Ciencia Latina
Revista Multidisciplinar

DOI: https://doi.org/10.37811/cl_rcm.v7i1.4661

Análisis de la ciberseguridad en el sector financiero de México con el fin de implementar la metodología Zero trust y mejorarla

José Antonio Zárate Urgell
a-zarateu@choapas.tecnm.mx
https://orcid.org/0000-0003-1442-0121
Tecnológico Nacional de México/ITS Las Choapas y
Universidad Americana de Europa (UNADE)

Selene García Nieves
s-garcian@choapas.tecnm.mx
https://orcid.org/0000-0002-9412-3110
Tecnológico Nacional de México/ITS Las Choapas

Angélica González Becerra
a-gonzalezb@choapas.tecnn.mx
https://orcid.org/0000-0002-6046-2958
Tecnológico Nacional de México/ITS Las Choapas

Itzel Antonio Toledo
i-antoniot@choapas.tecnm.mx
https://orcid.org/0000-0002-8871-5494
Tecnológico Nacional de México/ITS Las Choapas

Alejandrina Isabel Cruz Rodríguez
a-cruzr@choapas.tecnm.mx
https://orcid.org/0000-0001-8277-7259
Tecnológico Nacional de México/ITS Las Choapas
México

RESUMEN

Muchas de las entidades financieras mundiales se están haciendo eco de las grandes amenazas que deben lidiar a diario. Mediante esta investigación se pretende entender como es que funcionan las instituciones financieras, los peligros que afrontan y los retos. Se deducirá como es el nivel de seguridad a nivel informático y mediante las estadísticas determinar como es que reaccionan los sistemas. En este estudio se procederá a investigar como el método Zero Trust puede darle una capa de seguridad a los sistemas de las entidades financieras, las diferencias que tienen con los métodos de seguridad actuales y como se puede implementar teniendo en cuenta las debilidades y fortaleza del mismo.

Palabras clave: *ciberseguridad; zero trust; confianza cero; zt; ZTA*

Correspondencia: a-zarateu@choapas.tecnm.mx
Artículo recibido 28 diciembre 2022 Aceptado para publicación: 29 enero 2023
Conflictos de Interés: Ninguna que declarar

Cómo citar: Zárate Urgell, J. A., García Nieves, S., González Becerra, A., Toledo, I. A., & Cruz Rodríguez, A. I. (2023). Análisis de la ciberseguridad en el sector financiero de México con el fin de implementar la metodología Zero trust y mejorarla. Ciencia Latina Revista Científica Multidisciplinar, 7(1), 3384-3408. https://doi.org/10.37811/cl_rcm.v7i1.4661

Analysis of cybersecurity in the Mexican financial sector in order to implement the Zero trust methodology and improve it

ABSTRACT

Through this research, it is intended to improve the security of the financial entity of Mexico in order to implement the ZERO Trust methodology and be able to improve the system, therefore, it will be investigated how the financial system works and the improvements that could be made based on the results obtained.

Keywords: *cibersecurity; zero trust; zt; ZTA*

INTRODUCCIÓN

El sector financiero es uno de los sistemas donde más se invirtió en tecnología y seguridad para brindar un servicio que resguarde la información de los clientes. Esto viene de la mano del avance en los ataques a las entidades, estas son el blanco de organizaciones dedicadas los ciberdelitos, debido a los activos y datos que se encuentran en estas entidades. En el informe publicado por OAS.ORG menciona que el 2018 varios bancos fueron victimas de ataques cibernéticos, lo llamativo de estos ataques es que se los atacantes no eran del país de origen lo cual deja en claro los objetivos de los ciberdelincuentes a nivel global.

En otro informe provisto por Banxico (2021) de México menciona las estrategias que se implementaron en sus sistemas, desde los más básico (antivirus, firewalls, IDS, tokens de acceso, etc.) hasta la implementación de controles sofisticados. Menciona que a partir del año 2017 se elaboro un programa para reforzar el sistema financiero el cual comprendía, proteger la información y los procesos, abordar el tema desde una perspectiva tipo proactiva y de prevención de los riesgos. Ya por el 2020 el banco incremento la seguridad y madurez del sistema en donde incremento en 10 dominios de seguridad de la información.

El portal web f5.com menciona lo que es ZERO trust, el cual fue creado en el 2019 por John Kindervag que es analista principal de Forrester Research Inc., destaca que es una arquitectura donde termina con la idea fiable dentro de un perímetro definido, una red. Este es un modelo de seguridad el cual se centra en la verificación de cada usuario o dispositivo, el cual este dentro o afuera del perímetro, antes de que conceda el acceso. Esta centrado en la protección de datos y servicios, pero tambien se amplía a los activos de empresas y los sujetos, en este modelo:

- Supone que los atacantes están en la red.
- No se confía en nadie.
- No hay confianza implícita.
- Analiza y evalúa los riesgos dentro de la red.
- Mitiga los riesgos inherentes.

El informe sigue mencionando la importancia de una red ZERO trust, ya que en el pasado el lema era “confiar, pero verificar”, con este modelo el lema es “no confiar”, esto se debe a los ataques que se están viendo en el mundo sobre las organizaciones lo que

obliga a que las organizaciones deban reexaminar sus enfoques. Un punto a tener en cuenta es que la pandemia hizo que el trabajo se fuera a las casas donde estas son ahora las "oficinas" y esta modalidad de trabajo sigue aumentando lo cual deja atrás la seguridad perimetral.

En un informe de xatka.com menciona a las empresas como Microsoft, Google y Cisco que están considerando al sistema Zero trust como el futuro de la seguridad a nivel empresarial. Menciona que "monitoriza y autentifica continuamente a los usuarios que han accedido la red privada de la organización, incluso a los que están en la oficina de la compañía", esto se realiza que el usuario esta consultando diferentes datos o que esta usando herramientas dentro del sistema, este debe pasar por un nuevo proceso de verificación. Una de las grandes ventajas de este sistema es que dificultad los ataques de los ciberdelincuentes, menciona el informe que, si un intruso puede ingresar a la red, si este quiere seguir avanzando deberá "romper" las barreras que haya en cada nivel de profundidad, además las empresas podrán monitorizar los avances que den los usuarios dentro de la red, de esta forma se podrá tener conocimiento si un intruso logro eludir una barrera.

Ahora bien, no todo es reluciente entre las desventajas que se mencionan de este sistema es que usa mas recursos, es otras palabras esto es mayores costos y complejidad de la instalación, se debe tener en cuenta que este sistema puede configurar las zonas geográficas o tambien en el horario que no se permiten acceder a ciertos usuarios en la red.

En base estos antecedentes (xatka.com) y definiciones nos dejan en la necesidad de tener un sistema que sea seguro para las entidades bancarias, mejorando los sistemas que están preestablecidos. Tal como se mencionó, los ataques cada vez están siendo realizado por organizaciones de criminales que son financiados por los estados en algunos casos, por lo cual debemos preguntarnos: ¿Podrá el sistema Zero trust a mejorar la ciberseguridad en el sector financiero?

Objeto de investigación

- Mejorar la seguridad en los procesos financieros.

Campos de investigación

- Seguridad en los procesos realizados en el sector financiero. El objetivo primordial es la implementación del sistema Zero trust para añadir una capa de seguridad a los

servicios financieros.

METODOLOGÍA

El paradigma asumido es cuali-cuantitivo el cual incluye métodos del nivel teórico y empírico, esto permitirá la obtención de datos en cada etapa de la realización de la investigación.

La investigación aplicada se clasifica en estudios exploratívos, descriptivos y explicativos. En la primera etapa se consiguió la justificación de la investigación y determinar el problema que será explorativo-descriptivo. A medida que se explaye el estudio se presentara el marco teórico referencial que ser a de tipo analítico, descriptivo. Y en la última etapa de la investigación se realizará la solución del problema propuesto y su implementación.

En la practica cualquier estudio puede incluir varios tipos de investigación, en los cuales están los exploratívos que son las investigaciones de las posibles soluciones sobre el problema mencionado, descriptivos porque se describe el problema y la postura del autor y correlacional porque se medirán las variables que se intentaran ver si están relacionadas entre sí o no.

