UNIVERSIDAD ALEJANDRO DE HUMBOLDT
FACULTAD DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA
METODOLOGÍA DE LA INVESTIGACIÓN II
SECCIÓN: 0203

SOLUCIONES PARA LA SEGURIDAD INFORMÁTICA QUE AYUDE A PREVENIR EL ROBO DE DATOS EN LA RED EMPRESARIAL DE EUPHORIA-X

(Proyecto de Investigación)

Autor: Anthony Silva
C.I: 30886525
Profesor: Robert Soto

Caracas, junio del 2023

INTRODUCCION

La seguridad informática es un aspecto fundamental para proteger la información y los recursos de una red empresarial. Teniendo en cuenta que, con el crecimiento tecnológico y el valor de la información recaudada por las compañías con datos personales de sus clientes, el robo de datos puede tener consecuencias graves, como pérdida de confianza, daño reputacional, multas legales o sabotaje. Por eso, es importante adoptar medidas preventivas y correctivas para evitar que los ciberdelincuentes accedan a la red y comprometan la integridad, confidencialidad y disponibilidad de los datos.

Este estudio suministra información relevante sobre la ciberseguridad, que servirá de insumos para otras investigaciones similares en el área, producto a que las tecnologías avanzan de manera continua y progresiva a una velocidad voraz, para esto se aborda el siguiente objetivo general Implementar soluciones para la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.

El presente trabajo investigativo tomó como bases fundamentales para sustentar el desarrollo documentación en línea, como en físico, libros digitales, artículos de noticias actualizadas para una mejor relación a la actualidad siguiendo el modelo de una investigación documental. Aparte de esto se pudo aplicar una investigación de campo, aplicando una encuesta enviada por correo electrónico, dirigida a los trabajadores del departamento de ciberseguridad.

Para contemplar de mejor manera la estructura de la investigación, se debe conocer primeramente que en el capítulo uno se plantea el tema y explicación del entono en general, posteriormente un análisis de todas aquellas circunstancias que dan origen a la problemática actual detallando las causas. A partir de esto se establecen las interrogantes, el objetivo genera, así como también los específicos. Esto se respalda con la redacción de la justificación de la investigación, el cual aborda diversos puntos de vista como lo son el teórico, técnico y social. Para finalizar se presentan los cuadros de sistemas de variables.

Ya en el segundo capítulo, aparecen los antecedentes de la investigación dónde se toma un trabajo investigativo que tiene una temática similar al presente proyecto, tomándolo como una guía para el desarrollo de las bases teóricas, iniciando con el desarrollo de las variables con sus respectivos indicadores. Seguidamente se encuentra la descripción del contexto, en el a cuál se procede a detallar la misión, visión e historia de la empresa. Para finalizar con este capítulo se desarrollaron dos artículos de leyes venezolanas.

Para el tercer capítulo se inicia con la mención del diseño y tipo de investigación utilizada explicando los conceptos claves, respaldando estas definiciones con citas de autores. Se identifica el nivel investigativo en el cual se desarrollará el trabajo, prosigue hasta profundizar el tipo de población y muestra a utilizar. Al final, se abordan las técnicas e instrumentos de recolección de datos.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

La recolección y almacenamiento de información actualmente, rige el mundo sobre todo por el crecimiento del internet, se guardan datos de organismos nacionales, identificaciones personales, como empresas de comercio internacional. Todos estos conocimientos son los que impulsan el desarrollo, economía, crecimiento, control y organización de cualquier tipo de actividad. Incluso, una computadora convencional destinada para el hogar, maneja cantidades de informes valiosos que deben cuidarse. Por lo tanto, la seguridad informática es tan importante, ya que realiza diversos procesos para garantizar la protección e integridad de las distintas amenazas junto a los riesgos, para prevenir y detectar el uso de datos por personal no autorizado. De acuerdo con Samaniego, E. y Ponce, J. (2021) define ciberseguridad como:

> Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (p. 2)

En otras palabras, la ciber seguridad implementa medidas rigurosas y procesos, por los cuales se impiden el uso o visualización de la indagación por personal no autorizado sobre una red informática, los cuales pueden causar daños en los datos recolectados, comprometer la privacidad, disminuir el rendimiento del equipo, hasta teniendo la posibilidad de negar el acceso a los usuarios que si están autorizados para manejar dicha información.

Es necesario resaltar, que el mundo moderno está conectado, por consiguiente, un ataque puede ocasionar robo de identidad, intentos de extorción, así como también pérdida de datos de gran importancia, ante lo mencionado los líderes empresariales internacionales califican la amenaza cibernética como uno de los principales riesgos contemporáneos, por ello, constantemente se realizan esfuerzos para identificar nuevas y emergentes amenazas junto a las estrategias de los ciber ataques.

Por ende, la privacidad es uno de los objetivos claves por lo cual, los datos aportados no deben ser divulgados, para garantizar esto, solo las personas encargadas y autorizadas pueden visualizar los documentos. Dicho esto, se debe mantener la integridad de la información resguardándola, evitando que sea manipulada por terceros, pero manteniendo siempre la posibilidad de acceder y recuperarse, en caso de un desastre o incidente de seguridad que cause su pérdida o corrupción.

No obstante, el mundo de la ciberseguridad ha estado bajo tensión causado a la habitual e incontenible creación e introducción de malware y ransomware cada vez más sofisticados, desplegados en todas las plataformas. El incremento de teletrabajos o estudio en casa ha trasladado a millones de usuarios desde una red perimetral protegida a una casera que son más inseguras, lo cual facilita las violaciones y fuga de información en pequeñas y grandes empresas. De conformidad con Ramos, D. (2019) indica que:

> Debido al constante crecimiento de la tecnología de información a nivel mundial, las amenazas y riesgos hacia la seguridad informática son cada vez más frecuentes haciendo necesario que las organizaciones requieran implantar políticas, normas, procedimientos con el fin de reducir el impacto de las amenazas y riesgos. (p.2)

Así pues, el crecimiento tecnológico ha hecho que exista una cantidad mucho más robusta como también diversa de información valiosa a nivel mundial, pese a esto, están sujetas a amenazas y riesgos de ser vulneradas, este proceso es cada vez más frecuente, por lo cual se deben tomar medidas para contrarrestar dichas eventualidades. Como, por ejemplo: horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones denegadas, planes de emergencias, todo lo que permita un buen nivel de protección minimizando el impacto en el desempeño de los trabajadores y de la organización en general.

