
**UNIVERSIDAD TÉCNICA DE BABAHOYO**

**FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA**

**PROCESO DE TITULACIÓN**

**OCTUBRE 2019–MARZO 2020**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS**

**TEMA:**

# Análisis para Detectar Amenazas y Vulnerabilidades en la red del GAD Municipal de Babahoyo de la Ciudad de Babahoyo

**EGRESADA:**

**Amanda Julexy Muñoz Macias**

**TUTOR:**

**Ing. Raúl Ramos Morocho**

**AÑO 2020**

## RESUMEN

En la actualidad la seguridad informativa es un tema de vital importancia para las empresas del sector público, es por eso que las redes inalámbricas deben tener una administración adecuada, debido a que es una de las tecnologías de comunicación más usadas hoy en día porque está incorporada en la mayoría de los dispositivos móviles, laptops y computadoras. El Gobierno Autónomo Descentralizado del cantón Babahoyo, brinda servicios públicos a través de diferentes procesos de los cuales su gran mayoría se manejan a través de las tecnologías de la información. La problemática que existe en el municipio de la ciudad de Babahoyo es que no existe un control adecuado que resguarde la seguridad de los equipos, recursos e información que se maneje en la red de datos presente en la institución. El objetivo del presente caso de estudio es identificar las vulnerabilidades existentes en la red del GAD municipal del cantón Babahoyo, para proceder a conocer las posibles amenazas que pueden atentar con la seguridad de la información que se gestiona en la institución. El presente caso de estudio presenta un enfoque metodológico cualitativo, ya que desea cualificar el estado de la red a través de un escaneo de red usando la herramienta de testeo OpenSource NMap. La política de seguridad que tiene que implementar el GAD de Babahoyo debe contener un plan de reacción ante ataques de red e incidentes de seguridad. Dicha política debe determinar las respuestas a varios tipos de incidentes, acciones para diferentes ataques a la red.



**Palabras clave**

vulnerabilidades, municipio, Babahoyo, red, análisis

## ABSTRACT

At present, information security is a topic of vital importance for public sector companies, which is why wireless networks must have adequate administration, because it is one of the most used communication technologies today because it is incorporated on most mobile devices, laptops and computers. The Decentralized Autonomous Government of the Babahoyo canton provides public services through different processes of which the vast majority are managed through information technologies. The problem that exists in the municipality of the city of Babahoyo is that there is no adequate control that protects the security of the equipment, resources and information that is managed in the data network present in the institution. The objective of this case study is to identify the existing vulnerabilities in the network of the municipal GAD of the Babahoyo canton, to proceed to know the possible threats that may threaten the security of the information managed in the institution. The present case study presents a qualitative methodological approach, since it wishes to qualify the state of the network through a network scan using the OpenSource NMap test tool. The security policy that the Babahoyo GAD has to implement must contain a reaction plan for network attacks and security incidents. This policy must determine the responses to various types of incidents, actions for different attacks on the network.



**Keywords**

vulnerabilities, municipality, Babahoyo, network, analysis

# INTRODUCCIÓN

En la actualidad la seguridad informativa es un tema de vital importancia para las empresas del sector público, es por eso que las redes inalámbricas deben tener una administración adecuada, debido a que es una de las tecnologías de comunicación más usadas hoy en día porque está incorporada en la mayoría de los dispositivos móviles, laptops y computadoras. Estos dispositivos se conectan a estas redes con el objetivo de automatizar tareas, acceder a servicios y por medio de estas confecciones se maneja grandes volúmenes de información.

Hoy en día la institución podrían tener acceso terceras persona a las redes inalámbricas sin restricciones y sin la de que esta se encuentre en las instalaciones de dicha institución, debido a que la señal no está limitada, solo le bastaría estar en el alcance de la señal o dentro de su radio de cobertura. La información que se gestiona el GAD Municipal de Babahoyo es muy importante y no puede ser accedido por personas no autorizadas, una tercera persona puede acceder a las redes inalámbricas sin la necesidad de que esta se encuentre en las instalaciones de dicha empresa, debido a que la señal no está limitada, solo le bastaría estar en el alcance de la señal o dentro de su radio de cobertura.

