PROJECT, DESIGN AND MANAGEMENT

ISSN: 2683-1597

PROJECT DESIGN & MANAGEMENT

Cómo citar este artículo:

Quissanga, F. C. & Fernandes, R. F. (2020). Importância da segurança da informação nas empresas corporativas do ramo da tecnologia de informação. *Project, Design and Management, 2*(1), 87-102. doi: 10.35992/pdm.v2i1.431

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE TECNOLOGÍA DE INFORMACIÓN CORPORATIVA

Fernando Cassinda Quissanga
Universidad Internacional Iberoamericana (México), Universidad Europea del Atlántico (España)
fernandoquissanga@hotmail.com· https://orcid.org/0000-0003-4468-7206
Roberto Fabiano Fernandes
FUNIBER – Fundación Universitaria Iberoamericana / Faculdade Cesusc / Universidade do sul de Santa Catarina (Brasil)
roberto.fabiano@funiber.org · https://orcid.org/0000-0002-6738-6572

Resumen: La importancia de la seguridad de la información en las empresas corporativas de tecnología de la información tiene el objetivo principal de proponer medidas de seguridad para proteger la información en las empresas corporativas de tecnología de la información. En este sentido, la investigación es cualitativa, exploratoria y descriptiva, ya que se basa en la búsqueda de material bibliográfico que permita sugerir medidas de seguridad para la protección de la información. Los datos secundarios se recopilaron sistemáticamente, buscando la palabra clave: medidas de seguridad y sus sinónimos. La búsqueda se realizó en bases de datos computarizadas, como Google Académico® y el Portal de Periódicos Capes. Se ha identificado un conjunto de sugerencias para medidas de seguridad que permiten a las empresas corporativas en el campo de la tecnología de la información aprovechar.
Se destaca como conclusión que las medidas preventivas, de detección y correctivas propuestas deben estar involucradas en un plan de seguridad y contingencia difundido en toda la organización.

Palabras clave: Seguridad de la información, Medidas de seguridad, Empresas corporativas.

IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS CORPORATIVAS DO RAMO DA TECNOLOGIA DE INFORMAÇÃO

Resumo: A importância da segurança da informação nas empresas corporativas no ramo da tecnologia da informação tem como o objetivo primário em propor medidas de segurança para proteger a informação nas empresas corporativas do ramo da tecnologia de informação. Neste sentido, a pesquisa é qualitativa, de

cunho exploratório e descritivo, pois tem como base a busca por material bibliográfico que possibilite sugerir medidas de segurança para a proteção das informações. Os dados secundários foram coletados de forma sistemática, buscando-se pela palavra chave – medidas de segurança e seus sinónimos. Realizou-se a busca em bases de dados computadorizadas, como o Google Académico® e o Portal de Periódicos Capes. Identificou-se um conjunto de sugestões de medidas de segurança que possibilitem as empresas corporativas do ramo da Tecnologia da Informação possam usufruir. Destaca-se como conclusão que as medidas preventivas, detetivas e corretivas propostas devem estar envolvidas em um plano de segurança e contingência disseminadas em toda a organização.

Palavras-chave: Segurança da informação, Medidas de Segurança, Empresas corporativas.

IMPORTANCE OF INFORMATION SECURITY IN CORPORATE INFORMATION TECHNOLOGY COMPANIES

Abstract: The importance of information security in corporate information technology companies has the primary objective of proposing security measures to protect information in corporate information technology companies. In this sense, the research is a qualitative, exploratory and descriptive, as it is based on the search for bibliographic material that makes it possible to suggest security measures for the protection of information. Secondary data were collected systematically, looking for the keyword - security measures and their synonyms. The search was carried out in computerized databases, such as Google Académico® and the Portal de Periódicos Capes. A set of suggestions for security measures that enable corporate companies in the field of Information Technology to take advantage of has been identified. It is highlighted as a conclusion that the proposed preventive, detective and corrective measures must be involved in a security and contingency plan disseminated throughout the organization.

Keywords: Information security, Security measures, Corporate companies.

Introducción

La seguridad de la información ha sido una preocupación en todo el mundo, la información se ha vuelto muy importante, y manejarla requiere mucho cuidado, y es necesario crear condiciones para protegerla. Por lo tanto, es imposible decir que estamos totalmente seguros, incluso cuando se trata de la seguridad de los países del primer mundo. Esto se debe a que las pérdidas económicas, los problemas psicológicos, deontológicos e ideológicos son muy grandes, en el presente siglo nos enfrentamos a varias dificultades para controlar el cibercrimen (*brute force*) y el espionaje (*sniffing*).

El Sniffing se entiende, de acuerdo con la definición del sitio web CERT.br (2012 p.19), *"La intercepción de tráfico, o sniffing, es una técnica que consiste en inspeccionar datos traficados en redes de computadoras, mediante el uso de programas específicos llamados rastreadores.*

Sin embargo, los golpes de estado, el fraude electoral, la filtración de información política, los secretos de estado y las desviaciones bancarias (que se llaman la técnica de phishing) han sido motivo de preocupación. El robo con tarjetas de crédito como clonación de tarjetas de crédito, suplantación de correo electrónico (suplantación de correo electrónico), alteración de notas en la base de datos de la universidad (Pharming).

Sin embargo, vale la pena mencionar que la seguridad de la información se ha convertido en la primera preocupación que se informa en este artículo. En 2018, la mayor

preocupación de los países era crear una legislación para prevenir el delito y poder llevar a los delincuentes ante la justicia, porque es muy difícil detectar cuándo estamos siendo objeto de un delito informático. Los mecanismos básicos de seguridad deben estudiarse en profundidad, como la identificación, autenticación, autorización, integridad, confidencialidad y disponibilidad de información.