Es bien sabido que, una de las problemáticas existentes que enfrentan muchas empresas, especialmente aquellas que han comenzado o culminado su proceso de digitalización, es la fuga de datos o fuga de información y, aunque normalmente tiene que ver con incidentes de ciberseguridad, se sabe que un ciberataque no es la única

causa tras este suceso en una empresa, en vista de que puede ser producida de diferentes maneras, sin embargo, las principales son dos tipos: internas las cuales vienen directamente por empleados o miembros de la organización y puede ocasionarse de forma intencional o inconsciente; externas que en su gran mayoría ocurre por accesos no autorizados e ilícitos a la recopilación custodiada por la organización, para poder hacerse con ellos siendo aplicados a diferentes fines, principalmente económicos.

Cabe mencionar, que una de las causas es no contar con un capital humano apto para resolver ante amenazas cibernéticas. Según el estudio Breakthrough realizado por Dell Technologies (2022) “El 55% de los encuestados consideran a los empleados como el eslabón más débil en estrategia de defensa ante ciberataques" (p. 8). Para mantener y garantizar la ciberseguridad de la organización, los recursos humanos tienen la responsabilidad de asegurar las áreas más sensibles, las cuales son las que poseen mayor exposición a terceros, así como los aspectos financieros, y las que manejan información altamente confidencial.

Adicionalmente, otro de los motivos son las brechas de seguridad, que son un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. Normalmente, es generado cuando un intruso logra eludir los mecanismos de resguardo. Algunos ejemplos, los cuales dan una visión de lo que puede llegar a causar uno de estos incidentes pueden ser: En el 2013 Yahoo! experimentó un intento de phishing que dejó 3.000 millones de cuentas expuestas a los hackers, Facebook presentando fallos internos en su software, se filtraron los datos personales de 29 millones de usuarios en 2018, eBay fue atacada en el 2014 por piratas informáticos que vulneraron muchas de las contraseñas de los clientes (Kaspersky, E. 2020).

Finalmente, planteados estos hechos mediante referencias actualizadas junto con argumentos respaldados con investigaciones previas, que sustenten el estudio acerca de las soluciones para la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X, destacando los factores que inciden en la misma, sus requerimientos tecnológicos, así como también los procesos necesarios para su aplicación.

Interrogantes de la Investigación

1. ¿Cuáles son los factores que inciden en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X?
2. ¿Cómo son los requerimientos tecnológicos que se llevan a cabo para las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X?
3. ¿Qué procesos optimizan las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X?

Objetivos de la Investigación

Objetivo General

Implementar soluciones para la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.

Objetivos Específicos

1. Definir los factores que inciden en la seguridad informática que ayude a prevenir el robo en la red empresarial de Euphoria-X.
2. Examinar los requerimientos tecnológicos necesarios para llevar a cabo las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.
3. Establecer los procesos que optimicen las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.

Justificación de la Investigación

Este estudio suministra información relevante sobre la ciberseguridad, que servirá de insumos para otras investigaciones similares en el área, producto a que las tecnologías avanzan de manera continua y progresiva a una velocidad voraz, de tal modo que, surgen nuevas amenazas, riesgos, defensas, medidas que constantemente deben ser actualizadas para garantizar el resguardo de la información.

Por otra parte, desde la perspectiva técnica, el estudio aporta a la red empresarial información que permite utilizarse con propiedad, aplicando los procedimientos, pasos o herramientas de detección de fallas o vulnerabilidades en el software para el fortalecimiento, prevención de las deficiencias y resguardo de los datos de una manera

segura y confiable.

Desde el punto de vista social, se espera que la indagación origine actitudes positivas hacia la comunidad en general. Todo esto derivado, a los diferentes beneficios aportados al aplicar las estrategias de protección cibernéticas como, por ejemplo: ahorrar en gastos imprevistos, obtención de una mejor reputación, adquirir la confianza del cliente, mayor productividad y preservar la integridad de la documentación.

Sistema De Variables

Cuadro 1.
Identificación y Definición de las Variables

OBJETIVOS ESPECÍFICOS	VARIABLES	DEFINICIÓN CONCEPTUAL
Definir los factores que inciden en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.	Factores que Inciden En La Seguridad Informática.	Circunstancias o elementos que pueden convertirse en los causantes de una acción o acontecimiento, que puede resultar ser favorable o, por el contrario, generar brechas o vulnerabilidades en la seguridad del sistema informático.
Examinar los requerimientos tecnológicos necesarios para llevar a cabo las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.	Requerimientos Tecnológicos de La Seguridad Informática	Condiciones que resulta ineludible o imprescindible para el desarrollo y utilización del software empleado, siendo en este caso diferentes tecnologías, las cuales condicionarán la efectividad del resguardo de los datos.
Establecer los procesos que optimicen las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.	Procesos Que Optimicen La Seguridad Informática	Conjunto de acciones que son ejecutadas para alcanzar el objetivo de fortalecer el resguardo de información, manteniendo así la confidencialidad de los datos.

Fuente: Silva, A. (2023)

Cuadro 2.

