Estrategia de Ciberseguridad para Fortalecer el Sector Financiero

Anthony Nieto, Manuel Meléndez, Albis Herrera
Docente: Osvaldo Solís
Facultad de Tecnología, Construcción y Medio Ambiente,
Licenciatura en Sistemas de programación, Asignatura: Metodología de la investigación
nietouniverse@gmail.com, melendezbonilla75@gmail.com, herreraalbis99@gmail.com, osolis1959@hotmail.com
DOI: 10.37594/sc.v1i4.1297

Resumen

El motivo que nos impulsó a realizar esta investigación fue, de hecho, los múltiples deditos digitales que se han registrado recientemente, esto nos llevó a querer crear una estrategia de ciberseguridad que ayudara tanto a usuarios corrientes como a empresas. Para un análisis profundo a la situación de ciberseguridad, investigamos varios puntos de vista, probabilidades a lo largo de los últimos años, artículos científicos, entre otras cosas como pros y contras de esta estrategia. Objetivo general: proponer una estrategia de ciberseguridad para fortalecer el sector financiero. Metodología: hipótesis: la ciberseguridad disminuye los ciberataques. Tipo de investigación: Proyectiva. Diseño de investigación: no experimental, transeccional. Enfoque: Mixto. Población: bancos de Panamá. Muestra: no probabilística, intencional. Sujetos: Personas. Resultado: el sector financiero con mayores sistemas informáticos son los más propensos a ser víctimas de un ataque cibernético en el país. Conclusión: La ciberseguridad es una forma de proteger sistemas, redes y programas de ataques digitales que intentan el robo de información o del control del dispositivo.

Palabras clave: ciberataque, ciberseguridad, confidencialidad, estrategia, sector financiero.

Cybersecurity Strategy to Strengthen the Financial Sector

Abstract

The reason that prompted us to conduct this research was, in fact, the multiple digital fingers that have been recorded recently, this led us to want to create a cybersecurity strategy that would help both ordinary users and companies. For an in-depth analysis to the cybersecurity situation, we researched several points of view, probabilities over the last years, scientific articles, among other things as pros and cons of this strategy. General objective: to propose a cybersecurity strategy to strengthen the financial sector. Methodology: hypothesis: cybersecurity reduces cyber-attacks. Type of research: Projective. Research design: non-experimental, transectional. Approach: Mixed. Population: banks in Panama. Sample: non-probabilistic, purposive. Subjects: Individuals. Result:

the financial sector with the largest computer systems are the most likely to be victims of a cyber-attack in the country. Conclusion: Cybersecurity is a way to protect systems, networks and programs from digital attacks that attempt to steal information or control the device.

Keywords: cyberattack, cybersecurity, confidentiality, strategy, financial sector.

1. INTRODUCCIÓN

- **Justificación**

La ciberseguridad como la protección de activos de información, mediante el tratamiento de las amenazas. Con el uso de las Tecnologías de la Información y la Comunicación, se facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, que conlleva serios riesgos y amenazas en un mundo globalizado; y las amenazas en el espacio digital adquieren una dimensión global que va más allá de la tecnología. La delincuencia informática y los delitos relacionados con ella, suponen un tipo de criminalidad característica y especial; y con la expresión delito informático, cibercrimen o ciberdelito se define a todo ilícito penal llevado a cabo a través de medios informáticos, incluido el blanqueo de capitales. [1].

La ciberseguridad es todo el proceso de prevención de daños a la confidencialidad, integridad y disponibilidad de los activos de información como resultado del uso de vulnerabilidades en los activos de información por amenazas. Por lo tanto, la confidencialidad, integridad y disponibilidad (CIA), que son los elementos clave de la seguridad cibernética, deben proporcionarse adecuadamente. Las redes inteligentes destacan por aportar eficiencia en la generación, transmisión y distribución de energía eléctrica, elemento principal de las infraestructuras críticas. El uso generalizado de las redes inteligentes requiere identificar y clasificar las amenazas y tomar precauciones contra ellas. Afectados de redes inteligentes al mínimo nivel por ataques cibernéticos requiere que los elementos esenciales de seguridad de la información se proporcionen al máximo nivel. En este contexto, en el estudio; Se introducen tipos de atacantes, tipos de ataque en redes inteligentes y enormes ataques cibernéticos en sistemas de energía. Además, se presentan los objetivos y requisitos clave de la ciberseguridad en las redes inteligentes. se presentan los objetivos y requisitos clave de la ciberseguridad en las redes inteligentes. [2].

