



UNIVERSIDAD TÉCNICA DE BABAHOYO

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E
INFORMÁTICA**

PROCESO DE TITULACIÓN

ABRIL 2022 - SEPTIEMBRE 2022

PROYECTO DE INVESTIGACIÓN

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

TEMA:

**“Vulnerabilidades de la seguridad de la información y su incidencia en el
departamento de sistemas del Municipio de Babahoyo”.**

EGRESADO:

HEYNER JOEL HUACÓN LÓPEZ

TUTOR:

ING. WELLINGTON MALIZA CRUZ

AÑO 2022

DEDICATORIA

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de los anhelos más deseados. A mis padres, por su amor, trabajo y esfuerzo de ellos pude culminar mi carrera universitaria, para tener un mejor futuro y seguir adelante como un profesional, A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que me abrieron las puertas y compartieron sus conocimientos.

AGRADECIMIENTO

Agradecemos a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad. Gracias a mis padres, por ser los principales iniciadores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que me inculcaron. Asimismo, quisiera agradecer a la Universidad Técnica de Babahoyo, en especial a mis docentes que me hicieron crecer como profesional día a día al impartirme sus valiosos conocimientos, agradezco a cada uno de ustedes por su paciencia, dedicación, apoyo y amistad.

ÍNDICE GENERAL

CARATULA	1
DEDICATORIA	2
AGRADECIMIENTO	3
ÍNDICE GENERAL	4
ÍNDICE DE TABLAS	6
ÍNDICE DE GRÁFICOS	7
ÍNDICE DE FIGURAS	8
RESUMEN	9
ABSTRACT.....	10
INTRODUCCIÓN	11
CAPITULO I. – DEL PROBLEMA.....	13
1.1 IDEA O TEMA DE INVESTIGACIÓN.....	13
1.2. MARCO CONTEXTUAL.....	13
1.2.1. Contexto Internacional.....	13
1.2.2. Contexto Nacional.....	14
1.2.3. Contexto Local.....	15
1.2.4. Contexto Institucional.....	16
1.3. SITUACIÓN PROBLEMÁTICA.....	16
1.4. PLANTEAMIENTO DEL PROBLEMA.....	17
1.4.1. Problema General.....	17
1.4.2. Subproblemas o derivados.....	17
1.5. DELIMITACIÓN DE LA INVESTIGACIÓN.....	18
1.6. JUSTIFICACIÓN.....	18
1.7. OBJETIVOS DE INVESTIGACIÓN.....	19
1.7.1. Objetivo general.....	19
1.7.2. Objetivos específicos.....	19
CAPITULO II.- MARCO TEÓRICO O REFERENCIAL.....	21
2.1. MARCO TEÓRICO.....	21
2.1.1. Marco Conceptual.....	22
2.1.2. Marco referencial sobre la problemática de investigación.....	47
2.1.2.1. Antecedentes investigativos.....	47
2.2. Hipótesis.....	50
2.2.1 Hipótesis general.....	50

3.1.1. Subhipótesis o derivadas.....	50
3.1.1. Variables.....	51
CAPITULO III. – RESULTADOS DE LA INVESTIGACIÓN.....	52
3.1. RESULTADOS OBTENIDOS DE LA INVESTIGACION.....	52
3.1.1. Prueba estadísticas aplicadas.....	52
3.1.2. Análisis e interpretación de datos.....	60
3.2. CONCLUSIONES ESPECÍFICAS Y GENERALES.....	70
3.2.1. Específicas.....	70
3.2.2. General.....	70
3.3. RECOMENDACIONES ESPECÍFICAS Y GENERALES.....	71
3.3.1. Específicas.....	71
3.3.2. General.....	71
CAPÍTULO IV.- PROPUESTA TEORICA DE APLICACIÓN.....	72
4.1. PROPUESTA DE APLICACIÓN DE RESULTADOS.....	72
4.1.1. Alternativa obtenida.....	72
4.1.2. Alcance de la alternativa.....	72
4.1.3. ASPECTOS BÁSICOS DE LA ALTERNATIVA.....	73
4.1.3.1. Antecedentes.....	73
4.1.3.2. Justificación.....	74
4.2. OBJETIVOS.....	75
4.2.1. General.....	75
4.2.2. Específicos.....	75
4.3. ESTRUCTURA GENERAL DE LA PROPUESTA.....	75
4.3.1. Título.....	75
4.3.2. Componentes.....	76
4.4. RESULTADOS ESPERADOS DE LA ALTERNATIVA.....	79
BIBLIOGRAFÍA.....	80
ANEXOS.....	84

ÍNDICE DE TABLAS

Tabla 1: Detalle – Hipótesis General. Fuente: (Heyner Huacón, 2022).....	52
Tabla 2: Detalle – Subhipótesis 1. Fuente: (Heyner Huacón, 2022).....	54
Tabla 3: Detalle – Subhipótesis 2. Fuente: (Heyner Huacón, 2022).....	56
Tabla 4: Detalle – Subhipótesis 3. Fuente: (Heyner Huacón, 2022).....	58
Tabla 5: Detalle-Pregunta 1. Fuente: (Heyner Huacón, 2022).....	60
Tabla 6: Detalle-Pregunta 2. Fuente: (Heyner Huacón, 2022).....	61
Tabla 7: Detalle-Pregunta 3. Fuente: (Heyner Huacón, 2022).....	62
Tabla 8: Detalle-Pregunta 4. Fuente: (Heyner Huacón, 2022).....	63
Tabla 9: Detalle-Pregunta 5. Fuente: (Heyner Huacón, 2022).....	64
Tabla 10: Detalle-Pregunta 6. Fuente: (Heyner Huacón, 2022).....	65
Tabla 11: Detalle-Pregunta 7. Fuente: (Heyner Huacón, 2022).....	66
Tabla 12: Detalle-Pregunta 8. Fuente: (Heyner Huacón, 2022).....	67
Tabla 13: Detalle-Pregunta 9. Fuente: (Heyner Huacón, 2022).....	68
Tabla 14: Detalle-Pregunta 10. Fuente: (Heyner Huacón, 2022).....	69

ÍNDICE DE GRÁFICOS

Gráfico 1: Ha utilizado la plataforma implementada en la actualidad en el Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).	60
Gráfico 2: Ha tenido algún inconveniente al momento de utilizar la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).	61
Gráfico 3: ¿Qué características le cambiaría o le agregaría para que funcione a la perfección la plataforma del Municipio de Babahoyo? Fuente: (Heyner Huacón, 2022).	62
Gráfico 4: A tenido algún problema con su información que se encuentra en la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).	63
Gráfico 5: Se siente conforme con las funcionalidades que ofrece la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).	64
Gráfico 6: Usted como usuario, cree que la plataforma del Municipio de Babahoyo, necesita mejoras. Fuente: (Heyner Huacón, 2022).	65
Gráfico 7: Al momento de utilizar la plataforma del Municipio de Babahoyo, se le ha colapsado. Fuente: (Heyner Huacón, 2022).	66
Gráfico 8: ¿Está de acuerdo con el tiempo de espera al momento de utilizar la plataforma del Municipio de Babahoyo? Fuente: (Heyner Huacón, 2022).	67
Gráfico 9: Funcionan todas las opciones que están implementada en la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).	68
Gráfico 10: ¿Cómo calificaría la plataforma del Municipio de Babahoyo? Fuente: (Heyner Huacón, 2022).	69

ÍNDICE DE FIGURAS

Figura 1: Elaborado por: INCIBE	27
Figura 2: Elaborado por INCIBE.	29
Figura 3: Elaborado por: CEUPE	41
Figura 4: Scanner de vulnerabilidades de aplicaciones Web (Wireshark). Fuente: (Heyner Huacón, 2022).....	78

RESUMEN

Con el desarrollo del presente proyecto de investigación titulado: “Vulnerabilidades de la seguridad de la información y su incidencia en el departamento de sistemas del Municipio de Babahoyo”, con el fin de analizar la problemática presentada de las vulnerabilidades e incidencias en el departamento de sistemas del Municipio de Babahoyo, con el objetivo de brindar un servicio eficiente y actualizado así poder alcanzar las metas que se tienen propuestas para los diferentes tipos de usuarios que harán usos de los servicios ya que es un gran número a diario.

Este proyecto de investigación nos aportara conocimientos significativos aplicando una investigación descriptiva, ya que así visualizamos cual es la realidad de los problemas que nos encontramos al momento de ir obteniendo las diferentes opiniones de los usuarios, de las preguntas mencionadas, obteniendo los resultados para analizarlos y evidenciar los problemas e inconsistencia y así implementado un scanner de vulnerabilidades para mejorar la calidad de servicios.

Palabras Claves: Seguridad de la información, vulnerabilidades, amenazas, riesgos, scanner, ISO 27001.

ABSTRACT

With the development of this research project entitled: "Vulnerabilities of information security and its incidence in the systems department of the Municipality of Babahoyo", in order to analyze the problems presented by the vulnerabilities and incidents in the systems department of the Municipality of Babahoyo, with the aim of providing an efficient and up-to-date service in order to achieve the goals that are proposed for the different types of users who will use the services, since there is a large number on a daily basis.

This research project will provide us with significant knowledge by applying a descriptive investigation, since in this way we visualize what is the reality of the problems that we encounter when obtaining the different opinions of the users, of the aforementioned questions, obtaining the results to analyze them and highlight problems and inconsistencies and thus implement a vulnerability scanner to improve the quality of services.

Keywords: Information security, vulnerabilities, threats, risks, scanner, ISO 27001.

INTRODUCCIÓN

En este presente proyecto de investigación se van a revisar las causas o aspectos que tiene la plataforma del Municipio de Babahoyo, la detección de vulnerabilidades en la información al momento de solicitar corroborar que no cuente con ninguna información alterada, a la presente línea de investigación Sistemas de Información y Comunicación, para valorar el desempeño de la institución.

Este trabajo se realizará en esta institución, con el propósito de mejorar la plataforma digital implementada y su efecto que tiene como desempeño diario para obtener datos sobre la importancia de tener o no tener vulnerabilidades al momento de solicitar o dejar la información personal y la solicitada en todos los procesos que lleva a cabo la plataforma del Municipio de Babahoyo, ya que así garantizaremos a todos los usuarios puedan hacer usos de todos sus servicios que ofrece.

El objetivo principal de esta investigación es realizar un análisis a la plataforma de información y su incidencia, es obtener una información detallada del funcionamiento tecnología del software, dando respuestas en aquellas situaciones en donde el usuario se haya visto afectado por alguna vulnerabilidad desconocida para él. Por ese motivo es vital importante realizar un análisis y detectar si hay alguna anomalía para dar a conocer las formas de que pueden vulnerar la seguridad de dicha plataforma con algún virus malicioso en el departamento de sistemas del Municipio de Babahoyo.

En todos los capítulos a tratar del presente proyecto de investigación se van a establecer parámetros y procedimientos de indagación, para así lograr establecer cuáles son las causas y efectos del problema. A través del método deductivo se podrá recopilar los datos por medio de encuestas con la finalidad de obtener todas las informaciones necesarias para esta investigación. Por tal razón se expone a continuación en este proyecto que permita detectar a tiempo las vulnerabilidades existentes, brindar posibles soluciones para tratar de asegurar los servicios y por ende conseguir beneficiar al Gobierno Autónomo Descentralizado Municipal del Cantón Babahoyo.

CAPITULO I. – DEL PROBLEMA.

1.1 IDEA O TEMA DE INVESTIGACIÓN.

Vulnerabilidades de la seguridad de la información y su incidencia en el departamento de sistemas del Municipio de Babahoyo.

1.2. MARCO CONTEXTUAL.

1.2.1. Contexto Internacional.

A nivel mundial existe un sinnúmero de empresa, organizaciones e instituciones, en la actualidad gracias al internet podemos comunicarnos con todos los habitantes del mundo, porque la comunicación es lo más importante que debe de haber y en especial un Municipio, con los diferentes equipos tecnológicos para garantizar los funcionamientos de los sistemas de información que poseen.

En muchos municipios se han implementados estos tipos de plataforma para así agilizar los procesos de información como Bogotá – Colombia.

El SisBIM es una herramienta básica para el apoyo a los procesos de toma de decisiones municipales relacionadas con la gestión del desarrollo territorial. Integra un conjunto clave de indicadores, un componente de geoinformación esencial y un mecanismo de interacción con los usuarios y comunidad en general denominado observatorio de desarrollo sostenible (Colnodo, 2016).

El Municipio de Colombia tienen una herramienta con el nombre de SisBIM es un proyecto que está coordinado por la Dirección de Desarrollo Territorial del Ministerio de Ambiente, Vivienda y Desarrollo Territorial y desarrollado por Colnodo, de mucha ayuda para la fácil aceptación de los usuarios en su uso habitual.

Se implementó en el Municipio de Perú un sistema que ayudara con los procesos para los diferentes usuarios. (Torres Cabanillas, 2017) afirma. “Contar con información oportuna y confiable es un factor crítico de éxito en la gestión de cualquier municipalidad”. En ese sentido, deben realizarse todos los esfuerzos en procura de tal cometido. El presente documento es el esfuerzo que, en ese sentido ha realizado un grupo de profesionales de la Gerencia de Gestión Institucional de la Municipalidad Provincial de Ica (MPI) y el Equipo a cargo del Informe sobre Desarrollo Humano del Programa de la Naciones Unidas para el Desarrollo (PNUD).

