, O Ryavý, and D Kolár, “Distributed password cracking with BOINC and hashcat”, Digit. Invest., vol. 30, pp. 161_172, Sep. 2019.

[26] K. D. Nguyen, H. Rosoff, and R. S. John, “Valuing information security from a phishing attack”, J. Cybersecur., vol. 3, no. 3, pp. 159_171, Nov. 2017.

[27] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, “Data breaches, phishing, or malware? Understanding the risks of stolen credentials”, in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. New York, NY, USA: ACM, Oct. 2017, pp. 1421_1434.

[28] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, “Generative adversarial nets”, in Proc. 27th Int. Conf. Neural Inf. Process. Syst. (NIPS), vol. 2. Cambridge, MA, USA: MIT Press, 2014, pp. 2672_2680.

[29] J. E. Tapia and C. Arellano, “Soft-biometrics encoding conditional GAN for synthesis of NIR periocular images”, Future Gener. Comput. Syst., vol. 97, pp. 503_511, Aug. 2019. K. Lee, B. Kaiser, J. Mayer, and A. Narayanan, ``An empirical study of

[30] J. Fuller, B. Ramsey, J. Pecarina, and M. Rice, “Wireless intrusion detection of covert channel attacks in ITU-T G.9959-based networks”, in Proc. 11th Int. Conf. Cyber Warfare Secur. (ICCWS), 2016, pp. 137_145.

[31] S. Sridhar and G. Manimaran, “Data integrity attacks and their impacts on SCADA control system”, in Proc. IEEE PES Gen. Meeting, Jul. 2010, pp. 1_6.

[32] W. Yang, Z. Zheng, G. Chen, Y. Tang, and X. Wang, “Security análisis of a distributed networked system under eavesdropping attacks”, IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 67, no. 7, pp. 1254_1258, Jul. 2020.

[33] D. Li, H. Zhou, and W. Yang, “Privacy-preserving consensus over adistributed network against eavesdropping attacks”, Electronics, vol. 8, no. 9, p. 966, Aug. 2019.

[34] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks”, IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2027_2051, 3rd Quart., 2016.

[35] M. Kneevic, S. Tomovic, and M. J. Mihaljevic, “Man-in-the-middle attack against certain authentication protocols revisited: Insights into the approach and performances re-evaluation”, Electronics, vol. 9, no. 8, p. 1296, Aug. 2020.

[36] M. Kneevic, S. Tomovic, and M. J. Mihaljevic, “Man-in-the-middle attack against certain authentication protocols revisited: Insights into the approach and performances re-evaluation”, Electronics, vol. 9, no. 8, p. 1296, Aug. 2020.

[37] The OWASP Foundation. (2006). Man-in-the-Browser Attack. Accessed: Mayo. 26, 2024. https://owasp.org/wwwcommunity/attacks/Man-in-the-browser_attack

[38] A. Mauraya, N. Kumar, A. Agrawal, and R. Khan, “Ransomware: Evolution, target and safety measures”, Int. J. Comput. Sci. Eng., vol. 6, no. 1, pp. 80_85, 2017.

[39] J. Petters. (Sep. 2020). What is an Insider Threat? De_nition and Examples. Accessed: Mayo. 29, 2024. https://www.varonis.com/blog/insider-threats/

[40]Kaspersky. (2017). ¿Qué es un ataque DDoS? - Significado de DDoS. Mayo 27 de de 2024. https://www.kaspersky.com/centro-de-recursos/amenazas/ataques-ddos

[41] Kaspersky. (2017). ¿Qué es un ataque DDoS? - Significado de DDoS. Mayo 28 de de 2024. https://www.kaspersky.com/centro-de-recursos/amenazas/ataques-ddostécnicas", Int. J. Di strib. Sensor Netw., vol. 13, núm. 12, diciembre de 2017,N.º de artículo 155014771774146.
[42] JA Hill, "'Robos bancarios SWIFT y artículo 4ª", J. Consum. Commercial Derecho, vol. 22, núm. 1, págs. 1–7, 2018.

[43] The OWASP Foundation. (2017). OWASP Top Ten. Mayo. 28, 2024. https://owasp.org/wwwproject-top-ten/2017/

[44] A. Mauraya, N. Kumar, A. Agrawal, and R. Khan, "Ransomware: Evolution, target and safety measures", Int. J. Comput. Sci. Eng., vol. 6, no. 1, pp. 80_85, 2017.

[45] K. Lee, B. Kaiser, J. Mayer, and A. Narayanan, "An empirical study of wireless carrier authentication for SIM swaps", in Proc. 16th Symp. Usable Privacy Secur. Berkeley, CA, USA: USENIX Association, Aug. 2020, pp. 61_79.

[46] K. Ullah, I. Rashid, H. Afzal, M. M. W. Iqbal, Y. A. Bangash, and H. Abbas, ``SS7 vulnerabilities_A survey and implementation of machine learning vs rule based _ltering for detection of SS7 network attacks,"IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1337_1371, 2nd Quart., 2020.

[47] https://cpl.thalesgroup.com/es/compliance/isoiec-270022013-compliance#:~:text=ISO%2FIEC%2027002%20es%20un,confidenciales%20y%20administraci%C3%B3n%20de%20claves.

[48] Diamantopoulou, V. "From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance", pp. 253-272, Conference Computer Security. ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers.

[49] https://listings.pcisecuritystandards.org/documents/PCI_DSS_v3-2es-LA.pdf

[50] Ibidem.

[51] IBM. (2020). IBM X-Force Threat Intelligence Index. https://www.ibm.com/account/reg/signup?formid=urx-42703

[52] Accenture. (2019). Future Cyber Threats. https://www.accenture.com/_acnmedia/pdf100/accenture_fs_threat-report_approved.pdf

[53] E. Mikalauskas. (Sep. 2020). Report: Buying Your Own Malware has Never Been Easier. https://cybernews.com/security/buying-your-own-malware-has-neverbeen-easier/

[54] H. Poston. (2020). Cybercrime at Scale: Dissecting a Dark Web Phishing Kit. Infosec. https://resources.infosecinstitute.com/cybercrime-at-scale-dissectingadark-web-phishing-kit/

[55] A. Lakhani. (Jul. 2020). How Threat Researchers Leverage the Darknet to Stay Ahead of Cyber Threats. Fortinet. https://www.fortinet.com/blog/threat-research/howthreatresearchers-leverage-darknet-to-stay-ahead-of-cyber-threats

[56] Accenture. (2019). Know Your Threat: AI is the New Attack Surface. Accessed: Feb. 15, 2021. [Online]. Available: https://www.accenture.com/acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf