UNIVERSIDAD ESTATAL

PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS
Y TELECOMUNICACIONES

CARRERA DE INFORMÁTICA

TRABAJO DE TITULACIÓN

Propuesta tecnológica previa a la obtención del título de:

INGENIERO EN SISTEMAS

"ANÁLISIS PROACTIVO DE AMENAZAS DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN PARA LA INFRAESTRUCTURA DE SERVIDORES Y RED DE LA DIRECCIÓN DE TIC DE UN GAD MUNICIPAL"

AUTOR:

Abel Fabricio Ramírez Borbor.

PROFESOR TUTOR:

LSI. Daniel Iván Quirumbay Yagual, MSIA.

LA LIBERTAD- ECUADOR

2020

AGRADECIMIENTO

- Agradezco a Dios por brindarme salud y bienestar para poder finalizar satisfactoriamente este trabajo de titulación y alcanzar mi objetivo, a mis padres quienes me han guiado por el camino del bien junto con mis hermanos y amigos que siempre fueron incondicional conmigo a mi tía Viviana por apoyarme en mis primeros años de estudio en la vida universitaria.

- A mis Docentes que me impartieron su conocimiento académico durante esta etapa educativa, y a mi Director de Tesis MSc. Daniel Quirumbay, quien fue un guía profesional durante esta etapa de mi vida.

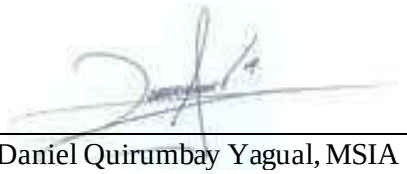
- A la Universidad Estatal Península de Santa Elena, que me ha dado la oportunidad de formarme en sus salones durante 5 años a través de las instrucciones y prácticas de sus docentes con alta experticia, a mis compañeros y docentes que estuvieron en todo mi proceso formativo para ser un profesional.

Abel Fabricio Ramírez Borbor

APROBACIÓN DEL TUTOR

En calidad de tutor de la propuesta tecnológica con título **"Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de TIC de un Gad Municipal"**, presentado por el señor egresado RAMIREZ BORBOR ABEL FABRICIO estudiante de la carrera de Tecnología de la Información, me permito declarar que luego de haber orientado, analizado y revisado, es aprobado en todas sus partes.

Particular que informo para los fines consiguientes.



Lsi. Daniel Quirumbay Yagual, MSIA

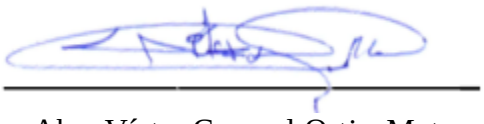
TRIBUNAL DE GRADO

Ing. Freddy Villao Santos, MSc.
DECANO DE LA FACULTAD

Ing. Samuel Bustos Gaibor, MGT.
DIRECTOR DE LA CARRERA

LSI. Daniel Quirumbay Yagual, MSIA.
PROFESOR TUTOR

Ing. Iván Coronel Suarez, MSc.
PROFESOR DEL ÁREA



Abg. Víctor Coronel Ortiz, Mgt.
SECRETARIO GENERAL

RESUMEN

La presente propuesta tecnológica tiene como finalidad implementar políticas de seguridad con plantillas SANS para un Gad Municipal en el área de Tecnología e Información, el cual no dispone de políticas de seguridad en caso de ataques cibernéticos que permitan la continuación de las operaciones y servicios de manera eficiente. Los mecanismos de seguridad de información carecen de eficiencia por la falta de documentos e informes escritos que garanticen actividades de contingencia en caso de ataques externos.

Por tal razón, resulta esencial implementar Políticas de Seguridad (SANS), que abarquen un conjunto de medidas, técnicas y posibles soluciones indispensables para la continuidad de las operaciones dentro de la empresa.

El objetivo general que persigue el proyecto es la elaboración de Políticas de Seguridad SANS con base en las plantillas establecidas, los cuales están basados en estándares internacionales como: ISO/EC, ISO/IEC/ 27001, SANS Security Policy, que proporcionan un análisis efectivo de impactos sobre la organización yfacilitan estrategias de recuperación para afrontar de manera oportuna las eventualidades que se presenten. Además, se manejó la metodología para identificación de vulnerabilidades OSSTMM, la misma que consta de 6 ítems, enfocada en la seguridad de la información, donde está basada en la planeación, descubrimiento, ataque y reporte, cuatro fases que permitirán examinar y emitir informes detallados con respecto a las vulnerabilidades del sistema encontradas, los mismos que serán de utilidad para la toma de decisiones respecto a mitigación de daños que puedan provocar.

Los resultados esperados son las medidas de contingencia con base en las políticas establecidas, para la reducción de ataques se puedan presentar mediante el uso de dominios de control y metodologías de vulnerabilidades basados en normas internacionales que agilicen las posibles soluciones a los problemas encontrados.

Palabras claves: Políticas de seguridad, vulnerabilidad, ataques cibernéticos, mitigación, dominios de control.

ABSTRACT

This technological proposal aims to implement security policies with SANS templates for a Municipal Gad in the area of Technology and Information, which does not have security policies in case of cyber-attacks that allow the continuation of operations and services efficiently. The information security mechanisms lack efficiency due to the lack of written documents and reports that guarantee contingency activities in case of external attacks.

For this reason, it is essential to implement Security Policies (SANS), which cover a set of measures, techniques and possible solutions that are indispensable for the continuity of operations within the company.

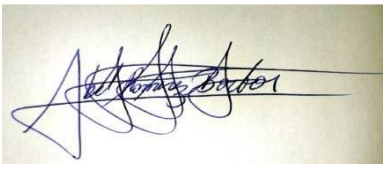
The general objective of the project is the development of SANS Security Policies based on the established templates, which are based on international standards such as: ISO/EC, ISO/IEC/ 27001, SANS Security Policy, which provide an effective analysis of impacts on the organization and facilitate recovery strategies to address in a timely manner the eventualities that arise. In addition, the methodology for the identification of OSSTMM vulnerabilities was used, which consists of 6 items, focused on information security, where it is based on planning, discovery, attack and reporting, four phases that will allow the examination and issuance of detailed reports regarding the system vulnerabilities found, which will be useful for decision making regarding the mitigation of damage they may cause.

The expected results are the contingency measures based on established policies, for the reduction of attacks can be presented through the use of control domains and methodologies of vulnerabilities based on international standards that streamline the possible solutions to the problems found

Keywords: Security policies, vulnerability, cyber-attacks, mitigation, control domains.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



RAMÍREZ BORBOR ABEL FABRICIO

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Las nuevas tecnologías han dado un salto cualitativo y cuantitativo, con la aparición y desarrollo acelerado de las innovaciones en las telecomunicaciones, la informática y el internet; con múltiples y variadas consecuencias que, a la vez que llegan a todos los puntos y sociedades del planeta, hacen de la inmediatez y facilidad de la comunicación su principal virtud [1].

Son tantos los aspectos y cuestiones que proporciona las TICs, que hoy en día se hace difícil más bien imposible, pensar un mundo sin las nuevas tecnologías de la información y comunicación. Si el fuego fue el inicio de la civilización humana y la máquina de vapor el arranque de los tiempos modernos industriales, la nueva realidad configurada por las Nuevas Tecnologías de la Información y la Comunicación nos lleva a un nuevo grado de civilización, a una nueva sociedad que aún está dando sus primeros pasos, cambiante y en rápida evolución y que puede llegar muy lejos en la historia de la Humanidad. Todo depende cómo sepamos y queramos utilizar las nuevas herramientas [1].

Los ataques cibernéticos han crecido de una manera exponencial estos últimos años, por las brechas de seguridad que poseen algunos programas o servidores, los ataques más comunes en los sistemas informáticos son denegación de servicio, secuestro de información, robo de dinero, espionaje, etc. Todos estos ataques son combinados para un objetivo en específico, en cual hay sistemas operativos que el antivirus que posee no puede detectarlas para su respectiva alerta [2].

En la actualidad estos ataques conllevan a diversas empresas e instituciones crear Plantillas de seguridad ya sea estas SANS u otras para el control de vulnerabilidades encontradas.

La finalidad del proyecto conllevaba principalmente a la realización de un análisis proactivo de amenazas informáticas utilizando la metodología de identificación de vulnerabilidades OSSTMM para determinar las posibles vulnerabilidades que pueden sufrir los sistemas de información, eligiendo de esta forma las vulnerabilidades más significativas dentro de la institución con la intención de solucionarlos.

CAPÍTULO I

1. Fundamentación

1.1 Antecedentes

La seguridad en los sistemas informáticos es una cuestión de gran importancia que viene siendo objeto de estudio desde 1970. El concepto de seguridad hace referencia a las medidas y al control destinados a la protección contra la negación de servicio y la ausencia de autorización (ya sea de forma accidental o intencionada) para descubrir, modificar, destruir datos o sistemas [3].

Al menos 74 países se han visto infectados por unos 45.000 ataques de un malicioso programa informático que encripta las computadoras y demanda dinero para desbloquearlas. Este virus afecto a hospitales en Inglaterra, empresas de EEUU, Canadá, China, Italia, Taiwán y Rusia., cuyo objetivo es 'secuestrar los archivos de una computadora para posteriormente pedir su rescate' a los usuarios a cambio de una suma de dinero cuyo valor puede ser pagado por bitcoin o transacción bancaria. La compañía rusa de seguridad informática Kaspersky ha detectado más de 45.000 ataques en 74 países alrededor del mundo. Medios comunican que compañías como Telefónica en España y Megafon en Rusia se han visto afectadas [3].

Un promedio de 133 ataques cibernéticos por segundo se registró en instituciones del Estado Ecuatoriano desde el pasado jueves 11 de abril del 2019, con la intención de saturar las páginas de internet y de esta manera paralizar los servicios públicos [3].

Portales como los del Servicio de Rentas Internas (SRI), Ministerio de Relaciones Exteriores, Consejo Nacional Electoral (CNE), Gobiernos Autónomos Descentralizados, Ministerio de Turismo, entre otros, resultaron afectados. Existen empresas que brindan servicios de pentesting informático en la red informática, como es CISCO, Aner, Symantec que han elaborado investigaciones, análisis y estudios sobre el tema [4].