1.2.2. Contexto Nacional.

En el Ecuador para los Municipios tener una buena plataforma sin ninguna vulnerabilidad es muy indispensable en todo su ámbito ya que muchos usuarios van hacer uso de sus servicios y necesitan tener su información segura.

En el Municipio de Guayaquil cuentan con una plataforma web. (Guayaquil, 2019), con la finalidad de que el Gobierno Autónomo Descentralizado Municipal de Guayaquil, pone a disposición de la ciudadanía en general, una herramienta que permite a los usuarios el acceso a una serie de recursos y servicios basados en información

geográfica referenciada del Cantón Guayaquil. La misma está diseñada para explorar y descargar una variedad de datos que son de utilidad para un mayor conocimiento del territorio.

En la Casa Somos de San Marcos se presentó el Sistema de Trámites Internos del Municipio de Quito, Sitra, que permitirá introducir al funcionario municipal los principios de la gestión y administración de los documentos y archivos. Esto permitirá la adecuada organización, acceso, preservación y difusión del patrimonio documental de la ciudad (Lozano, 2019).

En la municipalidad de Quito se está implementando un nuevo sistema de gestión documental reducirá tiempos de respuesta, para ayudar a sus usuarios con sus respectivos tramites.

1.2.3. Contexto Local.

En la Provincia de Los Ríos, Cantón Babahoyo son varias municipalidades que de a poco se van modernizando con la tecnología, ya que se van implementando en las diferentes plataformas para ir garantizando su seguridad y no tengan vulnerabilidades en la información en los servicios que se ofrece a sus usuarios, para que no tengan ningún inconveniente al solicitar un servicio de sus datos ingresados.

1.2.4. Contexto Institucional.

En la actualidad el Municipio de Babahoyo cuenta con una plataforma ya implementada, Gobierno Autónomo Descentralizado Municipal del Cantón Babahoyo (GADM), que ofrece diversos servicios e información para sus usuarios, del equipo técnico interno del Municipio ha sido desprendida y constante; lo que ha permitido llevar a cabo los aspectos técnicos requeridos para su ciudadanía.

Mediante este proyecto de investigación se va a identificar el problema de las vulnerabilidades de la seguridad de la plataforma de información y sus incidencias, en el cual se identificará el problema y se dará una propuesta de solución para así garantizar su disponibilidad.

1.3. SITUACIÓN PROBLEMÁTICA.

En un mundo cambiante y altamente competitivo, no solo basta con planificar, organizar, ejecutar y controlar, las instituciones tienen la capacidad para recolectar la información y transformar con rapidez en un bien o servicio más que basarse en una dirección, se apunta hacia un proceso productivo, efectivo, eficiente y eficaz, con la finalidad de ir mejorando la calidad administrativa en el uso de la información.

Los sistemas informáticos o plataformas son muy importantes ya que gracias a ellos las instituciones públicas o privadas, manejan la información de manera cómoda y sencilla sin necesitar información en papel ya que por algún motivo se puede dañar o extraviar y no nos permitirá obtener de manera rápida los datos requeridos por el usuario.

Después de realizar el análisis, El Municipio de Babahoyo siendo una empresa pública está expuesta a varias vulnerabilidades que pueden perjudicar ciertas informaciones que tienen guardada. Por lo tanto, se dará una solución y verificación a esos problemas para que no sean tan vulnerables, es que con esta investigación se mejorara la plataforma de la institución ya antes mencionada.

1.4. PLANTEAMIENTO DEL PROBLEMA.

1.4.1. Problema General.

¿Cómo solucionar las vulnerabilidades de la plataforma de información y su incidencia en el departamento de sistemas del Municipio de Babahoyo?

1.4.2. Subproblemas o derivados.

- ¿Cuáles son los factores que afecta a la plataforma de información y su incidencia en el departamento de sistemas del municipio de Babahoyo?
- ¿Cómo valorar la infraestructura tecnológica que soporta el software para garantizar información del departamento de sistemas del Municipio de Babahoyo?
- ¿Cómo mejorar el rendimiento de la plataforma de información del departamento de sistemas del Municipio de Babahoyo?

1.5. DELIMITACIÓN DE LA INVESTIGACIÓN.

Delimitación de Contenido:

Campo: Ingeniería en Sistemas.

Área: Desempeño de Software.

Aspecto: Seguridad Informática.

Delimitación Espacial:

La presente investigación se realizará en el Municipio de Babahoyo.

Delimitación Temporal:

El proyecto de investigación tiene como duración 5 meses que corresponde del mes de abril 2022 – septiembre 2022

Delimitación Teórica:

La presente investigación se enfoca en encontrar los factores de las vulnerabilidades de la seguridad informática y su incidencia, que dispone el departamento de sistemas del Municipio de Babahoyo.

1.6. JUSTIFICACIÓN.

El propósito de esta investigación consiste en realizar un estudio de tal manera, que se dará a conocer las diferencias que cuenta la plataforma (GADM), mediante la integración de sistemas y recursos tecnológicos con los que cuenta el Municipio de Babahoyo.

De esta forma se ofrecerá a nuestros habitantes de nuestra ciudad las soluciones para los diferentes problemas que se presentan en la plataforma, se considera que el análisis y solución de la seguridad de la información será un excelente aporte para la mejora y el fortalecimiento institucional, la misma que ampara y acoge los lineamientos institucionales con mayor énfasis e integración.

También los requerimientos más aptos de acuerdo con las necesidades de las vulnerabilidades del sistema de información, así como el hardware necesario para que influya de una manera necesaria en los procesos a realizar y mantener la seguridad.

1.7. OBJETIVOS DE INVESTIGACIÓN.

1.7.1. Objetivo general.

Realizar un análisis a la plataforma de información y su incidencia en el departamento de sistemas del Municipio de Babahoyo.

1.7.2. Objetivos específicos.

- Determinar los factores que afecta a la plataforma de información y su incidencia en el departamento de sistemas del municipio de Babahoyo.
- Valorar la infraestructura tecnológica que soporta el software para garantizar información del departamento de sistemas del Municipio de Babahoyo.

- Evaluar el rendimiento de la plataforma de información del departamento de sistemas del Municipio de Babahoyo.

CAPITULO II.- MARCO TEÓRICO O REFERENCIAL.

2.1. MARCO TEÓRICO.

Las vulnerabilidades es una debilidad o fallos en los sistemas de información, ya que pone en mucho riesgo toda la seguridad de los datos pudiendo permitir ataques que puedan comprometer la integridad, disponibilidad o la confidencialidad de la información, por eso hay que encontrar y eliminarlas lo antes posible, para así evitar eros o carencia de la información de los usuarios.

Según (Silva Coelho, Segadas de Araújo, & Kowask Bezerra, 2014, pág. 107), Después de identificar los activos que deben ser protegidos en la organización, se deben considerar las probabilidades de cada activo de ser vulnerable a las amenazas. Para ello, hay que prestar atención a la información que pueda quedar comprometida, creando listas de prioridades, por ejemplo; En los servicios de seguridad que puedan verse comprometidos, tal como la confidencialidad, integridad y disponibilidad.

Se está de acuerdo con lo antes mencionado por los autores de las vulnerabilidades porque cada empresa sea pública o privada necesita contar con sistemas o plataformas de información que no carezcan de ningún problema, ya sea por amenazas en el software o por un fallo humano, para así mejorar los procesos que realizar a diario para sus usuarios y darle un excelente servicio.

2.1.1. Marco Conceptual.

¿Qué son las vulnerabilidades?

De acuerdo con (López, 2010, pág. 14), Probabilidades que existen de que una amenaza se materialice contra un activo. NO todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento (TEAM, Tipos de Vulnerabilidades y Amenazas informáticas, 2020).

Tipos de amenazas a la seguridad.

Existen diversos tipos de amenazas que afectan a la seguridad de un sistema de información y, en general, a los sistemas informáticos. Estos pueden deberse a motivos de índole diferente, ya sea de manera intencionada o no, por lo que, según esto, se agrupan en dos grandes grupos: las amenazas que Surgen por vulnerabilidades provocadas por errores accidentales y las que se explotan de forma intencionada (CABALLERO GONZÁLEZ & CLAVERO GARCÍA, 2017, pág. 83).

Accidentales: errores humanos, fallos software/hardware.

Las amenazas accidentales son aquellas producidas por acciones que, a pesar de no buscar la explotación de vulnerabilidades, ocasionan la exposición de la información e incluso producir la alteración y/o pérdida de la misma (CABALLERO GONZÁLEZ & CLAVERO GARCÍA, 2017, pág. 83).

Es muy importante ser conscientes de que, aun siendo amenazas accidentales, estas pueden afectar a la disponibilidad, la confidencialidad y la integridad de la información. Dentro de las amenazas accidentales podemos encontrar las producidas por:

- **Erros humanos:** Estos erros, aun sin ser intencionados, pueden provocar daños irreparables o exponer la información.
- **Ataques directos.** Son aquellos que se realizan con las acciones frontales de personas que pretenden acceder al sistema de forma no autorizada o provocar un mal funcionamiento mediante el uso de acciones directas contra el sistema de información. A continuación, se describen algunos de los ataques más frecuentes:
- **Mediante el uso de programas maliciosos.** Son programas o aplicaciones diseñados para explotar una vulnerabilidad del sistema de información.
- **Fuerza bruta.** Estos ataques tratan de averiguar las credenciales de acceso al sistema probando todas las combinaciones posibles hasta encontrarlas y obtener el acceso al sistema.

- **Denegación de servicios (Denial of Service, DOS).** Se trata de un ataque a una computadora o una red que provoca que un recurso o la propia red quede fuera de servicio. Una variante es el ataque distribuido de denegación de servicio (Distributed Denial of Service, DDOS), que consiste en generar la sobre carga desde varios puntos de conexión, convirtiéndolo en un ataque más efectivo.
- **Acceso a las instalaciones.** Es un ataque externo debido a que IO realiza personal ajeno a la empresa u Organización, pero IO hace desde dentro las instalaciones, para lo cual debe acceder a ellas.
- **Personal interno.** Son ataques realizados por personal interno de la empresa u organización con el fin de provocar un daño por descontento con la empresa, por robo de datos para lucrarse, espionaje, o cualquier otra motivación.
- **Ataques indirectos.** Son acciones en las que la persona que genera el ataque involucra a personal de la empresa u organización, mediante el engaño, para Obtener el acceso al sistema. Un claro ejemplo de este tipo de ataques es;
- **Ingeniería social.** Es una práctica basada en la manipulación mediante el engaño de los usuarios, generalmente por teléfono, simulando ser técnico de la organización, o un compañero y de esta forma obtener información

o las credenciales para un acceso al sistema. Se basa en el principio de que en cualquier sistema el eslabón más débil es el usuario.

- **Caballo de Troya.** Consiste en la presentación de una aplicación atractiva para el usuario, que no se presenta como dañina, pero que al ejecutarla está dando acceso remoto no autorizado al asaltante.

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. NO constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma (López, 2010, pág. 14).

Identificar una vulnerabilidad.

El primer paso para realizar es la identificación de vulnerabilidades conocidas. En este paso se utiliza la información de puertos TCP/UDP abiertos, los banners asociados a los servicios, las firmas del sistema operativo y toda la información pertinente de las etapas anteriores. Se realiza el análisis de vulnerabilidad mediante el uso de herramientas automáticas a las cuáles se les suministra la información de encontrada en etapas previas, por ejemplo, la información de puertos TCP/UDP abiertos y así se evita que las herramientas realicen acciones innecesarias como las pruebas en puertos cerrados (Vega Briceño, 2020, pág. 71).

Análisis de las vulnerabilidades.

El análisis de vulnerabilidades o proceso de evaluación de vulnerabilidades consiste en; identificar, evaluar y categorizar vulnerabilidades de seguridad en sistemas en un momento dado. Cuando se ofrece el servicio de análisis de vulnerabilidades, generalmente se refiere a un servicio basado parcial o totalmente en herramientas automatizadas que hacen gran parte del trabajo pero que también se hace necesario la revisión de manual cuando surgen algunas dudas (Vega Briceño, 2020, pág. 40).

Definición de un sistema de vulnerabilidad.

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal Configurado que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta (Martha Irene Romero Castro, 2018, pág. 30).

Vulnerabilidades en sistemas informáticos

Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes

posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos (INCIBE, 2017).

Por su parte, una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas (INCIBE, 2017).



Figura 1: Elaborado por: INCIBE

Fuentes de amenazas.

Las más comunes en el ámbito de sistemas de información son:

- Malware o código malicioso: permite realizar diferentes acciones a un atacante.

Desde ataques genéricos mediante la utilización de troyanos, a ataques de

precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivo, configuración o componente específico de la red.

- Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.
- APT o Amenazas Persistentes Avanzadas (Advanced Persistent Threats): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.
- Botnets: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.
- Redes sociales: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.
- Servicios en la nube: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

Fases del análisis de riesgo.