Del mismo modo, se entiende que el advenimiento de las redes sociales también permitió un aumento en el número de ataques de virus informáticos, espías para copias de credenciales, contraseñas de usuarios, varios códigos que se enviarán a una computadora remota donde los piratas informáticos buscan esta información para cometer delitos. Otra técnica ampliamente utilizada por los *Crackers* es la ingeniería social, cuyo objetivo es engañar a las personas para tener acceso a la información que les permite ingresar a las computadoras o dispositivos informáticos.

Con base en estas descripciones, el objetivo general de este artículo es sugerir medidas de seguridad para proteger la información en las empresas corporativas de tecnología de la información.

Método

Esta investigación se entiende como cualitativa, exploratoria y descriptiva, ya que se basa en la búsqueda de material bibliográfico que permita sugerir medidas de seguridad para la protección de la información. Los datos secundarios se recopilaron sistemáticamente, buscando la palabra clave – medidas de seguridad y sus sinónimos. La búsqueda se realizó en bases de datos computarizadas, como Google Académico® y el Portal de Periódicos Capes. Google Scholar® para Creswell (2010) es una base de datos gratuita que proporciona una amplia variedad en la búsqueda bibliográfica de diversas fuentes, como tesis, resúmenes y artículos, con la ventaja de poder obtenerlos en su totalidad. En cuanto al portal de Periódicos Capes, este fue elegido como fuente de búsqueda para ofrecer acceso a los textos completos de artículos seleccionados en más de 15,000 revistas internacionales, nacionales y extranjeras, y 126 bases de datos con resúmenes de documentos en todas las áreas del conocimiento (Portal de Periódicos da Capes). En cuanto al análisis, se considera el uso de análisis de datos descriptivos, ya que permite organizar, resumir y describir los aspectos importantes de un conjunto de características observadas o comparar esas características entre dos o más conjuntos.

Descripción de las principales pérdidas económicas causadas por la falla de la seguridad de la información.

Con base en la búsqueda literaria, se identificaron algunas pérdidas económicas cuando no hay precaución y control o el uso y la aplicación de medidas basadas en la seguridad de la información.

Coopamootoo (2018) Sugerí a las compañías que protegen la privacidad de los empleados en las interacciones en línea:

> En las interacciones fuera de línea, necesitamos divulgar información sobre nosotros para generar confianza con los demás. Cuando nos movemos en línea, hay diferencias: las empresas deben participar para facilitar la interacción en línea y necesitan mantener información sobre nosotros para hacerlo. Estas compañías tienen el deber de proteger nuestra privacidad, pero

> nuestra información puede estar en riesgo de pérdida accidental de datos o ataques maliciosos.

Sin embargo, la protección y privacidad de la información ha sido una preocupación y temor de los usuarios que tienen servicios en estas empresas. La vulnerabilidad de los datos que pueden usarse para ataques cibernéticos, no solo para el robo de computadoras en el caso de datos bancarios, sino también mediante el uso de ingeniería social y redes sociales.

La mayoría de los usuarios de la tecnología de la información moderna corren muchos riesgos, ya que permiten fallas debido a la falta de precaución y control de la causa. Muchos no tienen una preparación específica sobre seguridad de la información, y la preparación debe basarse en el conocimiento, todos debemos conocer estas técnicas de seguridad de la información para poder proteger, porque la experiencia nos muestra que no solo los usuarios, sino Las empresas también permiten la mayor parte del tiempo para exponer los datos de sus clientes como lo menciona Futurelearn, (2018):

> El ataque cibernético de TalkTalk vio los datos personales de 157,000 clientes, incluidos los detalles de la tarjeta de crédito, que se lanzaron en octubre de 2015. Como resultado, la compañía perdió alrededor de £ 60 millones y más de 100,000 clientes, pero los clientes también estaban abiertos a posibles fraudes de identidad: en algunos casos, los estafadores usaron los datos para permitirles ser dueños como ingenieros de TalkTalk, contactando a los clientes y persuadirlos para que instalen malware en sus máquinas.

Sin embargo, nos enfrentamos a una situación precaria, notamos que, además de que la compañía falla con el sistema de seguridad, los clientes también facilitan el robo de datos, ya que no tienen conocimiento de seguridad de la información y permiten que los delincuentes implementen ingeniería social.

Sin embargo, los ataques cibernéticos en los últimos años han traído muchas dificultades, el malware pertenece a varios grupos de virus informáticos de aproximadamente 31 familias presentes, por ejemplo, el trojan, worms o bugs, dropper y backdoor, son la base de muchas pérdidas económicas, las falsas identidad, espionaje, robo de datos, tipos de fraude informático y envío de datos a una computadora remota, incluso si están geográficamente distantes o en diferentes continentes.

Las inversiones en el área financiera corren graves riesgos, los atacantes son la base de estas situaciones, la evolución del cibercrimen y el ciberterrorismo, los clientes son sus objetivos porque a menudo han descuidado y permiten que sus datos sean robados, y a través de los robos digitales de los clientes para la empresa se ve afectada de la misma manera que su sistema de seguridad, también a veces permite el robo de información, cuando no tiene un sistema de seguridad adecuado para proteger sus datos.

Sin embargo, la empresa y los clientes deben estar protegidos para evitar que personas no autorizadas accedan a sus credenciales y estén equipados con todas las herramientas de seguridad de la información, por lo que las empresas corporativas y otros deben estar preparados para evitar las pérdidas económicas causadas por la violación de la seguridad de clientes, usuarios, empleados y antiguos trabajadores, que ya conocen todo el sistema de seguridad. En este caso, es importante revitalizar y reestructurar todo el sistema de seguridad para evitar tales situaciones, las políticas de seguridad no deben ser conocidas por terceros, esto hace que la empresa sea vulnerable.