Hoy en día toda entidad pública del estado ecuatoriano está expuesta a ataques por piratas cibernéticos en la red, esto puede ser por medio de spam, correos electrónicos, dispositivos conectados a la red como impresoras, pc, etc. Uno de los casos es el del Municipio de Baltimore en el Departamento de Obras públicas en EE. UU, que ha sido propenso de secuestro de información de vital importancia de la Empresa, dejando inoperable el funcionamiento de la entidad y expuesto a que toda su información sea revelada, algunas de ellas de alta confidencialidad [5].

Ecuador se encuentra en el puesto 31 de la escala mundial de ataques cibernéticos según la compañía de seguridad informática kaspersky, esto tras quitar el asilo político a Julian Assange, Hasta la fecha se han registrado más de 40 millones de ataques cibernéticos, de los 20 millones en promedio que se reciben. Los ataques provienen de EE.UU., Brasil, Holanda, Alemania, Francia, Austria, Reino Unido incluso de Ecuador [6].

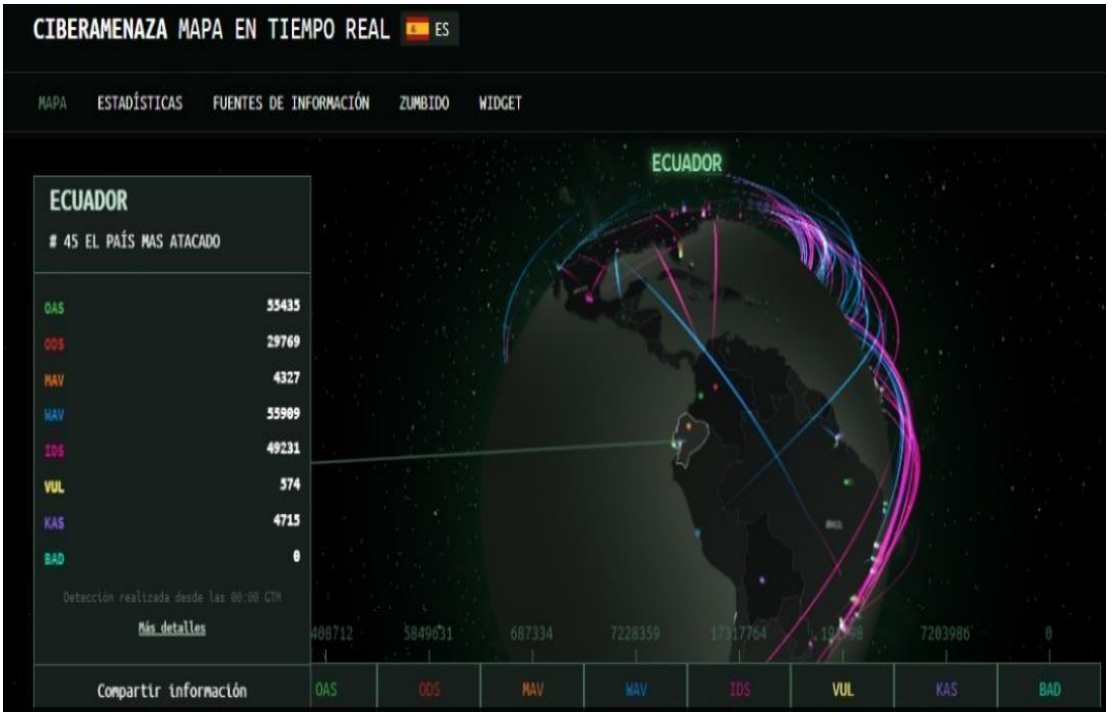


Fig. 1 Kaspersky monitoreo en tiempo real día 6 de septiembre del 2020 a las 19:31 pm hora Ecuador [7].

El departamento de Tecnologías de la información y la comunicación (TIC) del Gad Municipal, en los años anteriores ha establecido controles y mecanismos para la seguridad informática y seguridad de la información, pero como ya entendemos cada proceso trae puntos positivos y negativos; en esta situación la empresa "El Gad Municipal" necesita una auditoria/consultoría informática debido a que en sus sistema de administración de seguridad de la información (SGSI) hay falencias ya determinados como controles mal implementados y una mala gestión de la red, presentando pérdidas o fugas parciales de información de alta consideración para el negocio.

Los problemas que frecuentemente se dan en la entidad pública, son la mala asignación de IP a las máquinas, provocando IP repetidas causando que uno de los usuarios no tenga acceso a la red o al sistema. Actualmente la institución tiene un

sistema que monitoriza el ingreso de usuarios hora y fecha de conexión y la desconexión de ella, este sistema de control de usuarios esta realizado en java, este procedimiento maneja Spring Security, un Framework que permite gestionar todo referente a la seguridad en aplicaciones web, esto ayuda a salvaguardar la información del empleado y de la empresa en caso de ataques externos e internos.

La mala distribución y asignación de usuarios y claves para el manejo en los equipos de computación para el personal administrativo son uno de los mayores problemas que posee la entidad debido a que esto puede ser manejados por personas tanto internas como externas con el fin de extraer la información y usarla para usos indebidos.

Los avances de las Tecnologías de la Información y Comunicación (TIC) han hecho que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias instituciones y minimizar riesgos derivados de vulnerabilidades informáticas. Las Tecnologías de la Información y la Comunicación (TIC) son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información, y como respuestas a la necesidad gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, emitió Acuerdos Ministeriales No. 804 y No. 837 de julio y 19 de agosto de 2011 respectivamente de las Tecnologías de la Información y Comunicación según el Instituto Nacional de Evaluación Educativa del Estado Ecuatoriano [8].

Este estudio de análisis proactiva de amenazas tiene una gran similitud con el análisis y gestión de vulnerabilidades de sistemas informáticos, debido a que se encargan de la seguridad de la infraestructura organizacional de la empresa, usando técnicas que permitan controlar la seguridad de la información mediante el uso de herramientas de código abierto (OpenSource) [9].

Los riesgos de información a la seguridad informática que están expuestas las empresas de Ecuador surgen, cuando están presentes dos elementos: amenazas y vulnerabilidades. Ambas están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia de la otra. “Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan” [10].

Este proyecto busca la realización de pruebas de test de penetración a la red de datos para el diagnóstico de vulnerabilidades, en la infraestructura de red y en los servidores que posee el Gad Municipal en su departamento de TIC para salvaguardar la información interna de la empresa

Dado el estudio realizado de las vulnerabilidades que posee la entidad, se procederá a elaborar un plan estratégico para dar posibles soluciones a los problemas que son presentados en la red del Gad Municipal, estos estarán basados en plantillas de seguridad SANS (SysAdmin Audit, Networking and Security Institute) que están establecidos en normas y protocolos de seguridad, para así minimizar los riesgos de ataques contra intrusos en la institución. Por ende, esta propuesta tecnológica ha sido nombrada como "Análisis proactivo de amenazas de la seguridad informática y seguridad de la información para la infraestructura de servidores y red de un Gad Municipal".

1.2 Descripción del proyecto

Para el desarrollo de procedimientos de detección proactiva de amenazas se basará en el modelo de pruebas de pentesting o "test de penetración", y la metodología para identificación de vulnerabilidades como es OSSTMM (Manual de metodología de prueba de seguridad de código abierto) [11], El OSSTMM se centra en los detalles técnicos de exactamente qué artículos necesitan ser probados; qué hacer antes, durante y después de una prueba de seguridad; y cómo medir los resultados. Para esto se toma en cuenta sus fases y etapas que son adaptables a la guía del trabajo, en el análisis de las vulnerabilidades en la infraestructura de red [11].

La estructura del proyecto consta de un hibrido entre el modelo Pentesting y metodología para identificación de vulnerabilidades, también está basado en la guía de funcionamiento de un programa eficaz de las pruebas de penetración CREST [11]:

1.2.1 Recolección de información

En esta fase de la detección proactiva se perpetrará la recolección de toda la información posible del departamento de TIC´s del GAD Municipal disponible, conocer su estructura organizacional y como funciona su modelo de negocio, para así poder ver las posibles vulnerabilidades en los que se encuentra expuesto la empresa y la obtención de documentos de protocolos de seguridad si en el caso existiera. Este trabajo se realizará obteniendo información a través de entrevistas y encuestas a los entes que forman la institución en el departamento de TIC´s. (Ver anexo 1)

El diseño de la infraestructura de red del GAD Municipal está realizado con herramientas de la marca CISCO, el cual ha implementado equipos de alta gama en la comunicación y el acceso a internet ayudando a tener un acceso seguro a través de la red, posee un cuarto de servidores único para estos, los cuales son: Router, Switch, Catalyst, etc. Todos estos son de la marca CISCO, su topología de red es estrella, donde las computadoras que accedan a ella están conectadas a un punto central. La comunicación que se realiza en cada departamento es a través de la telefonía IP (esto significa que se envía señal de voz en forma digital en paquete de datos).

1.2.2 Identificación de Vulnerabilidades

Planificación

Planificar como se va a desarrollar el proceso de identificación de vulnerabilidades para ello debemos:

- Identificación de la infraestructura de red en la que se encuentra uno o varios servidores de la institución, conocer su configuración la tecnología que posee y la seguridad que brinda para salvaguardar la información.
- Obtener un inventario del servidor, el cual tendrá como datos:
    - ✓ Software instalado
    - ✓ Servicios que presta
- Usuarios que acceden al servidor, así como las tareas o procesos que realizan.
- Identificar los puertos que el servidor está utilizando según cada aplicación o herramienta instalada.

Para realizar la estructura de red, los usuarios, los puertos utilizados y que servicios presta el servidor se definirá un horario para la ejecución de las herramientas de identificación de vulnerabilidades, debido a que muchas de estas producen un bloqueo o denegación en los servicios y prestación de los servidores.

La información obtenida se deber adjuntar y guardar en un formato establecido.

Identificación y análisis

Se procederá al proceso de identificación y análisis de vulnerabilidades, para ello existen dos entornos para la identificación de vulnerabilidades en los servidores, que son:

Identificación de vulnerabilidades Interno, entorno privilegiado.

El ambiente interno dentro de la red, el cual debe tener los permisos necesarios para poder ejecutar las herramientas y consumir el recurso y servicios prestados por los servidores.

Herramientas de identificación de vulnerabilidad internas

La utilización de estas herramientas es una forma eficaz de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Para la verificación manual de eliminar falsos positivos, y descubrir el flujo de datos de entrada y salida del servidor. De los cuales se nombra algunos de ellos a continuación:

- Nessus
- Dmitry

Estos programas utilizados para detectar vulnerabilidades en los sistemas poseen una interfaz sencilla para el usuario y de fácil instalación, además nos indica las vulnerabilidades del sistema escaneado de una forma detallada y precisa con una solución brindada en formato pdf, son software libre con limitaciones en el caso de Nessus que brinda más herramientas tiene un costo por los servicios.