Operacionalización de las Variables

OBJETIVOS ESPECÍFICOS	VARIABLES	DIMENSIONES	INDICADORES	INSTRUMENTO	ÍTEMS
Definir los factores que inciden en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.	Factores que Inciden En La Seguridad Informática.	Nivel Técnico	➢ Factor Humano en la Ciberseguridad ➢ Seguridad Activa y Pasiva ➢ Seguridad Física y Lógica	Cuestionario	1 2 3
Examinar los requerimientos tecnológicos necesarios para llevar a cabo las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.	Requerimientos Tecnológicos de La Seguridad Informática	Nivel Técnico	➢ Software antivirus ➢ Firewall perimetral de red ➢ Servidor proxy ➢ End Point Disk Encryption ➢ Escáner de vulnerabilidades	Cuestionario	4 5 6 7 8
Establecer los procesos que optimicen las soluciones en la seguridad informática que ayude a prevenir el robo de datos en la red empresarial de Euphoria-X.	Procesos Que Optimicen La Seguridad Informática	Nivel Técnico	➢ Protocolos de seguridad ➢ Respaldo y planes de contingencia ➢ Priorización de riesgos	Cuestionario	9 10 11

Fuente: Silva, A. (2023)

CAPÍTULO II

MARCO TEÓRICO REFERENCIAL

Antecedentes de la Investigación

Duran, L. (2016) desarrolló un trabajo de investigación en la Universidad Central de Venezuela, titulado Evaluación de la Seguridad Informática y Mitigación de Vulnerabilidades en una Infraestructura de Red Siguiendo los Lineamientos Propuestos por la Especificación NIST SP 800-115. El autor plantea su objetivo general como: Evaluar la situación actual en seguridad informática de la red de datos de una institución pública usando los lineamientos de la metodología NIST SP 800-115 y aplicar correctivos a las debilidades encontradas durante la ejecución de la misma.

En el presente trabajo se desarrolló como metodología una investigación de campo, utilizando un muestreo de 21 componentes de seguridad que van a ser revisados, para esto se aplica el método RIIOT por ser las siglas en ingles de Review, Interview, Inspect, Observe and Test que es una manera de asegurar un completo proceso de recolección de datos. Una de las conclusiones fue que, para tener una seguridad consistente en una red de datos, es fundamental mantener una evaluación continua, previniendo así posibles pérdidas de datos, originado por ataques maliciosos, reforzando constantemente la seguridad y reparando aberturas posibles en el sistema.

La presente investigación se toma como antecedente, debido a que, este trabajo empleó los contenidos teóricos Propuestos por la Especificación NIST SP 800-115 y procedimientos enfocados a los sistemas tecnológicos para el correcto resguardo de los datos, mostrando como la planificación metódica arroja resultados positivos, permitiendo una mejora en la ciberseguridad, demostrando la gran importancia de una evaluación continua y actualización de los sistemas informáticos.

Bases Teóricas

Seguridad Informática

Puede ser vista como una disciplina la cual, su objetivo principal sea proteger la integridad y privacidad de los datos almacenados en un sistema informático, como también a los usuarios. A pesar de los avances en los sistemas siempre existe la posibilidad de alguna vulnerabilidad, por lo que es necesario estar en una constante

mejora, en concordancia con lo antes mencionado hornetsecurity (s.f.) indica lo siguiente “La escala de un ataque cibernético es cada vez más devastadora y el riesgo de ser víctima de un ciberataque aumenta cada día” (Párr. 1). Esto a causa de la gran cantidad de información valiosa y personal que es recolectada por las empresas, siendo de utilidad para diferentes contextos.

Factores que Inciden en la Seguridad Informática

En términos simples, los factores pueden ser circunstancias o elementos que pueden convertirse en los causantes de una acción o acontecimiento, que puede resultar ser favorable o, por el contrario, generar brechas o vulnerabilidades en la seguridad del sistema informático. Ante lo mencionado, Ferrer, J. (2014) indica que “Un factor es un elemento que influye en algo. De esta manera, los factores son los distintos aspectos que intervienen, determinan o influyen para que una cosa sea de un modo concreto.” (parr.1). Por ende, es una causa directa sobre un hecho en diversos ámbitos y sentidos.

Se hace de vital importancia destacar y abordar de manera correcta a estos elementos o circunstancias, los cuales permiten tener un mejor resguardo de la red, garantizando la privacidad. Entre los factores más influyentes se puede encontrar: a) Factor Humano como Solución de la Ciberseguridad. b) Seguridad Activa y Pasiva. c) Seguridad Física y Lógica. Todas estas áreas serán desarrolladas y profundizadas seguidamente.

Factor Humano como Solución de la Ciberseguridad

No es sorpresa darse cuenta que el factor humano es superior a los sistemas programados y automatizados en diversas tareas, aparte de resolución de problemas que requieran un análisis de la situación, aunque, se debe tener presente que el error humano es la principal causa del quebrantamiento de los datos. Afirma Domínguez, R. (2020) [citado por Instituto Internacional de estudios en Seguridad Global (INISEG, 2020)] que “El factor humano influye de forma clave en un 80% de los ciberataques” (parr. 14). Es aquí, donde las industrias deben considerar sus protocolos, la preparación profesional del equipo encargado de ciberseguridad, puesto que son estos los que diseñan, desarrollan, despliegan, y configuran los sistemas, pero siempre se cometen errores y es común en el ser humano, por lo tanto, es más difícil controlar este factor.

Por otra parte, el personal a su vez puede ser la línea defensiva más sólida y eficiente

para poder actuar a tiempo, aplicar esto da una gran ventaja, por este motivo, el trabajador puede centrarse en proteger lo que posee un mayor riesgo de vulnerabilidad y determinar el objetivo primordial del atacante, aparte de aprender sobre el incidente reforzando el área afectada.