Aun hablando del fraude con tarjetas de crédito en el Reino Unido, es oportuno presentar el gráfico de las pérdidas económicas del fraude a lo largo de los años y poder conocer su estado actual:

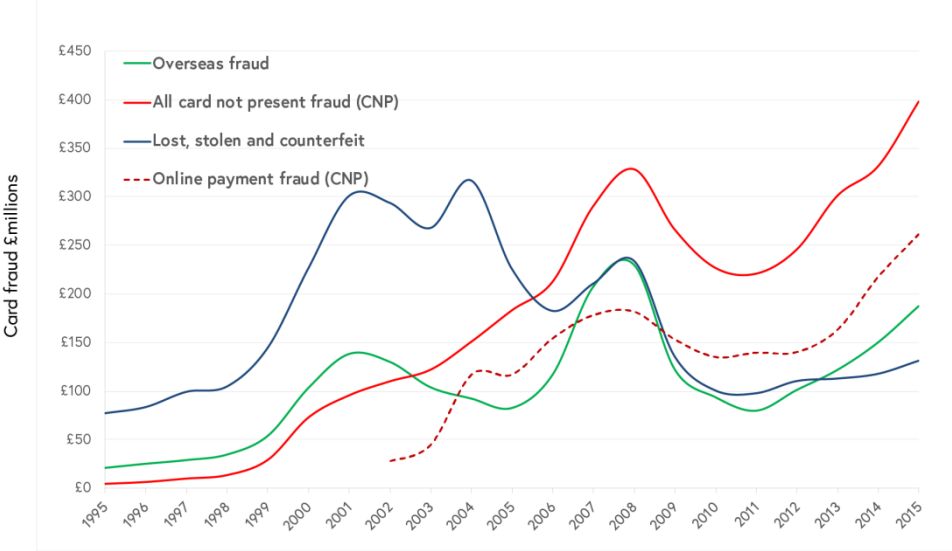

Figura 1. Gráfico de pérdidas anuales con tarjetas emitidas en el Reino Unido
Nota: Fuente: Futurelearn (2018).

Al hacer una auto observación en la figura 1, es posible analizar que de 1995 a 2015 hay un aumento sustancial en los ataques informáticos a las tarjetas de crédito, que resultaron de pérdidas financieras en el rango de 0 a 450 millones de euros, valores que las empresas están sujetas a quiebra. Es probable que las empresas corporativas cuyo capital financiero es mayor pierdan más cuando no hay prevención contra *Crackers* y plagas virtuales.

En la figura 1, se puede ver que los pagos fraudulentos realizados en línea tienen una escala superior a los 250 millones de euros, una gran cantidad de dinero robado por fraude financiero, por lo que es necesario evitar que prevengamos el cibercrimen.

En el caso de robos, pérdidas y falsificaciones mencionados en la figura 1, se menciona una escala superior a los 300 millones de euros.

Sin embargo, la figura 1 también se refiere a las tarjetas de crédito realizadas sin fraude bancario, del orden de los 400 millones de euros.

Según Financial Fraud Action in the United Kingdom (2017, p. 10): presenta las pérdidas económicas causadas por robos a través de pagos en línea con tarjetas de crédito: "Las pérdidas por fraude financiero en tarjetas de pago, bancos remotos y cheques totalizaron £ 768.8 millones en 2016, un aumento del 2% en comparación con 2015". Sin embargo, hay innumerables dificultades y pérdidas económicas debido a la falta de seguridad de la información, y a menudo notamos que algunas compañías exponen nuestros datos y esto generalmente ha causado fraude, y muchas buscan una compensación por parte de la compañía, otros no, y guardan silencio sin saber a dónde acudir, en este caso, debemos ser muy cuidadosos, cómo y dónde colocamos nuestras credenciales, el tipo de redes sociales a las que pertenecemos, el tipo de negocio o compra en línea, todos estos factores deben ser tratado con especial atención.

> Las nuevas tecnologías erradican las formas existentes de cometer fraude, pero también introducen otras vulnerabilidades que los estafadores se adaptan

> para aprovechar. El chip y el PIN dificultaban el uso de una tarjeta robada y, por lo tanto, el robo de la tarjeta se rechazó. Sin embargo, los delincuentes han identificado que el pago en línea se ha convertido en una debilidad ya que no pueden usar Chip y PIN. El fraude en línea es ahora la forma más común de fraude de pagos en el Reino Unido (Financial Fraud Action in the United Kingdom, 2017, p. 18).

Frente a este fraude, lo que se destaca es que cada profesional bancario debe estar preparado para saber cómo administrar la gestión de documentos y procesos y, a su vez, la información y los activos financieros, deben comportarse como un profesional que tiene el banco. Al igual que su bandera, no sabemos en términos concretos cuál fue la base para extorsionar, pero creemos que los bancos deberían promover un salario equilibrado para su personal técnico, como la capacitación en los campos de seguridad de la información, ética y ética profesional.

Según el sitio Terra (2018):

> La filtración de 11.5 millones de documentos, los llamados PanamaPapers, de la firma de abogados y consultoría panameña Mossack Fonseca, la cuarta firma de abogados offshore más grande del mundo, habría revelado detalles de cientos de miles de clientes que usan paraísos fiscales en el extranjero supuestamente por evasión de impuestos, lavado de dinero, narcotráfico y tráfico de armas.