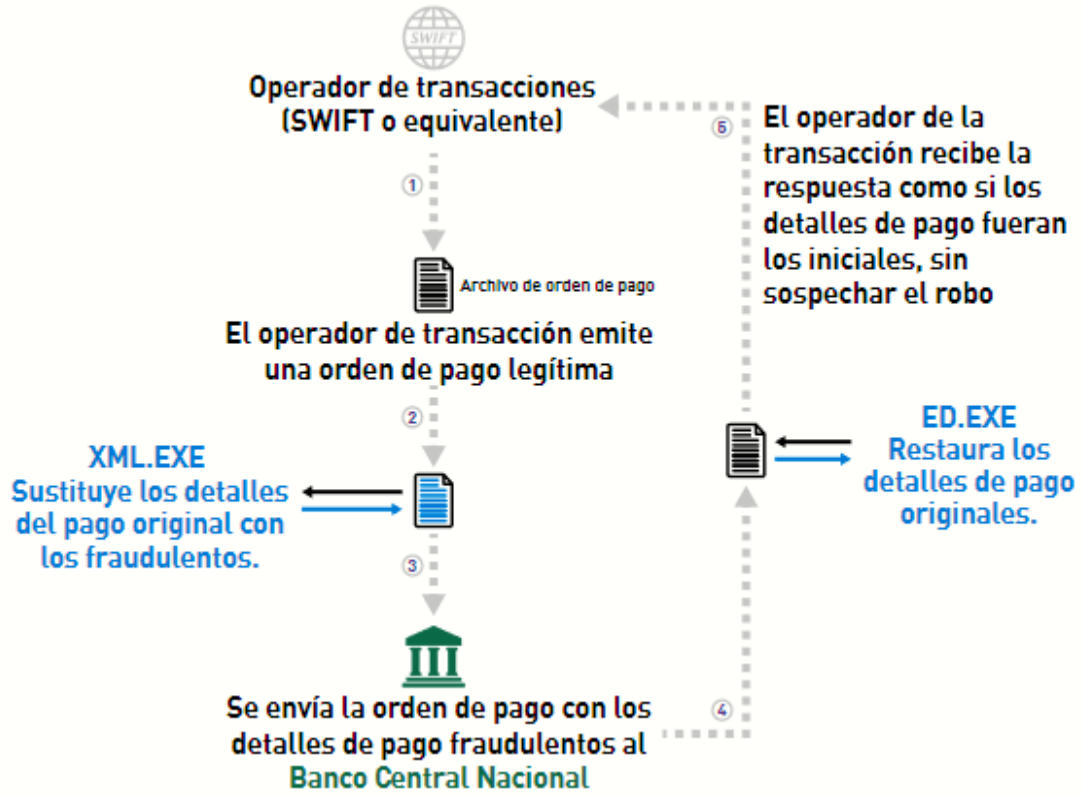
CIBERATAQUES

Como se mencionó anteriormente, los ciberdelincuentes cada vez están mejor organizados y además tienen financiación, en el informe de aos.org menciona este hecho. Destaca que estos delincuentes atacaran a los bancos o entidades donde proporcione el mayor retorno de la inversión. Estos grupos son altamente especializados y tienen experiencia en el sistema bancario, por ende, sirve toda la información que tienen para poder infiltrarse en el sistema, se destaca el profundo conocimiento sobre las redes, accesos a los recursos de software de alta y técnicas sofisticadas en las cuales se manejan estos grupos. Estas sofisticaciones permiten a los grupos atacar a manera global a cualquier entidad, un ejemplo de ello es el llamado grupo Fin7 el cual pueden ingresar a los sistemas y robar alrededor de USD 1.000 millones a las entidades financieras.

Otro punto que los delincuentes se aprovechan es de las debilidades de los cajeros automáticos mediante el software Ploutus, el cual dio muchos resultados favorables a tal punto que exportan al exterior este software. Ahora bien, los atacantes se están centrando en nuevos objetivos entre los cuales están los sistemas de pagos como SWIFT O SPEI de México, donde los atacantes han podido violar las seguridades que se tienen

en la arquitectura y los procesos de los bancos. En la siguiente imagen vemos el proceso del ataque contra los sistemas de pagos:

Ilustración 1 *Violación a los sistemas financieros*



En un informe del Grupo IB menciona que encontró que los grupos sofisticados como por ejemplo "moneyTaker" estabas realizando tareas de rastrillaje (recopilación de información), bien se sabe que para realizar ataques sofisticados primeramente se debe realizar un sondeo de las redes en las cuales están los sistemas a atacar, de esta forma se puede entender este comportamiento como la antesala de un futuro ataque contra bancos latinoamericano o del caribe. El informe continúa diciendo que de esta forma fue que se atacaron los sistemas de pagos SPEI en el 2018 y UniTeller de un grupo de Asia oriental. Entre las posibles formas de protección es la de una asociación entre bancos y el sector financiero para poder compartir información el cual el Foro Económico Mundial se presta ayudar para desarrollar estas capacidades de defensas y estimular estas asociaciones.

En el informe de infosegurity México, nos explica como fueron los ataques cibernéticos evolucionando y como las entidades financieras fueron desarrollando mejoras en la seguridad, una de esas mejoras son las ciber cajas fuertes en la nube, estas cajas fuertes utilizan contraseñas o métodos biométricos. Sigue mencionando que muchos de los

ataques están dirigidos a las entidades financieras que esto se acentuó en plena pandemia el cual la dificultad consiste en detectar y contrarrestar las amenazas avanzadas, por ejemplo, en el 2020 los ataques a las entidades financieras crecieron en 238%, y los ataques ransomware aumentaron 9 veces más. Se menciona que los ciberataques tienen éxito en un 88% y solamente el 22% son identificados.

Las entidades financieras deben monitorear aquellos que no conocen y poder predecir el comportamiento de las amenazas mediante IA analítica predictiva. De esta forma pretenden las entidades poder tener mejor seguridad en sus sistemas frente a las amenazas cada vez más complejas de las organizaciones criminales.

SISTEMA FINANCIERO

Cuando hablamos del sistema financiero debemos entender que es el motor que permite que el sistema comercial funcione. Ahora bien, que es y como funciona este sistema. Este sistema comprende de una serie de elementos que en conjunto proporcionan los medio para la adquisición de los recursos. Los agentes o bien se podría decir, los intermediarios son lo s que captan a los inversionistas en los mercados financieros. Este sistema se rige por un mercado que se controla y coordina las transacciones que se realizan, los precios y el valor de las mismas. En el se establecen los valores de cobros y los intereses que se generaran.

Entre las funciones del sistema financiero son:

- Canalizar los recursos económicos que se encuentren activos.
- Establece un funcionamiento eficiente de modo que sea trasparente las transacciones.
- Estimulación y crecimiento económico del sistema financiero del país, que corresponde al PBI, el cual trabaja por medio de los sistemas de ahorros e inversiones efectivas.
- Establece un control sobre los riesgos.
- Asigna eficientemente los recursos económicos que ingresan a los agentes económicos. Esto se da a cambio de garantías para los usuarios.

Este sistema tiene elementos y cada uno de ello cumple con las funciones específicas, entre ellas mencionan los activos financieros que son los medios que pueden financiar las actividades económicas, se debe entender que el activo es el dinero y permite esta

movilización, de allí se deriva el resto. Estos se destacan por generar rentabilidad, fija o variables, según su adquisición.

Los intermediarios financieros son un conjunto de instituciones que realizan las actividades financieras, estas se encargan de canalizar los procesos entre los agentes financieros y los recursos que se encuentran disponibles. Además, facilitan los procedimientos y permiten que las instituciones procedan a ejecutarlas.