Seguridad Activa y Pasiva

La seguridad activa es la primera línea de defensa, destinada a evitar posibles daños informáticos implementando medidas que impidan o asuman fallos o ataques externos. Protege las redes de vulnerabilidades, reduce la probabilidad de una brecha y brinda información sobre las amenazas. Esta debe reaccionar al ataque y volver a la normalidad en el menor tiempo y costo posible. Por otro lado, la seguridad pasiva está encargada de solucionar o minimizar los efectos provocados por un ataque informático cuando ya se ha producido. Pone en marcha todos los mecanismos necesarios para loquear el ataque y recuperar la información que se pretende robar, para esta etapa es importante contar con un plan de contingencia o de respuesta eficaz.

Seguridad Física y Lógica

La seguridad física es la protección del hardware, los datos, documentos y equipos. Brinda protección contra desastres naturales, incendios accidentales, vandalismo, robo, así como también el acceso no autorizado o ilegal, aparte de los puertos USB que son de suma importancia, por tal razón estos son un punto de acceso para poder sacar información de gran valor. Por su parte la seguridad lógica es la protección del software, incluye identificación de usuarios, contraseñas de acceso, autentificación, derechos de acceso e incluso niveles de autoridad. Estos medios son necesarios para garantizar que solo personal autorizado sea capaz de realizar acciones o acceder a los datos en una red. Una brecha de seguridad lógica da origen a datos internos invisibles, los cuales son imperceptibles hasta que se intentan procesar o visualizar los datos.

Requerimientos Tecnológicos de La Seguridad Informática

Cuando se habla de un sistema informático se sabe que lleva diversos requerimientos específicos, que son condiciones que resulta ineludible o imprescindible para el desarrollo y utilización del software empleado, siendo en este caso diferentes tecnologías, las cuales condicionarán la efectividad del resguardo de

los datos. Para respaldar lo antes mencionado, Según la Real Academia Española (RAE, 2014) un requisito es una "circunstancia o condición necesaria para algo" (parr.1). Es importante mencionar que estos pueden ser tangibles e intangibles, naturales o impuestos.

Los avances tecnológicos son completamente necesarios y esenciales, para brindar una correcta aseguración en una organización ampliando las posibilidades y efectividad al momento de afrontar una situación de riesgo. Principalmente se deben proteger los dispositivos endpoints como computadoras, routers o dispositivos inteligentes, a su vez siendo de suma importancia las redes y la nube. Esto puede lograrse gracias: a) Software antivirus. b) Firewall perimetral de red. c) Servidor proxy. d) End Point Disk Encryption. e) Escáner de vulnerabilidades. A continuación, se profundiza sobre cada uno de los puntos anteriores.

Software antivirus

Primeramente, se debe saber con certeza ¿qué es un software antivirus? Para ello es necesario resaltar a VANGUARDIA (2018) “Los antivirus son programas informáticos creados para la prevención, bloqueo, detección y eliminación de ciertos archivos o ejecutables dañinos que se descargan en el ordenador, sin previo aviso, al navegar por internet.” (parr. 1). Estos son de gran importancia, ya que evita retrasos o contratiempos en el ámbito laboral ofreciendo servicios de monitoreo activo, que impidan el acceso de archivos o documentos riesgosos, garantizar su detención y eliminación apenas ingrese al computador, así como también bloquear páginas web inseguras.

Todos los computadores conectados a una red deben tener un antivirus implementado que sea de calidad, otro punto importante para el buen funcionamiento de este software, es que se debe mantener actualizado, de no ser así, puede dar la impresión de tener una seguridad tangible y real cuando es todo lo contrario, producto del constante lanzamiento de nuevos y poderosos malwares.

Firewall perimetral de red

Esta es una herramienta primordial en la ciberseguridad, dedicada a escanear y monitorear el tráfico de red, tanto entrante como saliente, tiene la capacidad de bloquear o permitir el tráfico definido según las reglas impuestas por el administrador,

es la primera línea de defensa en seguridad y se ha mantenido así durante más de 25 años, este posee distintos tipos como por ejemplo el firewall por hardware, el cual necesita un dispositivo especifico, viene comúnmente instalado en los routers utilizados para acceder a internet, es por este motivo que todos los dispositivos que estén detrás de este estarán protegidas.

Servidor proxy

En términos sencillos es un intermediario entre la conexión personal y el servidor al cual se intenta acceder, se encargara de filtrar los paquetes que circulan entre estas conexiones, bloqueará a los sitios que se presuman sospechosos o inseguros como también limita el acceso a direcciones, que esté prohibida su visita dentro de un ambiente laboral, resguardará la dirección IP utilizando una completamente distinta, eliminando las limitaciones geográficas al poder acceder a servicios, los cuales en la región original no está disponible.

End Point Disk Encryption

Se basa en un proceso de encriptación o codificación de los datos protegiéndolos contra el acceso no autorizado, posee una seguridad sólida asegurando que la información importante de la empresa, este completamente resguardada, como también claves para que nadie pueda leerlas o guardarlas, elimina la posibilidad de instalación de archivos corruptos en los sistemas operativos, bloquea archivos albergados en dispositivos de almacenamiento, servidores o computadoras.

Escáner de vulnerabilidades

Este último punto posee una relevancia destacable, se trata de una herramienta, la cual debe implementar todo tipo de empresas, sin importar el tamaño o sector al que se dedique. Permite analizar y gestionar los puntos débiles encontrados en el sistema, brindando una alerta en la brevedad al detectar un problema, lo que reduce considerablemente el tiempo para la resolución de los conflictos, producidos por el simple hecho de saber en qué sitio específicamente habrá que asegurar.

Procesos que Optimicen la Seguridad Informática

La seguridad está en constante cambio, por lo que tiene que ser más ágil, es por esto que se hace necesario enfatizar que los procesos para esto son un conjunto de acciones

que son ejecutadas para alcanzar el objetivo de fortalecer el resguardo de información, manteniendo así la confidencialidad de los datos. Es necesario citar a Westreicher, G. (2020) el cual lo define como "Un proceso se trata entonces, en general, de una serie de operaciones realizadas en orden específico y con un objetivo" (parr.2). Este concepto puede ser aplicado a muchos ámbitos tales como, procesos judiciales, biológicos, informáticos, electorales, psicológicos, etc.