Según el departamento de ciencias de la computación de la Universidad Estatal de Carolina del Norte de EEUU, nos dice que los tipos de vulnerabilidades se pueden clasificar en dos partes los cuales son Implementación de errores o fallas de diseño.

El CWE (Common Weakness Enumeration) significado es una lista desarrollada por la comunidad de debilidades de seguridad de software comunes. Sirve como un lenguaje común, un dispositivo de medición para herramientas de seguridad de software y como una línea de base para la identificación de debilidades, mitigación y esfuerzos de prevención [12].

CWE-79: Neutralización incorrecta de la entrada durante la generación de la página web ('Secuencia de comandos entre sitios'), esto se da cuando se obtiene los datos de un usuario y no está correctamente validado, lo que permite al código ser inyectado en la aplicación y posteriormente mostrado a un usuario final. CWE-89: Neutralización incorrecta de elementos especiales utilizados en un comando SQL ('Inyección SQL'), ocurren cuando la entrada del usuario no se valida correctamente y la entrada se usa directamente en una consulta de base de datos.

No validar la entrada permitirá a un usuario malicioso manipular directamente los datos devueltos por la base de datos con el fin de obtener información potencialmente confidencial. CWE-242: Uso de la función inherentemente peligrosa, la vulnerabilidad se produce cuando se utiliza un método dentro de código inherentemente inseguro. Tales métodos o las funciones no deben usarse, porque los atacantes pueden usar conocimiento del dominio público o funciones con vulnerabilidades conocidas con el objetivo de explotar dichas debilidades en la aplicación. CWE-22: Limitación incorrecta de un nombre de ruta a un directorio

restringido ('Recorrido de ruta'), ocurre cuando se permite a los usuarios ver archivos o carpetas fuera de los previstos por la aplicación. CWE-209: Exposición de información a través de un mensaje de error, esto se produce cuando se muestra información o un error directamente a un usuario.

Estos errores pueden contener información confidencial o incluso credenciales de autenticación a los sistemas de los usuarios, lo cual esto permitirá a los atacantes dar un mayor acceso a la aplicación. Un error al establecer el atributo HTTPOnly permite mitigar el riesgo de scripts del lado del cliente, el acceso no http a las cookies del navegador. Dicha vulnerabilidad permite que el código del lado del cliente pueda acceder a las cookies, permitiendo el acceso a la información de la sesión u otra información confidencial datos a ser robados en scripts de sitios o ataques de phishing.

CWE-472: Control externo del parámetro web inmutable supuesto, ocurre cuando los datos en campos ocultos no se validan correctamente y el campo es implícitamente confiable. Confiar en esta forma de entrada del usuario puede generar problemas como SQL injection y cross site scripting, o puede permitir información inexacta para ser insertada en la base de datos.

CWE-78: Neutralización incorrecta de elementos especiales utilizados en un comando del sistema operativo ('Inyección de comandos del sistema operativo'), ocurre cuando la entrada del usuario se ejecuta directamente. Esta vulnerabilidad permite que los usuarios maliciosos puedan ejecutar directamente comandos en el host como usuario de confianza. CWE-285: Autorización incorrecta, la vulnerabilidad ocurre cuando el acceso a una característica particular no está

protegido, otorgar acceso a recursos a cualquier persona, incluidos usuarios malintencionados o funcionalidad. zzCWE-778: registro insuficiente, la vulnerabilidad se produce cuando un evento crítico no se registra. CWE-501: Infracción de límites de confianza, se produce cuando se confía en los datos no confiables se mezclan en una estructura de datos. CWE-434: Carga sin restricciones de archivo con tipo peligroso, puede ocurrir cuando el sistema no está diseñado adecuadamente para manejar archivos potencialmente maliciosos. CWE-400: Consumo de recursos no controlado, la vulnerabilidad existe cuando un sistema no impone restricciones o límites en la cantidad de recursos que un usuario es capaz de solicitar. Potencialmente, esto puede conducir a la denegación de servicio, ya que los recursos pueden ser atados arbitrariamente con poco esfuerzo.

Identificación de vulnerabilidades Externo, entorno no privilegiado

El entorno en este caso se constituye de un ambiente fuera de la red accediendo a los servicios y recursos de los servidores vía internet, mediante una conexión externa. Por el cual se tendrán muchos bloqueos de seguridad como el firewall y todos los equipos de seguridad tanto hardware como software que impiden el acceso libre a los recursos.

Herramientas de identificación de vulnerabilidad externas

Las herramientas permitirán realizar escaneo fuera de la red, para buscar agujeros donde podrían presentar incidentes. A continuación, se nombrará las aplicaciones que se utilizaran para el análisis, algunas vienen embebidas en el sistema operativo Kali Linux y son de gran beneficio para realizar pruebas de seguridad. También se utilizarán otras aplicaciones que son externas a Kali Linux, algunas de las cuales son pagadas, pero con versiones con cierta funcionalidad gratuita para la comunidad.

- ISS Internet Scanner (Aplicación Externa)

- A2SV (Aplicación Externa)
- Uniscan (Kali Linux)
- WhatWeb (Aplicación Externa)

- Lynis (Aplicación Externa)
- D-TECT (Aplicación Externa)
- Nessus Security Scanner (Aplicación Externa)
- Retina Network Security Scanner (Aplicación Externa)
- Nmap (Kali Linux)

1.2.3 Análisis de vulnerabilidades

Se debe evaluar de todos los resultados obtenidos, en especial las coincidencias con secuelas observados con anterioridad, para así compararlos con el de todas las herramientas, luego de ello se procede a listar las vulnerabilidades aceptadas y analizadas en la Tabla de registro de Vulnerabilidades.

Gestión

De cada escaneo que se realizara tanto interno como externo se adquiere una tabla de vulnerabilidades las cuales se deben analizar para separar los falsos positivos y los falsos negativos de las vulnerabilidades reales, este análisis se llevara a cabo en base a todo el conjunto de información presentado por las diferentes herramientas utilizadas.

Según el reporte anual de ciberseguridad de CISCO 2018 nos dice que los ataques más comunes en las organizaciones los loT (Internet de las cosas) y DDoS (Denegación de Sericio) [13].

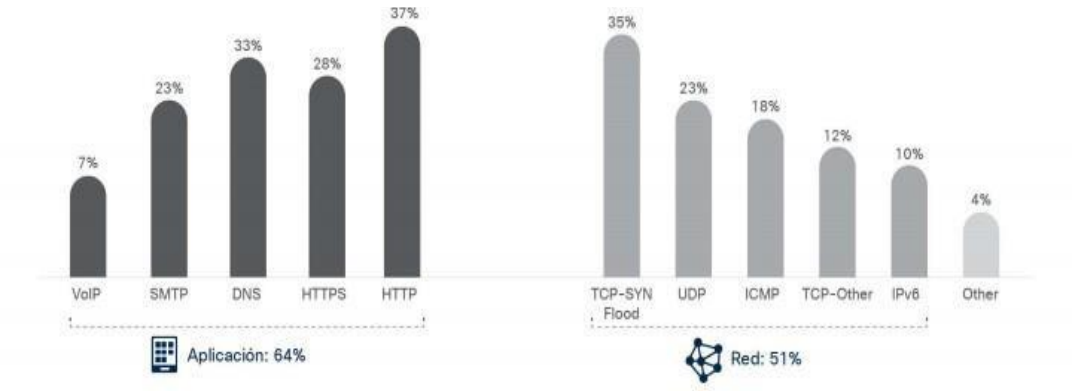


Fig. 1 Los ataques DDoS aumentó en 2017[13].

Categoría de amenaza	Ene-Sep 2016	Ene-Sep 2017	Cambio
CWE-11 9: Errores del búfer	493	403	(-22%)
CWE-20: Validación de entrada	227	268	+15%
CWE-264: Permisos y privilegios de acceso	137	163	+18%
CWE-200: Fuga / divulgación de información	125	250	+100%
CWE-310: Temas criptográficos	27	17	(-37%)
CWE-78: Inyecciones de comando del OS	7	15	+114%
CWE-59: Siguiente enlace	5	0	

Fig. 2 Actividad de la categoría de amenaza CW [13].

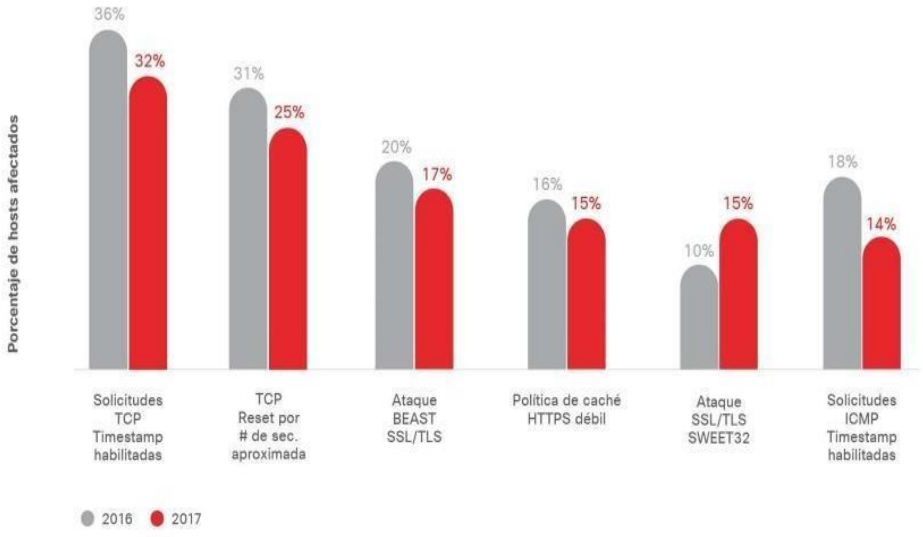


Fig. 3 Vulnerabilidades de baja gravedad más a menudo detectadas, 2016 – 2017[13].

Fig. 4 Principales 10 extensiones de archivos maliciosos, enero a septiembre de 2017[13].