El presente caso de estudio implementa la metodología cualitativa porque se logra entender características sobresalientes a través de los procesos que se realizan en una red informática. Se utiliza como herramienta de recolección de datos a la observación para conocer las anomalías físicas de la red durante una visita al GAD Municipal de Babahoyo. La línea de investigación del presente caso de estudio se organiza al desarrollo de sistemas de la información, comunicación y emprendimientos

empresariales y tecnológicos donde la sublínea retribuye a procesos de transmisión de datos y telecomunicaciones.

# DESARROLLO

Las empresas que utilizan internet han crecido drásticamente en la última década. Los ataques a la aplicación web han aumentado. La seguridad de las redes es un gran desafío para cualquier organización como resultado del aumento de los ataques. Existen diferentes enfoques para mitigar varios riesgos de seguridad: codificación defensiva, endurecimiento (firewall), monitoreo y auditoría. Estas soluciones encontraron más hacia la prevención de ataques o de los tipos de monitoreo.

El Gobierno Autónomo Descentralizado del cantón Babahoyo, brinda servicios públicos a través de diferentes procesos de los cuales su gran mayoría se manejan a través de las tecnologías de la información. La problemática que existe en el municipio de la ciudad de Babahoyo es que no existe un control adecuado que resguarde la seguridad de los equipos, recursos e información que se maneje en la red de datos presente en la institución. Las redes de telecomunicaciones deben mantenerse correctamente instaladas de acuerdo a los estándares de calidad, con el fin de ofrecer información íntegra, confiable y que esté disponible cuando se la solicite. (Cano, 2004)

La evaluación de vulnerabilidad y las pruebas de penetración son dos enfoques ampliamente que deben utilizar las organizaciones para evaluar la seguridad de las redes. Ambas soluciones son diferentes y complementarias entre sí. En este artículo se proporcionan comparaciones de estos dos enfoques. Se ha descubierto que las pruebas de penetración se comparan mejor con la evaluación de vulnerabilidad, ya que explota la vulnerabilidad, mientras que la evaluación de vulnerabilidad es superior en términos de cobertura sobre las pruebas de penetración.

El crecimiento constante de las redes de comunicaciones estimula la búsqueda de nuevas herramientas, con el fin de mantener el estado de estas redes en óptimas condiciones. El correcto manejo de la información y de procesos es esencial para resguardar la seguridad de los datos que se manejan en la institución. Se debe delimitar el acceso a los procesos más importantes a los empleados que autorizados.

El objetivo del presente caso de estudio es identificar las vulnerabilidades existentes en la red del GAD municipal del cantón Babahoyo, para proceder a conocer las posibles amenazas que pueden atentar con la seguridad de la información que se gestiona en la institución. Si no se hace un análisis periódico del estado de la red, se puede correr el riesgo que los servicios y protocolos que se utilizan en la configuración de una red LAN, se encuentren desactualizados, lo que puede provocar que la red sea vulnerada poniendo peligro la integridad de los recursos, equipos e información, siendo la última el activo más importante para cualquier institución. (CARPENTIER, 2016)

El presente caso de estudio presenta un enfoque metodológico cualitativo, ya que desea cualificar el estado de la red a través de un escaneo de red usando la herramienta de testeo OpenSource NMap. Además como herramienta de recolección de datos se utiliza a la observación con el objetivo de identificar a cada uno de los activos presentes en la red del GAD municipal e Babahoyo. Se hace uso de una ficha de observación como instrumento metodológico para la recolección de esta información.

Para la metodología seleccionada se identificaron cuatro etapas para lograr el objetivo expuesto. Las etapas se detallan a continuación:

Etapa 1. Identificación de activos. En primer lugar, se procedió identificar la estructura de la red, determinar todas las computadoras y otros dispositivos asociados y preparar un plan de red utilizando el software de mapeo de red apropiado. Después de la

identificación de los dispositivos clave, es necesario delinear los sistemas críticos y asignarles prioridad.