Ahora bien, en cuanto a la situación de la seguridad en los sistemas financiero el informe de OAS de la seguridad financiera de México resalta que solo el "43% identifica ocurrencia de eventos de malware diariamente" en las instituciones grandes, "el 24% "en entidades medianas, y el "14%" en las entidades pequeñas. Destaca la importancia que se deben tener a los ataques y que las entidades financieras deben estar preparadas. Las autoridades que conforman el sistema financiero mexicano son:

- Secretaria de hacienda y crédito público.
- Comisión Nacional Bancaria y de valores.
- Comisión Nacional de Seguros y Finanzas.
- Comisión Nacional de Sistema de Ahorro para el retiro.
- Comisión Nacional para la protección y defensa de los usuarios de servicios Financieros.
- Instituto para la protección al ahorro Bancario.
- Servicio de administración tributaria.

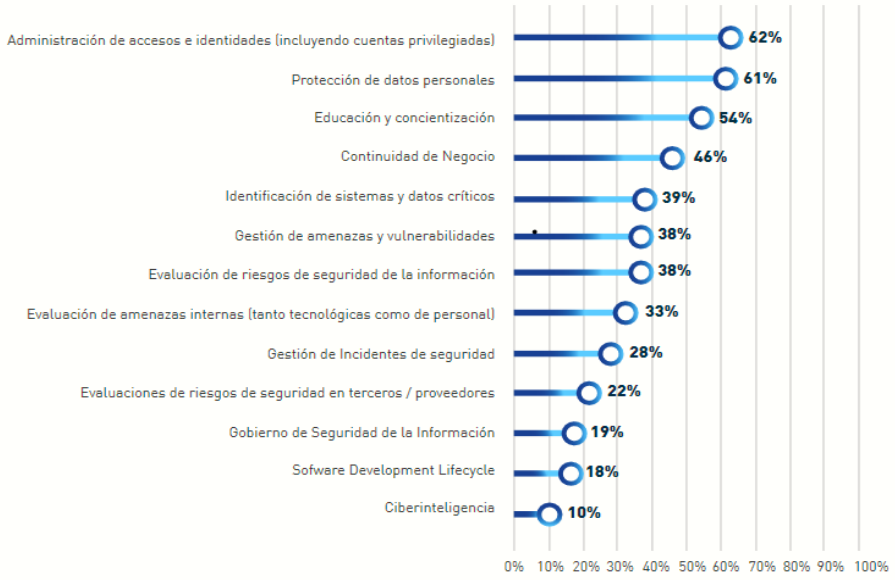
En el informe señala que muchas entidades tienen los servicios tercerizados, y los mas contratados son las pruebas de seguridad/ Análisis de vulnerabilidades que tiene un 74%, y un 65% en pruebas de seguridad. (de las muestras que se tienen en el informe). En cuanto a las aplicaciones de las normas ISO 27001 para el sector bancario de México se registra un 71% se concordancia, en frente de un 68% respecto a las entidades de América latina y el caribe.

Las detecciones y análisis de los eventos a nivel digital son muy importantes respeto al sistema de gestión de los riesgos, entre las cuales están los firewalls en un 85% en total, actualizar los softwares y/ o parches de seguridad en un 76%, copias de seguridad automatizadas en un 68%, redes privadas, IDS/IPS, secure e-mail, etc., un 54%. Se informa que el 100% de las entidades implementa medidas de seguridad en el hardware como

tambien en los mecanismos de autenticación, auditorias/ pruebas de penetración y controles de cifrado.

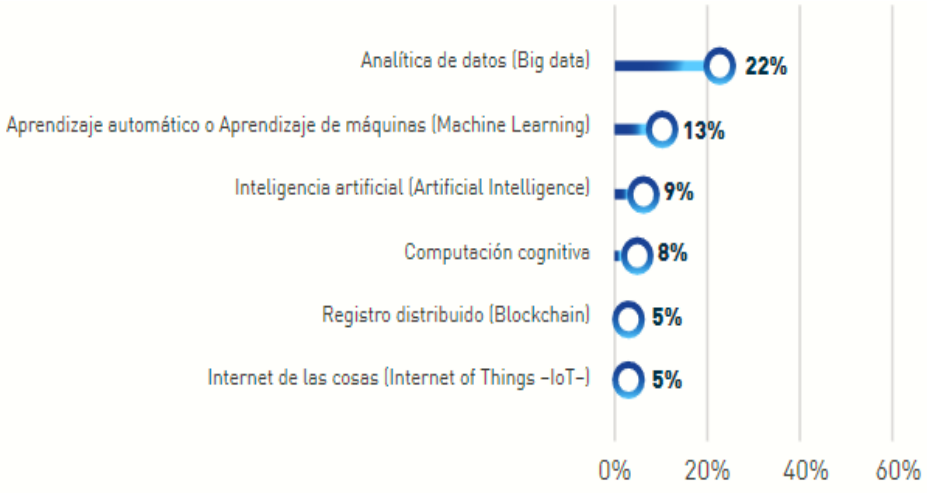
Otro hallazgo es la implementación de procesos/ programas que se implementan en las entidades financieras que están asociadas a la seguridad digital el cual el 62% tiene una administración de accesos e identificación, el 61% con protección de datos, el 54% en educación y concientización y el 46% en la continuidad del negocio.

Ilustración 2 *Métodos de seguridad implementados por las entidades financieras*



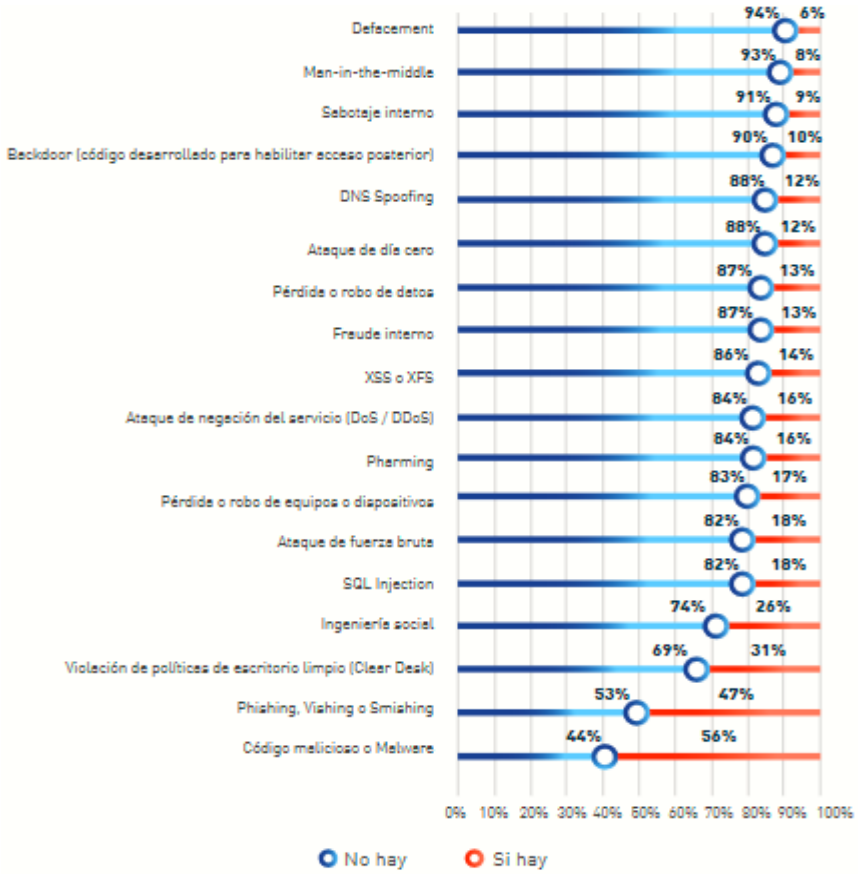
A pesar de que muchas entidades están tomando conciencia de robusteces sus sistemas de información hay otros que aun estas rezagadas, en el informe señala que el 22% de las entidades implementa analítica de datos en herramienta, controles o los procesos, solamente el 13% de la entidad implementa el aprendizaje automático o machine learning y solamente el 9% utiliza inteligencia artificial.

Ilustración 3. *Implementación de métodos de seguridad*



Los riesgos que se consideran de mayor atención son los robos de información o ataques de tipo ransomware, aun así, las entidades detectaron que los eventos de seguridad mas comunes fueron el código malicioso en un 56%, phishing en un 47%, violaciones a las políticas de escritorio limpio en un 31%, defacement en un 6% y el sabotaje interno en un 9%.