Además del análisis de los bancos, también se hace un acercamiento sobre las dos compañías corporativas de telefonía móvil, que podemos designar como competidores, Samsung y Apple. Estas compañías tienen un sistema de seguridad muy robusto, tienen muchos expertos en seguridad de la información, para proteger prototipos, patentes y la industria telefónica. Sin embargo, estas compañías son líderes en el mercado de telefonía internacional, pero si no se utilizan métodos avanzados de seguridad de la información en estas compañías, una falla es fatal, no es necesario tener mucho cuidado, en este caso debemos tener cuidado para evitar situaciones desastrosas, como en 2012 en California, donde Samsung, acusada de violar las patentes solo por la apariencia de los dispositivos y las funciones táctiles, que se requería para pagar millones de dólares, imaginamos que es un prototipo, el escándalo sería mayor. En este caso, la empresa surcoreana se vio obligada a indemnizar, según Oficina Net, (2015):

> El 24 de agosto de 2012, un jurado en San José, California, juzgó Samsung culpable de violar una serie de patentes de su mayor competidor, el mismo jurado condenó a la compañía surcoreana a pagar el equivalente a $ 930 millones de daños a Apple. Por su parte, el tribunal federal de apelaciones de Washington, EE. UU., confirmó, en partes, la decisión del jurado de San José, tratando de revertir parte de la sentencia, alegando que Samsung fue injustamente condenado por violar patentes relacionadas solo con la apariencia de los dispositivos y las funciones táctiles del dispositivo móvil de la empresa Apple.

Algunas prácticas en inseguridad de la información.

Después de los daños causados por las principales pérdidas económicas causadas por la falla de la seguridad de la información, es oportuno mencionar varias prácticas que permiten fallas en la seguridad de la información. La mayoría de los usuarios de la información hacen posible que ocurran estas fallas, porque muchos de ellos tienen una educación inadecuada para la protección de los datos de la computadora, lo que hace

posible, es decir, se traduce en una puerta abierta para los ciberdelincuentes, *Crackers* y espías informáticos que aprovechan la oportunidad para cometer delitos cibernéticos.

Según Laureano (2005, p. 15 apud. Shirey, 2000) tenemos la definición de algunos términos importantes con respecto a la seguridad de la información:

> Amenazas
>
> En inglés, usamos el término "threat" para definir la amenaza. Y tenemos varios tipos de threat:

- Amenaza inteligente: circunstancia donde un adversario tiene el potencial técnico y operativo para detectar y explotar la vulnerabilidad de un sistema;
- Amenaza: violación potencial de seguridad. Existe cuando existe una circunstancia, potencial, acción o evento que podría violar la seguridad y causar daños;
- Amenaza de análisis: un análisis de la probabilidad de sucesos y las consecuencias de acciones perjudiciales para un sistema;
- Consecuencias de una amenaza: una violación de seguridad resultante de la acción de una amenaza. Incluye: divulgación, usurpación, desilusión e interrupción.

Existen varias amenazas, ya que podemos ver que los estafadores utilizan mucho la ingeniería social, haciéndose auténticos de un determinado banco o servicio, persuadiendo al cliente para que se registre, para robar sus credenciales, Internet, sobre todo, las redes sociales permiten acceso indebido a la información, mencionando que una de las formas más rápidas de propagación de virus informáticos son los sitios pornográficos. Los delincuentes han sido uno de sus favoritos porque incluso algunos, adolescentes y adultos, sin saber que los delincuentes usan estos sitios para el robo de computadoras. Dado que la contaminación ocurre cuando abrimos la imagen o el video, en este caso, el virus tiene la capacidad de presentarse como un archivo adjunto al documento y replicarse en el huésped en poco tiempo.

Según Martinelli (2008, p. 46):

> Muchos virus se disfrazan de supuestos juegos, características, en archivos adjuntos. Los creadores de virus también usan la ingeniería social para llegar a sus víctimas, reclamando el registro en instituciones gubernamentales, seguridad, pornografía y diversión gratuita. Los mensajes de texto infectados a veces reemplazan la línea del remitente haciéndose pasar por personas conocidas, lo que aumenta las posibilidades de contaminación.

Sin embargo, los virus informáticos son tan rápidos y destructivos en el proceso de transmisión que cada uno presenta su especificidad. Sin embargo, la regla es la misma y se basa en el comportamiento de los virus biológicos que atacan las células humanas, mientras que los virus informáticos atacan los sistemas operativos en sus respectivos archivos. Toda empresa que maneja información debe tener una sala de control de seguridad de la información para evitar que se pierdan sus datos. En esta recomendación se realiza el gasto de cualquier inversión en seguridad de la información, es importante contratar especialistas en el área de seguridad de la información o crear un departamento que supervise la gestión de archivos y documentos. Las empresas se quejan de varios robos de computadoras porque algunas de ellas no invierten en protección de datos.

Las empresas corporativas deben dar ejemplo en la protección de datos, no deben desperdiciar información porque están sujetas a perder reputación y otras pérdidas financieras. Como ejemplo, podemos mencionar a la compañía Coca-Cola, a la que no le gustaría saber la fórmula de su refresco.

Sin embargo, las grandes empresas nunca han fallado y siempre se han diferenciado al proteger sus activos. Trate de imaginar el sistema de seguridad que tienen estas compañías, que requiere mucho control e inversión. Sin embargo, se entiende que esta cultura debe trasladarse a otras empresas corporativas.

Según Laureano (2005, p. 17):

> Para implementar mecanismos de seguridad, es necesario clasificar las posibles formas de ataques a los sistemas:
>
> - Interceptación: el acceso a la información por parte de entidades no autorizadas (violación de la privacidad y confidencialidad de la información) se considera intercepción.
> - Interrupción: se puede definir como la interrupción del flujo normal de mensajes al destino.
> - Modificación: consiste en la modificación de mensajes por parte de entidades no autorizadas, violación de la integridad del mensaje.
> - Personificación: se considera la personificación como la entidad que accede a la información o transmite un mensaje haciéndose pasar por una entidad auténtica, una violación de la autenticidad.