El desarrollo tecnológico y la transformación digital, permite a las empresas ser mucho más productivas y responder de manera eficiente a las necesidades y peticiones de los consumidores, sin embargo, esto las convierten en blancos principales hacia ataques cibernéticos, es por esto que para las empresas, implementar procesos y medidas de seguridad que ayuden a prevenir riesgos y realizar acciones en el menor tiempo posible se hace cada vez más importante, teniendo en cuenta las diversas amenazas que enfrentan. Es por eso que se aplican: a) Protocolos de seguridad. b) Respaldo y planes de contingencia. c) Priorización de riesgos. Con el objetivo de mantener la eficiencia de sus servicios en un momento de crisis.

Protocolos de seguridad

Primeramente, la definición de protocolos de seguridad según el Grupo ATICO34 (s.f.) expresa que "Los protocolos de seguridad informática son las reglas o normas diseñadas para garantizar la confidencialidad, la integridad y la disponibilidad de la información." (parr. 2). Esto quiere decir, que son los procedimientos utilizados para evitar que la información pueda ser observada, destruida o manejada por aquellos que están autorizados para trabajar con esta.

Aunque, hay que tomar en cuenta que existen diversos tipos de protocolos tales como: el protocolo de control de transmisión o TCP y protocolo de internet o IP (TCP/IP). Por medio de estos, los dispositivos que se encuentran conectados a la red pueden comunicarse y transmitir información, otro es el HTTP o protocolo de transferencia de hipertexto utilizado para emitir mensaje por la red desde el navegador al servidor web, cifra la información y evita que pueda ser interceptada, Protocolo SSH (Secure Shell) permite el acceso remoto a un servidor por medio de un canal seguro en el que toda la información es cifrada y el Protocolo DNS, el cual convierte las

direcciones URL a direcciones IP, para poder acceder a sitios web.

Respaldo y planes de contingencia

Según Martins, J. (2022) define plan de contingencia como "Un plan de contingencia empresarial es una estrategia sobre cómo responderá tu organización en caso de eventos importantes o críticos para el negocio que te hagan desviar de tus planes originales." (parr.3). La importancia de implementar uno de estos es que, si se ejecuta adecuadamente, puede mitigar el riesgo, disminuir el impacto y garantizar volver a la normalidad en el menor tiempo posible. Una vez se tenga el plan se debe compartir este modelo con las personas adecuadas y hacer supervisiones de este con frecuencia, para asegurar que siga siendo efectivo teniendo en cuenta nuevas posibilidades que antes no estaban presentes.

Priorización de riesgos

La gestión de riesgos de seguridad tecnológica, es la mejor manera de prepararse para un futuro, el cual es incierto, muchas veces las empresas se tornan demasiado conservadoras la evaluación para evitar el desperdicio de recursos, aunque es preferible aplicar el capital necesario para evitar que los contratiempos puedan ser sumamente destructivos en caso de llegar a ocurrir, puede pasar que se tenga que realizar trabajo duplicados entre departamentos o riesgos graves, los cuales no son percibidos, para que esto no pueda suceder lo mejor es estar un paso adelante, contando con un sistema jerárquico sobre estas amenazas y cómo atacarlas.

Descripción Del Contexto

La empresa Euphoria-X ubicada en Caracas, Venezuela (Chacao), contempla como función principal brindar un espacio donde pueda realizarse compra y venta de productos o servicios en los mercados internacionales, aprovechando las oportunidades de negocio que se presentan. Esta actúa como intermediaria entre los productores y los consumidores, facilitando las operaciones comerciales y generando beneficios por la diferencia de precios.

Misión

Su misión trading es ofrecer a sus clientes la oportunidad de invertir en los mercados financieros de forma eficiente, segura y rentable. Encargándose de ejecutar las órdenes

de compra y venta de activos financieros que sus clientes le solicitan, ya sean acciones, divisas, materias primas, índices, criptomonedas u otros. Además, puede brindar asesoramiento, formación y análisis a sus clientes para ayudarles a tomar las mejores decisiones de inversión. Buscando generar valor para sus clientes y para sí misma, cumpliendo con los más altos estándares de calidad, ética y transparencia.

Visión

Ser un referente en el mercado financiero, ofreciendo soluciones innovadoras y personalizadas a los clientes, basadas en el análisis, la estrategia y la gestión de riesgos. Creando valor a largo plazo, aprovechando las oportunidades que brinda la globalización junto a la digitalización, adaptándose a los cambios constantes del entorno económico. Fomentando el desarrollo profesional y humano del equipo, contribuyendo al bienestar de la sociedad mediante la libertad financiera a escala global.

Breve Reseña Histórica

La empresa se fundó en el año 2010 por un grupo de expertos en finanzas, economía y tecnología, con el objetivo de ofrecer servicios de inversión en los mercados financieros globales. Se especializó en el trading algorítmico, utilizando sistemas informáticos avanzados para analizar y ejecutar operaciones de forma automática y eficiente. Esta se diferenció de sus competidores por su innovación, su transparencia y su rentabilidad.

Euphoria-X creció rápidamente y se expandió a diferentes países y regiones, contando con un equipo multidisciplinar y multicultural, formado por más de 500 profesionales de distintas áreas y nacionalidades. La empresa también estableció alianzas estratégicas con otras entidades financieras, académicas y tecnológicas, para mejorar sus servicios y su conocimiento del mercado.