Ilustración 4 *Porcentaje de éxito de los ataques a las entidades financieras*

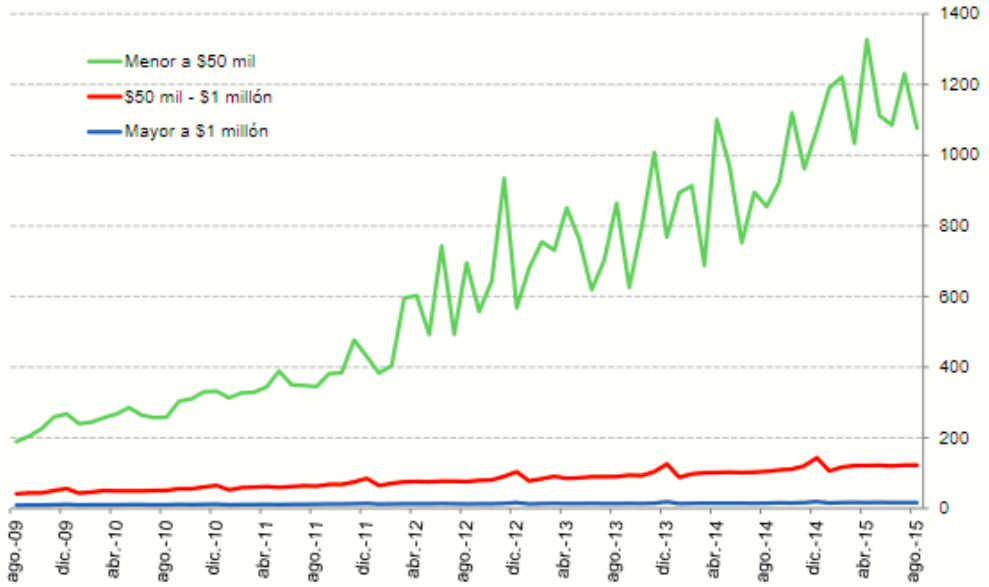


SISTEMA DE PAGOS

En el informe de UAN (banco de México) menciona que los sistemas de pagos son lo que comprende a la infraestructura, reglas, participantes y medios que aseguran que el dinero circule. Entre los cuales están las transferencias electrónicas, domiciliarias, cheques y liquidación en el mercado financiero. De a poco el dinero esta dejando de ser eficiente porque no se requiere que nadie lo traslade, el cual baja las posibilidades de robo. Los bancos y entidades financieras pueden supervisar los movimientos dentro del sistema

El SPEI es un sistema de pagos que el operador es el banco central el cual permite transferir fondos junto a información para que el participante receptor acredite las cuentas de sus clientes. Este sistema tiene un gran crecimiento en México por las ventajas que ofrece además que muchas de sus transacciones son de bajos montos.

Ilustración 5 Operaciones con SPEI

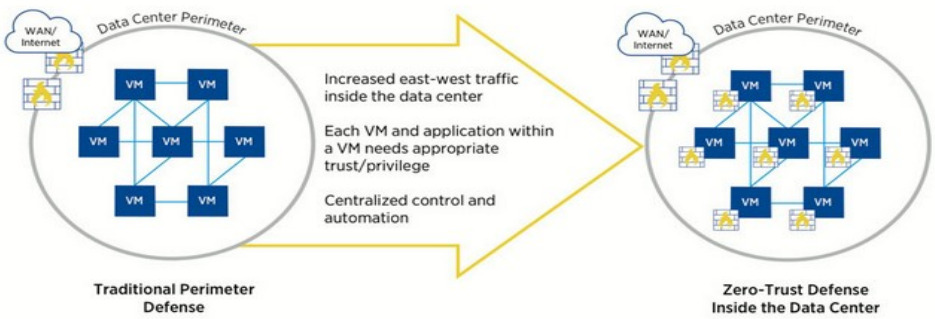


Otro de los sistemas disponibles en México es DALI el cual es un depósito central de los valores que se lleva el registro y guarda los instrumentos de los mercados de dinero y/o capitales, liquida valores en el que se realizan la compensación y liquidación de las operaciones de los participantes.

ZERO TRUST vs VPN

Tal como hemos visto anteriormente, este modelo de seguridad Zero trust se basa en no confiar en nadie, esto no solamente se establece para los usuarios que están afuera de la red, sino también los que están adentro de la misma. En otras palabras, la autenticación es necesaria para que los usuarios tengan accesos a los recursos, este sistema trata a cada identidad y dispositivo conectado como una amenaza potencial. En la siguiente imagen se puede observar cómo funciona el método Zero trust:

Ilustración 6 *Comparación de seguridad Zero trust y la seguridad convencional. Fuente netronome.com*



El funcionamiento de este sistema se establece con dar privilegios mínimos para que los usuarios puedan realizar sus actividades o trabajos de forma exitosa. Pensándolo, esto requiere no solamente quien tiene acceso al sistema, sino quien tiene el acceso y en qué circunstancias.

El sistema autentica y protege a los usuarios constantemente, esto sirve principalmente porque muchos empleados deben cambiar de dispositivos, ubicaciones o plataformas para realizar sus trabajos, por ejemplos en los empleados que hacen home office. Si el sistema detecta algún comportamiento anómalo, lo que hace es cerrar la sesión del usuario y si el usuario quiere ingresar al sistema, este debe volver a autenticarse. Este sistema esta supervisando o controlando a los usuarios y detecta todos los movimientos que cada uno de ellos realiza dentro del sistema donde este.

Los datos de identidad en el sistema que se utilizan para verificar al usuario desempeñan un papel fundamental porque allí está la información clave como la identidad, el acceso, los datos de comportamiento, los roles y grupos. Este sistema se vale de los datos que relaciona para la toma de decisiones, para ello se vale de la inteligencia artificial y en especifico los modelos de machine learning que pueden clasificar comparando los datos.

En cuanto a las VPN, estas están siendo reemplazadas por las fallas que tienen y que Zero trust puede solventar. Cuando se produce una brecha en las VPN en el canal cifrado que se conecta a un usuario con la organización, este produce accesos a potenciales atacantes a todos los recursos de las empresas. Muchas empresas están emigrando sus datos a la nube o tienen versiones mixtas y las VPN están siendo obsoletas. Debemos tener en cuenta que el nuevo sistema agrega una desventaja potencial, porque puede generar una complejidad adicional en cuanto a la implementación y mantenimiento, esto se debe porque las autorizaciones deben estar actualizadas para todos los usuarios, dispositivos y recursos, y esto requiere de un trabajo adicional, pero se debe comprender que de esta forma los departamentos de IT lograran un mayor control en los recursos y una reducción de vulnerabilidades a cambio. En las redes Zero trust se pueden realizar los procesos mediante herramientas que automatizan y brindan ayuda a las tareas administrativas de la red, entre ellas están:

- Peri meter 81: Este ofrece dos formas de mantener seguras las aplicaciones y las redes de una organización, ya que lo hace en la nube como en entornos locales. peri

meter 81 utiliza una arquitectura definida por el software que tiene una gran flexibilidad al incorporar nuevos usuarios y tiene mas visibilidad de la red.

- Nordlayer: Este ofrece una solución de seguridad de acceso a la red que se basa en el marco de Security Service Edge, esta entrega una solución de seguridad de las redes e incorpora principios claves de Zero trust y da un acceso seguro de forma remota, lo cual esto se traduce como minimizar los riesgos de una organización.
- ZScaler Private Access: Este es un servicio de red de confianza el cual esta basado en la nube que controla los accesos a las aplicaciones privadas de una organización, esto no incide si esta ubicado en centro de datos o en una nube publica, con este servicio las aplicaciones son invisibles para los usuarios que no están autorizados. Un punto a favor de este servicio es que minimiza los riesgos al evitar la propagación de software maliciosos (malware) y los riesgos que pueden ser laterales. El alcance de este sistema abarca a cualquier aplicación privada.
- Cloudflare Access: Este servicio de red tiene una red patentada con puntos de accesos distribuidos que alcanzan a todo el mundo, esto permite que los accesos sean seguro y de alta velocidad a los recursos que tiene una organización. Al igual que los otros servicios este puede registrar cada evento o acción y los intentos de acceder a un recurso de parte de los usuarios.
- CrowdStrike Falcon: Este es una protección de identidad, tiene como objetivo el reducir los costos y riesgos al minimizar los recursos de ingeniería y eliminar los procesos de seguridad. Tiene un control unificado de las identidades lo cual facilita la implementación de estrategias de tipo autenticación y brinda una mejor experiencia de los usuarios. Otro factor importante es que tiene una visibilidad completa de las actividades de las cuentas y los end point, esto brinda datos como la ubicación, origen y destino, tipo de iniciación de las sesiones.