Podemos observar que los ataques cibernéticos pueden afectar tanto a ordenadores, teléfonos móviles como a redes informáticas inalámbricas. Los ciberataques utilizan las brechas de seguridad presentes en las tecnologías de información para pasar a copiar, borrar o reescribir la información de la víctima y se aprovechan de las vulnerabilidades que presentan la mayor parte de las estructuras cibernéticas como, por ejemplo, las redes sociales. En consecuencia, hemos elaborado una lista en

la que se van a describir las amenazas o ciberataques más extendidos hasta la fecha:

- Código dañino: se trata de la amenaza más común dentro del ciberespacio.
- Gusano: se trata de códigos dañinos calificados como independientes, al estar diseñados para reproducirse a sí mismos, es decir, realizar copias de sí mismo y enviarlas a todos aquellos ordenadores que estén conectados a través de la red.
- Troyano: es un software que suele aparentar ser inofensivo o incluso realizar tareas necesarias para el usuario, pero que en realidad su objetivo es el robo o destrucción de la información acumulada en el dispositivo.
- Bomba lógica: son ciberataques cuya finalidad no es extenderse ni actuar continuamente, sino pasar a la acción en un momento determinado preestablecido por el atacante. Pero es desde la autoría desde donde podemos, de forma más contundente y operativa, trazar una posible clasificación de los atacantes que nos permita una lectura de este nuevo escenario de conflicto: Estados: Aunque pueda parecer llamativo, el hecho de que los Estados pueden ser el origen de numerosas amenazas cibernéticas ha provocado que la complejidad de la situación en la que se encuentra el ciberespacio aumente considerablemente. [3].

- **Descripción de la temática o problema de investigación**

Mientras las organizaciones financieras sigan siendo blancos lucrativos para la mayoría de los cibercriminales, deberán continuar trabajando en mejorar sus defensas para mitigar la posibilidad de ser víctimas de las mayorías de las amenazas. Sin embargo, para construir mecanismos de defensas lo suficientemente fuertes las empresas financieras necesitan tener un enfoque balanceado, que consiste en invertir tanto en capacitación para empleados como en soluciones tecnológicas adecuadas y contar con un protocolo para anticipar ataques y tener capacidad de respuestas rápidas para que la información y la transacción estén protegidas.

- **Antecedentes investigativos**

En lo que respecta a Panamá, el vocero de Frontera Security, advirtió que la mayoría de las empresas no cuentan con el personal y la tecnología adecuada para proteger su información en los diferentes estados donde se procesa y se utiliza. [4].

Es importante elevar estas connotaciones y divisiones a través de los avances tecnológicos de la humanidad; si bien es cierto este fenómeno hace parte de un título grande y contextualizado en un todo, estas afectaciones a la ciberseguridad y Seguridad Digital tuvieron nacimiento mucho más antes de lo que imaginamos, por ende, la importancia y lugar de relevancia que tiene para muchos sectores de la Economía. [5].

Enfatizar sobre las principales causas que se derivan de este estudio, a partir de una aproximación que permita focalizar los intereses de las organizaciones, los estados y las naciones para poder buscar el sentido de estas amenazas cibernéticas. [6]

- **Formulación de la interrogante**

¿Cómo la ciberseguridad ayuda a disminuir el índice de ciberataques en el sector financiero?

- **Objetivos**

Objetivo General

Proponer una estrategia de ciberseguridad para fortalecer el sector financiero.

Objetivos específicos

- Hacer un diagnóstico de la situación de ciberseguridad en el país.
- Identificar los elementos que integran la estrategia de ciberseguridad en el sector financiero.
- Recomendar la estrategia de ciberseguridad al sector bancario en Panamá.

- **Breve desarrollo teórico y conceptual**

Los conceptos teóricos son los siguientes:

- Ciberataque: son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas también pueden tener intenciones políticas, criminales o personales, y pueden comprometer información clasificada o generar delitos cibernéticos, como el robo de identidad.
- Ciberseguridad: La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. [7].
- Confidencialidad: Es uno de los tres objetivos principales de la seguridad de la información, junto con la integridad y la disponibilidad. En pocas palabras, la confidencialidad es la prevención del acceso no autorizado a los datos. Esto incluye tanto evitar que personas no autorizadas vean datos sensibles, como evitar que personas autorizadas vean más datos de los que deberían tener acceso. Solo los usuarios autorizados pueden acceder a recursos, datos e información. [8].
- Estrategia: Es un plan de alto nivel sobre cómo su organización protegerá sus activos durante los próximos años (dos a cinco años). Obviamente, debido a que la tecnología y las amenazas cibernéticas pueden cambiar de manera impredecible, es casi seguro que tendrá que actualizar su estrategia antes de lo planeado. [9].
- Sector Financiero: Es un componente de la economía de una nación creada por el flujo y

reflujo de capital en la industria financiera. Los servicios financieros incluyen todo, desde banca personal hasta la industria de seguros, y pueden constituir una parte considerable de la economía de una nación. [10].