Bases Legales

Según La Constitución de la República Bolivariana de Venezuela (CRBV, 1999) expone en su artículo 55:

> Toda persona tiene derecho a la protección por parte del Estado, a través de los órganos de seguridad ciudadana regulados por ley, frente a situaciones que

> constituyan amenaza, vulnerabilidad o riesgo para la integridad física de las personas, sus propiedades, el disfrute de sus derechos y el cumplimiento de sus deberes. (p. 179)

En concordancia con la Ley Especial Contra Delitos Informáticos (LECDI) (2001) expresa en el Artículo 20:

> Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero. (p.5)

CAPÍTULO III

MARCO METODOLÓGICO

Diseño y Tipo de Investigación

El presente trabajo investigativo posee dos modalidades como estrategia de investigación: primeramente, se encuentra la investigación documental, la cual se basa en el análisis y la interpretación de fuentes de información escritas, gráficas o audiovisuales. Su objetivo es recopilar, seleccionar, organizar y evaluar la información relevante para un tema o problema de estudio. La investigación documental se puede aplicar a diversas áreas del conocimiento y requiere de una metodología rigurosa y sistemática, para resaltar lo anteriormente mencionado la Universidad Pedagógica Experimental Libertador (UPEL, 2016) indica que:

> Se entiende por Investigación Documental, el estudio de problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos. La originalidad del estudio se refleja en el enfoque, criterios, conceptualizaciones, reflexiones, conclusiones, recomendaciones y, en general, en el pensamiento del autor. (p.20)

En el mismo orden de ideas, se puede añadir que, el proyecto investigativo que se encuentra en curso aplica esta modalidad, debido a la consulta y recopilación de información provenientes de otras fuentes, principalmente electrónicas como páginas webs, documentos en línea, blogs en línea e investigaciones previas actualizadas, tomándolas como sustento y bases argumentales para poder desarrollar un análisis junto a una conclusión sobre la temática planteada.

Por otro lado, la Investigación de campo es un método de estudio que consiste en recoger datos e información directamente de la realidad que se quiere analizar. Para ello, el investigador se traslada al lugar donde ocurren los hechos o fenómenos de su interés y los observa, registra y documenta de forma sistemática y rigurosa. La investigación de campo permite obtener un conocimiento más profundo y veraz de la realidad, así como contrastar hipótesis y teorías previas. Es pertinente señalar a Arias, F. (2012) el cual define:

> La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental. (p.31)

Así pues, en este escrito se aplica la investigación de campo para conocer las opiniones y experiencias de un grupo de personas que participan en la empresa Euphoria-X. Para ello, se diseña un cuestionario con preguntas. Luego, se analiza las respuestas y se extrae las principales conclusiones sobre el impacto de las soluciones o puntos de vistas planteados a la empresa.

Nivel de la Investigación

En esta ocasión se desarrollará un nivel de tipo proyectivo, es un tipo de investigación que busca solucionar problemas o situaciones mediante la creación de planes o modelos que se basan en el análisis integral de todos los aspectos involucrados. El nivel proyectivo implica el uso de la imaginación, la creatividad y la participación de los actores en el proceso. De hecho, Hurtado, J. (2010) señala lo siguiente: "la investigación proyectiva tiene como objetivo diseñar o crear propuestas dirigidas a resolver determinadas situaciones" (p.133).

El objetivo principal es saber las causas de los problemas que se encuentran en la red con los datos personales de los usuarios, junto a los clientes, una vez identificadas, el desarrollo de las soluciones debe comenzar, mediante el análisis e interpretación de los datos y conclusiones, arrojadas por la recolección de información, aplicando estas en corto, medio y largo plazo para garantizar una mayor seguridad, como también una estabilidad sólida, tanto en el servicio como también en el entorno laboral.

Población y Muestra de la Investigación

Población de la Investigación

En el ámbito de la metodología, se entiende por población al conjunto de elementos que comparten una o más características comunes y que son objeto de estudio. Para ampliar esto, Arias, F. (2012) enfatiza que "es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación" (p.81). Es por tanto que se aplica este método para obtener información

sobre el fenómeno de estudio, como la opinión de los empleados del departamento de ciberseguridad.

Primeramente, se debe determinar qué tipo de población está presente en el trabajo, el cual es "accesible", siendo este el conjunto de individuos o elementos que pertenecen a la población objetivo y que están disponibles para ser estudiados mediante una investigación. En el mismo orden de ideas, Arias, F. (2012) refiere que la población accesible "es la porción finita de la población objetivo a la que realmente se tiene acceso y de la cual se extrae una muestra representativa." (p.82). Aclarado estos puntos, esta población es perteneciente a cincuenta (50) empleados del Departamento de Ciberseguridad de la empresa Euphoria-X ubicada en Chacao de la ciudad de Caracas, esta cantidad fue tomada para recolectar información veraz para resolver la problemática en cuestión.

Cuadro 3. Población de la Investigación

Población	Cantidad
Empleados del Departamento de Ciberseguridad de la Empresa Euphoria-X	50

Fuente: Silva, A. (2023)

Muestra de la Investigación

Una muestra es una parte de la población que se selecciona para estudiarla y obtener información sobre el fenómeno de interés. La muestra debe ser representativa de la población, es decir, debe reflejar sus características y variabilidad. Es pertinente señalar a Tamayo y Tamayo, M. (2011) quien lo define como "Instrumento de gran validez en la investigación; en éste el investigador selecciona las unidades representativas a partir de las cuales obtendrá los datos que le permitirán extraer inferencias acerca de la población que se investiga" (181). Partiendo de este concepto se tiene que una población de 50 personas y se procederá a realizar un proceso para determinar la cantidad representativa o muestra.

Se decide tomar la misma cantidad perteneciente a la población como muestra sin la necesidad de aplicar criterios de selección. En ese sentido Arias, F. (2012) aclara

que: “si la población, por el número de unidades que la integran, resulta accesible en su totalidad, no será necesario extraer una muestra” (p.83). Por lo tanto, la muestra de este estudio será igual a la población, exactamente 50 personas, lo que representa el 100% de la población que labora en el Departamento de Ciberseguridad de la empresa Euphoria-X.