Etapa 2. Evaluaciones de vulnerabilidad. Actualmente hay muchos escáneres de vulnerabilidad disponibles. Para realizar esta etapa se selección NMap, como se mencionó anteriormente. La mejor práctica es utilizar varias herramientas de evaluación de vulnerabilidades y crear una imagen completa de las violaciones de seguridad después del escaneo.

Etapa 3. Revisión de vulnerabilidades. Este paso se centra en estimar la gravedad de las vulnerabilidades identificadas y priorizar dentro de los problemas críticos. La mejor solución es "aprovechar la corrección de vulnerabilidades" y determinar lo necesario que permitan combinar datos de diversos escáneres de evaluación.

Etapa 4. Remediación de vulnerabilidades.- Existen tres formas comunes de abordar las vulnerabilidades de la red para el administrador de la red: corrección manual, herramientas de implementación de parches y herramientas de corrección automatizadas. En caso de implementación de parches, se debe realizar una exploración secundaria en busca de vulnerabilidades.

Como normas de aplicación dentro de la infraestructura de red existen una serie de criterios que velan por nuestra segundad e integridad, así como por inversiones y una serie de recomendaciones que, aunque no son de obligado cumplimiento se garantizan la independencia al estandarizar su uso. El Soporte Informático que se trata de un servicio mediante el cual los especialistas en apoyo informático o expertos en digital le ofrecen asistencia técnica, soporte remoto ante algún problema y asesoramiento a los usuarios y organizaciones que trabajan cada día con las nuevas tecnologías. (Chicano Tejada, 2015)

La seguridad informática establece principios que garantizan las buenas prácticas de mantener a la información confiable, integra y disponible, lo que conlleva un plus para la protección de los datos más importantes de la institución. Una información integra significa que esta se mantiene igual sin sufrir ninguna modificación durante su transmisión. La información confiable demuestra que esta es manejada solo por personas autorizadas y la información disponible es que esta esta accesible para poder utilizarla en cualquier momento.

La seguridad de la red se puede dividir en dos ramas: seguridad de los sistemas informáticos y seguridad de la comunicación. Existen numerosas fuentes de vulnerabilidades en ambas esferas de seguridad. Las principales fuentes de vulnerabilidades son fallas de diseño, fallas de desarrollo de software, problemas de administración de seguridad, implementación incorrecta, tecnologías cambiantes y procesos problemáticos para reparar sistemas vulnerables. (Correa & BATTO, 1987)

Existen múltiples tipos de ataques de red que evolucionan debido a los tipos de vulnerabilidades mencionados anteriormente. Estos ataques pueden clasificarse según el alcance y otras características. Los ataques comunes son espionaje, modificación de datos, suplantación de identidad, ataques de contraseña, DOS y DDOS, hombre en el medio, troyanos, gusanos, virus y ataques de capa de aplicación.

Para cada tipo de estos ataques, hay una serie de contramedidas. Sin embargo, para crear un sistema de seguridad de red eficiente, es necesario utilizar un enfoque integrado. Incluye la creación de un documento de política de seguridad, evaluación de vulnerabilidad en 5 pasos, Sistema de prevención de intrusiones, un sistema para registrar/rastrear incidentes de seguridad, Plan de respuesta a incidentes y métodos de gestión de riesgos de seguridad. (González, 2010)

El presente caso de estudio se delimita solamente a informar sobre el estado de la red del GAD municipal de Babahoyo, por lo que no se pretende manipular, ni reconfigurar los parámetros de funcionamiento de la red predeterminados de la institución. El presente servirá como guía para que el administrador de la red tome las medidas necesarias para resolver los inconvenientes encontrados.