Al abordar el mecanismo de seguridad de la información, es necesario mencionar el tipo de seguridad física (*Hardware*) y lógica (*Software*). Deben estudiarse en profundidad porque, en su mayor parte, somos más cautelosos en uno y no en el otro. Se recomienda que no tenga sentido contar con un mecanismo de seguridad lógico (*software*) robusto y un sistema de seguridad física sin protección (*hardware*), lo que puede suceder es el robo de dispositivos informáticos.

Se sugiere que uno esté preparado para las dos formas de seguridad de la información e invertir mucho para tener protección en nuestras instalaciones y en un perímetro determinado.

Trazar las diferentes formas de robo de computadoras

Según Oliveira (2009, p. 14-15) las amenazas organizacionales se dividen en cinco:

- Amenazas físicas;
- Amenazas lógicas;
- Amenaza ocupacional;
- Amenaza a la confidencialidad;
- Amenaza ambiental.

Aunque existen varias amenazas en las empresas, en este momento enfatizaremos las amenazas físicas y lógicas, ya que es el objetivo de nuestra investigación.

> Sin embargo, el malware es un software diseñado para infectar cualquier programa. Los worms tienen la capacidad de replicarse. Los programas de spyware están diseñados para espiar a los usuarios y recopilar información para monitorear a la víctima. El phishing generalmente se envía por correo

> electrónico y captura información extremadamente confidencial para llevar a cabo el fraude posteriormente (Quissanga, 2015, p. 6).

Sin embargo, se sabe que existen varios tipos de delitos informáticos, los que se llevan a cabo por medio de computadoras, ejecutados a través de Internet, de forma tecnológica, digital y otros delitos de naturaleza legal. El robo de computadoras está más extendido, por lo que algunos no tienen una ley, regulación o código penal, sin embargo, en el contexto actual, los países ven estudiar métodos para arrestar a los ciberdelincuentes, una tarea que no ha sido fácil, algunos se consideran demasiado alejados de la realidad, así como los artículos o decretos utilizados fuera de contexto que perjudican o benefician a los delincuentes, sin embargo, el control de los robos de computadoras debe hacerse un estudio más profundo y completo, implementando medidas de detección, porque hay varias formas de ataques cibernéticos.

Sin embargo, las empresas deben estar preparadas para prevenir ataques, esto implica utilizar todos los dispositivos de seguridad, tanto lógicos como físicos, y capacitar a su personal técnico o contratar empresas especializadas en el área de seguridad de la información, en caso de que no tenga todos herramientas de seguridad Cuando estamos expuestos en Internet, nos volvemos más vulnerables, por esta razón necesitamos implementar el firewall para evitar el tráfico innecesario que puede ser una ruta de transmisión de virus informáticos, en este caso todos los paquetes extraños, es decir, no autorizando el firewall elimina, niega todos paquetes sospechosos, permitiendo solo los autorizados.

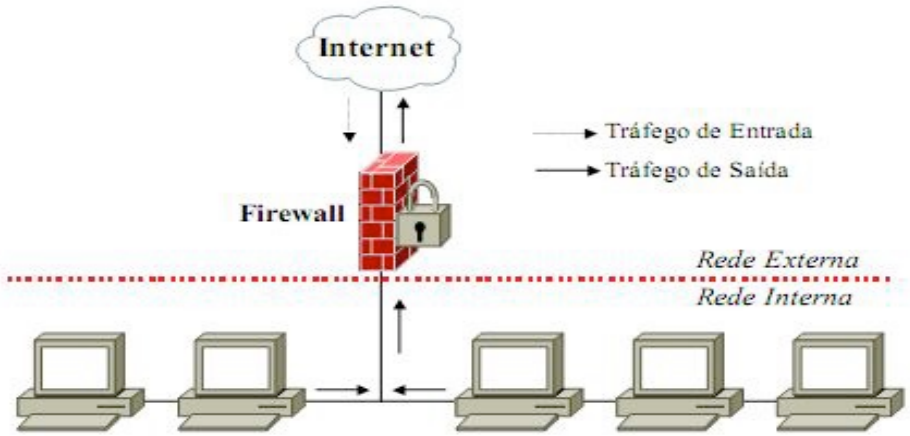

Figura 2. La defensa es más compleja que el ataque.
Nota: Fuente: Oliveira (2009, p.28).

Sin embargo, en la figura 2, se puede analizar que la defensa es más compleja que el ataque. Por lo tanto, debemos estar preparados para evitar cualquier violación de la seguridad de la información, porque si somos atacados, apenas podremos defendernos del ataque. El término pirata informático (*Hacker*) todavía se discute ampliamente, pero preferimos usar *Cracker* porque tiene una definición clara de ciberdelincuente. El *Hacker*, por otro lado, no necesariamente practica un delito virtual, pero ambos tienen las mismas capacidades que el *Hacker*, pero se presenta en forma defensiva y generalmente es contratado para proteger el sistema de seguridad de una empresa.

Las formas de robo de computadoras son muy silenciosas e impredecibles. Por lo tanto, la elección de un método de seguridad ha sido un gran desafío, debido a los problemas en los que vivimos. Mientras que algunos estudian las formas de protegerse, otros pasan mucho tiempo para detectar cualquier información que permita cometer

fraude virtual, sin embargo, las formas de ataque son diversas, cada una con su especificidad, cada caso es un caso, por lo que ha sido difícil de detectar las fallas de seguridad reales.