Cuadro 4. Muestra de la Investigación

Muestra	Cantidad
Empleados del Departamento de Ciberseguridad de la Empresa Euphoria-X	50

Fuente: Silva, A. (2023)

Técnica e Instrumento de Recolección de Datos

Técnica de Recolección de Datos

Las técnicas de recolección de datos son los métodos que se utilizan para obtener información sobre un fenómeno o problema de investigación. Estas técnicas permiten recabar datos cuantitativos o cualitativos, según el tipo de estudio y el diseño de la investigación. Sobre esta misma base Universidad Alejando de Humboldt (UAH, 2016) la define como “Las técnicas son aquellas que permiten la recolección de la información, es decir, el cómo acceder a los datos u opiniones sobre el tema que se está investigando y dar respuestas a las preguntas de investigación” (p. 33).

En este trabajo de investigación se utilizará la encuesta, la cual consiste en aplicar un cuestionario a un grupo de personas que representan a una población más grande. El objetivo es obtener y analizar datos sobre las opiniones, actitudes y comportamientos de los ciudadanos respecto a diferentes temas. Antes esto Arias, F. (2012) indica que “Se define la encuesta como una técnica que pretende obtener información que suministra un grupo o muestra de sujetos acerca de sí mismos, o en relación con un tema en particular “(p.72).

En este caso se utiliza la encuesta, gracias a que permite aplicarlo a un gran número de personas y la obtención de una gran cantidad de información sobre un amplio abanico de cuestiones a la vez, siendo de gran importancia ya que los resultados

obtenidos se muestran de manera ordenada y controlada, esto hace que se aborde la temática de una manera mucho más amplia, cubriendo puntos que de otra forma no hubiera sido posible, obteniendo respuestas de manera objetiva.

Instrumento de Recolección de Datos

Un instrumento de recolección de datos es cualquier recurso que utiliza el investigador para obtener información sobre el tema que le interesa. Para resaltar lo anterior Arias, F. (2012) explica que "es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información" (p. 68). Se aplica en esta ocasión un cuestionario, es un documento que contiene una serie de preguntas que sirve para recoger y analizar datos en una investigación o estudio. Para respaldar esto Palella, S. y Martins, F. (2012) expresa que "es un instrumento de investigación que forma parte de la técnica de la encuesta. Es fácil de usar, popular y con resultados directos […] Las preguntas han de estar formuladas de manera clara y concisa." (p. 131).

Como se menciona anteriormente se utilizará un cuestionario, el cual tendrá un total de 11 ítems, con preguntas cerradas, contando con una escala de Guttman y opciones de respuestas dicotómicas que en este caso son "Si" o "No", estas interrogantes van dirigidas a los cincuenta (50) empleados del Departamento de Ciberseguridad de la empresa Euphoria-X que serán respondidas de manera anónima (Ver Anexo A).

CONLUSIÓNES

A partir del trabajo investigativo realizado con anterioridad se logró contribuir al avance del conocimiento, la innovación y la protección de los datos e infraestructuras críticas frente a amenazas y ataques informáticos. Con los resultados y toda la información recaudada. Las consecuencias de una falta de ciberseguridad pueden ser muy graves, como la pérdida de información confidencial, el robo de identidad, el daño a la reputación, el incumplimiento de normativas legales, el sabotaje de operaciones o la extorsión económica. Por eso, es importante que las empresas inviertan en medidas de prevención, detección y respuesta ante las amenazas cibernéticas, así como en la formación y concienciación de sus empleados sobre las buenas prácticas de seguridad digital.

Continuando con esta misma base, existen una cantidad de factores los cuales delimitan las capacidades y el nivel de efectividad de la protección, tal es el caso del factor humano, el cual es la primera línea de defensa y en caso de encontrarse debilitada todos los demás sistemas se verán en decaída, a pesar de esto se logró mejorar en gran medida la capacitación del personal, detallando las deficiencias de los conocimientos obtenidos, de esta forma el contrafuego más potente, como lo es el recurso humano sea mucho más eficaz a la hora de reaccionar a alguna eventualidad que así lo requiera, mejorando con esto todos los sistemas automatizados a partir de los conceptos adquiridos.

No conforme con esto, se logra desarrollar nuevas tecnologías necesarias para poder estar actualizados y a la vanguardia con las competencias y todo tipo de ataques, reparando y reforzando vulnerabilidades escondidas que estaban presentes o que fueron realizadas recientemente, el mayor conflicto al realizar este proceso principalmente la destinación de los recursos al proceso de investigación, sin embargo, se hace de mucha utilidad estos nuevas adquisiciones ya que dan un plus en cuanto a la protección pasiva de los datos que son almacenados.

Otro punto importante que fue desglosado, son aquellos procesos que agilizan la toma de decisiones y respuestas rápidas por parte de todos los miembros de la organización, al realizar un análisis sobre las posibles medias a tomar se encuentran los

protocolos de seguridad, los cuales generan una seguridad al momento de realizar una acción urgente, permitiendo una correcta solución a la problemática reduciendo los tiempos de respuesta y detección de los fallos, se implementaron respaldos y planes de contingencia, con el fin de preservar aquella información valiosa que es de origen personal, minimizando los riesgos que conlleva los ataques informáticos, para poder realizar esto se tuvo que pasar por un proceso largo de priorizar los riesgos y niveles de atención a cada uno.