Podemos identificar los activos críticos de los sistemas de información que pueden suponer un riesgo para la empresa, realizando un análisis de riesgos. Análisis que nos

llevará a obtener una imagen rigurosa de los riesgos a los que se encuentra expuesta nuestra empresa. Estas fases son las siguientes (INCIBE, 2017).



Figura 2: Elaborado por INCIBE.

Tipos de vulnerabilidades

Conjuntamente con el nacimiento de la computación, también nacieron los programas o software que le permitían a aquellas primitivas maquinarias operar. Si bien estas máquinas procesaban la información de una manera precisa, lo cierto es que los programas que las controlaban eran de desarrollo y diseño humano, y por lo tanto su código muy factible de contener toda clase de errores (Castillo, 2020).

Vulnerabilidades de desbordamiento de buffer.

Esta condición se cumple cuando una aplicación no es capaz de controlar la cantidad de datos que se copian en buffer, de forma que si esa cantidad es superior a la capacidad del buffer los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original. Este problema se puede aprovechar para ejecutar código que le otorga a un atacante privilegios de administrador (Castillo, 2020).

Vulnerabilidades de condición de carrera (race condition).

La condición de carrera se cumple generalmente cuando varios procesos tienen acceso a un recurso compartido de forma simultánea. En este sentido, un buen ejemplo son las variables, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma (Castillo, 2020).

Vulnerabilidades de error de formato de cadena (format string bugs).

El motivo fundamental de los llamados errores de cadena de formato es la condición de aceptar sin validar la entrada de datos proporcionada por el usuario. Este es un error de diseño de la aplicación, es decir que proviene de descuidos en su programación. En este sentido el lenguaje de programación más afectado por este tipo de vulnerabilidades es C/C++. Un ataque perpetrado utilizando este método definitivamente conduce a la ejecución de código arbitrario y al robo de información y datos del usuario (Castillo, 2020).

Vulnerabilidades de Cross Site Scripting (XSS).

Las vulnerabilidades del tipo Cross Site Scripting (XSS) son utilizadas en ataques en donde las condiciones permitan ejecutar scripts de lenguajes como VBScript o JavaScript. Es posible encontrar este tipo de situaciones en cualquier aplicación que se utilice para mostrar información en un navegador web cualquiera, que no se encuentre debidamente protegido contra estos ataques (Castillo, 2020).

Vulnerabilidades de Inyección SQL.

Las llamadas “vulnerabilidades de inyección SQL” se producen cuando mediante alguna técnica se inserta o adjunta código SQL que no formaba parte de un código SQL programado. Esta técnica se utiliza con el propósito de alterar el buen funcionamiento de la base de datos de una aplicación, “inyectando” código foráneo que permita el proceso de datos que el atacante desee (Castillo, 2020).

Vulnerabilidades de denegación del servicio.

La técnica de denegación de servicio se utiliza con el propósito de que los usuarios no puedan utilizar un servicio, aplicación o recurso. Básicamente lo que produce un ataque de denegación de servicio es la pérdida de la conectividad de la red de la víctima del ataque por el excesivo consumo del ancho de banda de la red o de los recursos conectados al sistema informático (Castillo, 2020).

Vulnerabilidades de ventanas engañosas.

Sin duda esta es una de las vulnerabilidades más conocidas y comunes entre los usuarios, sobre todo para aquellos que ya llevan algunos años tras un monitor. Esta técnica, también conocida como “Windows Spoofing” permite que un atacante muestre ventanas y mensajes de notificación en la computadora de la víctima, que generalmente consisten en hacernos saber que somos ganadores de un premio o situaciones similares (Castillo, 2020).

Factores que inciden en el análisis.

los factores que determinan la elección de un determinado tipo de información. Por lo que resulta necesario identificar la influencia de algunos factores como el perfil de los directivos y las características de las empresas en la obtención de información (Coba Molina, 2016).

¿Qué es la seguridad informática?

La seguridad en las organizaciones tiene sus orígenes a principios de siglo XX, tenía como objetivo proteger las instalaciones físicas frente a los conflictos sociales y laborales de la época. La misma estaba orientada a salvaguardar las propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías y, de forma amplia, todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio (Sain, 2018).

Sistemas informáticos.

Según (Pagliari & Eterovic, 2012, pág. 152), Los sistemas informáticos de una organización están constantemente sometidos a amenazas, que involucran desde fallos técnicos hasta acciones no deseadas. Una metodología de análisis de riesgos informáticos permite determinar que probabilidad existe de que éstas amenazas ocurran y del impacto que producirían si sucedieran, además de la vulnerabilidad que los sistemas informáticos pueden presentar. El análisis de riesgos informáticos comprende la identificación y evaluación de las amenazas y vulnerabilidades que afectan a la información.

Amenazas informáticas.

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas) (TEAM, Tipos de Vulnerabilidades y Amenazas informáticas, 2020).

Tipos de Vulnerabilidades y Amenazas informáticas en la empresa.

Son muchas las vulnerabilidades y amenazas informáticas a las que están expuestas las empresas en la actualidad. Por eso la inversión en ciberseguridad y sistema de protección ha experimentado un gran aumento en los últimos años, siendo los profesionales en ciberseguridad uno de los perfiles más buscados en el sector de la informática (TEAM, Tipos de Vulnerabilidades y Amenazas informáticas, 2020).

- ❖ **Virus.** Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).
- ❖ **Gusanos.** Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.

- ❖ **Troyanos.** Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.

- ❖ **Ransomware.** El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).

- ❖ **Keyloggers.** Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Vulnerabilidades informáticas.

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas. Podemos diferenciar tres tipos de vulnerabilidades según cómo afectan a nuestro sistema:

Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados. Son vulnerabilidades de las que ya tienen conocimiento las empresas que desarrollan el programa al que afecta y para las cuales ya existe una solución, que se publica en forma de parche. Existen listas de correo relacionadas con las noticias oficiales de seguridad que

informan de la detección de esas vulnerabilidades y las publicaciones de los parches a las que podemos suscribirnos (Quiroz Zambrano & Macías Valencia, 2017).

Vulnerabilidades conocidas sobre aplicaciones no instaladas. Estas vulnerabilidades también son conocidas por las empresas desarrolladores de la aplicación, pero puesto que nosotros no tenemos dicha aplicación instalada no tendremos que actuar.

Vulnerabilidades aún no conocidas. Estas vulnerabilidades aún no han sido detectadas por la empresa que desarrolla el programa, por lo que, si otra persona ajena a dicha empresa detectara alguna, podría utilizarla contra todos los equipos que tienen instalado este programa. Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo (Quiroz Zambrano & Macías Valencia, 2017).

¿Qué es seguridad informática?

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en

la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas) (Pérez Porto & Merino, 2021).

Software de seguridad informática.

Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords).

Herramientas todas ellas de gran utilidad como también lo son los conocidos sistemas de detección de intrusos, también conocidos como anti-spyware. Se trata de programas o aplicaciones gracias a los cuales se puede detectar de manera inmediata lo que son esos programas espías que se encuentran en nuestro sistema informático y que lo que realizan es una recopilación de información del mismo para luego ofrecérsela a un dispositivo externo sin contar con nuestra autorización en ningún momento. Entre este tipo de espías destaca, por ejemplo, Gator (Pérez Porto & Merino, 2021).

Revisión Sistemática.

Una revisión sistemática es un método que permite a los especialistas obtener resultados relevantes y cuantificados. Esto puede llevar a la identificación, selección y presentación de pruebas en relación con la investigación en un tema en particular (Hernández Saucedo & Mejia Miranda, 2015, pág. 5).

¿Qué son las incidencias?

Una incidencia es toda interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos o consultas reportadas por los usuarios, el equipo del servicio o por alguna herramienta de monitorización de eventos (Servicetonic, 2018).

Actividades principales de la Gestión de Incidencias según ITIL v3.

✚ **Detección.** - Cuanto antes se detecte una incidencia, menor será su impacto en el negocio. Por lo tanto, es importante monitorizar los recursos con el objetivo de detectar incidencias potenciales y normalizar el servicio antes de que se produzca un impacto negativo en los procesos de negocio o, si esto no es posible, que el impacto sea mínimo.

✚ **Registro.** - Todas las incidencias del servicio deben ser registradas, y cada incidencia debe registrarse de forma independiente.

La información a registrar generalmente incluye:

- Identificador único.
- Categorización.
- Urgencia, impacto y prioridad.
- Fecha y hora.
- Persona/grupo que registra la incidencia.
- Canal de entrada.
- Datos del usuario.
- Síntomas.
- Estado.
- CIs (Configuration Items, elementos de configuración) asociados.

- Persona/grupo asignado para la resolución.
- Problema/Known error asociado.
- Actividades realizadas para la resolución.
- Fecha y hora de la resolución.
- Categoría del cierre.
- Fecha y hora de cierre.

✚ **Categorización.** - En esta actividad se establece el tipo exacto de la incidencia. Generalmente se establece una categorización multinivel con dependencias entre niveles. El número de niveles dependerá de la granularidad con la que necesitemos tipificar las incidencias.

✚ **Priorización.** - **Generalmente, la prioridad de la incidencia nos indica cómo se ha de gestionar. La prioridad de la incidencia suele depender de:**

- ❖ **La urgencia:** rapidez con que la incidencia necesita ser resuelta.
- ❖ **El impacto:** generalmente se determina por el número de usuarios afectados, aunque lo realmente importante es la criticidad para el negocio de los usuarios afectados por la incidencia. Al final, lo que realmente determina el impacto son los aspectos adversos que la incidencia tiene en el negocio.

✚ **Diagnóstico inicial.** - Cuando el personal de soporte de primer nivel recibe una incidencia, la diagnostica en base a los síntomas y, si está capacitado para ello, la resuelve.

✚ **Escalado.** – Existen dos tipos de escalado:

1. **Funcional:** el soporte de primer nivel se ve incapaz de resolver la incidencia y la asigna al grupo resolutor correspondiente.
2. **Jerárquico:** en caso de que se den ciertas circunstancias (incidencias graves o críticas, riesgo de incumplimiento del SLA) que se deban notificar a los responsables del servicio correspondiente.

✚ **Investigación y diagnóstico.** - Si la incidencia hace referencia a un fallo en el sistema, lo más probable es que se necesite investigar la causa del fallo. Las tareas más comunes dentro de esta actividad son las siguientes:

- ✓ Establecer exactamente qué es lo que no funciona correctamente y para qué secuencia de acciones del usuario (casuística).
- ✓ Establecer el impacto potencial de la incidencia.
- ✓ Determinar si la incidencia está producida por la implantación de un cambio.

- ✓ Buscar en la base de datos de conocimiento (base de datos de errores conocidos, registro de incidencias, etc.) posibles soluciones y/o workarounds.

✚ **Resolución.** - Cuando se detecta una solución potencial, ésta debería ser aplicada y testeada. Una vez comprobada la resolución, la incidencia se da por resuelta y se asigna al equipo de Service Desk para su cierre. Asimismo, se deben registrar todas las acciones realizadas para resolver la incidencia en el historial de la misma.

✚ **Cierre.** - Antes de cerrar la incidencia el equipo del Service Desk debería validar lo siguiente:

- Si el usuario está satisfecho con la resolución de la incidencia.
- Si el cierre ha sido categorizado.
- Si se han cumplimentado todos los datos necesarios.
- Si es un problema recurrente. En este caso, generar un problema.
- Eventualmente, se puede pasar una encuesta de satisfacción al usuario.

✚ **Por qué Gestión de Incidencias.** - Como hemos visto, toda empresa de servicios necesita la Gestión de Incidencias para prevenir o restaurar tan pronto como sea posible cualquier interrupción o reducción no planificada en la calidad de su servicio.

Sin embargo, debemos ser conscientes de los desafíos y riesgos de la Gestión de Incidencias con el fin de garantizar la mejor operación de servicio.

Flujo de la gestión de incidencias

El objetivo principal en la gestión de incidencias es detectar cualquier anomalía en el normal funcionamiento de los sistemas de información, aumentar la base de conocimientos (knowledge base) mediante la correcta entrada y clasificación de las incidencias y reportar la misma al área con las capacidades necesarias para solventar el problema detectado cumpliendo con los acuerdos de servicio (SLAs) aplicables a cada caso (CEUPE, 2017).

El ciclo de vida de la gestión de incidencias incluye cuatro pasos fundamentales:



Figura 3: Elaborado por: CEUPE

- **Registro:** el primer paso necesario para una correcta gestión de las incidencias es el registro de las mismas en el sistema. El origen de las incidencias es diverso, pudiendo ser tanto comunicadas directamente por el usuario final como por alertas automáticas implantadas en el propio servicio. Ha de comprobarse que la incidencia no esté previamente registrada en el sistema ya que no es infrecuente que diferentes usuarios alerten en un intervalo de tiempo corto de la misma incidencia. El incidente ha de quedar registrado bajo un número identificativo único que será facilitado al comunicador de la misma para su posterior seguimiento. La información básica a incluir en este punto es la referida al comunicador de la incidencia, la hora, los servicios afectados y una descripción del problema identificado. Además, se incluirá toda la información que pueda facilitar el cierre de la incidencia, tanto la aportada por el comunicador como la

información disponible en la base de datos de conocimiento. Finalmente, si el incidente puede estar afectando a otros usuarios se recomienda su notificación para que conozcan el estado del servicio y no se produzca un pico de llamadas al centro de gestión de incidencias.