COSTOS DE ZERO TRUST

En el informe de netronome se realizaron unas pruebas con un servidor Dell R730 de “dos sockets que contenía 24 núcleos en total. De CPU en total”. En este experimento se descubrió que se debía dedicar 24 núcleos de CPU a un vSwicht y al procesamiento de seguridad para obtener 10 Gb/s en rendimiento para los tamaños de paquetes de 512 Bytes. En otras palabras, lo que se quiere decir es que el 50% del recurso del servidor es están destinados para la ejecución de cargas de trabajo de aplicaciones o al generar

ingresos. Para contrarrestar las Agilio SmartNIC descargan el procesamiento OVS y se demostró que el rendimiento es mayor y ahorra los recursos del CPU. En vista de estos se debe considerar el equipo a utilizar para realizar estas tareas ya que demanda muchos recursos del hardware.

RETOS DE LA BANCA MEXICANA

En el artículo de investigación (Revista IUS) que se encuentra en scielo.org muestra los grandes retos que debe afrontar las bancas digitales de México, este señala como fue evolucionando la banca a partir de las tecnologías que fueron introduciéndose. Primeramente, en los 60´ se tenia como objetivo reducir los gastos, junto con ello la productividad y dar mejoras en el campo de la seguridad, pero había muchas limitaciones de la parte tecnológicas que hacían que la seguridad sea débil. Ya por los años 70´ se instalo el teleproceso, el cual mejoraba el servicio que se ofrecía a los clientes y tenia una mayor rapidez en la gestión. En los años 80´ se introdujo ofitamia, esta es una aplicación de la informática para el trabajo de oficina, el mayor problema era que los equipos eran incompatibles y había vacíos legales. Por los años 90´ fue cuando se introdujo el sistema de banca online, esto produjo mejoras en el ámbito de los procesos, no había que ir directamente al banco, sino que solamente se podría realizar transacciones mediante las terminales autorizadas. En la última etapa la cual es la que se está viviendo es de las cuales los bancos no tienen un limite geográfico, esto permite agilizar los tiempos y poder estar realizando cualquier movimiento con disponibilidad horaria y la posibilidad de ser atendido en todo momento. Algunas de estas ventajas se derivan del uso de las tecnologías que pudo trascender y ser una forma, el banco Mundial menciona que hay una relación directa entre la forma de uso de las tecnologías y la inclusión financiera, muchos de ellos tambien se debe a las innovaciones tecnológicas que realizan procesos más agiles.

Un avance importante es el reconocimiento de los documentos electrónicos, en el código civil del Distrito Federal, En el cual están el código de procedimientos civiles, en el articulo 89-114. De esta forma la ley le da a la información que esta contenida en los medios electrónicos calidad probatoria en el juicio y cualquier autoría administrativa, siempre y cuando tenga las características de integridad y atributos. Ya por el año 2012 la ley de firma digital en la cual regula el uso y los servicios que están relacionados con la misma.

Fundamentalmente se aplica a los actos entre particulares y las dependencias y entidades de la administración pública.

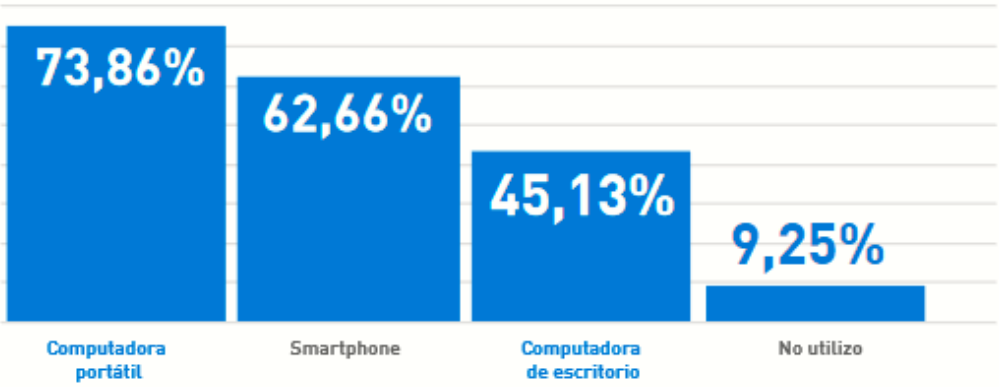
En el informe se señala que es primordial la adecuada identificación del usuario para evitar los fraudes y malas prácticas, en materia de banca electrónica. Entre los niveles de verificación de los usuarios esta el nivel 1 que verifica lo que se hace en la banca por teléfono con un operador a esta a través de preguntas de seguridad. En el segundo nivel verifica las claves de usuarios y las contraseñas de la banca por internet. En el tercer nivel verifica por medio de un dispositivo el cual se les conoce como el "Token" y el cuarto nivel se identifica la biométrica (que en México recién se inicia).

Las empresas que ofrecen los servicios financieros y productos por el medio de las tecnologías de la información, estas actividades se denominan Fintech. Estas empresas usan las tecnologías para que el sistema financiero sea menos costoso y mas eficiente, en fin, estas empresas son como puentes en trasferencias de divisas, préstamos, compras y ventas de títulos de tipo financiero. Las empresas que ofrecen este tipo de servicio deben saber que son más riesgosas para el usuario, porque muchas empresas Fintech no son reguladas, y están fuera de la posibilidad de acceder a los mecanismos de protección financiero. Esta modalidad esta en aumento porque, primero, porque si se analiza el presente, en México hay una clara oportunidad el cual mejora la inclusión financiera y el sistema bancario tradicional no está necesariamente cumpliendo con el propósito. En segundo lugar, la crisis que hubo en el 2008 en EEUU, muchas instituciones colapsaron el cual genero una desconfianza en el sistema financiero, y, en tercer lugar, los costos sobre el acceso a las redes y dispositivos móviles fueron disminuyen a lo largo del tiempo. En vista de esto el país es una oportunidad para las empresas Fintech, donde en "Fintech radar México" lo menciona como un atractivo. En vista de esto, las empresas que generalmente son startups, están transformando el sector financiero, esto a su vez es una amenaza la posición de los bancos que siempre dominaron este segmento.

Las empresas ya no tienen intermediarios y esto es gracias a que supieron utilizar las tecnologías e implementarlas a su favor, con esta forma se obtiene la descentralización, el cual no tiene un intermediario, como un banco o entidades financieras. Entre los servicios que brindan las Fintech están los servicios de pagos, el cual cualquier dispositivo puede aceptar pagos con tarjetas. Los prestamos se realizan mediante una plataforma. P2P, en ello las entidades financieras eligen a los usuarios que serán acreditados

mediante un modelo de riesgo y controlan los pagos, recuperación de fondos de los inversionistas. Y las criptomonedas, donde esta el bitso que es el puente entre esta moneda y el peso mexicano.