Oliveira (2009, p. 40) básicamente menciona que los atacantes realizan los siguientes pasos:

> Paso 1: El atacante, cuando penetra su red, rompe una determinada máquina.
>
> Paso 2: Instala un programa sniffer.
>
> Paso 3: este programa monitorea la red para acceder a los servicios de red, las capturas se realizan y se registran en un archivo de registro.
>
> Paso 4: Luego, el atacante recupera el archivo de log.

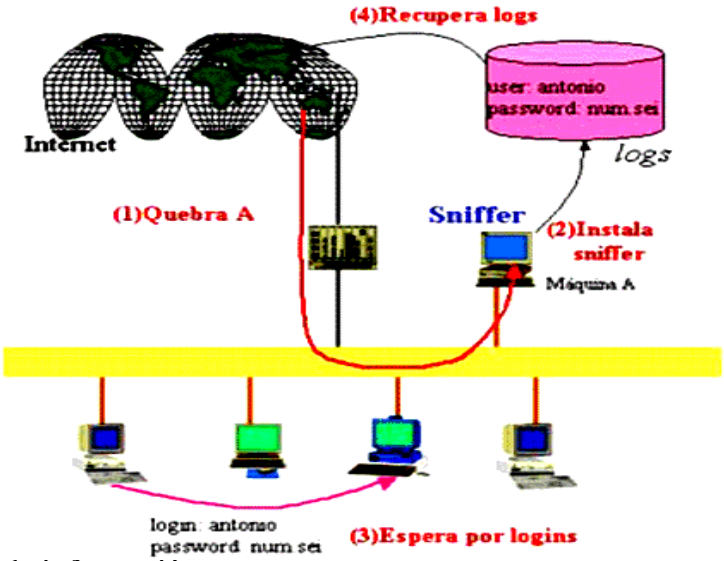

Figura 3. Robo de información
Nota: Fuente: Oliveira (2009, p. 40)

Las empresas corporativas de hoy presentan programas informáticos o aplicaciones para transferencias bancarias, consultas de saldo, extracción de extractos y varios tipos de pagos en línea, estas tareas que hacen que algunos usuarios sean vulnerables porque no tienen educación en seguridad, estas operaciones generalmente las realizan dispositivos teléfonos celulares utilizados por personas que pueden acceder a las credenciales, sin mencionar otras formas de cibercrimen. El fraude bancario, además de la ingeniería social, también envía mensajes extraños, o por correo electrónico, que generalmente contienen malware o spyware. Por ejemplo, podemos analizar el phishing.

Implementación de medidas de seguridad de la información.

Es importante contar con capacitación básica en técnicas de seguridad, las empresas deben capacitar a sus empleados para mejorar la seguridad de la información.

Según Oliveira (2009, p. 10) “No sirve de nada que una organización actúe virtualmente si la información que alimenta el sistema es vulnerable. Así como este es un factor diferencial para la globalización, la vulnerabilidad puede conducir al fracaso de una empresa".

Algunas prácticas inseguras:

1. Abrir correo electrónico sospechoso;
2. Compras en línea con tarjetas de crédito en compañías no seguras;
3. Dejar el bluetooth encendido en su teléfono celular;
4. Instalar software en su teléfono en sitios fuera de Play Store, Appstore, itunesstore y Googlestore;
5. Permitir que su dispositivo celular no esté protegido;
6. Permitir que personas no autorizadas accedan a sus credenciales;
7. Uso de sitios web sospechosos;
8. Usar su computadora sin una contraseña segura;
9. Uso de publicidad engañosa;
10. Usar dispositivos de almacenamiento en computadoras infectadas;
11. Usar el compartido de multimedia de origen dudoso;
12. Usar una red inalámbrica sin protección;
13. Usar una computadora sin antivirus actualizado o desprotegido;
14. Usar un servidor sin antimalware, antispyware y firewall.

Algunas compañías también permiten infracciones de seguridad, ya sea por parte de hardware o software, pero ahora abordaremos las fallas relacionadas con la parte lógica:

Fallas lógicas de seguridad en las empresas:

1. Permitir a los *Crackers* monitorear las credenciales de los clientes;
2. Permitir vulnerabilidad en los sistemas de seguridad;
3. Permitir la clonación de las tarjetas de crédito de los clientes;
4. Permitir la fuga de noticias y multimedia de los clientes;
5. Permitir la pérdida de datos y archivos confidenciales del cliente;
6. Permitir el desvío de datos bancarios;
7. Permitir desviaciones de fórmulas, patentes y prototipos;
8. Permitir el cambio de datos académicos en las universidades.

Defectos de seguridad físicos o de hardware que facilitan el cibercrimen:

1. Permitir el acceso de personas no autorizadas a la sala de control o seguridad (ingeniería social);
2. Permitir el acceso a cámaras de seguridad;
3. Permitir el acceso o robo de dispositivos informáticos (HDs, unidades externas, pendrives y CD) que contienen información confidencial;
4. Debido a la falta de atención, permitir el uso de cajeros automáticos (ATM) con tarjetas clonadas.

Sin embargo, para las medidas de seguridad de la información, recomendamos el protocolo SET, según Gonsalez (2011):

> El protocolo SET, (Secure Electronic Transaction) es un protocolo creado con el objetivo de proporcionar seguridad a tiempo para realizar una transacción en Internet. Este protocolo fue creado única y exclusivamente para realizar transacciones electrónicas seguras que ofrecen servicios como:
>
> - Autenticación;
> - Confidencialidad;
> - Integridad;
> - Intimidad;

- Verificación inmediata;
- No repudio.

Se sabe que existen muchas medidas de seguridad: preventivas, detectives y correctivas.