- **Clasificación:** conlleva las etapas de categorización, priorización y asignación de recursos. La incidencia es asignada a una categoría en función del tipo de incidente, los servicios afectados y el equipo responsable de su resolución. La prioridad dependerá del impacto que tenga la indisponibilidad del servicio en el negocio. Si el primer nivel no es capaz de resolver la incidencia, la asignará a los recursos que puedan cerrar la misma. Finalmente, se asocia un estado al registro y se estima el tiempo de resolución teniendo en cuenta los SLAs acordados para el servicio y la prioridad asignada.

- **Diagnóstico:** en un primer momento, se consulta la base de conocimiento existente para encontrar referencias sobre incidencias similares que hayan sido resueltas en el pasado. Si el registro no es cerrado, se ha de seguir el protocolo de escalado establecido. Es necesario actualizar toda la información disponible sobre el incidente en cada uno de los estados por los que pase el mismo, de modo que los intervinientes en la resolución puedan contar con todo el detalle actualizado.

- **Resolución:** una vez resuelto el incidente, se ha de recoger la confirmación por parte del usuario del correcto funcionamiento del servicio. Se actualizará la base de conocimiento para facilitar el cierre de una incidencia similar en el futuro, se reclasificará el incidente si es necesario y se cerrará.

Beneficios de la gestión de incidencias

Algunas de las ventajas más importantes de aplicar una estrategia de gestión de incidencias son:

- Prevención de incidencias
- Reducción o eliminación del tiempo de inactividad
- Mejora del tiempo medio de resolución (MTTR)
- Mejora de la experiencia del cliente
- Mayor fidelidad de los datos
- Mejora de la productividad

¿Qué es el procedimiento de gestión de incidencias?

Un procedimiento de gestión de incidencias es un conjunto de acciones para anticipar, resolver y documentar eventos no planificados en una organización. Su objetivo es guiar a los profesionales a través de una situación inesperada y ayudarles a volver a la normalidad lo más rápido posible (Douglas da Silva, 2021).

¿Por qué es importante realizar el seguimiento de incidencias?

El procedimiento de gestión de incidencias es una herramienta fundamental en el arsenal de cualquier empresa. Aquí hay tres razones (¡basadas en datos!) por las que debería hacer el control de incidencias y el control de seguimiento en tu compañía (Douglas da Silva, 2021).

1) Porque te prepara para lo peor. - Según un estudio de Deloitte, el 76% de los líderes corporativos cree que sus empresas responderían de manera eficaz si una crisis les golpeara mañana. Sin embargo, solo el 49% del liderazgo empresarial afirma que sus organizaciones se dedican a monitorear y detectar problemas con antelación.

Crear un procedimiento de gestión de incidencias para tu compañía te prepara para lo peor. Es decir, te ayuda a identificar tus vulnerabilidades y a tomar medidas concretas para protegerte de escenarios amenazantes.

2) Porque te ayuda a identificar amenazas. - El procedimiento de gestión de incidencias te ayuda a identificar las áreas que te hacen sentir más amenazado, como escándalos en el servicio al cliente o en el manejo de quejas, por ejemplo.

De acuerdo con el mismo estudio de Deloitte, los líderes temen:

- Dañar la reputación corporativa (73%);
- Sufrir crímenes cibernéticos (70%);
- Ser blanco de rumores (68%);
- Tener problemas en la cadena de suministro (66%);
- Tener problemas con las medidas reglamentarias (66%);
- Enfrentar desastres naturales (66%).

3) Porque protege tu éxito. - Según los encuestados en el estudio de Deloitte, la reputación corporativa (70%), el desempeño financiero (69%) y la eficiencia operativa (64%) fueron los elementos que tardaron más de

un año en recuperarse de crisis pasadas. Sin un procedimiento de gestión de incidencias, eres vulnerable a estos y otros daños.

¿Qué elementos debe tener un procedimiento de gestión de incidencias?

Hay pasos clave en cualquier proceso de resolución de incidencias. Estos pasos garantizan que no se pase por alto ningún aspecto de una incidencia y ayudan a los equipos a responder a los incidentes con eficacia y a evitar que se repitan (Novoseltseva, 2018).

- ❖ Descripción del incidente (¿fue una violación de seguridad, confidencialidad o de los valores de la cultura organizacional?);
- ❖ ¿Dónde se descubrió el incidente?;
- ❖ ¿Quién descubrió el problema?;
- ❖ ¿Cuándo se lo descubrió?;
- ❖ ¿Qué hizo el descubridor? ¿Reportó a alguien u ocultó el problema?;
- ❖ ¿A quién fue reportado el incidente?;
- ❖ ¿Cuándo se redactó el informe?;
- ❖ ¿Cuál fue la gravedad o clasificación del incidente?;
- ❖ ¿Cuándo se enteró el responsable del sector?;
- ❖ ¿Qué hizo el responsable del sector cuando se enteró del incidente?;
- ❖ ¿Quién realizó el control de seguimiento?;
- ❖ ¿Cuándo se realizó el seguimiento?

¿Qué es la ingeniería social?

La definición de ingeniería social abarca varios tipos de manipulación psicológica. En ocasiones, la ingeniería social puede tener resultados positivos, como fomentar

comportamientos saludables. En términos de seguridad de la información, sin embargo, la ingeniería social a menudo se utiliza únicamente para beneficio del atacante. En estos casos, la ingeniería social implica manipulación para obtener información confidencial, como datos personales o financieros. Por tanto, la ingeniería social también puede definirse como un tipo de ciberdelito (Bodnar, 2020).

¿Cómo funciona la ingeniería social?

La ingeniería social se aprovecha de los sesgos cognitivos de las personas, que son como fallos en el hardware humano. Por desgracia para los seres humanos, hay muchos sesgos cognitivos que las personas malintencionadas pueden aprovechar para obtener datos personales y financieros de las víctimas delante de sus narices. Por ejemplo, la tendencia humana de confiar en personas percibidas como amables, atractivas o con alguna autoridad puede usarse en nuestra contra en ataques de ingeniería social (Bodnar, 2020).

¿Por qué es tan peligrosa la ingeniería social?

Hay algo especialmente peligroso sobre las prácticas de manipulación de ingeniería social. A menudo, las víctimas de ingeniería social no se dan cuenta de que están siendo manipuladas hasta que es demasiado tarde, y el delincuente ya ha tenido acceso a los datos confidenciales que buscaban (Bodnar, 2020).

ISO 27001

La ISO 27001 es una norma internacional de Seguridad de la Información que pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan. Este estándar ha sido desarrollado por la Organización Internacional de Normalización (ISO: “International Organization for Standardization”) y por la Comisión Electrotécnica Internacional (IEC: “International Electrotechnical Commission”) (REVISTA, 2019).

Información del departamento de sistema del Municipio de Babahoyo.

El Gobierno Municipal de Babahoyo, representado por el Sr. Alcalde, Johnny Salcedo, Sr. Vicealcalde, y por sus Concejales; teniendo como fin mejorar la calidad de vida de la población promoviendo el desarrollo del cantón, y allanándose a la Constitución y las Leyes vigentes, atinadamente impulsaron el diseño de un Plan de Desarrollo y Ordenamiento Territorial el cual será una herramienta técnica fundamental para la toma de decisiones y el esbozo de estrategias que busquen la consecución del Buen Vivir de la población a quienes representan (sni, 2015).

2.1.2. Marco referencial sobre la problemática de investigación.

2.1.2.1. Antecedentes investigativos.

Después de realizar un análisis de la información referente al tema a tratar y verificado por la Universidad Técnica de Babahoyo. Se presenta a continuación los siguientes antecedentes investigativos.

Según, (Huilca Chicaiza, 2012). La inexistente aplicación de hacking ético para detectar vulnerabilidades en los servicios de la intranet es uno de los principales problemas que tienen la mayoría de instituciones públicas y privadas como es el caso del Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos pues esto conlleva a que no se puedan descubrir las deficiencias relativas en la seguridad de los servicios de la intranet provocando vulnerabilidad en la información, en la mayoría de casos se realiza la instalación de la red con sus respectivos servicios pero nunca se emplean herramientas para detectar vulnerabilidad existente en los mismos.

En esta investigación se va está tratando sobre un tema de hacking ético para así poder detectar las vulnerabilidades que posee el Gobierno Autónomo Descentralizado Municipal del Cantón Cevallos, los servidores son los que contiene la información y se lo ataca para analizar si son vulnerables los servicios que estos prestan, si están seguros o no, si pueden acceder a la información y ocasionar daños irreversibles.

La autora, (Morocho Toaza, 2013). El problema presentado en el Área de Sistemas en el Gobierno Autónomo Descentralizado Municipalidad de Ambato se produce principalmente por la desactualización del programa Adobe Reader, puesto que es el formato de archivo portable más utilizado para enviar o recibir información es el formato PDF y se debe tomar en cuenta que este programa es constantemente actualizado y parchado adquiriendo nuevas características y seguridades como por ejemplo una de las últimos cambios que se hicieron son la caja de arena y el aislamiento lo cual impiden o minimizan los riesgos de contagio de los computadores con malware.

La mala configuración de los correos electrónicos provoca que existan vulnerabilidades de la información, al no tomar en cuenta los requerimientos de la empresa y de los empleados de la misma, permitiendo que las organizaciones, empresas o personas de fuera envíen correos masivos no deseados a las cuentas de correo de los usuarios lo cual incrementa las formas de contagio de código malicioso en los computadores de los funcionarios (Morocho Toaza, 2013).

Por lo consiguiente, en el análisis del sistema en el Gobierno Autónomo Descentralizado Municipalidad de Ambato, por la mala configuración de los correos electrónicos provocaron vulnerabilidades en la información por no tomar en cuenta exigencias de los datos a tratar y por el desconocimiento de los PDF maliciosos.

De acuerdo con, (QUIRUMBAY YAGUAL, 2015). La rápida evolución informática en estos tiempos requiere que todas las organizaciones privadas y estatales adopten un conjunto mínimo de controles de seguridad para proteger sus sistemas de información. En vista de esta situación el GAD Municipal del Cantón Ciudad del Este tiene la necesidad de implementar políticas y normas de seguridad basados en estándares que permita regular los servicios que ofrece a través de todo el equipo tecnológico utilizado en la Institución Municipal.

La falta de estos controles de seguridad informática causa que esta área se encuentre expuesta a un nivel de amenaza muy alto que a su vez pudiera provocar la pérdida de información crítica y originar la paralización de todos los servicios que ofrece la institución, adicionalmente es importante destacar que las Instituciones Públicas

dispongan además de un Plan de Recuperación ante Desastres que permita de una manera oportuna y optima mantener la continuidad operativa y que sea aplicable específicamente al Centro de Procesamiento de Datos Municipal.

2.2. Hipótesis.

2.2.1 Hipótesis general.

¿Realizar un análisis a la plataforma de información que permitirá solucionar las vulnerabilidades que tiene el departamento de sistemas del Municipio de Babahoyo?

3.1.1. Subhipótesis o derivadas.

- Al determinar los factores que afectan a la plataforma de información y su incidencia en el departamento de sistemas del Municipio de Babahoyo.
- Con la evaluación de la infraestructura tecnológica que soporta el software se establecerá la necesidad para mejorar la información del departamento de sistemas del Municipio de Babahoyo.
- Haciendo la medición del rendimiento de los procesos de la plataforma de información del departamento de sistemas del Municipio de Babahoyo.

3.1.1. Variables.

Variables Independientes.

Vulnerabilidades de la seguridad de la información y su incidencia.

Variables Dependientes.

Departamento de sistemas del Municipio de Babahoyo.

CAPITULO III. – RESULTADOS DE LA INVESTIGACIÓN.

3.1. RESULTADOS OBTENIDOS DE LA INVESTIGACION.

3.1.1. Prueba estadísticas aplicadas.

- Prueba del Chi Cuadrado

HIPÓTESIS

H₀: Realizar un análisis a la plataforma de información que permitirá no solucionar las vulnerabilidades que tiene el departamento de sistemas del Municipio de Babahoyo.

H₁: Realizar un análisis a la plataforma de información que permitirá solucionar las vulnerabilidades que tiene el departamento de sistemas del Municipio de Babahoyo.

Detalle	Pregunta 8	Pregunta 9	Total
Si	80	110	190
No	71	41	112
Total	151	151	302

Tabla 1: Detalle – Hipótesis General. Fuente: (Heyner Huacón, 2022).

$$X^2_{calc} = \sum \frac{(f_0 - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(80 - 95)^2}{95} + \frac{(71 - 56)^2}{56} + \frac{(110 - 95)^2}{95} + \frac{(41 - 56)^2}{56}$$

$$X^2_{calc} = 2.36 + 4.01 + 2.36 + 4.01$$

$$X^2_{calc} = 12.74$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1) (2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.05$$

Regla de decisión

$$X^2_{calc} > \text{Valor crítico}$$

$$12.74 > 3,841$$

Decisión

Podemos derivar que el análisis de nuestra prueba de Chi cuadrado, no da como resultado que no son independientes, es con lo que nos encontramos una hipótesis alterna por mediante esta observación que se realizó los valores hallados por la muestra realizada, se encontró que al realizar un análisis a la plataforma de información que permitirá solucionar las vulnerabilidades que tiene el departamento de sistemas del Municipio de Babahoyo.