Ilustración 7 *Medios digitales más usados para realizar transacciones. Fuente: SG/OEA*



Mediante las investigaciones se está viendo que las Fintech están ganando terreno en diversos negocios, el cual la amenaza para las instituciones crediticias es cada vez mayor. En el informe de BBVA research menciona que la abundancia de los servicios gratuitos para el cliente esta realizando una desagregación de la oferta de los bancos, esto produce una luz donde aquellos que no se adapten podrían perder el papel de interlocutor central entre el cliente y su vida financiera, muchas personas jóvenes en las cuales se les denomina MILLENIAM utilizan estos servicios, un 55% de ellos lo utilizan, porque obtienen todos los servicios de los startups. En base a estos índices, muchos bancos han establecidos alianzas con estas empresas, o directamente las compraron. En el estudio de "The future-proof digital bank" señala que uno de cada tres bancos está dispuesto a colaborar con una empresa *fintech* y uno de cada cuatro consideraría una adquisición. En otro informe *Blurred lines* de PWC, las entidades financieras tradicionales creen que el fenómeno fintech podría poner en riesgo casi 25% del negocio actual en los próximos cinco años. Sin embargo, las *fintech* consideran que podría llegar hasta 33% del negocio actual de las entidades financieras tradicionales. A su vez, se estima que las *fintech* están presionando a la baja los márgenes y la rentabilidad de las entidades financieras, como reconoce 67% de los encuestados. Los sectores más afectados serán el de banca de consumo, medios de pago, así como los servicios de gestión de activos y patrimonio. El informe sigue mencionando que las entidades financieras no están teniendo una respuesta ante la llegada de estas empresas de tecnologías financieras.

Solo el 32% tiene un acuerdo con ellas y el 25% dice que no tiene ninguna. La incertidumbre regulatoria es un obstáculo y preocupa a la hora de establecer un lazo con las empresas fintech, porque no hay una definición clara de quien las regula o como las regula, de esto se desprende que la ley de tecnologías financieras debe expandirse.

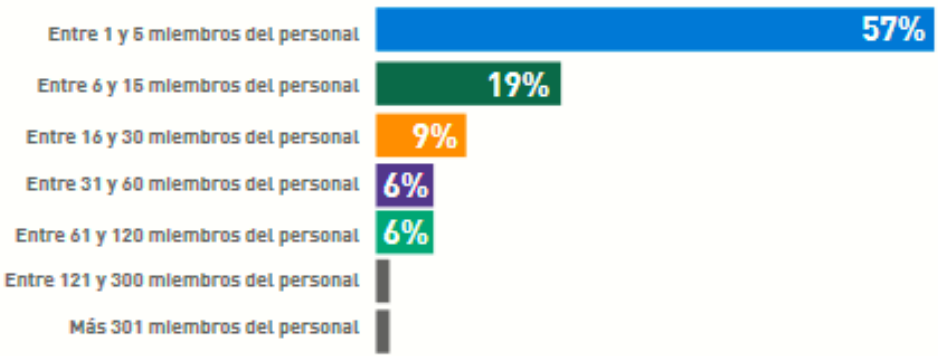
Al entrar al mercado esta empresas y ofrecer los servicios esto genera una competencia directa con los bancos como ya se mencionó, pero a la par de ello en esta empresas tambien hay reclamos de los usuarios porque muchos sufrieron fraude, esto se debe a que se generan muchas transacciones u operaciones que se realizan con internet, con la pandemia estos tipos de hechos fueron en aumento en muchas partes del mundo lo cual da entender que las entes regulatorios deben vigilar para tratar de evitar estos ciberdelitos. Estas empresas de tipo fintech deben estar formalmente en el sistema financiero porque al estar de forma privada estas no están reguladas y no tienen supervisión.

RESULTADOS Y DISCUSIÓN

Los resultados que se obtuvieron corresponden a la investigación de cómo están las entidades financieras con respecto a la seguridad en sus sistemas, tambien se quiere capturar los problemas que tienen y como fueron atacadas para finalmente demostrar como es que el método trust Zero podrá ayudar a las entidades en temas de seguridad.

Uno de los puntos que se debe tener en cuenta es el personal que tendrá a cargo la tarea de administrar el sistema, en las encuestas realizadas del informe de OEA, muchas entidades tienen pocas personas que conforman el equipo que manejan los procesos que están asociados a la seguridad digital en el informe se ven estos resultados:

Ilustración 8 SG/*OEA información recolectada de entidades bancarias.*

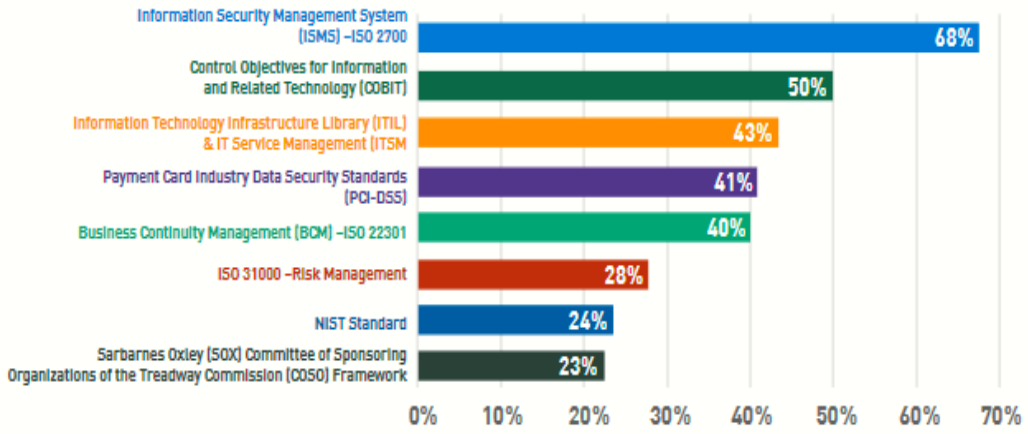


Muchas de las empresas consideran que tienen el numero de personas adecuadas, el 82% piensa que debe creer en un lapso corto, el 15% de los bancos grandes, el 16% de los bancos medianos y el 22% de bancos pequeños considera que se debe mantener el

equipo como esta. Se debe tener en cuenta que la proporción del personal debe ir de la mano del tipo de tareas a realizar, en estos sistemas donde se demanda muchos recursos entre ellos el humano, debe tener la cantidad idónea del personal.

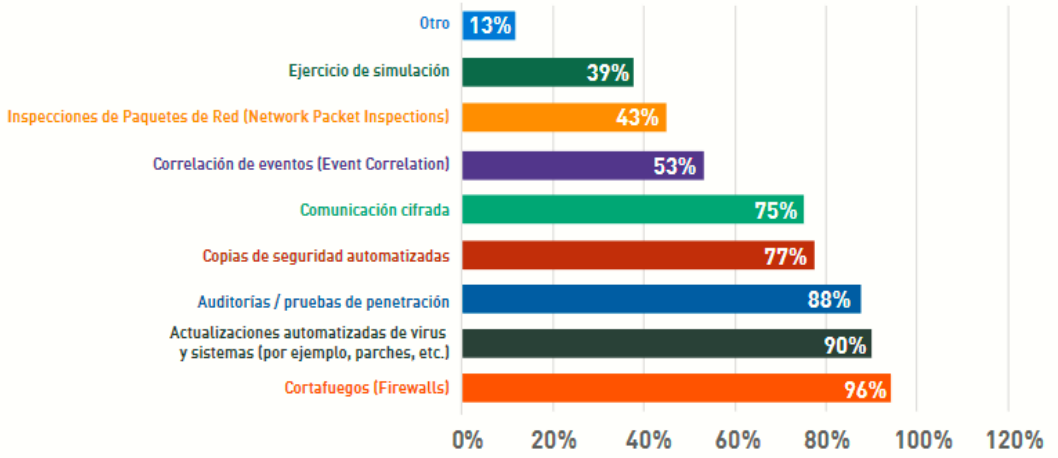
Las entidades bancarias deben tener un sistema seguro y con medidas de seguridad de nivel internacionales, según la encuesta de OAS menciona que el 68% de las entidades adopto norma de seguridad internacionales como las ISO-27001, el 50% adopto Control Objetives for Information and Releted Technology (COBIT), el 43% adopto Information Technology Infraestructure Library (ITIL) & IT Service Management (ITSM) y el 41% adopto Payment Card Industry Data Security Standars (PCI-DSS).