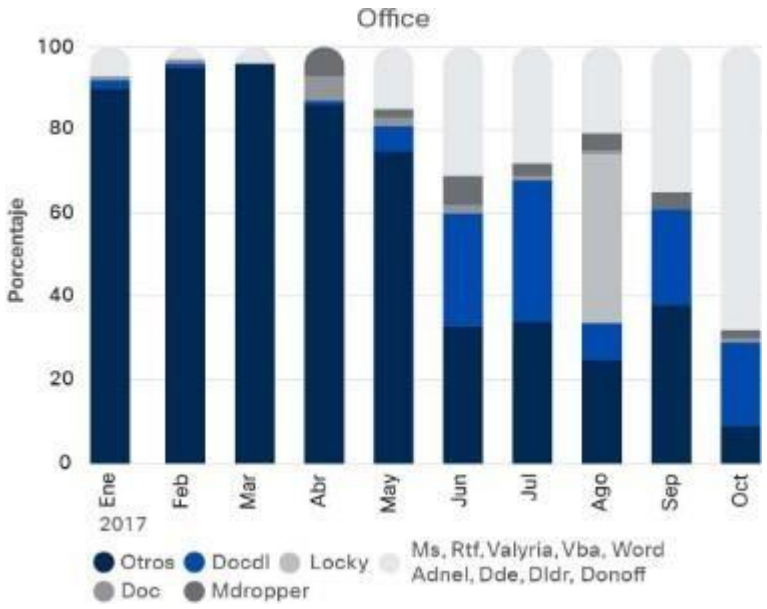


Fig. 5 Tres tipos principales de extensiones de archivos maliciosos y relaciones familiares de malware [13].

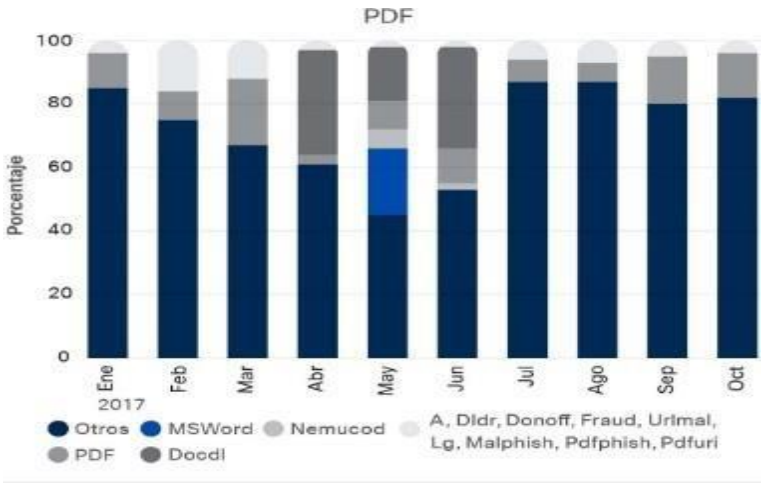


Fig. 6 Tres tiposprincipales de extensiones de archivos maliciosos y relaciones de familias de malware [13].

Identificación de la acción que se aprovecha de la vulnerabilidad

La identificación de vulnerabilidad que pueden causar daños y bajas en los recursos que posee la empresa, como son los servidores su configuración, con los servicios que presta en donde cada vulnerabilidad puede ocasionar daños físicos o lógicos. [14]

Posibles soluciones a vulnerabilidades Encontradas

Investigación de vulnerabilidad y verificación

Una vez identificadas las vulnerabilidades en el departamento de TIC del GAD Municipal, procedemos a clasificarlas según su tipo de riesgo, ya sean estos en servidores, aplicaciones de escritorio o en aplicaciones web, dentro del departamento de TIC´s del GAD Municipal, donde se escogerán las 10 más críticas, para la búsqueda de posibles soluciones, según lo demande cada vulnerabilidad encontrada, para ello nos valemos del estado de cada vulnerabilidad presentado en el reporte según la herramienta utilizada, ya que en este consta el correctivo de las falencias encontradas.

1.2.4 Presentación de la información e informe final

Este proceso indica el final del ciclo de la identificación de vulnerabilidades; en el que se deben presentar a cada administrador de los servidores el informe final juntamente con los registros de vulnerabilidades y los correctivos que se deben aplicar.

En el informe final se establecerán políticas para las soluciones de las vulnerabilidades encontradas en la red, las cuales estarán basadas en Plantillas de Política de Seguridad (SANS). Se entregará en el documento las recomendaciones que puede ayudar a las correcciones de las fallas encontradas.

Instituto de seguridad de la información (SANS)

Es la fuente más grande y confiable en proveer una buena certificación de seguridad de la información en el mundo. Este instituto brinda diferentes temas, políticas o controles disponibles en las tecnologías avanzadas, redactadas por excelentes

especialistas en el ámbito de Sistemas, Auditoria, Redes y Seguridad. Cabe mencionar que Sans está encargado indispensablemente en desarrollar, mantener, actualizar y poner a disposición la mayor serie de documentos de investigación sin costo alguno.

Los recursos de SANS Security Policy tienen como objetivo principal conceder plantillas y herramientas necesarias aproximadamente para 27 aspectos relacionados con el desarrollo e implementación de políticas de seguridad informática.

Según SANS, Una política es típicamente un documento que describe los requisitos o reglas específicas que se deben cumplir [15].

1.3 Objetivos

1.3.1 Objetivo General

Detectar vulnerabilidades en la infraestructura de servidores y red en el Departamento de TIC del GAD Municipal, mediante el uso de diferentes herramientas de software libre OpenSource, para mejorar la seguridad de la información de la empresa.

1.3.2 Objetivos Específicos

- Identificar las diferentes herramientas de software libre para efectuar escaneos y análisis en la infraestructura de red del departamento de TIC del GAD Municipal.

- Identificar y analizar las vulnerabilidades más críticas que pueden existir y comprometer el manejo de información en los sistemas de procesamientos de datos de la institución.
- Elaborar informes técnicos de los resultados obtenidos con el escaneo de vulnerabilidades y del grado de incidencia de inseguridad de la información en la Infraestructura de Tecnología del departamento de TIC's del Gobierno Autónomo Descentralizado Municipal.
- Sugerir la implementación de políticas de seguridad aplicando plantillas de SANS (Instituto de Auditoría, Redes y Seguridad SysAdmin) y estándares en los sistemas de información de la empresa para proteger los datos de la empresa.

1.4 Justificación

Actualmente el departamento de informática y tecnologías de Sistema de Información del GAD Municipal, no cuenta con políticas de seguridad estandarizadas, que garanticen minimizar los riesgos que estos puedan causar, por lo tanto, se requiere el planteamiento de políticas de seguridad que faciliten el control de errores, para ello se tiene una carta de aprobación por parte de la Municipalidad, entregada la Facultad de Sistemas y Telecomunicaciones, en la dirección de informática, este documento no se adjunta como anexo para salvaguardar la seguridad de la Institución.

Con la implementación de las políticas de seguridad podrá gestionar las posibles soluciones a las vulnerabilidades encontradas y tomar en cuenta las recomendaciones dadas, para la toma de decisiones. Esto servirá como guía para las

posibles auditorias informáticas que el Estado hace a los GAD Municipales de la Provincia.

Con el desarrollo del uso de las tecnologías TIC en las empresas públicas y privadas, y la aparición de los inconvenientes de seguridad que acarrea la utilización de estas, da la necesidad de la utilización de técnicas que permitan vigilar la seguridad de los datos debido a que un desempeño defectuoso de los mismos puede ocasionar en una fuga de información que pueda causar pérdidas económicas para la compañía [16].

Todos los días las instituciones públicas están sometidas a peligros que ponen en riesgo la integridad de la información que manejan y con ello la viabilidad de estas. Estos peligros no únicamente surgen del exterior sino además del interior de las mismas organizaciones por lo cual para trabajar de manera segura se requiere garantizar los datos y la información de valor con asistencia de un Sistema de Seguridad de la Información.

La seguridad informática tomó enorme apogeo, gracias a las cambiantes condiciones tecnológicas que se da día a día. La oportunidad de interconectarse por medio de redes ha abierto nuevos horizontes a las instituciones para mejorar su eficacia de producción y poder examinar más allá de las fronteras nacionales, lo cual lógicamente trajo consigo, la aparición de diversas amenazas para los sistemas de información.

Estos peligros que día a día aparecen, hacen que se desarrolle un documento de políticas de seguridad que orientan en la utilización correcta de estas destrezas tecnológicas y sugerencias para conseguir el más grande beneficio de estas virtudes,

y evadir la utilización indebida de la mismas, lo cual puede ocasionar serios inconvenientes a los bienes, servicios y operaciones del Gobierno Municipal, y la información obtenida va a servir como utilidad primordial para futuras auditorias informáticas que el estado ecuatoriano realice a la empresa.

Esta detección proactiva tiene como finalidad dar las posibles soluciones a los problemas que puede estar enfrentando el departamento de TIC´s del GAD Municipal. Dichas soluciones se basarán en normas y protocolos estandarizados que permitan una óptima regularidad para salvaguardar la información que se encuentre comprometida por una vulnerabilidad.

La detección de las vulnerabilidades que se testearan en la infraestructura de red del GAD Municipal tiene como propósito detectar vulnerabilidades en la que pueda estar comprometida, los datos el departamento de TIC´s, para posterior a ello analizar esos datos y tomar decisiones que ayuden a la solución del problema que ha sido presentado.

El presente proyecto está alineado a los objetivos del Plan Nacional de Desarrollo específicamente los siguientes ejes:

Eje1.- Derecho para todos Durante una Vida [17].

Objetivo 8.- Promover la transparencia y la corresponsabilidad para una nueva ética social [17].

Política 8.3.- Impulsar medidas para la prevención, control y sanción de conflictos de interés y opacidad en las contrataciones y servicios del estado [17].

Meta

Mejorar los índices de percepción ciudadana sobre la corrupción en los sectores públicos y privados:

Eje2.- Economía al servicio de la sociedad [17].

Objetivo 5.- Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [17].

Política 5.6.- Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación ente el sector público, productivo y las universidades [17].

Estas políticas y lineamientos del buen vivir dan un buen equilibrio socioeconómico entre los ciudadanos, conllevando a ser más competitivos, esta propuesta tecnológica ayuda a promover la transparencia en el ámbito informático, ayudando a la protección de datos e impulsando el cambio productivo.

1.5 Alcance del Proyecto

La implantación de Políticas de Seguridad SANS, permitirá el control del cumplimento de las reglas estándares y procedimientos que de cumplirse al encontrarse con las vulnerabilidades en los sistemas de información.

Con las Plantillas de Seguridad se podrán estudiar las amenazas encontradas para determinar el factor riesgo que poseen y como esto puede afectar a la empresa, conllevando a la toma de decisiones de los sistemas de información.