Durante la visita realizada al GAD municipal de Babahoyo se logró detectar la mala distribución de la red, ya que los cables se encuentran dispersos por todos lados sin sus respectivas canaletas, ni una correcta administración de los recursos tecnológicos disponibles en la institución. Esto conlleva a problemas transmisión de los datos, porque pueden existir interferencias en la interconectividad, causando muchas veces que la información transmitida no llegue a su destino. La mala ubicación del cableado que está expuesto a daños físicos, y que seguridad informática para mantener una infraestructura tecnológica de transmisión de datos. (Gómez, 2003)

Durante la identificación de los activos se pudo evidenciar todos los recursos disponibles para el funcionamiento de la red del GAD de Babahoyo. Con respecto al hardware se pudo detectar los siguientes componentes:

| **Cantidad** | **Componente** |
|---|---|
| 1 | Switch |
| 2 | Router inalámbrico |
| 10 | Computadoras Core 2duo con 2gb RAM |
| 9 | Computadoras  Intel Core i3 |

Tabla 1. Componentes de hardware de la red del GAD de Babahoyo

En relación al software se pude identificar que diez de los equipos cuentan con el Sistema operativo Windows 7 y nueve cuentan con el sistema operativo Windows 10.

En la infraestructura se pudo identificar que no existe una instalación adecuada de la red, el cableado no está estructurado correctamente, así como también se pudo observar el libre acceso de cualquier persona presente en GAD de Babahoyo pueda a conectar cables y otros equipos que no forman parte de la red institucional. Los cables parecen telaraña, y es muy difícil distinguir el procedente de cada uno, y además que puedan presentar daños futuros por el estando en que se encuentran. (Chicano Tejada, 2015)

En la identificación de las vulnerabilidades, estas se las pudo clasificar como físicas y lógicas. En las físicas se pudo determinar que la red no se encuentra instalada, acorde con los estándares de calidad establecidos para resguardar la información que circula por ese medio. Esto puede provocar pérdida de información valiosa o interrupción de procesos importantes que se realizan en la institución, esto debido a la incorrecta instalación de los componentes y equipos de red que la conforman.

Para determinar qué tipo de vulnerabilidades lógicas existen en el la red del GAD municipal de Babahoyo se utilizó la herramienta de testeo OpenSource. NMap utiliza paquetes IP sin procesar de una manera refrescante para determinar qué hosts están en la red, incluidos los servicios y sistemas operativos que están ejecutando. NMap también puede determinar los filtros de paquetes que están utilizando los hosts y otros tipos de filtros de paquetes/firewalls y otras características. Es utilizado principalmente por organizaciones que tienen redes grandes y es por eso que ha sido diseñado. NMap es una técnica realmente rápida para escanear toda la red. NMap es altamente compatible con varios sistemas operativos tanto en consola como en interfaz gráfica. (Fisher, 1988)

Un simple comando NMap puede escanear más de 1660 puertos TCP en el destino. NMap clasificó los puertos en seis estados diferentes que no son propiedades intrínsecas del puerto, pero representan cómo los considera el NMap. Entonces, los seis estados de los puertos clasificados por NMap se detallan en la siguiente la tabla # 2:

| **Estado** | **Significado** |
|---|---|
| Abierto | Una aplicación está tomando activamente conexiones de TCP, datagramas de UDP y las asociaciones de SCTP se consideran un puerto abierto. El objetivo principal del escaneo de puertos es encontrar los puertos abiertos. Los hackers encuentran los puertos abiertos como bulevar para el ataque. También intentan explotar los puertos abiertos mientras los administradores intentan cerrarlo |
| Cerrado | Un puerto accesible pero ninguna de las aplicaciones lo está escuchando. Es útil para el descubrimiento de host. |
| Filtrado | NMap no puede determinar si el puerto está abierto debido al filtrado de paquetes. |
| Sin filtrar | Esto significa que se puede acceder al puerto, pero NMap no puede determinar si el puerto está cerrado o abierto. Escanear estos puertos con otros tipos de escaneo puede resolver el problema. |
| Abierto/filtrado | Esto significa que NMap no puede determinar si el puerto está abierto o filtrado. Esto ocurre cuando los puertos abiertos no dan respuesta. Un escaneo UDP, IP, FIN, NULL y Navidad puede resolver estos puertos. |

| | |
|---|---|
| Cerrado/filtrado | Esto significa que el puerto está en un estado en el que NMap no puede determinar si el puerto está cerrado o filtrado. Se puede usar para escanear ID de IP. |

Tabla 2. Estados puertos según NMap.