Para finalizar, implementar soluciones para la seguridad informática es una tarea fundamental para proteger la información confidencial y sensible de una empresa. El robo de datos en la red empresarial puede tener consecuencias graves, como pérdidas económicas, daños a la reputación, demandas legales o sanciones regulatorias. Por eso, es necesario adoptar medidas preventivas, como el uso de antivirus, firewalls, cifrado, autenticación, copias de seguridad y auditorías periódicas. Estas soluciones ayudan a detectar y bloquear posibles amenazas, así como a recuperar los datos en caso de un incidente. De esta forma, se garantiza la integridad, disponibilidad y confidencialidad de la información, y se evita que caiga en manos de ciberdelincuentes o competidores desleales.

REFERENCIAS

Arias, F. (2012). ***El proyecto de investigación: Introducción a la metodología científica.*** https://t.me/c/1614591896/278

Constitución de la República Bolivariana de Venezuela (1999). Gaceta Oficial de la República Bolivariana de Venezuela, No. 36.860. Diciembre 30, 1999. https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/siteal_venezuela_1006.pdf

Dell Technologies (2022) ***The Breakthrough Study***. https://www.delltechnologies.com/asset/esar/solutions/businesssolutions/industry-market/dell-technologies-breakthrough-report.pdf

Duran, L. (2016) ***Evaluación de la Seguridad Informática y Mitigación de Vulnerabilidades en una Infraestructura de Red Siguiendo los Lineamientos Propuestos por la Especificación NIST SP 800-115.*** Universidad Central de Venezuela http://saber.ucv.ve/bitstream/10872/15019/1/TEG_18020023_Final.pdf

Ferrer, J. (2014) ***Definición de Factores.*** https://enciclopedia.net/factores/

Grupo ATICO34. (s.f.) ***protocolos seguridad informática.*** https://protecciondatos-lopd.com/empresas/protocolos-seguridad-informatica/

Hornetsecurity (s.f.) ***Seguridad informática.*** https://www.hornetsecurity.com/es/knowledge-base/seguridad-informatica/

Hurtado De Barrera, J. (2010). ***Metodología de la Investigación. Guía para la Comprensión Holística de la Ciencia.*** https://t.me/c/1614591896/280

Instituto Internacional de estudios en Seguridad Global INISEG (2020) ***Factor humano y ciberseguridad, un riesgo en crecimiento.*** https://www.iniseg.es/blog/ciberseguridad/factor-humano-y-ciberseguridad.

Instituto Internacional de estudios en Seguridad Global INISEG (2020) ***Factor humano y ciberseguridad, un riesgo en crecimiento.*** https://www.iniseg.es/blog/ciberseguridad/factor-humano-y-ciberseguridad.

Kaspersky, E. (2020) ***¿Qué es una brecha de seguridad?*** https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach

Ley Especial Contra Delitos Informáticos (LECDI) (2001) Gaceta Oficial de la República Bolivariana de Venezuela N.º 37.313. Octubre 30, 2001. http://www.conatel.gob.ve/wp-content/uploads/2014/10/PDF-Ley-Especial-contra-los-Delitos-Inform%C3%A1ticos.pdf

Palella, S. y Martins, F. (2012) ***Metodología de la Investigación Cuantitativa***. https://t.me/c/1708242346/7

Ramos, D. (2019) ***Seguridad Informática.*** https://www.researchgate.net/publication/351658001_Seguridad_Informatica

Real Academia Española (RAE) (2014) ***Requisito.*** https://dle.rae.es/requisito

Samaniego, E. y Ponce, J. (2021) ***Fundamentos de seguridad informática.*** Editorial Grupo Compás. https://www.researchgate.net/publication/354054517_Libro_Fundamentos_de_seguridad_informatica

Tamayo y Tamayo, M. (2011). ***El Proceso de la Investigación Científica.*** https://t.me/c/1614591896/282

Universidad Alejandro De Humboldt. (2016). **Manual Para La Elaboración Y Presentación Del Trabajo De Grado (Tg-Uah).** https://t.me/c/1614591896/276

Universidad Pedagógica Experimental Libertador. (2016). ***Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales***. https://t.me/c/1614591896/277

VANGUARDIA (2018) ***¿Qué es un antivirus y para qué sirve?*** https://vanguardia.com.mx/tech/que-es-un-antivirus-y-para-que-sirve-DPVG3433213

Westreicher, G. (2020) ***Proceso***. https://economipedia.com/definiciones/proceso.html

[ANEXO “A”]

Modelo del Instrumento: El Cuestionario

El presente cuestionario tiene como objetivo principal realizar una encuesta de 11 preguntas las cuales van a ser respondidas por los cincuenta (50) empleados del departamento de ciberseguridad de manera anónima referente a diversos factores que tienen que ver con la seguridad de la información, esto con el fin de alimentar el trabajo de investigación para el análisis de la situación planteada en la empresa

N°	Pregunta o items	Si	No
1	¿Considera el factor humano como una clave indispensable para la ciberseguridad de la empresa?		
2	¿Se deben realizar medidas para reforzar o desarrollar la seguridad Activa y Pasiva?		
3	¿Considera que la seguridad física y lógica que se aplica actualmente está quedando atrás con respecto a nuevas tecnologías?		
4	¿Se utiliza comúnmente en los sistemas un software antivirus?		
5	¿Debería desarrollarse un Firewall perimetral de red más eficiente y actualizado?		
6	¿Es necesario destinar recursos a desarrollar un servidor proxy que sea único de la empresa haciendo que sea más difícil entrar al sistema?		
7	¿El Sistema de End Point Disk Encryption brinda una cobertura total hacia la compañía como a los usuarios?		
8	¿Se utiliza regularmente el escáner de vulnerabilidades para detectar aperturas o fallos en el sistema?		
9	¿Se realizan prácticas para poner a prueba los protocolos de seguridad preestablecidos?		
10	En caso de una pérdida total de los datos por parte de un ataque ¿se cuenta con un plan de respaldo junto a un plan de contingencia?		
11	¿la empresa posee una escala para priorizar los riesgos y así responder adecuadamente con respecto a ellos?		