El presente proyecto abarcara las siguientes fases:

- Fase de recolección de información
- Fase de identificación de vulnerabilidades
- Fase de análisis de vulnerabilidades
- Fase de reportes

El estudio de las vulnerabilidades encontradas permitirá visualizar los ataques más frecuentes a lo que está expuesto la empresa, cabe indicar que este análisis en profundidad no está direccionado a crear software o sistemas de antivirus para combatir las vulnerabilidades a los sistemas o servidores.

Las plantillas de seguridad SANS ayudaran al control de manejo de las vulnerabilidades, para minimizar el riesgo de pérdida de información, esto no asegurar la solución óptima al problema encontrado.

1.6 Metodología

1.6.1 Metodología de Investigación

La metodología de la investigación tiene como propósito mostrar los elementos indispensables para la búsqueda, recolección e interpretación de los datos, lo cual es de esencial consideración para el avance del proyecto [14].

Se utilizará la metodología de investigación diagnóstica para conocer los procesos de la gestión del GAD Municipal, donde las técnicas que se utilizarán para la recolección de información serán la encuesta y la entrevista, estas investigaciones serán llevadas a cabo tanto a empleados del departamento de sistemas (usuarios internos) como a los empleados de la Institución (usuarios externos); en tanto que las entrevistas se las realizó al director del departamento de informática del

Municipio. Los instrumentos asociados a las técnicas para catalogar aclaraciones antes nombradas fueron el cuestionario y la guía de entrevista.

Para el desarrollo de la propuesta se utilizará la metodología de investigación exploratoria por el motivo que actualmente existe poco estudio entre las tecnologías y la gestión de políticas de seguridad en los Gobiernos Municipales. Se realizará un análisis de las vulnerabilidades que comprometan la información de la empresa, además se indagará información con el objetivo de poder realizar una comparación entre nuestra propuesta y los diferentes planes de seguridad de políticas existentes en los municipios.

1.6.2 Metodología para la identificación de vulnerabilidades

Para que tenga éxito el proceso de identificación de vulnerabilidades en las redes de datos se deben enmarcar varios aspectos que se relacionan entorno a la seguridad y que son de vital importancia para los administradores de los mismos, de tal forma que se pueda delimitar el problema y nos permita meternos de lleno en la seguridad garantizando el cumplimiento de confidencialidad, integridad, disponibilidad y autentificación. A este proceso se lo ha dividido en cuatro fases que son [18]:

- Recolección de Información
- Identificación de vulnerabilidades
- Posibles soluciones
- Reportes

Fig. 7 Proceso de Identificación de las Vulnerabilidades [18].

Autor: Ramírez Borbor Abel

1.6.3 Metodología para el Desarrollo del Proyecto

Para el desarrollo de las políticas de seguridad se utilizó la metodología OSSTIMM (Open Source Security Testing Methodology Manual), que es una prueba de penetración que evalúa la seguridad el nivel de riesgo y también describe los pasos a seguir antes, durante y después de la prueba de penetración [19].

Para el estudio de esta propuesta se propone utilizar la metodología para la identificación de vulnerabilidades y las fases de Pentesting.

Esta metodología OSSTMM, consta de 7 fases, el proyecto posee las fases más primordiales de acuerdo con las necesidades que se plantea en el Pentesting, como son Descubrimiento, Investigación y verificación de vulnerabilidades, Valor de evaluación de riesgo, Reportes:

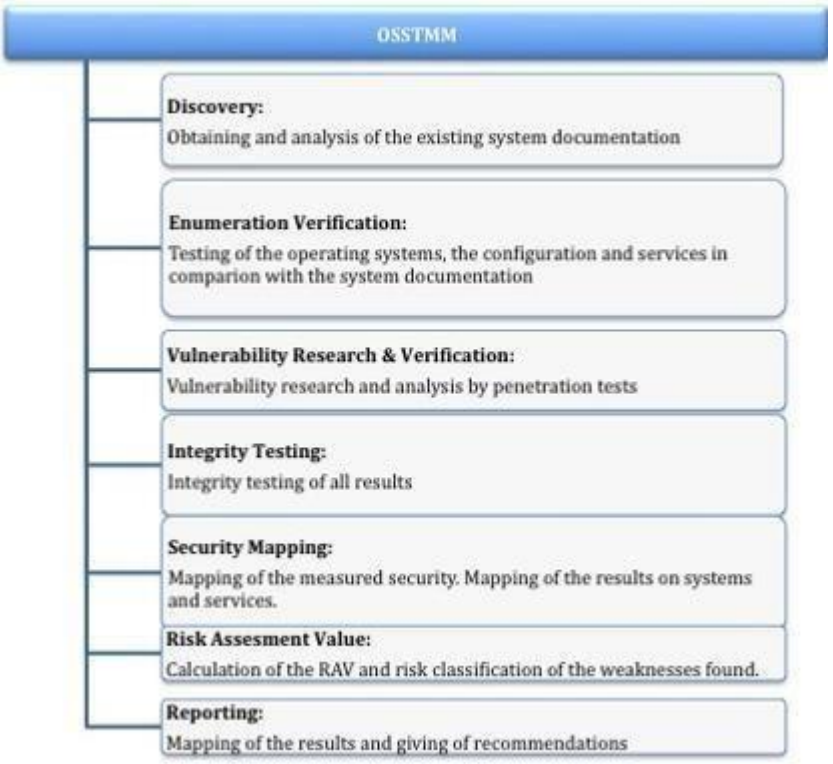


Fig. 8 Metodología OSSTMM [18].

1.6.4 Análisis de Resultados de Encuestas

La encuesta fue dirigida a aquellos usuarios que serán beneficiados directamente con el proyecto, en nuestro caso las personas que hacen el uso de las aplicaciones y servidores del GAD Municipal. Se realizado dos encuestas dirigidas al Departamento de informática y tecnología y otra al Jefe de Dirección, teniendo un alcance de 6 personas. La encuesta se enfoca en los mecanismos de seguridad que actualmente posee la empresa y la importancia de realizar el análisis proactivo.

A continuación, se presenta el análisis y la debida conclusión de cada pregunta que se realizó a las 6 personas en el Departamento de Informática, estos están representados en gráficos de Pastel para mayor compresión.

Pregunta 1:

¿Existe un área o persona responsable de seguridad informática y seguridad de la información en la empresa?

RESPUESTA	FRECUENCIA	PORCENTAJE
Si	0	0%
No	6	100%
TOTAL	6	100%

Tabla 1 Persona responsable de la seguridad informática

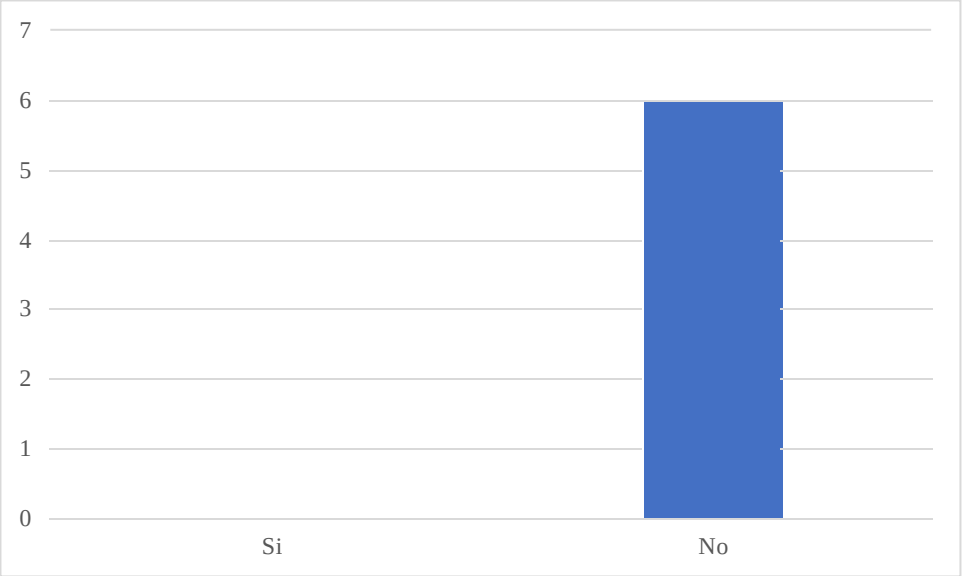


Fig. 2 Persona responsable de la seguridad informática

Análisis

El 100% de la población nos da como respuesta que no hay una persona a cargo de la seguridad informática de la Institución.

Conclusión

Se puede apreciar que hace falta una persona que se encargue de salvaguardar los datos de los usuarios, en caso de accidentes o ataques por terceros.

Pregunta 2:

¿Qué software utiliza en la empresa para controlar software malicioso?

RESPUESTA	FRECUENCIA	PORCENTAJE
Antivirus	3	50%
Anti-Spam	0	0%
Antospyware	0	0%
Cortafuegos/firewall	3	50%
Otros, indique cuáles	0	0%
TOTAL	6	100%

Tabla 2 Software para controlar informes maliciosos

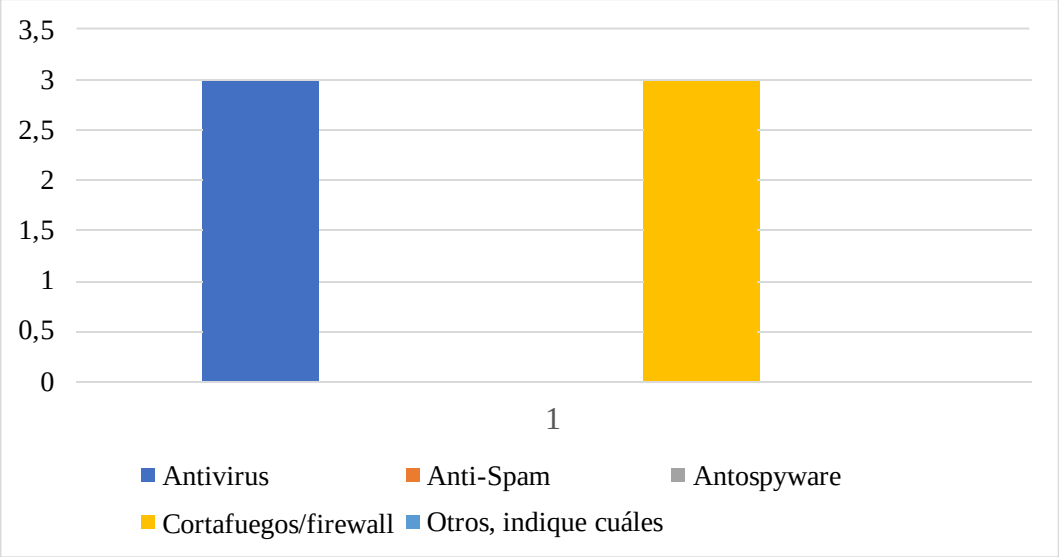


Fig. 3 Software para controlar informes maliciosos

Análisis

La institución usa el antivirus 50% y cortafuegos 50% para detectar software malicioso que puedan penetrar los servidores en la red de la Institución.