Medidas preventivas

Estas son medidas de precaución contra ataques informáticos. Por ejemplo, se aconseja a los servidores que instalen firewalls, usen técnicas criptográficas, establezcan una contraseña segura, creen copias de seguridad o copias de seguridad redundantes. Para dispositivos informáticos como computadoras, recomendamos instalar un antivirus completo con todas las funciones, especialmente antimalware, antispyware y antispam, y se someten a un proceso de actualización constante. Para el control físico, debe instalar cámaras de vigilancia, alarmas, contratar a una compañía de protección física para controlar el espacio y es necesario contratar a un *Hacker* para monitorear y probar los sistemas de seguridad. Sin olvidar la formación de técnicos en el sistema de seguridad.

Medidas de detección

Estas medidas son necesarias cuando desea monitorear o auditar la seguridad de su empresa o si hay un rastreador de atacantes. Estas son medidas que pueden llevarse a cabo con la presencia del *Hacker* contratado para monitorear todos los recursos e informar el estado de seguridad de la compañía.

Medidas correctivas

Las medidas de este tipo son preocupantes, pero su impacto es mayor cuando las medidas anteriores no se llevaron a cabo en su totalidad, aunque anteriormente hemos declarado que el problema de seguridad es muy delicado y requiere grandes inversiones que las empresas no siempre están preparadas financieramente para respaldar esta situación. Son aquellas que suceden en una emergencia, sin ser planificados, y dañan el entorno de las tecnologías de la información, por lo tanto, deben resolverse rápidamente para la salud de la empresa. Es necesario medir los riesgos, ya que las pérdidas de datos a menudo son irreparables, por esta razón, el *Hacker* debe evaluar los riesgos que tienen la empresa al usar este o aquel tipo de seguridad, sabiendo que hasta ahora no tenemos sistemas de seguridad completamente seguros.

Política de seguridad y contingencia.

Amenazas físicas;

> Son aquellos a los que se exponen los recursos materiales utilizados en el entorno de información, poniendo en riesgo la integridad operativa de la organización. Desafortunadamente, en muchas empresas, se gasta mucho en seguridad de la información y terminan olvidando proteger sus activos (Oliveira, 2009, p. 15).

Seguridad física

La seguridad física también es muy común, incluidos incendios, descargas eléctricas, tormentas, problemas eléctricos, uso indebido de equipos, acceso inadecuado a la sala de seguridad y al centro de procesamiento de datos.

Las medidas de seguridad física son:

1. Colocar guardias en el centro de control;
2. Colocar puertas con cerraduras;

3. Instalación de cámaras de vigilancia;
4. Instalar alarmas transmitidas directamente al centro de control policial;
5. Instalar extintores de incendios;
6. Instalar firewall físico;
7. Instalar sistemas de escuchas;
8. Usar No-Breaks.

Según Oliveira (2009, p. 15):

Amenaza lógica

"*Ocurren cuando hay un cambio en la capacidad funcional debido a fraude, accidente o error de recursos*".

Seguridad lógica

La seguridad lógica es más extensa:

1. Criptografía: es el arte de escribir y ocultar códigos para que la información sea irreconocible;
2. Firewall: tiene la función de permitir o prevenir paquetes. Siendo uno de los fundamentos de la seguridad;
3. Gateway de circuitos: tiene la función de permitir o denegar comandos específicos de aplicaciones específicas a través de un servidor proxy, y operan en la capa 4 del modelo OSI;
4. Bastion Hosts: son aquellos que los hosts, antes de llegar a la red interna, necesitan ir a bastionhosts primero, con o sin permiso;
5. Behavior-Based Intrusion Detection: se utiliza para desviar el comportamiento normal del usuario;
6. Protocolo Radius: es un sistema de seguridad cliente/servidor;
7. NAT - Network Address Translation: se usa para guardar direcciones IP;
8. Sistemas basados en red (SDIR) o Network-Based Intrusion Detection System (NIDS): también monitorean el tráfico de red desde encabezados y contenido de paquetes;
9. Single Sign-On (SSO): es un método que utiliza autenticación única y transparente para varios sistemas corporativos;
10. Honeypot: se utiliza ampliamente para probar sistemas de seguridad, lo que permite una mayor visibilidad del estado real de la empresa, también se utiliza para preservar la red de ataques;
11. Red privada virtual (VPN): son responsables de garantizar la autenticidad, privacidad, integridad de los datos, especialmente la tecnología de cifrado;
12. Kerberos: tiene una clave secreta para cada usuario;
13. Knowledge – Based Intrusion Detection: los ataques se detectan como un antivirus;
14. Sistemas de detección de intrusos (IDS): tiene como objetivo monitorear y acompañar la acción interna y externa de la red;

15. Escriba la URL en el navegador: permite usar los sitios acreditados de manera segura;
16. DMZ - Zonas desmilitarizadas: es una red intermedia compuesta por firewall, servidores y conmutador, que permanece entre la red interna y la externa.

Resultados

La investigación se llevó a cabo para proponer medidas de seguridad para empresas corporativas en la industria de tecnología de la información. En este entendimiento, se han propuesto dos formas de protección de la seguridad de la información: lógica (*Software*) y Física (*Hardware*).

Los mecanismos básicos de seguridad deben estudiarse en profundidad, como la identificación, autenticación, autorización, integridad, confidencialidad y disponibilidad de información.

Hoy en día, debe haber una mirada especial a las redes sociales, ya que también permiten numerosos ataques de virus informáticos, espías para copias de credenciales, contraseñas de usuario, varios códigos, lo que permite enviarlos a una computadora remota y, por lo tanto, otorgar a los *Crackers* cometer el crimen.