Para identificar las vulnerabilidades lógicas presentes en la red del GAD municipal de Babahoyo, se procedió a realizar el escaneo con la herramienta seleccionada, y con el respectivo permiso del administrador de la red se conectó una laptop a unos de los puntos de red. El dispositivo conectado tenía instalado la herramienta, lo que facilitó realizar el escaneo de la red del GAD de Babahoyo.

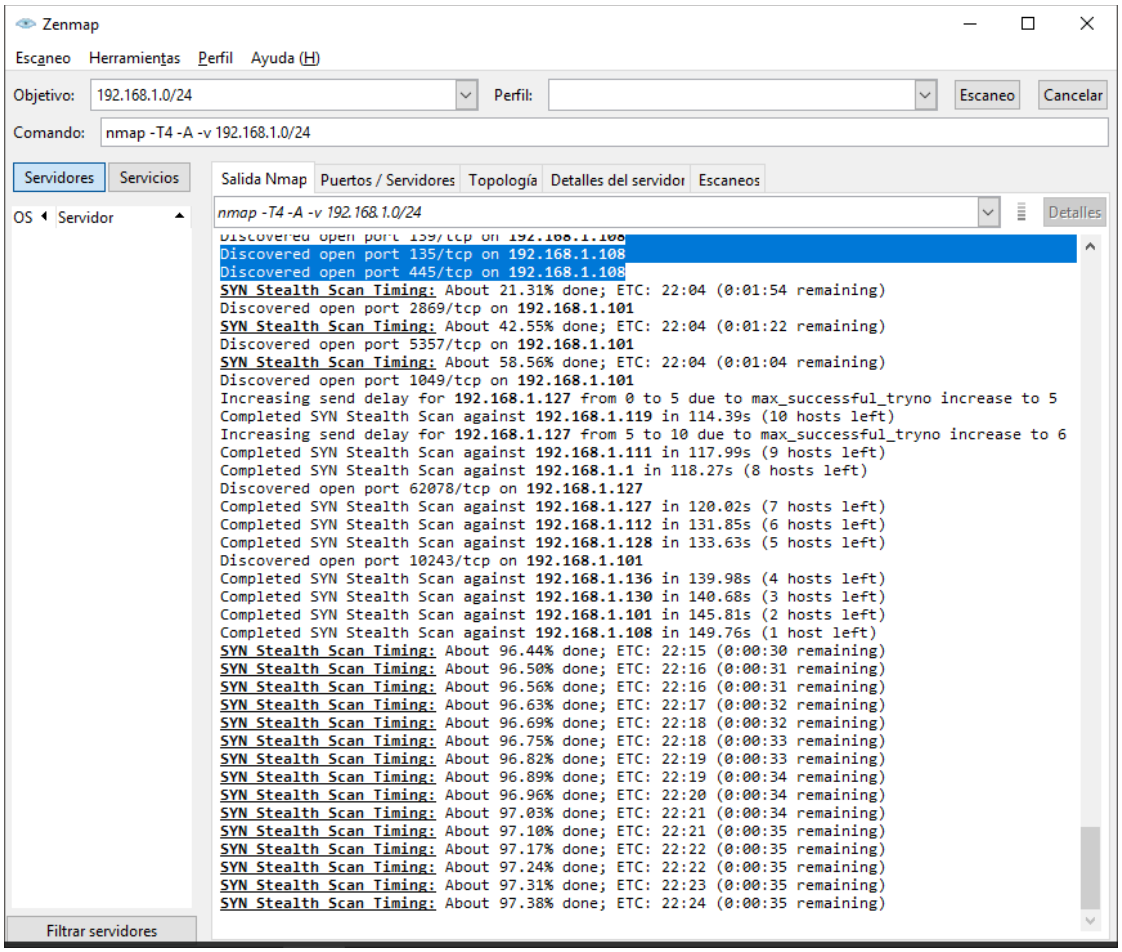


Fig. 1. Pantalla de inicio de escaneo de NMap

El proceso tuvo una duración de 20 minutos aproximadamente, donde el informe final presentó puntos críticos en los terminales de la red. Aquí se pudo evidenciar que existen algunos equipos con demasiados puertos abiertos, estos innecesarios, puesto que no hay procesos informáticos relacionados con las funciones que realiza del municipio.