Conclusión

Los softwares para detección maliciosa deben estar en constante actualización para así tener una mayor seguridad en los datos en los servidores.

Pregunta 3:

¿Cuáles de los siguientes mecanismos de autenticación utiliza en la empresa?

RESPUESTA	FRECUENCIA	PORCENTAJE
Firma electrónica digital	0	0%
Clave de Acceso	6	100%
No tiene	0	0%
Otros, indique cuáles	0	0%
TOTAL	6	100%

Tabla 3 Mecanismos de autenticación

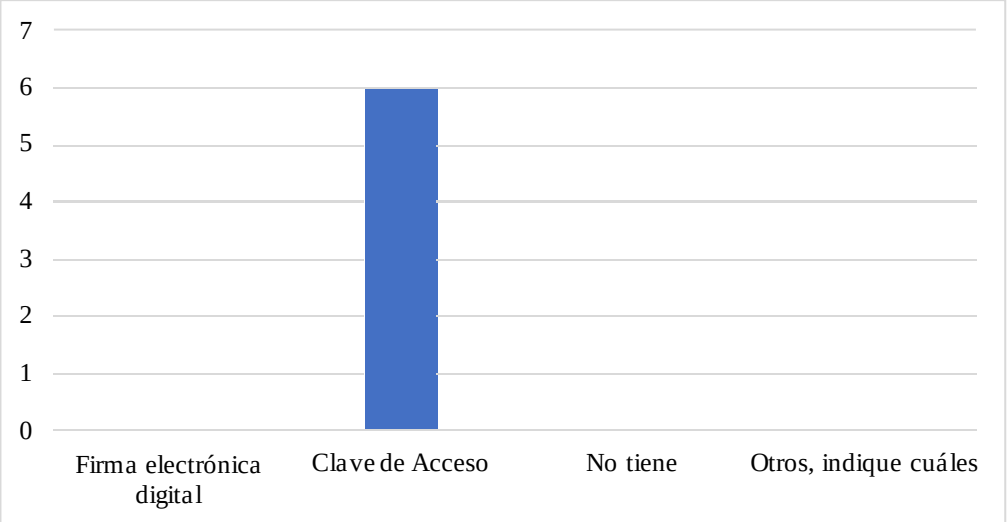


Fig. 4 Mecanismos de autenticación

Análisis

El mejor mecanismo utilizado es la clave de acceso es el más utilizado en la empresa es el equivalente al 100% por la seguridad que brinda.

Conclusión

Hay diferentes mecanismos de seguridad los cuales dan diferentes resultados, pero la clave de acceso es una fiabilidad que la institución utiliza para proteger información del usuario.

Pregunta 4:

¿Cuál es el tipo de backup que realiza a los servidores la empresa?

RESPUESTA	FRECUENCIA	PORCENTAJE
Backup completo	0	0%
Backup difrencial	0	0%
Backup incremental	6	100%
Backup espejo	0	0%
TOTAL	6	100%

Tabla 4 Tipo de Backup del servidor

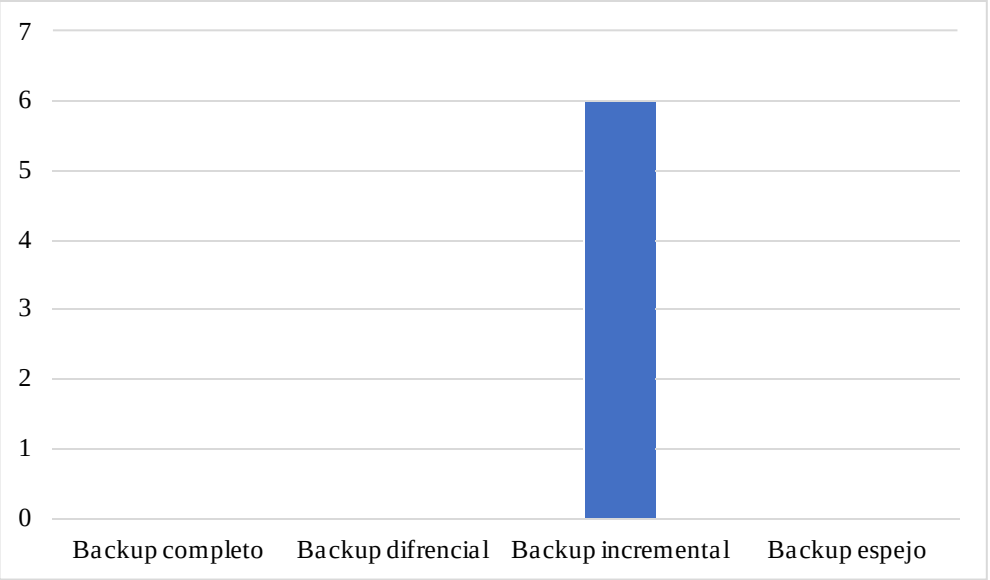


Fig. 5 Tipo de Backup del servidor

Análisis

Se denota que el 100% de las personas sabe que el respaldo de información que se realiza es un backup incremental por la garantía de seguridad que utiliza.

Conclusión

Toda información que posee la empresa tendrá un Backup de forma recursiva.

Pregunta 5:

¿Qué servicios y sistemas considera más críticos en términos de disponibilidad?

RESPUESTA	FRECUENCIA	PORCENTAJE
De almacenamiento de datos	3	50%
Servicios de comunicación	0	0%
Sistemas de procesamientos de datos	3	50%
Otros	0	0%
TOTAL	6	100%

Tabla 5 Servicios y sistemas más críticos en términos de disponibilidad

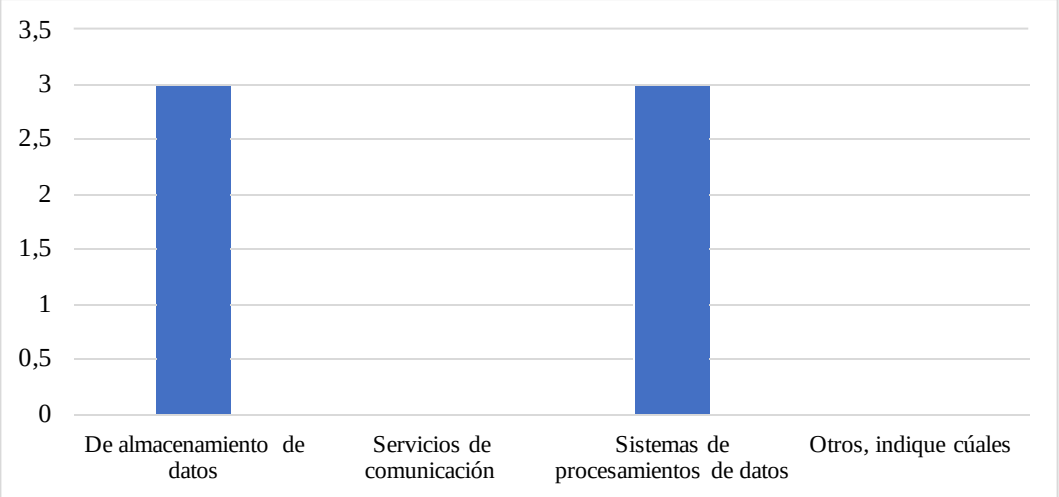


Fig. 6 Servicios y sistemas más críticos en términos de disponibilidad

Análisis

El departamento de informática considera que los servicios más críticos que en términos de disponibilidad son de almacenamiento de datos con un 50%, y el de sistema de procesamiento de datos 50%, todo esto por la gran cantidad de información que es almacenada en ambas.

Conclusión

La información almacenada dentro del departamento informático tiene que tener toda la medida de seguridad que puedan garantizar al usuario la protección de datos.

Pregunta 6:

¿Existe el apoyo necesario de las máximas autoridades en temas de tecnología?

RESPUESTA	FRECUENCIA	PORCENTAJE
Si	6	100%
No	0	0%
TOTAL	6	100%

Tabla 6 Apoyo de autoridades en temas de tecnología

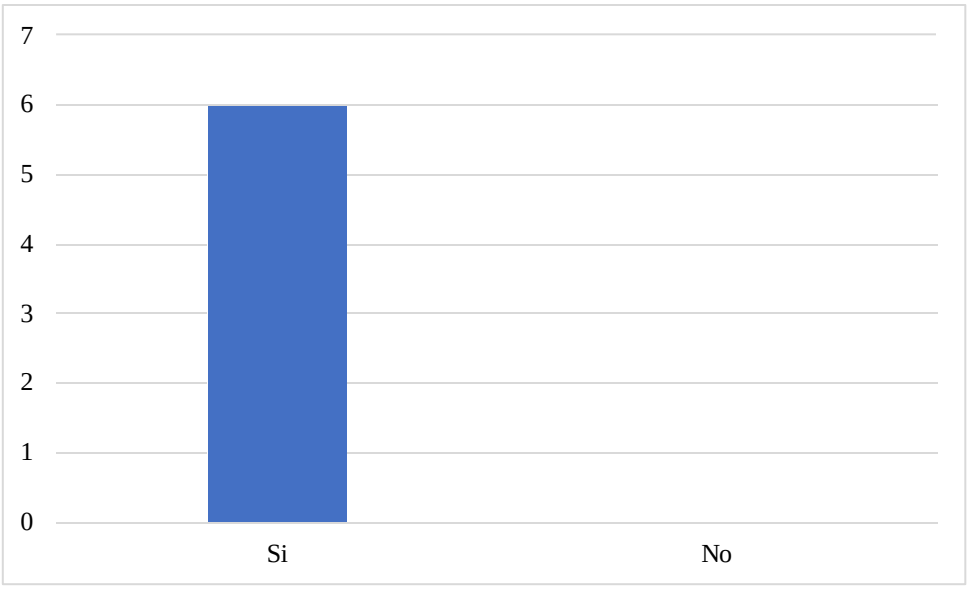


Fig. 7 Apoyo de autoridades en temas de tecnología

Análisis

El 100% de los encuestados tiene conocimiento que es necesario el apoyo de las autoridades para el respectivo progreso considerando que la protección de datos hoy en día es un derecho por parte de las personas.