Es de destacar que, aunque es algo que ya ha sido ampliamente estudiado y difundido en la literatura, el constante estudio e investigación sobre el tema de la seguridad de la información ayuda a la prevención, reduciendo así los gastos económicos innecesarios basados en medidas preventivas de seguridad, que son medidas de precaución. de ataques informáticos, por ejemplo en servidores, es aconsejable instalar firewall, antimalware, antispyware y usar técnicas criptográficas, poner una contraseña segura, crear copias de seguridad o copias de seguridad redundantes.

Cuanto a las medidas de detección, estas se necesitan cuando si desea monitorear o auditar la seguridad en las empresas o si hay un rastreador de atacantes. Estas son medidas que pueden llevarse a cabo con la presencia del *Hacker* contratado para monitorear todos los recursos e informar el estado de seguridad de la compañía.

Con respecto a las medidas correctivas, es preocupante, pero su impacto es mayor cuando las medidas anteriores no se llevan a cabo en su totalidad. Finalmente, se recomienda que, en general, se adopte un plan de contingencia para evitar ataques a empresas corporativas para que se puedan implementar todas las medidas propuestas.

Conclusión

Los ataques cibernéticos han traído muchas dificultades, el malware pertenece a varios grupos de virus informáticos, como el trojan, worms o bugs, dropper y backdoor, son la base de muchas pérdidas económicas, identidad falsa, espionaje y robo de datos, tipos de fraude informático y envío de datos a una computadora remota, incluso si están geográficamente distantes o en continentes diferentes.

Las pérdidas económicas causadas por fallas en la seguridad de la información se han convertido en un escándalo que involucra a grandes figuras del mundo. Sin embargo, los golpes de estado, el fraude electoral, la filtración de información política, los secretos de estado y las desviaciones bancarias han preocupado a todos. No obstante, las políticas para crear legislación para castigar a los ciberdelincuentes son la mejor salida. Estos casos despertaron a la comunidad internacional a medida que los gobiernos de las empresas volvieron sus intenciones sobre la seguridad de la información, que era una preocupación nacional que ahora se ha convertido en un problema global.

En cuanto a estos ataques a las empresas, se sabe que son más expresivos por *Crackers* o *Hackers*, y un número menos representativo de ex empleados. Con este fin, se recomienda que se utilicen medidas de seguridad preventiva, detectivesca y correctiva dentro de un plan de seguridad y contingencia.

Las medidas de seguridad identificadas y propuestas se basan en la física y la lógica. Para el control de la seguridad física, se presta especial atención al entorno físico de la organización.

En cuanto a la seguridad lógica, que es más exhaustiva, especialmente para la seguridad de la información para empresas corporativas, la sugerencia es el uso de criptografía, el uso de un firewall que permite o impide la entrada o salida de paquetes de datos importantes.

Referencias:

CERT.br. (2012). Cartilha de Segurançapara Internet: Interceptação de tráfego (Sniffing). 4.0-Versão. São Paulo. Disponible en: http://cartilha.cert.br/.

Coopamootoo, K. (2018). Cyber Security: Privacidade online e offline. [vídeo]. Newcastle University. Retrieved from https://www.futurelearn.com/courses/cyber-security/0/steps/19596.

Creswell, J. W. (2010) Projeto de pesquisa métodos qualitativo, quantitativo e misto. In: Projeto de pesquisa métodos qualitativo, quantitativo e misto.

Financial Fraud Action UK. (2017). Fraud The Facts: This category covers fraud on cards that have been. Retrieved from https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf.

Futurelearn. (2018a). Cyber Security: Riscos pessoais decorrentes de violação de privacidade nos negócios. [vídeo]. Newcastle University. Retrieved from https://www.futurelearn.com/courses/cyber-security/0/steps/19598.

Futurelearn (2018b) Cyber Security for Small and Medium Enterprises: What can we learn from this attack? Universidade Deakin. Retrieved from https://www.futurelearn.com/courses/cyber-security-business#what-is-upgrade.

Gonsalez. Y. J. (2011) Que es Protocolo SET. Universidad de le Salle. Retrieved from https://www.researchgate.net/publication/261551164_QUE_ES_PROTOCOLO_SET

Martinelli, H. (2008). *Vírus de Celular: Estudo e classificação para um protótipo de defesa: O início das ameaças: Quanto às formas de propagação mais comuns temos*. Uniritter. Brasil - RS, Porto Alegre.

Laureano, M. A. P. (2005) Gestão de segurança da informação. Retrieved from http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf.

Oficina da Net. (2015) Samsung é condenada a pagar indenização milionária a Apple. Retrieved from https://www.oficinadanet.com.br/post/14544-samsung-e-condenada-a-pagar-indenizacao-milionaria-a-apple.

Oliveira, G. (2009). *Segurança de redes:As ameaças organizacionais.* Escola Superior Aberta do Brasil - Vitoria - Espírito Santo.

Quissanga, F. C. (2015).*Caracterização de vírus informáticos em telefonia móvel celular:Propagação e infecção.*(Trabalho de conclusão do curso) Escola Superior Aberta do Brasil -ESAB - Vitoria - Espírito Santo.

Portal de periódicos capes. Missão e Objetivos. Retrieved from https://www.periodicos.capes.gov.br/index.php?option=com_pcontent&view=pcontent&alias=missao-objetivo&Itemid=144.

Terra (2016). Panama Papers. Retrieved from https://www.terra.com.br/noticias/mundo/panama-papers-geram-denuncias-e-investigacoes-em-todo omundo,814039f797239995dea030884e41f8faakajlviv.html.

Fecha de envío: 14/03/2020
Fecha de revisión: 14/04/2020
Fecha de aceptación: 02/06/2020