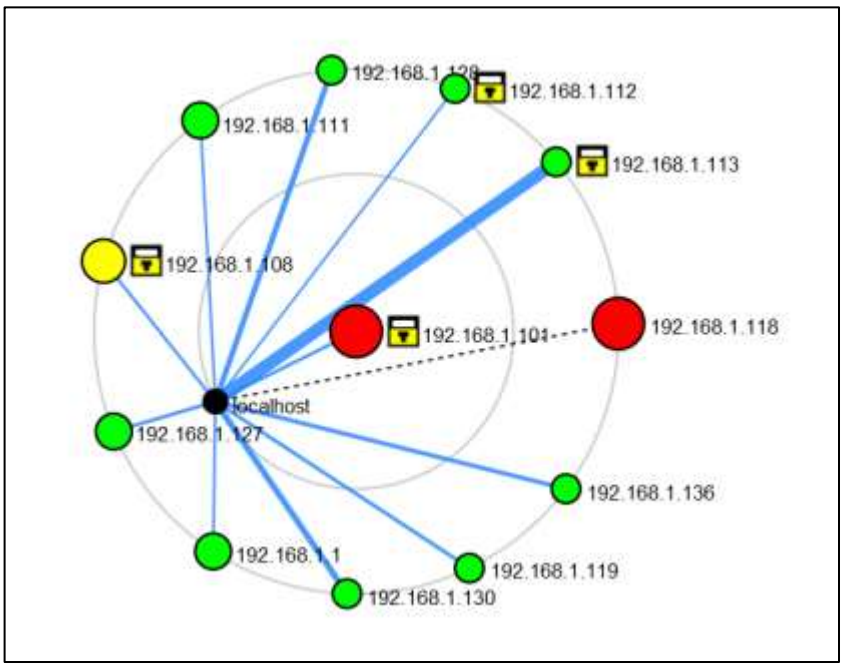


Diagrama 1. Resultado topológico del escaneo de NMap.

El diagrama # 1 muestra que existen equipos con problemas críticos de seguridad de red, como se mencionó anteriormente hay equipos que tienen muchos puertos abiertos innecesarios dando origen a vulnerabilidades peligrosas por poseer una configuración inadecuada. Este problema que se presenta en los terminales de red del GAD, establecen que necesitan ser corregidos de manera inmediata. (Ferezin, 2018)

También se pudo notar, que algunos terminales aún tienen Windows 7, como sistema operativo funcional, esto actualmente representa un gran peligro para las organizaciones que manejan grandes cantidades de información y manejan procesos importantes y confidenciales, porque a este sistema ya no cuenta con soporte. Esto representa que puedan existir muchas brechas de seguridad, vulnerabilidades de red y de configuración

que puede provocar pérdidas de información, y además retrasos en procesos de prioridad alta que se gestionen en la organización.

Las vulnerabilidades que pueden surgir de fallas de seguridad de software y hardware en el GAD municipal de Babahoyo, se deben gestionar con políticas y regulaciones utilizadas dentro de un sistema de red. Es posible describir varias fuentes importantes de vulnerabilidades que deben abordarse al crear una política de seguridad coherente.

Además de las vulnerabilidades que se han encontrado, hay problemas de administración de seguridad. Si la gestión de seguridad no está bien organizada, por ejemplo, si no se utiliza un cifrado seguro de datos seguros y cortafuegos dentro de la red, o si las políticas de seguridad del usuario no están definidas o no están controladas, el sistema de red puede experimentar problemas de seguridad.

Con el creciente número de redes inalámbricas, es absolutamente esencial planificar la seguridad comenzando desde el nivel de hardware y terminando con políticas. Los componentes centrales de la gestión de seguridad que debe tener el GAD municipal de Babahoyo deben ser la gestión de riesgos, políticas de seguridad de la información, clasificación de la información, monitoreo de seguridad y educación en seguridad para los usuarios de la institución. (Garcia-Teodoro, Diaz-Verdejo, Maciá-Fernández, & & Vázquez, computers & security, 28)

Hay tres pilares de seguridad de la información, y estos son los que debe adoptar el GAD municipal de Babahoyo en la gestión de la seguridad de la red de datos institucional, que son la confidencialidad, la integridad y la disponibilidad. Los conceptos relacionados con las personas que usan esa información son autenticación, autorización y no exención de responsabilidad. Estos son los tres resultados principales

del objetivo de toda la seguridad de la red, incluyendo evitar que entren cosas malas a la red y perturbar los ataques que superan los controles del perímetro y eventualmente superarán su firewall de defensas bien planificado e implementado.