SUBHIPÓTESIS #1

H₀: Al no determinar los factores que afectan a la plataforma de información y su incidencia en el departamento de sistemas del Municipio de Babahoyo.

H₁: Al determinar los factores que afectan a la plataforma de información y su incidencia en el departamento de sistemas del Municipio de Babahoyo.

Detalle	Pregunta 1	Pregunta 5	Total
Si	100	115	215
No	51	36	87
Total	151	151	302

Tabla 2: Detalle – Subhipótesis 1. Fuente: (Heyner Huacón, 2022).

$$X^2_{calc} = \sum \frac{(f_o - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(100 - 107.5)^2}{107.5} + \frac{(51 - 43.5)^2}{43.5} + \frac{(115 - 107.5)^2}{107.5} + \frac{(36 - 43.5)^2}{43.5}$$

$$X^2_{calc} = 0.52 + 1.29 + 0.52 + 1.29$$

$$X^2_{calc} = 3.62$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1) (2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.05$$

Regla de decisión

$$X^2_{calc} > Valor\ crítico$$

$$3.62 > 3,841$$

Decisión

Al conseguir por la prueba del Chi Cuadrado nos dio como resultado, que la hipótesis nula, como punto de los resultados obtenidos rechazaron la hipótesis nula, esto significa que al no determinar los factores que afectan a la plataforma de información y su incidencia en el departamento de sistemas del Municipio de Babahoyo.

SUBHIPÓTESIS #2

H₀: Con la no evaluación de la infraestructura tecnológica que soporta el software se establecerá la necesidad para mejorar la información del departamento de sistemas del Municipio de Babahoyo.

H₁: Con la evaluación de la infraestructura tecnológica que soporta el software se establecerá la necesidad para mejorar la información del departamento de sistemas del Municipio de Babahoyo.

Detalle	Pregunta 2	Pregunta 4	Total
Si	120	100	220
No	31	51	82
Total	151	151	302

Tabla 3: Detalle – Subhipótesis 2. Fuente: (Heyner Huacón, 2022).

$$X^2_{calc} = \sum \frac{(f_o - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(120-110)^2}{110} + \frac{(31-41)^2}{41} + \frac{(100-110)^2}{110} + \frac{(51-41)^2}{41}$$

$$X^2_{calc} = 0.90 + 2.43 + 0.90 + 2.43$$

$$X^2_{calc} = 6.66$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1) (2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.05$$

Regla de decisión

$$X^2_{calc} > \text{Valor crítico}$$

$$6.66 > 3,841$$

Decisión

La prueba del Chi Cuadrado obtuvimos el análisis de los resultados, no es independiente esto quiere decir, que hallamos a la hipótesis alterna que con la evaluación de la infraestructura tecnológica que soporta el software se establecerá la necesidad para mejorar la información del departamento de sistemas del Municipio de Babahoyo.

SUBHIPÓTESIS #3

H₀: Haciendo la medición del rendimiento de los procesos de la plataforma de información del departamento de sistemas del Municipio de Babahoyo.

H₁: Haciendo la medición del rendimiento de los procesos de la plataforma de información del departamento de sistemas del Municipio de Babahoyo.

Detalle	Pregunta 6	Pregunta 7	Total
Si	135	115	250
No	16	36	52
Total	151	151	302

Tabla 4: Detalle – Subhipótesis 3. Fuente: (Heyner Huacón, 2022).

$$X^2_{calc} = \sum \frac{(f_0 - f_e)^2}{f_e}$$

$$X^2_{calc} = \frac{(135 - 125)^2}{125} + \frac{(16 - 26)^2}{26} + \frac{(115 - 125)^2}{125} + \frac{(36 - 26)^2}{26}$$

$$X^2_{calc} = 0.8 + 3.84 + 0.8 + 3.84$$

$$X^2_{calc} = 9.28$$

Grados de Libertad

$$v = (\text{cantidad de filas} - 1) (\text{cantidad de columnas} - 1)$$

$$v = (2 - 1) (2 - 1)$$

$$v = 1(1) = 1$$

Nivel de significancia

$$1\% = 0.05$$

Regla de decisión

$$X^2_{calc} > \text{Valor crítico}$$

$$9.28 > 3,841$$

Decisión

Los resultados obtenidos por la prueba Chi Cuadrado, nos dice que la hipótesis alterna no es independiente, nos encontramos con los datos analizados, que haciendo la medición del rendimiento de los procesos de la plataforma de información del departamento de sistemas del Municipio de Babahoyo.

3.1.2. Análisis e interpretación de datos.

1.- ¿Ha utilizado la plataforma implementada en la actualidad en el Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Si	100	66%
No	51	34%
Total	151	100%

Tabla 5: Detalle-Pregunta 1. Fuente: (Heyner Huacón, 2022).

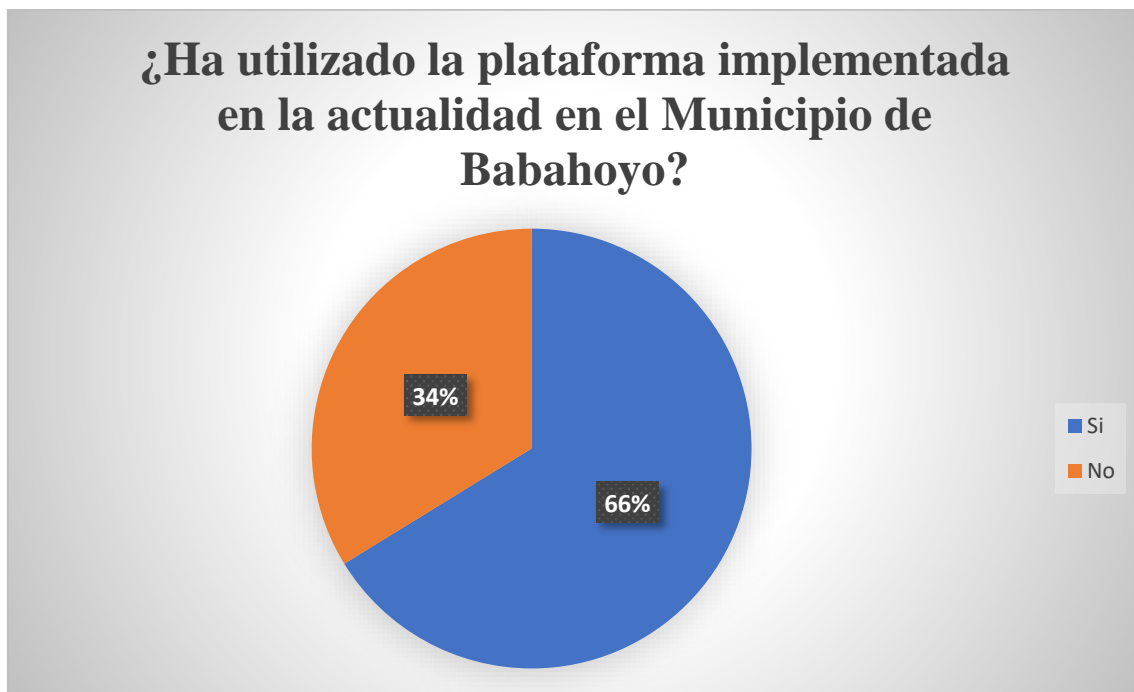


Gráfico 1: Ha utilizado la plataforma implementada en la actualidad en el Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

Los datos obtenidos por la muestra son de un 34% de las personas que no han utilizado la plataforma, mientras el 66% si lo han hecho.

2.- ¿Ha tenido algún inconveniente al momento de utilizar la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Si	100	66%
No	51	34%
Total	151	100%

Tabla 6: Detalle-Pregunta 2. Fuente: (Heyner Huacón, 2022).

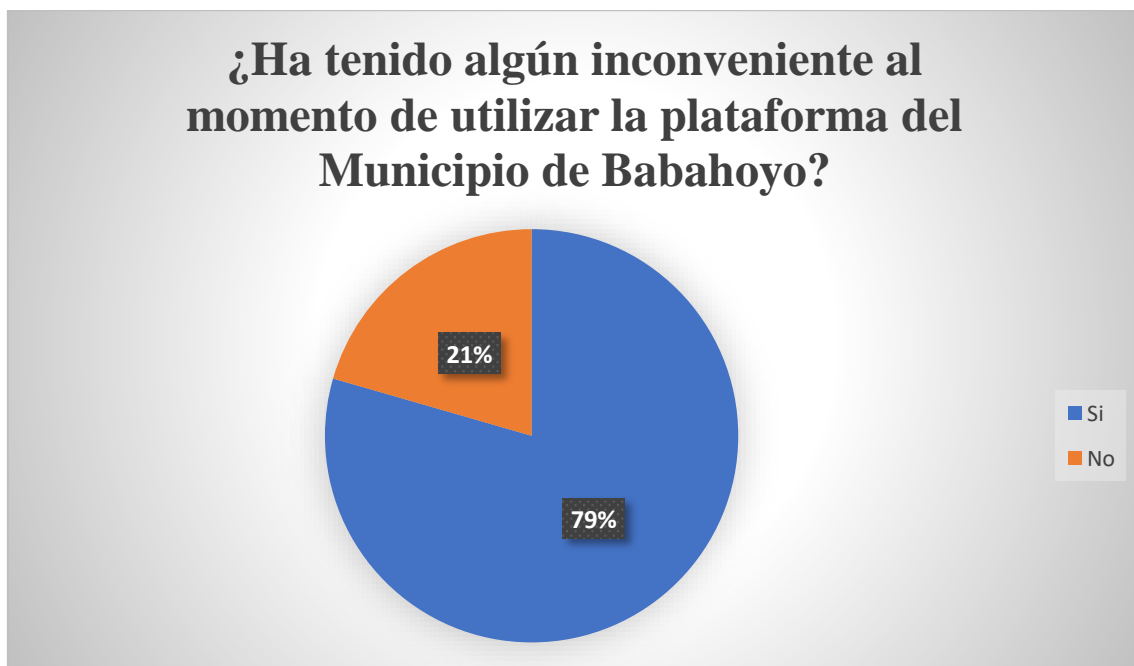


Gráfico 2: Ha tenido algún inconveniente al momento de utilizar la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

Los datos de esta muestra es el 79% de los usuarios encuestados si han tenido algún inconveniente al momento de utilizar y un 21% no han tenido ningún problema.

3.- ¿Qué características le cambiaría o le agregaría para que funcione a la perfección la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Mayor rapidez	45	30%
Uso fácil	95	63%
Nueva interface	11	7%
Total	151	100%

Tabla 7: Detalle-Pregunta 3. Fuente: (Heyner Huacón, 2022).

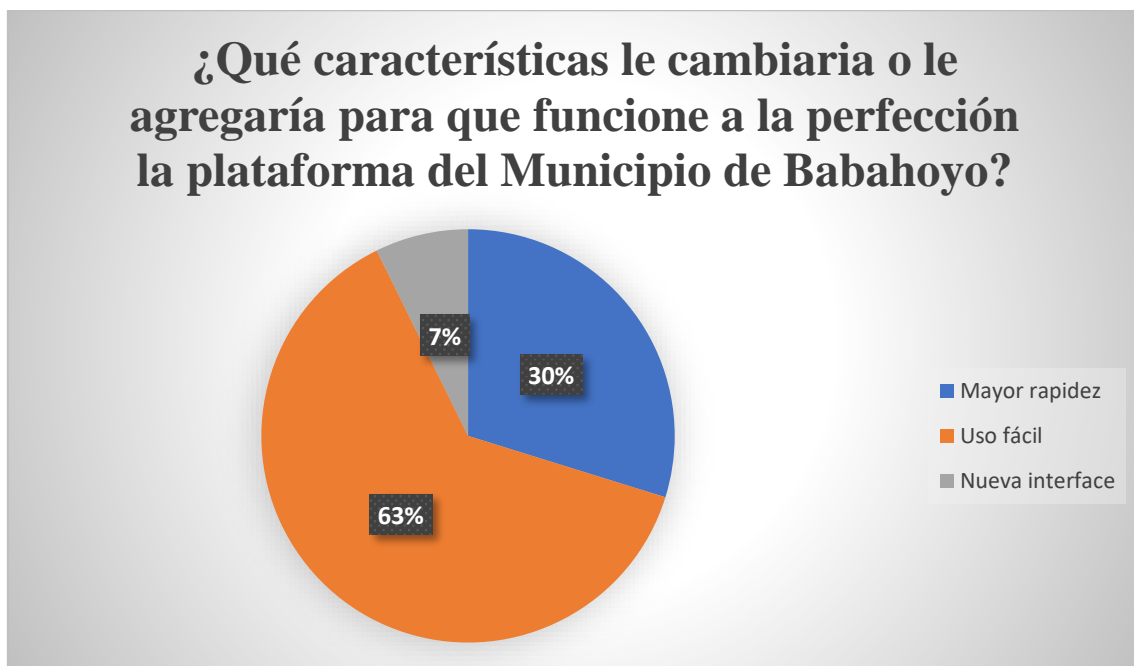


Gráfico 3: ¿Qué características le cambiaría o le agregaría para que funcione a la perfección la plataforma del Municipio de Babahoyo? Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

El 63% de los usuarios encuestados si le cambiarían o le agregarían alguna función, mientras el 30% ven un uso fácil y el 7% quieren una nueva interface.