2. METODOLOGÍA

- **Método y/o Procedimiento metodológico**

- Hipótesis: La ciberseguridad disminuye los ciberataques.
- Tipo de investigación: Proyectiva.
- Diseño de investigación: No experimental transeccional.
- Enfoque: Mixto.
- Población: Bancos de Panamá.
- Muestra: No probabilística, intencional.
- Sujetos: Personas.

- **Aspectos éticos**

Respeto por la propiedad intelectual, utilización de normas IEEE.

3. RESULTADOS Y DISCUSIÓN

La ciberseguridad es la protección de sistemas, datos, softwares y hardware que están conectados a Internet. Su objetivo es principalmente proteger los datos, muchos de ellos confidenciales, de las empresas evitando el robo de los mismos, los ataques cibernéticos y las usurpaciones de identidad.

Los sectores financieros con mayores sistemas informáticos son más propensos a ser víctimas de un ataque cibernético, sin embargo, nadie está libre. Además, cada vez son más frecuentes y se producen a un ritmo más acelerado.

Es por eso que la inversión es ciberseguridad es un aspecto clave que todas las empresas deben considerar. La tecnología se ha vuelto una pieza fundamental de todos los negocios a nivel mundial lo que hace que seamos más propensos a los ataques y es precisamente por ello que protegerlas no es algo que deba tomarse a la ligera.

La ciberseguridad es fundamental en el sector financiero, ya que cualquier brecha de seguridad puede tener consecuencias graves, como robo de información confidencial, pérdida de dinero y daño a la reputación de la empresa. Además, los ataques cibernéticos son cada vez más sofisticados y frecuentes, lo que hace que la protección de los activos financieros sea una tarea constante y compleja.

Para garantizar la seguridad de los activos financieros, las empresas deben implementar medidas de protección adecuadas, como el uso de software de seguridad, la educación del personal sobre buenas prácticas de seguridad y la realización de pruebas de penetración para detectar vulnerabilidades. Además, es importante tener un plan de respuesta a incidentes para actuar rápidamente en caso de una brecha de seguridad.

Tabla 1.

Diagnóstico de la situación de ciberseguridad en Panamá

Condición	Sector Financiero
Los ciberataques han aumentado en gran medida a lo largo de los últimos años.	Debido a la acelerada trasformación digital impulsada por la pandemia, el sector financiero se ha convertido en uno de los principales objetivos de los ciberdelincuentes. A nivel mundial, los bancos fueron atacados en promedio 700 veces por semana durante el 2021, un aumento del 53% respecto al 2020. Estafas de phishing y ataques de denegación de servicio, hasta ataques sofisticados por parte de actores de estados-nación, las amenazas cibernéticas dirigidas a los bancos están en constante aumento. Las estadísticas nos dicen que el ataque por medio de malware, como virus troyanos, gusanos informáticos, spyware, entre otros, es la forma de ciber amenaza más utilizada por los ciber atacantes. Panamá no escapa de toda esta situación. De acuerdo con el reporte de inteligencia de amenazas de Check Point, partner de Soluciones Seguras, el sector banca y finanzas del país se ha convertido en el blanco perfecto de los hackers y es el sector que más ciberataques recibe. Es así que una organización del sector fue atacada en promedio 1415 veces por semana en el 2022.

Condición	Sector Financiero
Poca inversión actual a la ciberseguridad por parte de las empresas.	Aún con las amenazas digitales incrementando significativamente, el nivel de madurez en cuanto a ciberseguridad se refiere es bajo. El sector banca y finanzas debe invertir más en seguridad digital y capacitación a sus empleados, para seguir así las recomendaciones para proteger los datos y prevenir ataques por parte de hackers en el ciber espacio. Datos preocupantes nos muestran que en España, solo el 36% de las empresas cuentan con un plan formalizado para responder a un ciber ataque…
Inmunidades (puntos positivos de la ciber seguridad)	Aunque todavía el panorama se vea verde en temas de ciberseguridad, y quede un largo camino para que el sector banca y finanzas logre implementar una estrategia sólida para la protección de datos que mejore la situación en el alza de ataques realizados por piratas informáticos, debido al aumento en las estadísticas de estos ataques y el aumento del uso de las tecnologías, se espera que las PYMES y las grandes empresas dediquen por lo menos un 10% extra de su presupuestos a mejorar la ciberseguridad. Otro punto positivo a destacar es que, Panamá cuenta con leyes que ayudan a proteger los datos, como puede ser la Ley de Protección de Datos Personales en la República de Panamá por medio de la Ley 81 de 26 de marzo de 2019. Esta Ley establece los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales en nuestro país para personas naturales y jurídicas.