Ilustración 9 *Marcos de seguridad adoptados. Fuente: SG/OEA*



En cuanto a las medidas de seguridad que se tienen presentes en los sectores financieros se obtuvieron buenos resultados, se tiene conciencia de los ataques cibernéticos y los sistemas que implementan son adecuados, aunque en muchos aspectos brindan zonas donde los atacantes se pueden aprovechar. Se debe tener en cuenta que los ataques ransomware están muy activos en el presente donde secuestran información, en la imagen se puede ver que algunas organizaciones no realizan backup automatizados lo cual es una posibilidad en caso de un ataque de perder los datos. Mas de la mitad de las instituciones censadas no tienen una correlacione de eventos, lo cual esto podría indicar un futuro ataque en base a algunos movimientos anómalos. Entre las observaciones a los resultados, se observa que muchas instituciones no inspeccionan los paquetes de red, en los cuales los atacantes se valen de ello para poder penetrar las defensas y capturar información valiosa.

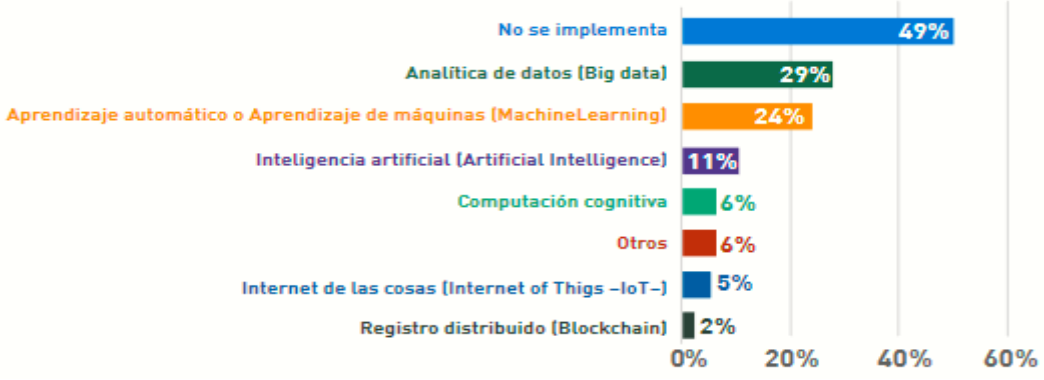
Ilustración 10 *Medidas de seguridad adoptadas Fuente: SG/OEA*



Muchas de las medidas que se implementan en las instituciones bancarias se les suma las herramientas que se implementan para mejorar la seguridad, con ello hablamos de que las instituciones tienen sistemas de detección de intrusos/ prevención de intrusos en un 85%, los sistemas de gestión para identidad y acceso en un 66%, El 85% de los bancos tienen implementados el monitoreo de amenazas y vulnerabilidades. Un dato a destacar, según ACCENTURE (2017), solo el 40% de los bancos mundiales tiene sistemas y procesos que están realizados de forma adecuada "para satisfacer los requisitos de resiliencia cibernética".

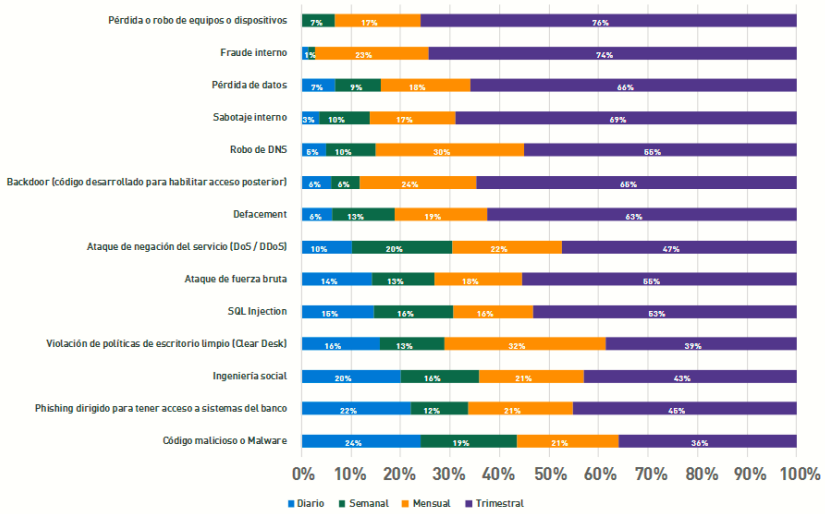
Las tecnologías emergentes brindan soluciones o mejoras a los antiguos sistemas, dándoles capas de seguridad adicional que obstaculiza la intrusión de los atacantes, en el informe de la OEA muestra que son pocas las instituciones que se valen de estas herramientas en las mejoras de la seguridad, en el 50 % no se implementa el uso de estas tecnologías, en la siguiente imagen así lo revela. El aprendizaje automático o machine learning es una herramienta muy poderosa que puede detectar cualquier movimiento que sea anómalo, Zero Trust tiene esta tecnología, por ejemplo.

Ilustración 11 *Aplicaciones de las tecnologías emergentes. Fuente: SG/OEA.*



Tal como se menciono en toda la investigación, las entidades financieras son blancos de los ataques por lo valioso de sus datos y además por administrar el capital de empresas, personas, etc. En la siguiente imagen se puede apreciar que, por ejemplo, los códigos maliciosos son diarios, los ataque tipos phishing, la inyección de código SQL, la obtención de credenciales a base de fuerza bruta, Ddos, entre otros. Pero a su vez un ítem a destacar que se observa a largo plazo la perdida de datos, el fraude interno, robos de los equipos, etc. Estos nos demuestran que la seguridad en estos sistemas no debe ser pasiva sino reactiva lo cual las entidades deben saber a los peligros que están expuestos todos los días, el porcentaje de los distintos ataques es alto y no solamente del exterior sino tambien del interior de las entidades, por ende, se debe actualizar los sistemas e implementar mejoras para poder hacer frente a estos ataques internos. La ingeniería social esta cada vez acaparando mas terreno para obtener credenciales en base a manipulación.

Ilustración 12Eventos *de seguridad. Fuente: SG/OEA*



En el sitio de internationalIT.com publicó porque el método Zero Trust es mejor que los sistemas actuales de seguridad, en numeros muestra que 72% de las organizaciones están en procesos de adoptabilidad o que ya adoptaron Zero Trust, el 90% de las organizaciones menciona que implementar el método Zero Trust esta entre las prioridades TI y la seguridad. Él método puede reducir los costos de violaciones de datos en aprox. 1.76 millones de dólares. Entre las ventajas es que Zero Trust “tienen 2 veces mas probabilidad de evitar interrupciones críticas” debido a los ataques, y para el 2026 se espera que el mercado de este método este por los 52 mil millones de dólares.

Mediante los informes que se analizaron observamos la información proveniente de distintas entidades donde todas señalan un mismo echo, las entidades financieras son las que mas invierten en seguridad y no es para menos, tal como se observo los grupos de ciber atacantes dirigen sus esfuerzos en la captura de datos, divisas e información relevantes de estas entidades. Sumado a ellos las bancas están perdiendo terreno por las pequeñas empresas, que aprovecharon las novedades tecnológicas para ampliar sus servicios y no tener como intermediarios a ninguna entidad financiera. Pero esto sumado a las dificultades que tienen los usuarios porque quedan expuestos a fraudes se debe pensar en cómo reparar o remedir este asunto, por ende, las entidades financieras deben mejorar su seguridad y poder atraer a los usuarios, además de tener un sistema de seguridad de alto nivel para poder ofrecer tranquilidad a los usuarios.

El sistema de seguridad Zero Trust a mostrado que la seguridad es fundamental, de ahí que el sistema que comprende este método es altamente seguro. No confía en nadie, todos los usuarios dentro del sistema son potenciales amenazas y controla los movimientos que realiza cada uno de ellos, en caso de que uno de ellos tenga alguna actividad sospechosa trunca la sesión y el usuario debe logiarse devuelta. Esto supone una mejora y una nueva etapa en la seguridad de las entidades bancarias donde se realizan transacciones constantes y la seguridad e integridad en cada una de ellas es fundamental. Cabe mencionar que esto le da una capa extra de seguridad al sistema, porque en caso de que alguien pueda entrar al sistema si este quiere acceder a más recursos deberá sortear las barreras que implementa el sistema, esto lo hace adecuado para implementarlo y ponerlo en funcionamiento, aunque la desventaja principal es que consume muchos recursos al tener que validar tantas veces, vigilar las sesiones, los movimientos, etc., a pesar de este punto es viable la implementación porque el consumo de recursos no se compara con la seguridad de que las transacciones están mas seguras y las amenazas son mínimas.