4.- ¿Ha tenido algún problema con su información que se encuentra en la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Si	100	66%
No	51	34%
Total	151	100%

Tabla 8: Detalle-Pregunta 4. Fuente: (Heyner Huacón, 2022).

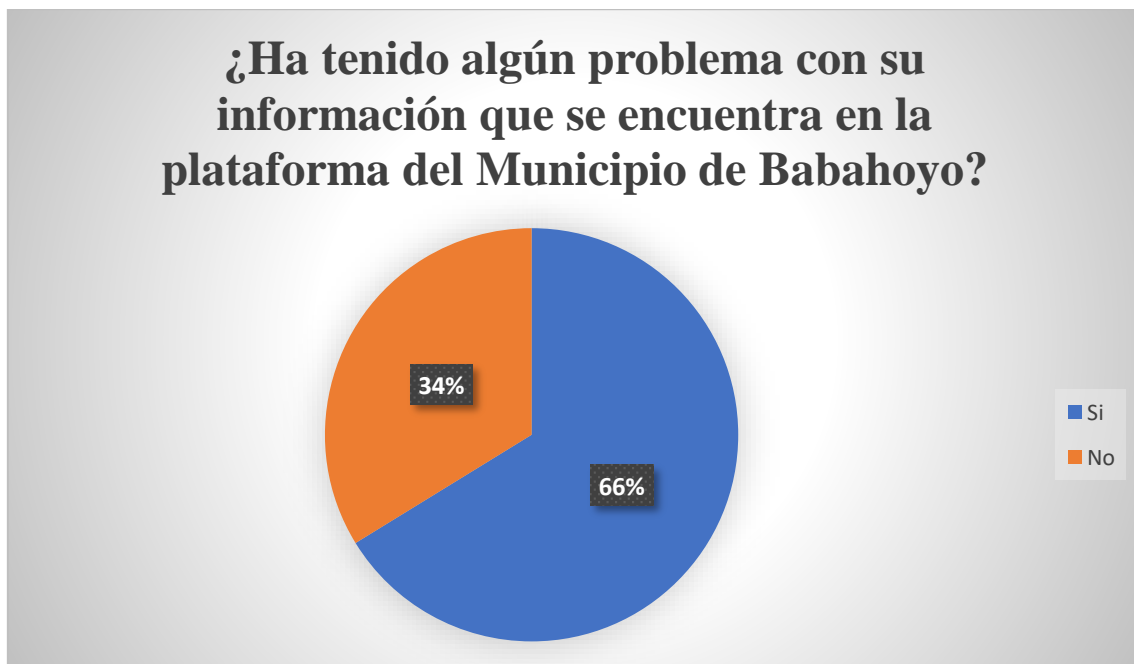


Gráfico 4: A tenido algún problema con su información que se encuentra en la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

En los resultados de la muestra el 66% de los usuarios admiten que si han tenido problema con su información que tienen subida y mientras el 34% no presentan ninguna alteración en sus datos.

5.- ¿Se siente conforme con las funcionalidades que ofrece la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Si	115	76%
No	36	24%
Total	151	100%

Tabla 9: Detalle-Pregunta 5. Fuente: (Heyner Huacón, 2022).



Gráfico 5: Se siente conforme con las funcionalidades que ofrece la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

Tal como podemos analizar en el cuadro 76% de los usuarios se sienten conforme y mientras el 24% no están conformes con las funcionalidades que les ofrecen.

6.- ¿Usted como usuario, cree que la plataforma del Municipio de Babahoyo, necesita mejoras?

Detalle	Frecuencia	Porcentaje
Si	135	89%
No	16	11%
Total	151	100%

Tabla 10: Detalle-Pregunta 6. Fuente: (Heyner Huacón, 2022).

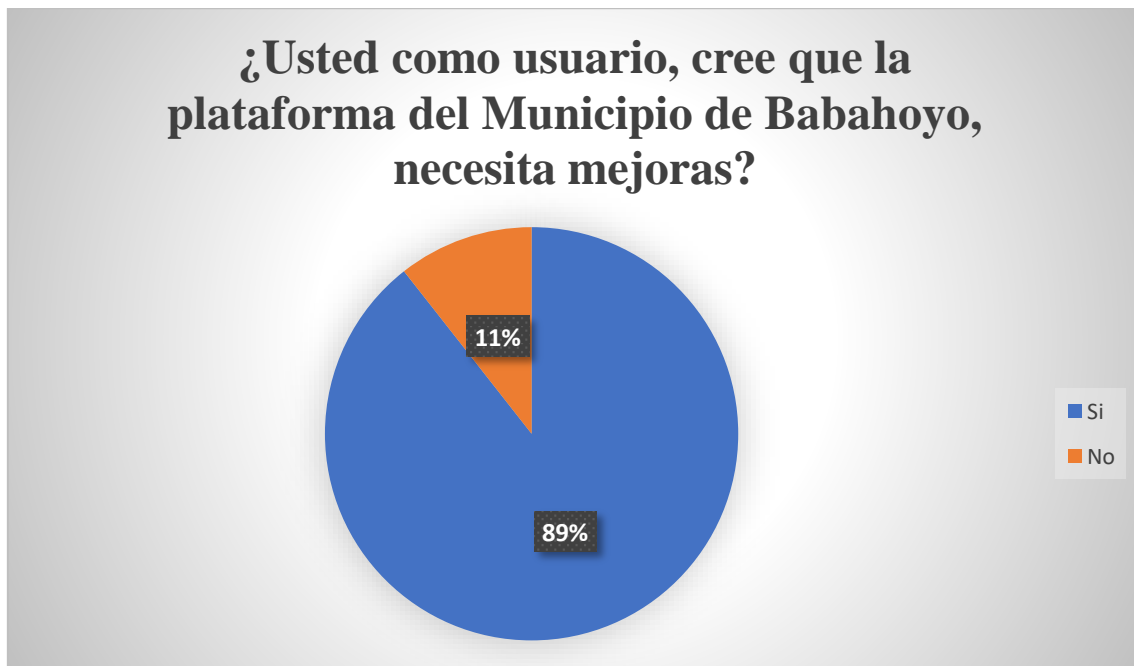


Gráfico 6: Usted como usuario, cree que la plataforma del Municipio de Babahoyo, necesita mejoras. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

La información obtenida nos refleja que el 89% los usuarios quieren una mejora en la plataforma, mientras que el 11% no piensan que necesita una mejora.

7.- ¿Al momento de utilizar la plataforma del Municipio de Babahoyo, se le ha colapsado?

Detalle	Frecuencia	Porcentaje
Si	115	76%
No	36	24%
Total	151	100%

Tabla 11: Detalle-Pregunta 7. Fuente: (Heyner Huacón, 2022).

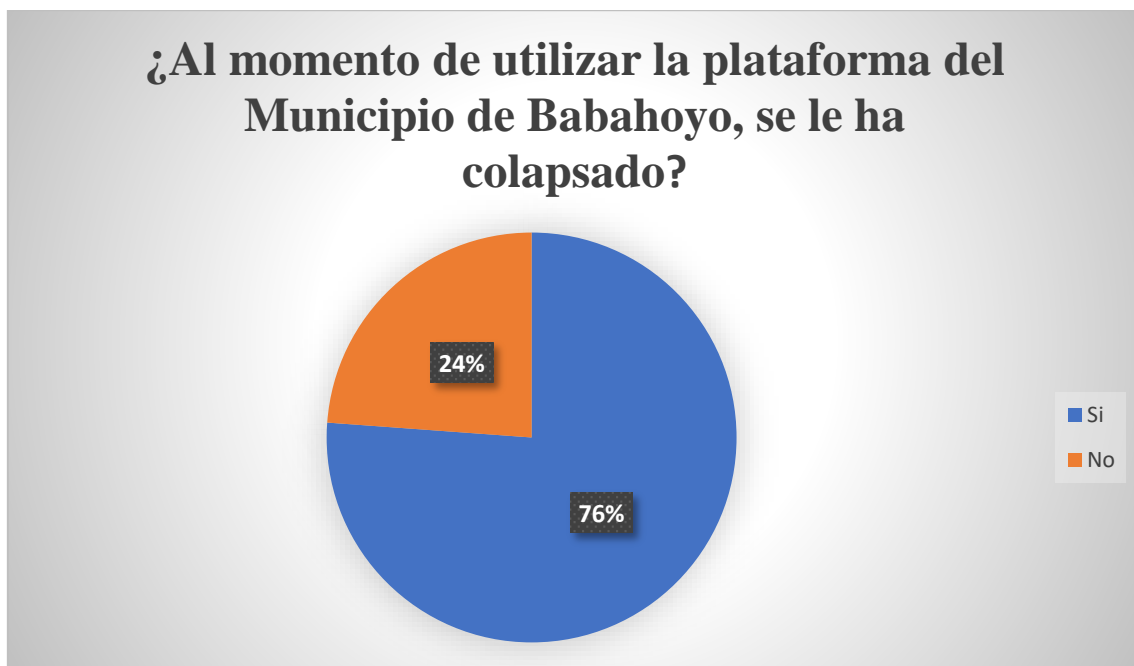


Gráfico 7: Al momento de utilizar la plataforma del Municipio de Babahoyo, se le ha colapsado. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

El 76% de los datos nos indica que los usuarios encuestados indican que han sufrido algún colapso al momento de utilizar la plataforma y el 24% no han tenido ningún problema.

8.- ¿Está de acuerdo con el tiempo de espera al momento de utilizar la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Si	80	76%
No	71	24%
Total	151	100%

Tabla 12: Detalle-Pregunta 8. Fuente: (Heyner Huacón, 2022).

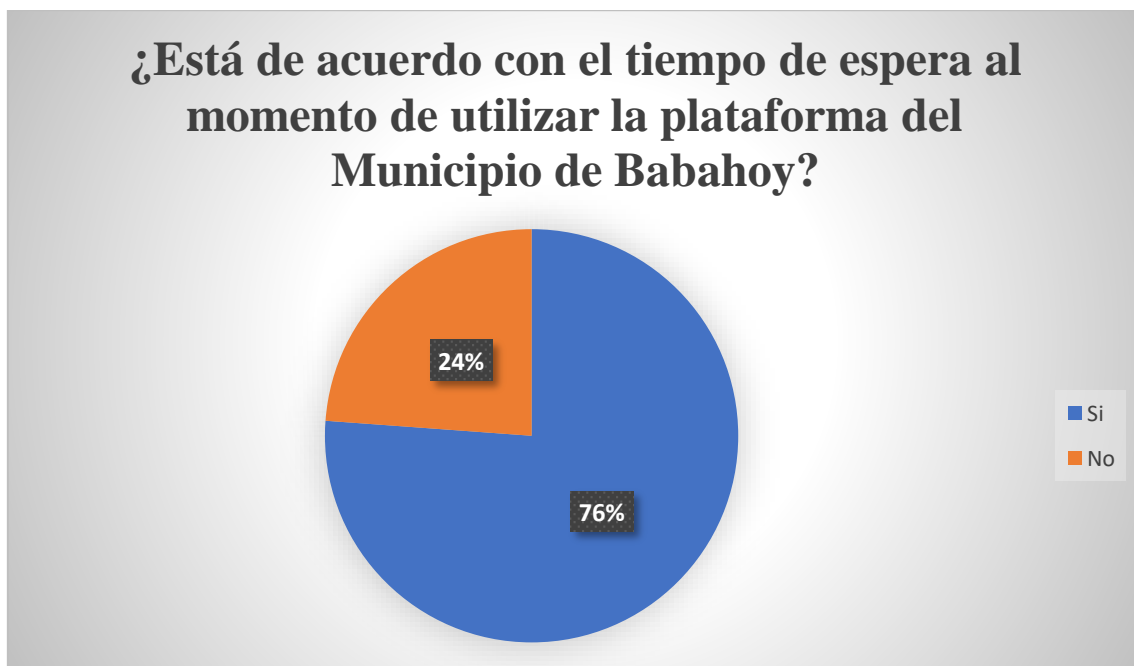


Gráfico 8: ¿Está de acuerdo con el tiempo de espera al momento de utilizar la plataforma del Municipio de Babahoyo? Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

En este análisis nos proporciona el 76% de los usuarios no tienen problema por el tiempo de espera y el 24% indica que no están de acuerdo con el tiempo de espera.

9.- ¿Funcionan todas las opciones que están implementada en la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Si	100	66%
No	51	34%
Total	151	100%

Tabla 13: Detalle-Pregunta 9. Fuente: (Heyner Huacón, 2022).



Gráfico 9: Funcionan todas las opciones que están implementada en la plataforma del Municipio de Babahoyo. Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

La información observada nos muestra que el 73% dicen que funcionan todas las funciones implementadas mientras que un 27% no les funciona y les proporcionan errores.

10.- ¿Cómo calificaría la plataforma del Municipio de Babahoyo?