Conclusión

El apoyo de las autoridades es un factor fundamental en la implementación de nuevas tecnologías que ayuden al desarrollo e innovación de nuevas cosas,

especialmente si se trata en el tema de salvaguardar los datos de las personas, a través de políticas seguridad.

Pregunta 7:

¿Ha tenido algún incidente de seguridad en el último periodo laboral?

RESPUESTA	FRECUENCIA	PORCENTAJE
Si	6	100%
No	0	0%
TOTAL	6	100%

Tabla 7 Incidente de seguridad en el último periodo laboral

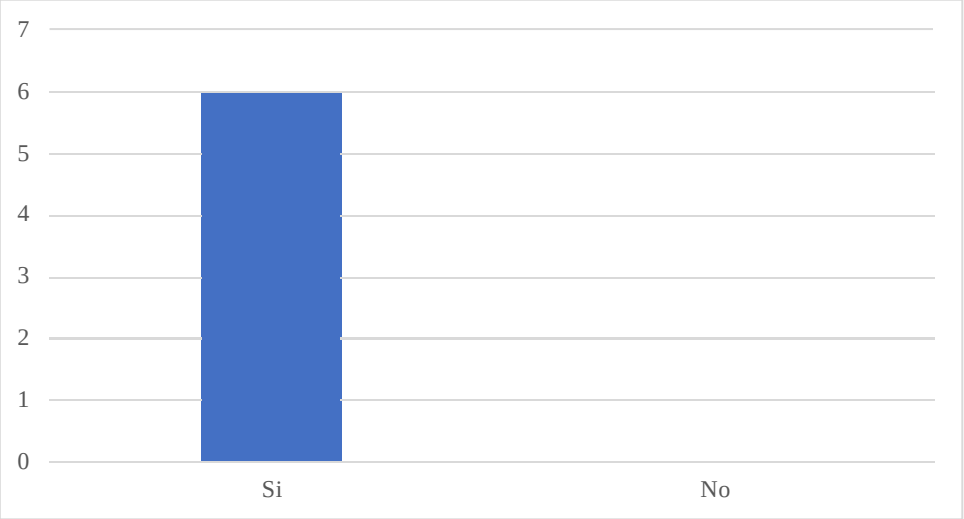


Fig. 8 Incidente de seguridad en el último periodo laboral

Análisis

Los accidentes de seguridad en los últimos tiempos a sido uno de los grandes factores primordiales por las empresas debido a la gran información que poseen y es por eso que hoy en día muchas empresas invierten más dinero y recursos en la parte tecnológica.

Conclusión

Para los accidentes de seguridad informática siempre se debe tener un plan de contingencia o políticas de seguridad de lo que se debe hacer cuando suceda este tipo de catástrofe.

Pregunta 8:

¿Conocen que son los CSIRT?

RESPUESTA	FRECUENCIA	PORCENTAJE
Si	0	0%
No	6	100%
TOTAL	6	100%

Tabla 8 CSIRT

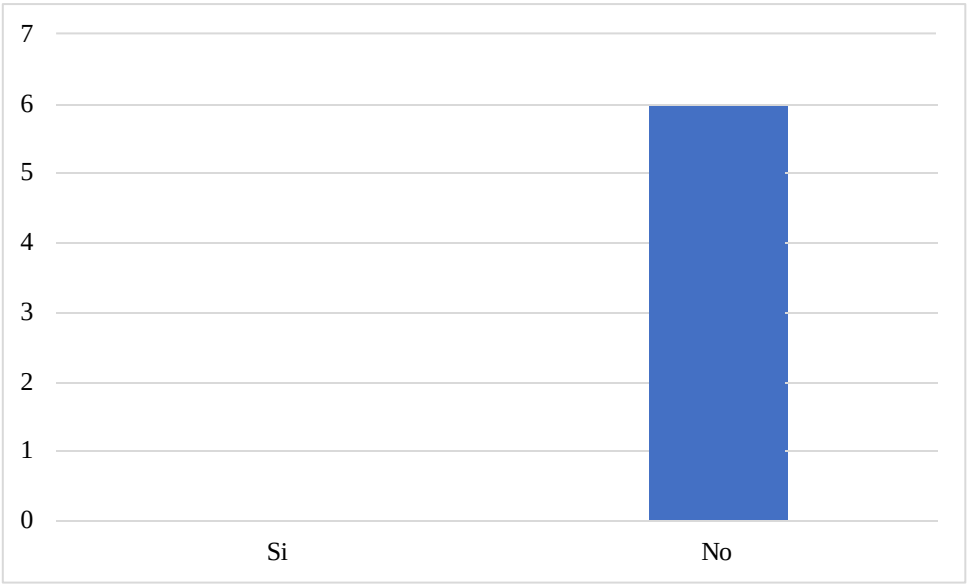


Fig. 9 CSIRT

Análisis

Uno de los problemas que existen en los departamentos informáticos es la falta de información, como es el del CSIRT, que es un equipo de respuesta ante Emergencias Informáticas, que ayudan en la prevención de en caso de incidencias.

Conclusión

El conocimiento de las nuevas tecnologías incluye también el nuevo conocimiento de las medidas y políticas de seguridad que se implemente hoy en día en caso de incidentes o robo de información por parte de terceros.

Pregunta 9:

¿Le gustaría implementar un sistema de Incidente de Seguridad Informática?

RESPUESTA	FRECUENCIA	PORCENTAJE
Si	6	100%
No	0	0%
TOTAL	6	100%

Tabla 9 Intención de implementar un sistema de incidente de seguridad informática

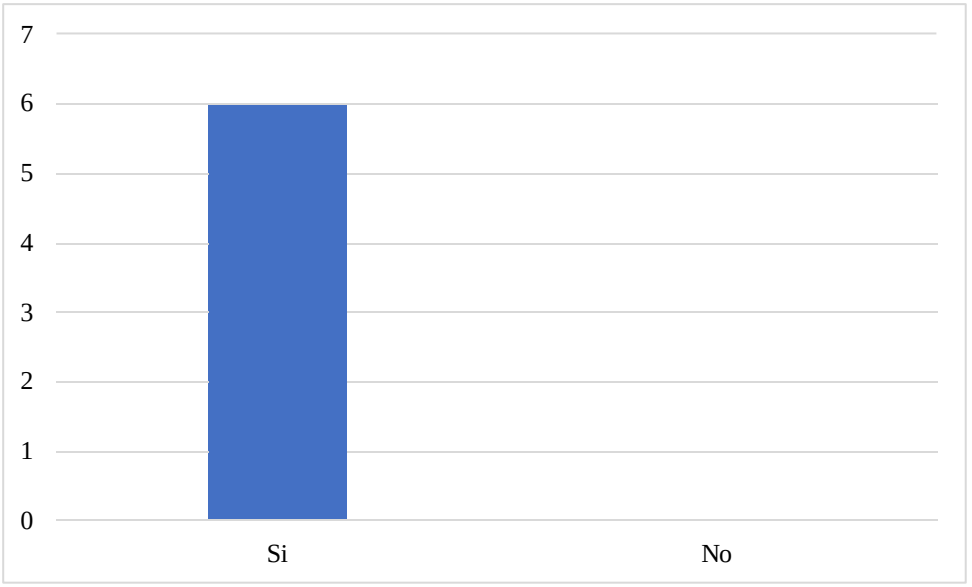


Fig. 10 Intención de implementar un sistema de incidente de seguridad informática

Análisis

Hoy en día la implementación de medidas de seguridad es de vital importancia en las empresas, se pudo evidenciar debido a que esto ayudaría a la protección de los datos de las personas.

Conclusión

La implementación de políticas de seguridad no solo permitirá la mitigación de los accidentes ocasionados por terceros por el robo de información, sino que servirá como un plan de contingencia que hacer en caso de que se presenten.

1.6.5 Resultados Esperados

La implementación de políticas de seguridad en el departamento de TIC del GAD Municipal permitirá conseguir los siguientes resultados.

- Obtener información de los diferentes programas OpenSource, para escoger las mejores herramientas que ayuden al escaneo de las vulnerabilidades.
- Generación de documentación de políticas de seguridad SANS y estándares para la posible solución de incidencias presentadas.
- La incrementación y protección y fiabilidad en los sistemas y redes del departamento.
- Análisis de resultados obtenido por las herramientas de Ciberseguridad de tipo open source.
- Mejorar la seguridad informática en la empresa para salvaguardar la información en la que se pueda estar comprometida.

CAPÍTULO II

2 Propuesta

2.1 Marco Contextual

2.1.1 Generalidades del GAD

El GAD Municipal de [redacted] está situado en el centro de la ciudad de [redacted] frente al parque Vicente Rocafuerte, diagonal a la iglesia matriz de [redacted]. Con la proyección de la población permanente, el Cantón [redacted] ocupa el 50,29%, de la población total de la Provincia de [redacted] según proyección proporcionada por el INEC en base al Censo al 2.010, esta población está asentada en una extensión territorial de 97,47% del tamaño de la superficie territorial de la Provincia.

Es importante considerar que dentro del cantón [redacted] existe una población flotante que es representativa, en especial en época de temporada invernal y que no está considerada por no contar con datos estadísticos oficiales. En el [redacted] en el sector centro norte, en las parroquias de Colonche y Manglaralto, la densidad poblacional más alta gira en torno a los poblados de San Juanito, La Entrada, Las Núñez, Olón, Manglaralto, Dos Mangas, Cadeate, San Antonio, Sitio Nuevo, Valdivia, Sinchal, Barcelona, Loma Alta, Ayangue, Palmar, Monteverde, Bambil Collao, Febres Cordero, Colonche, San Marcos, Salanguillo, Guangala, etc. En la Parroquia [redacted] la densidad más alta se localiza en poblados como San Pablo, Syros, Las Gaviotas, Punta Blanca, Barandúa, El Morillo, San Vicente, Buena Fuente y El Azúcar [20].