La confidencialidad es en realidad para asegurarse de que las personas equivocadas no tengan la autorización para leer algunos de los archivos y documentos confidenciales, cuando estos archivos están siendo copiados o leídos por alguien que no está autorizado y esto se denomina pérdida de confidencialidad. Por ejemplo, los datos de investigación, los registros médicos y de seguros, las especificaciones de nuevos productos y las estrategias de inversión corporativa son absolutamente un documento confidencial, si todos estos archivos están siendo leídos o copiados por alguien no autorizado, esto causará una gran pérdida para la compañía o las personas en particular.

.

La integridad en la seguridad de la red es garantizar que todos los datos, ya sean médicos, comerciales o financieros, sean precisos. Cuando tenemos muchos archivos confidenciales guardados en nuestro sistema, tenemos que mantenerlos seguros, una vez que los guardamos; tenemos que asegurarnos de que todos esos datos e información sean precisos. Una vez que el archivo del documento o la información de especificación particular se han cambiado o leído de manera inesperada, el resultado también se conoce como pérdida de integridad en la seguridad de la red.

La disponibilidad en la seguridad de la red impide que los piratas informáticos accedan a ellos para eliminar un sistema o toda la red como para matar uno o más procesos comerciales críticos. La disponibilidad de una seguridad de red es el atributo más importante en las empresas orientadas a servicios que dependen de información útil

e importante. La información y los datos pueden borrarse o volverse inaccesibles, lo que resulta en una pérdida de disponibilidad.

El GAD de la municipalidad de Babahoyo, debe gestionar las medidas esenciales, como los procedimientos adecuados de autenticación de usuarios, la supervisión eficiente del sistema y los administradores profesionales del sistema, son solo el trasfondo del marco de seguridad. Se recomienda encarecidamente crear un documento de política separado donde se describan todas las especificaciones, reglas de acceso, procedimientos de monitoreo y control y comportamientos de los empleados. Analizando las políticas de seguridad de red y las evaluaciones de vulnerabilidad encontradas a través escaneos periódicos de la red.

Un plan de seguridad de red debe realizar monitoreo, alertas e informes sobre todos los tipos de amenazas de red a nivel interno y externo. Las medidas de protección externa incluyen defensa perimetral, segmentación de red, sistemas antimalware y de prevención de intrusos, control de acceso y configuración segura. A nivel de seguridad física, se debe prohibir el acceso no autorizado a servidores y almacenamientos de datos con información confidencial, y se deben implementar mecanismos de respaldo de datos. A nivel interno, se deben implementar medidas como la configuración segura, el control de acceso, el uso de software antimalware y preventivo de intrusos, así como la segmentación de la red. (Daswani, 2018)

# CONCLUSIONES

La red del GAD de Babahoyo, presenta deficiencias en su instalación, lo que ocasiona que existan debilidades físicas que pueden ocasionar fallas al momento de transmitir los datos y gestionar procesos. También se realizó el escaneo de red pertinente en el GAD municipalidad de Babahoyo, donde se utilizó la herramienta NMap, se encontraron varias vulnerabilidades lógicas en la configuración de los terminales de red. Existen muchos puertos abiertos que no se están utilizando, lo que puede ocasionar ataques y/o fugas de información importante para la institución.

También se pudo observar que existen equipos con sistemas operativos ya obsoletos, aunque si bien es cierto, hace poco terminó el soporte del Windows 7, se debe tomar en cuenta que cada día los piratas informáticas buscan vulnerabilidades para atacar sistemas informáticos y sustraer información importante de las organizaciones. Es por eso que mantener un sistema sin soporte es muy peligrosa para esta institución, más aun cuando esta brinda servicios públicos. Es por eso que el GAD de Babahoyo debe aplicar una política de seguridad robusta donde se gestione la correcta seguridad de la red.