Detalle	Frecuencia	Porcentaje
Muy satisfecho	80	53%
Satisfecho	40	26%
Insatisfecho	31	21%
Total	151	100%

Tabla 14: Detalle-Pregunta 10. Fuente: (Heyner Huacón, 2022).

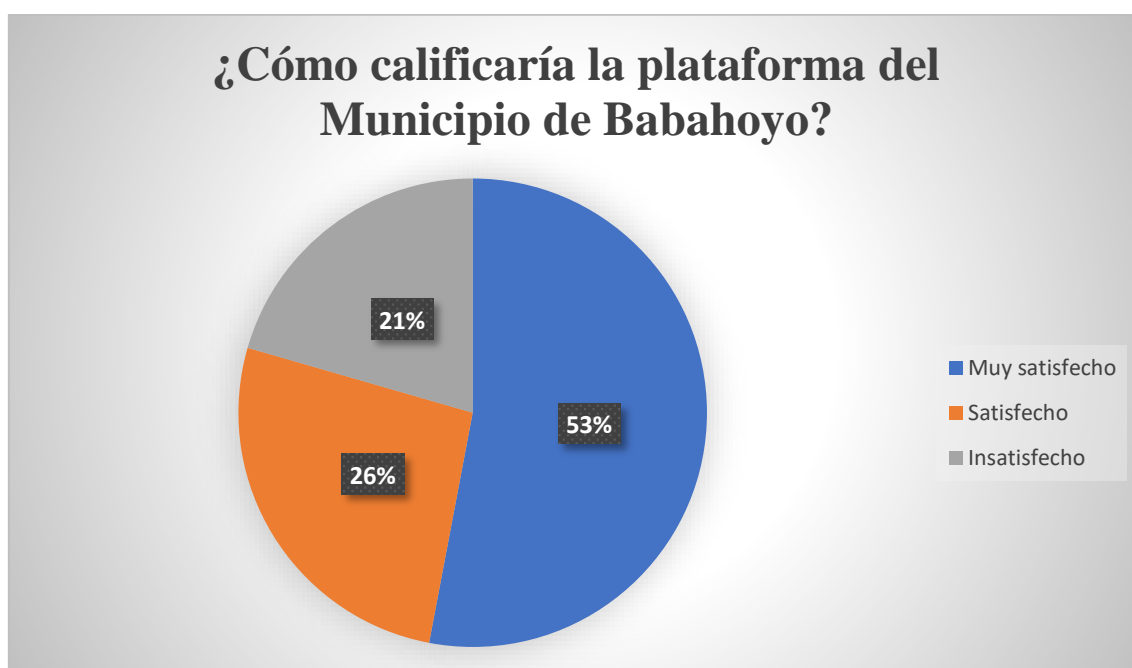


Gráfico 10: ¿Cómo calificaría la plataforma del Municipio de Babahoyo? Fuente: (Heyner Huacón, 2022).

Análisis e interpretación

Los usuarios califican de manera que el 53% están muy satisfecho, el 26% se encuentran satisfecho y el 21% se encuentran insatisfecho con la plataforma.

3.2. CONCLUSIONES ESPECÍFICAS Y GENERALES.

3.2.1. Específicas.

Luego de haber analizado e interpretado los resultados conseguidos por las encuestas de la investigación, se dedujo que hay deficiencia en los servicios brindados por las vulnerabilidades en el departamento de sistemas del Municipio de Babahoyo en su plataforma.

En respecto a los servicios que ofrece la plataforma no se conoce por que surgen estos inconvenientes, los usuarios que utilizan por primera vez y los que ya han utilizado se encuentran familiarizados con ciertos problemas que se presentar cuando existe vulnerabilidades de la seguridad, esto afecta a la información solicitada creando perdidas.

Al no realizar la implementación de nuevas tecnologías y correcciones a las vulnerabilidades de la seguridad de la información en el departamento de sistemas del Municipio de Babahoyo, esto sería de mucha ayuda a para que los usuarios no tengan problemas a futuro, la institución determino un manejo de dichas nuevas tecnologías sería de gran ayuda para mejorar las vulnerabilidades.

3.2.2. General.

Al concluir este proyecto de investigación en el Municipio de Babahoyo correspondiente a la Provincia de Los Ríos, se expresa que el servicio brindado por el departamento de sistemas, es muy importante para los usuarios que hacen uso diario, se detectaron una anomalía en la seguridad de la información, alojada en la plataforma.

3.3. RECOMENDACIONES ESPECÍFICAS Y GENERALES.

3.3.1. Específicas.

Se recomienda mejorar el área de sistemas para que no sufra ningún inconveniente en su información alojada en la plataforma del Municipio de Babahoyo.

La plataforma no tenga pérdida de información al momento que un usuario haga uso de sí misma.

Que se utilice de medios de comunicación para informar a los usuarios sobre los problemas que se estén presentando.

Saber cuáles son las vulnerabilidades e incidencias que se presentan y tener bien en claro, cual es el tema a solucionar para así no tener ninguna dificultad.

3.3.2. General.

Se recomienda a los usuarios del Municipio de Babahoyo, Provincia de Los Ríos, que se acerquen al departamento de sistema de la institución a informar sobre cualquier inconveniente o problema surgido al momento de hacer uso de algún servicio de los que ofrece la plataforma. Analizar posibles herramientas o componentes a implementar para un proyecto, se debe analizar un análisis costo – beneficio y por ende el técnico para garantizar la fiabilidad.

CAPÍTULO IV.- PROPUESTA TEORICA DE APLICACIÓN.

4.1. PROPUESTA DE APLICACIÓN DE RESULTADOS.

4.1.1. Alternativa obtenida.

Con los datos obtenido por la prueba del Chi Cuadrado nos da como alternativa la hipótesis alterna por medios de los resultados, que refiere: Con el desarrollo de una infraestructura para garantizar la seguridad de la información en los procesos del departamento de sistemas del Municipio de Babahoyo.

4.1.2. Alcance de la alternativa.

Implementar políticas de seguridad para garantizar todos los recursos disponibles y la disponibilidad de la información.

Al implementar este proyecto de investigación hay que analizar sus respectivos procesos de las vulnerabilidades de la información y las normas que con llevan realizarlo, para tomar en cuenta los tipos de actualización del proyecto, así que de manera mejorar el departamento.

Mejorar la calidad de servicios en el departamento se ofrece implementar un Scanner de vulnerabilidades de aplicaciones Web, para general una mayor seguridad en la información que opera el departamento al momento que los usuarios hacer uso por medio de la plataforma que tiene implementada la Municipalidad de Babahoyo, ya que

será favorable para todos los que harán uso del sistema mencionado y optimizar todos los recursos necesarios.

4.1.3. ASPECTOS BÁSICOS DE LA ALTERNATIVA.

4.1.3.1. Antecedentes.

En el Municipio de Babahoyo, de la provincia de Los Ríos, no se ha encontrado algún tipo de proyecto de investigación a implementar sobre las vulnerabilidades, para mejorar la seguridad de la información, que se ven afectados los usuarios con este problema.

En la actualidad se presentan inconvenientes al momento de aglomeraciones queriendo realizar rápidos sus trámites, ya que les dan un determinado tiempo y esto hace que haya mucha carga en la saturación de los servicios que nos brindan en el sistema, ya que con muchos servicios y procesos que ofrecen a sus usuarios, existe una inconformidad generando molestias.

Al aplicar un Scanner de vulnerabilidades de aplicaciones Web y realizar las medidas necesarias en el departamento de sistemas, con la tecnología propuesta se manejará de una mejor forma la plataforma, ya que así se preverá cualquier inconsistencia que se visualice o alguna vulnerabilidad al hacer uso de la información de los usuarios que vayan a solicitar en ese momento y así están protegidos de que realicen un ataque al departamento de sistemas del Municipio de Babahoyo.

4.1.3.2. Justificación.

El propósito de este proyecto de investigación aparece sobre la problemática que existe en el departamento de sistemas del Municipio de Babahoyo, provincia de Los Ríos, se suscitan algunos inconvenientes con la vulnerabilidades e incidencias ya antes mencionadas, esta propuesta es implementar un Scanner de vulnerabilidades para asegurar la información.

A través de un Scanner de vulnerabilidades de aplicaciones Web, que se viene implementado a nivel local e internacional, con el objetivo de ir mejorando la calidad de servicios para todos los usuarios del Municipio de Babahoyo, con el cual se garantizara un servicio eficaz, se esperar ofrecer de una manera eficiente en los procesos que realicen, para así aprovechar todos los recursos y no haya ninguna vulnerabilidad de la información transmitida por la red.

La misión es implementar un Scanner de vulnerabilidades de aplicaciones Web y así mejorar los servicios de un ambiente neutral, para que así haya una calidad de la información ya que a este software se facilitara la detección de vulnerabilidades.

La visión es lograr un servicio de calidad y eficiente para todos los usuarios que hacen uso a diario del sistema.

Los beneficiados con la implementación de este proyecto de investigación son para los usuarios del Municipio de Babahoyo, ya que así estará segura su información.

4.2. OBJETIVOS.

4.2.1. General.

Mejorar la calidad del departamento de sistema del Municipio de Babahoyo que ofrece sus servicios en la plataforma para garantizar la seguridad de la información de sus usuarios.

4.2.2. Específicos.

- Mejorar los servicios del departamento de sistema del Municipio de Babahoyo, con nuevos procesos de seguridad contra las vulnerabilidades.
- Implementar una infraestructura tecnológica que soporte las mejoras de los servicios para sus usuarios.
- Desarrollar una arquitectura para la seguridad de la información por medio de un Scanner de vulnerabilidades de aplicaciones Web (Wireshark), para mejorar el departamento de sistema del Municipio de Babahoyo.

4.3. ESTRUCTURA GENERAL DE LA PROPUESTA.

4.3.1. Título.

“Desarrollar una arquitectura de scanner de vulnerabilidades para mejorar la calidad del departamento de sistema del Municipio de Babahoyo en los servicios que ofrece para garantizar la seguridad de la información transmitida por la red”.

4.3.2. Componentes.

Wireshark

Se trata de un software gratuito que permite analizar el tráfico red en tiempo real. Pero su particularidad es que a menudo es la mejor herramienta para solucionar los problemas de Red como la latencia o actividad maliciosa como intentos de piratería (CSO, 2022).

Tomcat Apache

Es un contenedor Java Servlet, o contenedor web, que proporciona la funcionalidad extendida para interactuar con Java Servlets, al tiempo que implementa varias especificaciones técnicas de la plataforma Java: JavaServer Pages (JSP), Java Expression Language (Java EL) y WebSocket (Eulises Ortiz, 2020).

HTTP

El Protocolo de transferencia de hipertexto (HTTP) es la base de la World Wide Web, y se utiliza para cargar páginas web con enlaces de hipertexto. HTTP es un protocolo de la capa de aplicación diseñado para transferir información entre dispositivos en red, y se ejecuta sobre capas de la pila de protocolos de red (cloudflare, 2018).

El método GET

El método GET es adecuado para la personalización de páginas web: el usuario puede guardar búsquedas, configuraciones de filtros y ordenaciones de listas junto al URL como marcadores, de manera que en su próxima visita la página web se mostrará según sus preferencias (Desarrollo Web, 2020).

El método POST

El método POST transmite datos de una página PHP a otra. A diferencia del método GET, estos datos no están visibles en la URL. De ahí que este método sea el más utilizado (Matarazzo, 2022).

Vulnerabilidades

En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes (Banco Santander, S.A., 2017).

SGSI

un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de

información minimizando a la vez los riesgos de seguridad de la información (Firma-e, 2013).

Apache JMeter

JMeter es una herramienta que facilita la gestión integral de los procesos de pruebas de rendimiento, no obstante, no es la única puesto que tenemos otras como: Micro Focus LoadRunner, IBM RPT, SilkPerformer, WebLoad, NeoLoad, OpenSTA, otras (Terrera, 2019).

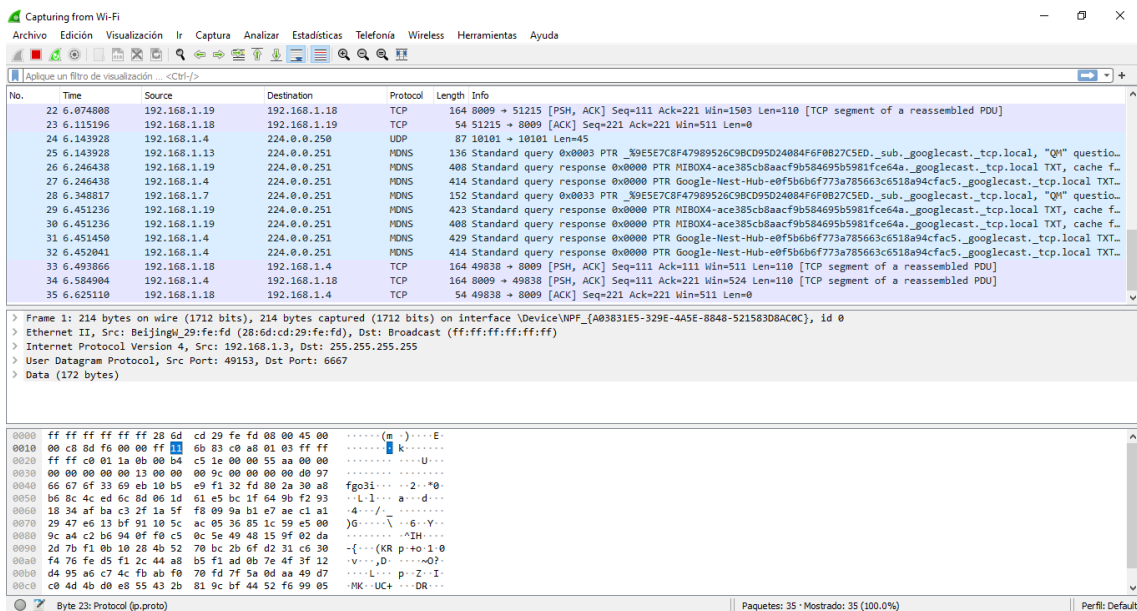


Figura 4: Scanner de vulnerabilidades de aplicaciones Web (Wireshark). Fuente: (Heyner Huacón, 2022).