Fuente: elaboración propia 2023.

Tabla 2.

Estrategia de ciberseguridad

Pasos	Descripción
Diagnóstico	Ayuda a identificar periódicamente los riesgos cibernéticos dentro de la empresa y relacionados con sus sistemas, datos.
Establecer una estrategia	Debe combinar un plan de acción en caso de ataque y un buen plan de prevención, para evitar al máximo que ese ataque llegue a producirse.
Una solución sobre la ciberseguridad	Darles algunas soluciones para evitar ciberataque, por ejemplo: Detección de amenaza, bloqueo de malware y el control de acceso de datos.
Capacitación para los empleados sobre la ciberseguridad	Capacitación a los integrantes dentro del sector financiero sobre la ciberseguridad para evitar los ciberataques y así asegurar las informaciones de las personas.

Fuente: elaboración propia 2023.

Tabla 3.

Ventajas y desventajas de la estrategia de ciberseguridad

Ventajas	Desventajas
Privacidad. Cuando adquieres un servicio de ciberseguridad, puedes conservar de forma ideal los datos privados de tus empleados, clientes y proteger de esta manera su intimidad. Protección de tus equipos: No solo los softwares deben estar protegidos, también los hardware también necesitan medidas de protección para mantener su integridad. Para preservar el sistema del método de piratería, se necesita ciberseguridad. Los datos entrantes y salientes se conservan bien con la ayuda de las medidas de seguridad de Internet. Cuando se actualizan periódicamente, los agentes de seguridad de Internet funcionan muy bien y siguen protegiendo tu ordenador personal de cualquier tipo de amenaza.	También puede hacer que su sistema sea muy lento. Debe mantenerse actualizado con todo el software para evitar violaciones de seguridad. La configuración incorrecta del firewall puede bloquear a los usuarios de algunas acciones. También puede hacer que la seguridad del sistema a veces sea demasiado débil o demasiado alta. La seguridad absoluta no es posible. El costo asociado con la implementación y el mantenimiento de los sistemas dentro de la empresa.

Fuente: elaboración propia 2023.

4. CONCLUSIONES

1. Diagnóstico de la situación de ciberseguridad en Panamá

La mayor parte del ataque cibernético es en el sector financiero en el año 2021 como Estafas de phishing y ataques de denegación de servicio, hasta ataques sofisticados para que los banco o el sector financiero no sufra más estos ciberataques deben invertir en la ciberseguridad ya que asa brinde una mejor privacidad a sus clientes y así no puedan ser hackeado.

Por otra parte, deben darles capacitaciones a sus empleados o enseñarles sobre la ciberseguridad y en la inmunidad es que la empresa logre implementar una estrategia sólida para la protección de datos que mejore la situación para que no haya más ataques cibernéticos.

2. Conclusión: Pasos para estrategia de ciberseguridad

En conclusión, la ciberseguridad es la transformación digital en estos tiempos, ayuda a proteger o defender las computadoras de amenazas o ataques maliciosos, ya que también se conoce como seguridad tecnológica de la información o seguridad de la información electrónica. La ciberseguridad es una forma de proteger sistemas, redes y programas de ataques digitales que intentan el robo de información o del control del dispositivo, las ampliaciones de ciberseguridad o medidas de seguridad están aumentando cada vez más se debe a que también en la actualidad hay más amenazas creativas, por lo tanto, hay que darle capacitaciones a los empleados para que no sucedan los ciberataques y darles una estrategia dentro del sector financiero.

3. Ventajas y desventajas de la estrategia de ciberseguridad

Casi todo se ha vuelto digital hoy en día. Desde educación hasta entretenimiento, desde operaciones bancarias hasta consultas médicas, se puede hacer cualquier cosa de forma digital. Y como sabemos que todo tiene sus pros y sus contras para hacer el balance.

Aquí hemos hablado sobre las ventajas y las desventajas de la ciberseguridad y por qué es necesaria. En resumen, la ciberseguridad actúa como defensora de los datos importantes de nuestras preciadas organizaciones

Conocer las ventajas y desventajas de la ciberseguridad supone un gran beneficio para las empresas y gobiernos cuyo núcleo se soporta en base a la tecnología, especialmente si manejan datos con altos niveles de privacidad.

REFERENCIAS BIBLIOGRÁFICAS

- A. Gómez. 2020.
- BANCO MUNDIAL. 2023.
- C. Alvarado. Panamá. 2018.
- Infosecurity. México.
- Itech Sas. 2021.
- Jori. TechEdu.
- Ortiz Ruiz. 2019.
- Ortiz Ruiz. (2020). LIBRO SOBRE A APLICAO PRACTICA DA INVESTIGACAO CRIMINAL TECNOLOGICA.
- Z. Gunduz. 2018.