La política de seguridad que tiene que implementar el GAD de Babahoyo debe contener un plan de reacción ante ataques de red e incidentes de seguridad. Dicha política debe determinar las respuestas a varios tipos de incidentes, acciones para diferentes ataques a la red. Esta política también debe determinar las personas responsables de tratar los diferentes tipos de problemas de seguridad y procedimientos de exhalación. En general, es necesario recordar que la funcionalidad de la red y la seguridad de la red funcionan con propósitos cruzados, y la clave para una protección exitosa de la red es la gestión y priorización efectiva de riesgos, el también brindar la

educación a los usuarios de la red para que no divulguen información valiosa de la institución.

## Bibliografía


Cano, J. J. (2004). Inseguridad informática: un concepto dual en seguridad informática. . *Revista de Ingeniería*, 40-44.

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Barcelona: Ediciones ENI.

Chicano Tejada, E. (2015). *Gestión de incidentes de seguridad informática. IFCT0109.* IC Editorial.

Correa, C. M., & BATTO, Y. Z. (1987). Derecho informático. *Ediciones Depalma.*

Cozmediano, L. &. (2015). Miedo al delito en contextos digitales: Un estudio con población urbana. Eguzkilore. 23, 175-190.

Daswani, D. (2018). *La amenaza hacker.* Grupo Planeta.

De La Garza, L. M. (2014). Comunicación pública en Internet. *Creaciones Copyright.*

Díaz Gómez, S. M., Díaz Miralles, M., Barrio Serrano, L., & Rodríguez Guerra, Y. (2016). Texto de parafunciones en sistema braille para pacientes ciegos y de baja visión. *Revista Archivo Médico de Camagüey*, 188-197.

DORDOIGNE, J. (2015). *Redes informáticas - Nociones fundamentales.* Ediciones ENI.

Estrada, A. C. (2016 ). *Seguridad en Redes.* DarFE.

Estupiñan, A. D., Pulido, J. A., & & Jaime, J. A. (2013). Análisis de Riesgos en Seguridad de la Información. *Ciencia, innovación y tecnología,*, 1, 40-53.

Ferezin, L. (2018). *El muro digital: Acciones disruptivas para impulsar a México.* México: Penguin Random House Grupo Editorial México.

Fisher, R. P. (1988). *Seguridad en los sistemas informáticos.* . Ediciones Díaz de Santos.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & & Vázquez, E. (computers & security, 28). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Techniques, systems and challenges*, 18-28.

Gómez, D. G. (2003). Sistemas de Detección de Intrusiones. Sistemas De Detección De Intrusiones.

González, J. (2010). *Seguridad Informática.* Madrid. .

Anexo # 1. Ficha de observación

<table>
<tr><td rowspan="2">Ficha de Observación</td><td>Caso de Estudio: Análisis para Detectar Amenazas y Vulnerabilidades en la red del GAD Municipal de Babahoyo de la Ciudad de Babahoyo.</td></tr>
<tr><td>Responsable: Amanda Julexy Muñoz Macías</td></tr>
<tr><td>Fecha: 08 de enero de 2019<br><br>Hora: 14:30<br><br>Lugar: GAD municipal de Babahoyo.</td><td>OBSERVACIÓN<br><br>Se observó una red LAN y cableado el cual no está estructurado, 1 switch, 2 router inalámbricos, 19 terminales.<br><br>El cable es UTP categoría 6. Se usa una topología en Árbol, debido conectados desde al switch a los terminales, ya la salida al internet es por medio del router. Se notó que algunos cables se están deteriorando.<br><br>Las características de las computadoras son 10 computadoras con procesado Core 2duo con 2gb RAM, disco duro de 500gb y sistema operativo Windows 7<br><br>También hay 9 Computadoras con procesador Intel Core i3, memoria de 4gb, disco duro de 500gb y sistema operativo Windows 10.</td></tr>
</table>