CONCLUSIONES

En base a los resultados y la discusión, se entiende que el método trust mejora sustancialmente los sistemas financieros debido a su arquitectura. En los informes observamos como Zero Trust resguardar a las personas dentro de una red, por ejemplo, muchas personas están trabajando desde casa y eso hace que las redes no solamente sean de un lugar específico, sino que la persona puede trabajar desde cualquier lugar,

este método novedoso ayuda a resguardar las conexiones, a la vez que realiza un seguimiento de todos los movimientos que realiza y como es que utiliza los recursos del sistema.

Muchas empresas, organizaciones e instituciones y entidades están comprendiendo las amenazas cibernéticas y sus peligros, que cada vez son mas complejos los ataques y muchos de ellos ni siquiera despiertan o activan los sensores que están destinado a la seguridad de los sistemas. Muchos ataques tienen como destino el secuestro de los datos y robos por ende los sistemas antiguos deben ser mejorados, o bien implementar cambios para que los servicios pueden brindarse de forma segura para los usuarios. Este sistema que es visto como la seguridad del futuro, es lo que necesita las entidades financieras debido que como hemos observado son blancos de la mayor parte de los ataques debido a la información que tienen y las transacciones que realiza, por ello, por mas que a nivel de hardware sea un tanto costoso, esta mejora dará seguridad a nivel interno y externo, se podrá monitorear las actividades y en caso de que haya algún movimiento anómalo, la sesión se cerrara. Esto dará la seguridad que se necesita para hacer frente a los futuros ataques y dificultará la entrada de personas no autorizadas al sistema.

LISTA DE REFERENCIAS

Informe del portal OAS. Extraído del sitio web https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Oficina Federal de Investigaciones de EE. UU. (FBI), “Three members of notorious international Cybercrime Group “Fin7” in custody for role in attacking over 100 U.S. Companies”, 1 de agosto de 2018 www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

ZERO Trust. Extraído del sitio web https://www.f5.com/es_es/services/resources/glossary/zero-trust

Banco de México. Extraído del sitio web https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf

Cisco. (2018). Reporte Anual de Ciberseguridad CISCO 2018. Obtenido de www.cisco.com: www.cisco.com/c/es_co/products/security/security-reports.html#~stickynav=3

Bankdirector. (2018). 2018 Risk Survey. Obtenido del sitio web www.accenture.com; www.accenture.com/t20170419T051104Z__w__/us-en/_acnmedia/PDF-49/Accenture-Building-Confidence-Solving-Bankings-Cybersecurity-Conundrum-Info.pdf#zoom=50

World Bank Group. (2018). Financial Sector's Cybersecurity: Regulations and Supervision. Obtenido de documents.worldbank.org;http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

World Economic Forum. (2018). The Global Risks Report 2018, 13th Edition. Obtenido de www3.weforum.org; www3.weforum.org/docs/WEF_GRR18_Report.pdf

Empresas que abalan el sistema Zero Trust. Extraído del sitio web https://www.xataka.com/pro/que-sistema-zero-trust-que-microsoft-google-cisco-consideran-futuro-ciberseguridad-empresarial

Banco de México (sistemas de pagos). Extraído del sitio web http://uae.uan.mx/d/f/album_uae/Sistemas_de_pagos_en_Mexico.pdf

BID & FELABAN. (2014). PYME y Bancos en América Latina y el Caribe el "Missing Middle" y losBancos - Séptima Encuesta 2014.Obtenido de www.felaban.net;www.felaban.net/archivos_publicaciones/archivo20150702202150PM.pdf

BDO. (2017). Cyber Security in Banking Industry. Our perspective. Obtenido de www.bdo.in; www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=.pdf&disposition=attachment

Definiciones financieras. Extraído del sitio web https://archivos.juridicas.unam.mx/www/bjv/libros/11/5140/5.pdf

Zero trust vs VPN. Extraído del sitio web https://geekflare.com/es/zero-trust-solutions/

Retos de la banca mexicana. Extraído del sitio web https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100087

Fintech. Extraído del libro. Dib, Daniela, "Panorama del Fintech en México", Endeavor México, febrero, 2017, p. 21.

Encuesta MILLENIAM. Extraído del sitio web https://www.bbvaresearch.com/wp-content/uploads/2015/12/Situacion-Banca_Dic15_Cap6.pdf

BBVA research. Extraído del sitio web https://www.bbvaresearch.com/wp-content/uploads/2015/12/Situacion-Banca_Dic15_Cap6.pdf

Informe de Blurred lines. Extraído del sitio web http://informes.pwc.es/fintech/

Cajas fuertes en la nube. Extraído del sitio web https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjuvKG52Nb6AhWwQ7gEHRTBCjYQFnoECAkQAw&url=https%3A%2F%2Fes.wikipedia.org%2Fwiki%2FCaja_fuerte&usg=AOvVaw0lnyDlec_rjWIhNzmoLZPk

Informe de infosecurity. Extraído del sitio web https://www.infosecuritymexico.com/es/blog/la-evolucion-de-ciberataques-en-la-industria-financiera.html

https://www.cobiscorp.com/

https://expansion.mx/

https://www2.deloitte.com/mx/es.html

https://www.totalsec.com.mx/index.php

https://ecaldima.com/

https://www.banxico.org.mx/

https://www.eleconomista.com.mx/

https://itmastersmag.com/

Netronome. Extraído del sitio web https://www.netronome.com/blog/zero-trust-security-for-cloud-data-centers-how-much-does-it-cost/

Implementación de Zero Trust. Extraído del sitio web https://www.infosecuritymexico.com/es/blog/un-enfowur-zero-trust-para-asegurar-la -seguridad-en-la-unbe.html.

Phishing. Extraído del sitio web https://www.pandasecurity.com/es/security-info/phishing/

Inyección de SQL. Extraído del sitio web https://www.avast.com/es-es/c-sql-injectionDdos. Extraído del sitio web https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Ingeniería social. Extraído del sitio web https://www.avast.com/es-es/c-social-engineering

Fuerza Bruta. Extraído del sitio web https://latam.kaspersky.com/resource-center/definitions/brute-force-attack

International IT. Extraído del sitio web https://www.internationalit.com/post/confianza-cero-estad%C3%ADsticas-y-tendencias-para-2022-y-futuro?lang=es

Software ploutus. Extraído del sitio web https://www.segurilatam.com/seguridad-por-sectores/financiero/ploutus-d-una-nueva-generacion-de-malware-atm_20170615.html

Swift. Extraído del sitio web https://docs.swift.org/swift-book/

Spei. Extraído del sitio web https://www.banxico.org.mx/servicios/sistema-pagos-electronicos-in001.html

Money taker. Extraído del sitio web https://www.cyberscoop.com/money-taker-group-ib-banking-hack-russia/

ISO 27001. Extraído del sitio web https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Accenture. Extraído del sitio web https://www.accenture.com/ar-es

IDS. Extraído del sitio web https://www.checkpoint.com/es/cyber-hub/what-is-an-intrusion-detection-system-ids/

IPS.Extraído del sitio web https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

Firewall. Extraído del sitio web https://www.mcafee.com/es-ar/antivirus/firewall.html

Secure email. Extraído del sitio web https://www.secmail.com/content/en/108/202189/Home.html

Código civil distrito federal, articulo 89-114. Extraído del sitio web http://docs.mexico.justia.com.s3.amazonaws.com/estatales/distrito-federal/codigo-civil-para-el-distrito-federal.pdf

Token. Extraído del sitio web https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/

P2P. Extraído del sitio web https://www.andaluciaesdigital.es/educarparaproteger/adolescentes/capitulos/perfilestics/redes-p2p.html