4.4. RESULTADOS ESPERADOS DE LA ALTERNATIVA.

Con la propuesta de este proyecto de investigación, es para establecer un departamento de sistemas que funcione de una manera fiable, detecte vulnerabilidades de una manera rápida y precisa para así garantizar la información de sus usuarios.

Mejorar los servicios y procesos internos que ofrece la plataforma del Municipio de Babahoyo, para que haya una mejor comunicación en los requerimientos que solicita los usuarios.

Los resultados obtenidos por medio de las encuestas realizadas a los usuarios se vean plasmado en la mejoría de la plataforma, generando un informe al departamento de sistema si se encuentra algún fallo o problema suscitado.

Establecer un departamento de sistema del Municipio de Babahoyo seguro y que no haya ningún inconveniente al recibir múltiples solicitudes por los usuarios.

BIBLIOGRAFÍA

- Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Revista Científica Dominio De Las Ciencias*, 9 - 11.
- Banco Santander, S.A. (13 de Abril de 2017). Obtenido de <https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.>
- Bodnar, D. (29 de Octubre de 2020). *Avast Academy*. Obtenido de <https://www.avast.com/es-es/c-social-engineering>
- CABALLERO GONZÁLEZ, C., & CLAVERO GARCÍA, J. A. (2017). *Salvaguarda y seguridad de los datos*. Madrid: Editorial Paraninfo.
- Castillo, R. (2 de Diciembre de 2020). *Vulnerabilidades informáticas*. Obtenido de <https://www.tecnologia-informatica.com/vulnerabilidades-informaticas/>
- CEUPE. (10 de Agosto de 2017). *ceupe*. Obtenido de <https://www.ceupe.com/blog/flujo-de-la-gestion-de-incidencias.html?dt=1656990422777>
- cloudflare. (20 de Noviembre de 2018). Obtenido de <https://www.cloudflare.com/es-es/learning/ddos/glossary/hypertext-transfer-protocol-http/>
- Coba Molina, M. (2016). Factores que influyen en la obtención de información gerencial en los directivos de las Pymes en Tungurahua-Ecuador. *Paakat*, 9.
- Colnodo. (31 de Mayo de 2016). *APC*. Obtenido de <https://www.apc.org/es/news/sisbim-sistema-basico-de-informacion-municipal-de->
- CSO. (5 de Julio de 2022). *computerworld*. Obtenido de <https://cso.computerworld.es/tendencias/que-es-wireshark-asi-funciona-la-nueva-tendencia-esencial-en-seguridad>
- Desarrollo Web. (11 de Agosto de 2020). Obtenido de <https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/get-vs-post/#:~:text=El%20m%C3%A9todo%20GET%20es%20adecuado,se%20mostrar%C3%A1%20seg%C3%BAAn%20sus%20preferencias.>

- Douglas da Silva. (6 de Septiembre de 2021). *Blog de Zendesk*. Obtenido de zendesk.com.mx/blog/gestion-incidencias-procedimiento/
- Eulises Ortiz, A. (26 de Marzo de 2020). *hostdime*. Obtenido de <https://www.hostdime.com.ar/blog/que-es-apache-tomcat/>
- Firma-e. (2013 de Febrero de 2013). Obtenido de <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>
- Guayaquil, G. M. (13 de Abril de 2019). *Geoportal-Guayaquil*. Obtenido de <https://geoportal-guayaquil.opendata.arcgis.com/>
- Hernández Saucedo, A. L., & Mejia Miranda, J. (1 de Febrero de 2015). *Computación e Informática*. Obtenido de <https://www.redalyc.org/pdf/5122/512251501005.pdf>
- Huilca Chicaiza, G. N. (Noviembre de 2012). *HACKING ÉTICO PARA DETECTAR VULNERABILIDADES EN LOS SERVICIOS DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN CEVALLOS*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/2900/1/Tesis_t764si.pdf
- INCIBE. (20 de Marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido de [https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20\(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo](https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo)
- López, A. (2010). *Seguridad informática*. Madrid: Editex,.
- Lozano, V. (13 de Agosto de 2019). *Quitoinforma*. Obtenido de <http://www.quitoinforma.gob.ec/2019/08/13/nuevo-sistema-de-gestion-documental-reducira-tiempos-de-respuesta/>
- Martha Irene Romero Castro, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Alcoy: 3Ciencias.
- Matarazzo, D. (2022). *Apprenez les langages HTML5, CSS3 et JavaScript pour créer votre premier site web*. RI3HTCSJA.

Morocho Toaza, A. L. (Abril de 2013). *ANÁLISIS HEURÍSTICO DE MALWARE APLICADO A LA DETECCIÓN DE DOCUMENTOS PDF MALICIOSOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO*. Obtenido de

https://repositorio.uta.edu.ec/bitstream/123456789/4933/1/Seminario_t813si.pdf

Novoseltseva, E. (2018). *apiumhub*. Obtenido de <https://apiumhub.com/es/tech-blog-barcelona/proceso-y-herramientas-de-gestion-de-incidencias/>

Pagliari, G. A., & Eterovic, J. (2012). *Metodología de Análisis de Riesgos Informáticos*. España: Editorial Academica Espanola.

Pérez Porto, J., & Merino, M. (2021). *Definición de seguridad informática*. Obtenido de <https://definicion.de/seguridad-informatica/>

QUIRUMBAY YAGUAL, D. I. (2015). *DESARROLLO DEL ESQUEMA DE SEGURIDAD, PLAN DE RECUPERACIÓN ANTE DESASTRES INFORMÁTICOS Y SOLUCIÓN PARA EL NIVEL DE EXPOSICIÓN DE AMENAZAS Y VULNERABILIDADES APLICADA A LOS SERVIDORES Y EQUIPOS DE COMUNICACIÓN DEL CENTRO DE DATOS DE LA MUNICIPALIDAD DEL EST.* Obtenido de <https://www.dspace.espol.edu.ec/retrieve/88647/D-84693.pdf>

REVISTA, U. (11 de Diciembre de 2019). *INGENIERÍA Y TECNOLOGÍA*. Obtenido de <https://www.unir.net/ingenieria/revista/iso-27001/>

Sain, G. (13 de 05 de 2018). *pensamientopenal*. Obtenido de <https://www.pensamientopenal.com.ar/system/files/2018/05/doctrina46557.pdf>

Servicetonic. (20 de Diciembre de 2018). *servicetonic*. Obtenido de <https://www.servicetonic.com/es/itil/itil-v3-gestion-de-incidencias/#:~:text=Una%20incidencia%20es%20toda%20interrupci%C3%B3n,herramienta%20de%20monitorizaci%C3%B3n%20de%20eventos>.

Silva Coelho, F. E., Segadas de Araújo, L. G., & Kowask Bezerra, E. (2014). *Gestión de la Seguridad de la Información*. Colombia: ISBN: (ebook).

sni. (2015). Obtenido de http://app.sni.gob.ec/sni-link/sni/PORTAL_SNI/data_sigad_plus/sigadplusdocumentofinal/12600002200

01_PDOT%20TEXTO%20BABAHOYO%20ACTUALIZADO%202015-
2020_13-04-2016_22-01-20.pdf

TEAM, A. (10 de Noviembre de 2020). *Tipos de Vulnerabilidades y Amenazas informáticas*. Obtenido de <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas>

TEAM, A. (10 de Noviembre de 2020). *Tipos de Vulnerabilidades y Amenazas informáticas*. Obtenido de <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas>

Terrera, G. (22 de Noviembre de 2019). Obtenido de <https://testingbaires.com/que-es-jmeter/>

Torres Cabanillas, L. (25 de Mayo de 2017). *Sistema de información para la municipalidad de Ica Perú*. Obtenido de <https://www.gestiopolis.com/sistema-de-informacion-para-la-municipalidad-de-ica-peru/>

Vega Briceño, E. (2020). *Planificación y ejecución de evaluaciones de seguridad informática desde un enfoque de ethical hacking*. Alcoy: 3Ciencias.

ANEXOS



6.- Usted como usuario, cree que la plataforma del Municipio de Babahoyo, necesita mejoras.

SI()

NO()

7.- Al momento de utilizar la plataforma del Municipio de Babahoyo, se le ha colapsado.

SI()

NO()

8.- ¿Está de acuerdo con el tiempo de espera al momento de utilizar la plataforma del Municipio de Babahoyo?

SI()

NO()

9.- Funcionan todas las opciones que están implementada en la plataforma del Municipio de Babahoyo.

SI()

NO()

10.- ¿Cómo calificaría la plataforma del Municipio de Babahoyo?

Muy Satisfecho ()

Satisfecho ()

Insatisfecho ()

Encuesta - Heyner Huacón



CERTIFICADO DE ANÁLISIS
magister

Proyecto De Investigación

8%
Similitudes

< 1%
Texto entre comillas

< 1% similitudes entre comillas
1% Idioma no reconocido

Nombre del documento: PROYECTO FINAL - ETAPA HEYNER
HUACON.docx
Tamaño del documento original: 738,01 kb
Autor: Heyner Huacón

Depositante: Heyner Huacón
Fecha de depósito: 31/8/2022
Tipo de carga: url_submision
fecha de fin de análisis: 31/8/2022

Número de palabras: 12,452
Número de caracteres: 83,554


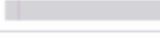

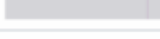

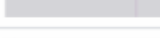

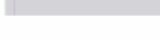
Ubicación de las similitudes en el documento:



Fuentes principales detectadas






Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	 gstarsoft.cl Ingeniería Social - GSTARSOFT CIBERSEGURIDAD https://gstarsoft.com/es/ciberseguridad/servicios/ingenieria-social/	< 1%		Palabras idénticas < 1% (24 palabras)
2	 protecciondatos-lapd.com Exploits o vulnerabilidades informáticas ¿Qué son? ¿CÓ...? https://protecciondatos-lapd.com/en/empresas/exploits-vulnerabilidades-informaticas/ 4 fuentes similares	< 1%		Palabras idénticas < 1% (29 palabras)
3	 aplumhub.com Proceso y herramientas de gestión de incidencias Aplumhub https://aplumhub.com/es/tech-blog/barridos/proceso-y-herramientas-de-gestion-de-incidencias/	< 1%		Palabras idénticas < 1% (26 palabras)
4	 www.unir.net ISO 27001 ¿En qué consiste esta norma de seguridad? UNIR https://www.unir.net/ingenieria/revista/iso-27001/ 1 fuente similar	< 1%		Palabras idénticas < 1% (60 palabras)
5	 Documento de otro usuario Tarea 10 - Modelo de Seguridad Informática35... #73uaf El documento proviene de otro grupo 4 fuentes similares	< 1%		Palabras idénticas < 1% (67 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	 repositorio.ug.edu.ec http://repositorio.ug.edu.ec/bitstream/iredug/12862/3/TESE_ALAWA_LOPEZ_YADIRA_01-07-2015.pdf.txt	< 1%		Palabras idénticas < 1% (20 palabras)
2	 repositorio.utmachala.edu.ec https://repositorio.utmachala.edu.ec/bitstream/48000/1281/1/SCUACE-2019-CA-0621005.pdf	< 1%		Palabras idénticas < 1% (17 palabras)
3	 Documento de otro usuario PRACTICA_0036311631_Experiencia_00.docx #625uaf El documento proviene de otro grupo	< 1%		Palabras idénticas < 1% (15 palabras)
4	 info.inclusion.gob.ec DATOS https://info.inclusion.gob.ec/index.php/geoport	< 1%		Palabras idénticas < 1% (13 palabras)

Fuentes mencionadas (sin similitudes detectadas)

Estas fuentes han sido citadas en el documento sin encontrar similitudes.

-  <https://www.cloudflare.com/es-es/learning/ddos/glossary/hypertext-transfer-protocol-http/>
-  <https://www.apc.org/es/news/sisbim-sistema-basico-de-informacion-municipal-de>
-  <https://geoport.guayaquil.opendata.arcgis.com/>
-  <https://www.dspace.espol.edu.ec/retrieve/88647/D-84693.pdf>
-  <https://www.gestioipolis.com/sistema-de-informacion-para-la-municipalidad-de-ica-peru/>