2.1.2 Misión

Nuestro Gobierno Autónomo Descentralizado Municipal, es administrador, gestionado, facilitador y regulador de bienes y servicios públicos permanentes, de calidad, con eficiencia, cobertura y acceso, mediante procesos, programas y proyectos inclusivos, participativos, transparentes para la sociedad, aplicando la solidaridad, el respeto, la responsabilidad y equidad

2.1.3 Visión

El Gobierno Autónomo Descentralizado Municipal en el 2.019 será una institución con capacidad administrativa, operativa y financiera, sólida e innovadora, generadora del desarrollo sostenible y sustentable del cantón, para los ciudadanos e inversionistas locales, nacionales y extranjeros, aplicando la gestión por resultados con transparencia, solidaridad, justicia y probidad

2.1.4 Ubicación

Provincia de [redacted], Cantón [redacted], Av. [redacted] y Calle 10 de agosto.

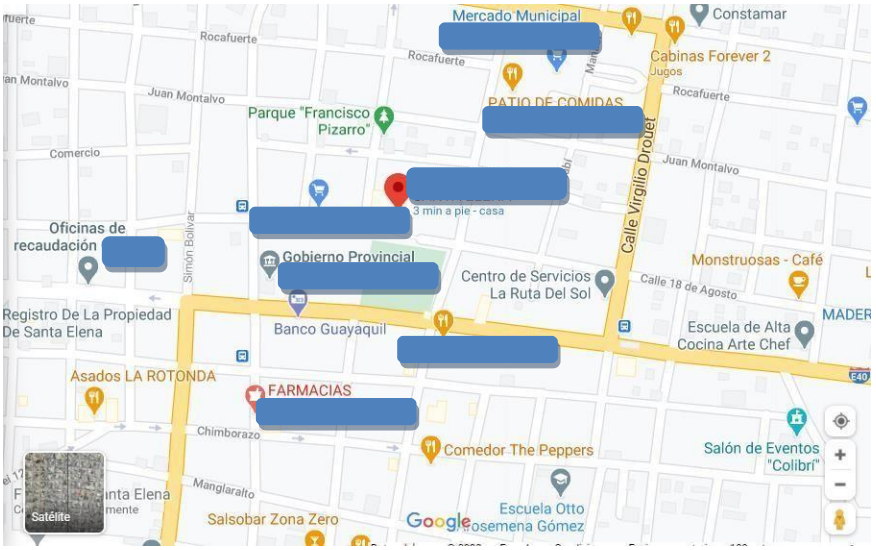


Fig. 11 Ubicación GAD: Google Maps

2.1.5 Estructura Organizacional

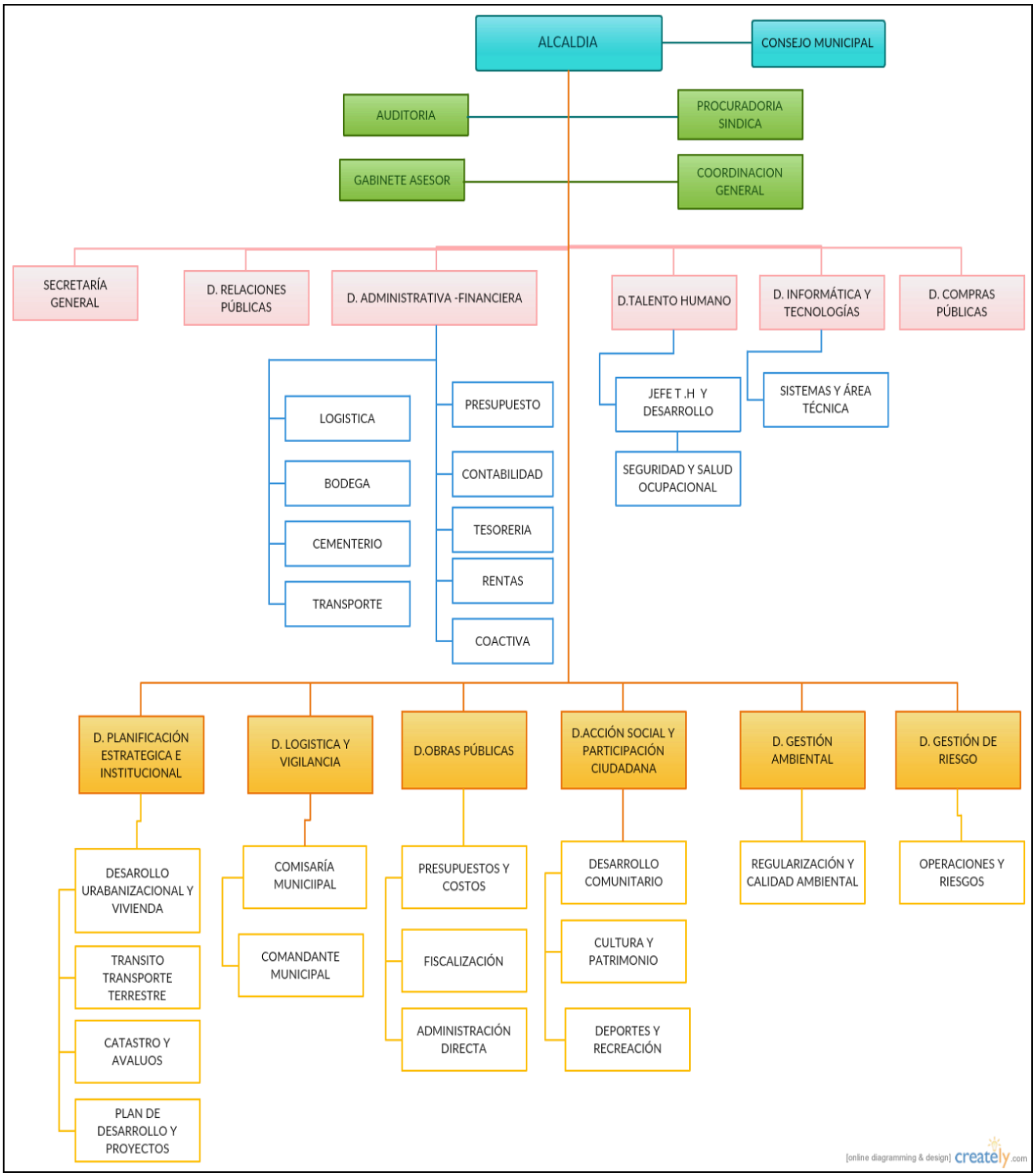


Fig. 12 Estructura organizacional GAD MUNICIPAL

2.2 Marco Conceptual

2.2.1 Seguridad de la Información

Son medidas que sirven para evitar acciones no autorizadas que puedan afectar los principios de la seguridad de la información (confidencialidad, autenticidad, integridad), el cual garantiza el correcto funcionamiento del equipo y su accesibilidad para los usuarios legítimos [19].

El 80% de los hechos que vulneran la seguridad de información personal u organizacional, se debe a causas humanas. La negligencia, el no tener medidas de prevención son unas de las principales razones de la perdida, robo o alteración de información digital clave [21].

2.2.2 Políticas de Seguridad

Las políticas de seguridad informática es un conjunto de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información con el objetivo de minimizar los riesgos que puedan afectar los datos [22].

2.2.3 Hacking Ético

Hacking ético, es un test de intrusión donde tiene como fin obtener información y vulnerabilidades del sistema, con el objetivo de reportar a la empresa u organización para las respectivas tomas de decisiones, para prevenir la catástrofe cibernéticos, como es el robo de información [23].

2.2.4 Seguridad Informática

La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilizan de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización [24].

2.2.5 Kali Linux

Kali Linux es una distribución de Linux basada en Debian destinada a las pruebas de penetración avanzadas y la auditoría de seguridad. Kali contiene varios cientos de herramientas que están orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa [25].

2.2.6 Pentesting

Son un conjunto de técnicas usadas para medir, auditar y evaluar la seguridad de redes y aplicaciones web de igual manera todo lo relacionado con los sistemas de información.

2.2.7 Hackers de Sombrero Blanco

Son hacker con sentido ético, encargado de investigaciones de seguridad con fines no maliciosos. Permiten encontrar vulnerabilidades para indicar y demostrar la falta de seguridad presentada en una organización o para probar sus propios códigos

2.2.8 Hackers de Sombrero Negro

Son hacker que violan la seguridad para obtener provecho personal, se puede decir que son los causantes de los virus malware, ransomware etc. Son expertos en seguridad que se aprovechan de las vulnerabilidades para robar información, modificarla o secuestrarla

2.2.9 Hackers de Sombrero Gris

Son hacker que pueden actuar impulsados con dos intenciones, una de ellas puede ser para fines personales o también para ayudar en la seguridad de una organización y de acuerdo con el objetivo de las pruebas de penetración, se presenta la clasificación del hacker

2.2.10 Hacking de aplicaciones Web

¿Qué es una aplicación web?

Una aplicación Web es un sitio Web que contiene páginas con contenido sin determinar, parcialmente o en su totalidad. El contenido final de una página se determina sólo cuando el usuario solicita una página del servidor Web. Las aplicaciones Web se crean en respuesta a diversas necesidades o problemas [26].

Las aplicaciones web, no son perfectas suelen tener fallos de programación que afectan en gran parte a la seguridad de la aplicación. Esto se debe por el gran número de líneas de código que supera las decenas de millar o inclusive más, por ende, es difícil percatar el error para dar una solución. Un fallo en la base de datos o en algún

componente de la aplicación pueden afectar al resto del sistema, y estar expuestos a los atacantes [26].

Los principales problemas de la programación de sistemas web se dividen en dos, las entradas y salidas del sistema. Los datos de entrada son proporcionados por el usuario, maquina o programa, estos son procesados por la aplicación para realizar procesos específicos. Mientras que los datos de salida es la información obtenida a partir de alguna entrada o un proceso interno del sistema [27].

Los ataques más graves que se presentan en las aplicaciones web, son aquellos que exponen datos confidenciales u obteniendo el acceso restringido a los servidores o red en los que se ejecuta el sistema. Para las organizaciones cualquier ataque que cause un tiempo de inactividad puede resultar con elevadas pérdidas [26].

2.2.11 Tipos de ataques a aplicaciones web

Autenticación rota: Permiten al atacante descifrar contraseñas débiles, lanzar ataques de fuerza bruta u omitir el inicio de sesión [28].

SQL Inyección: Es quizás el ataque más complejo, el atacante ejecuta comandos en el propio servidor de la base de datos del sistema para así recuperar datos arbitrarios de la aplicación [28].

Cross-Site Scripting (XSS) son un tipo de inyección, en la que se inyectan secuencias de comandos maliciosas en sitios web benignos y de confianza. Estos ataques ocurren cuando un atacante utiliza una aplicación web que envía código malicioso [29].

Peticiones falsificadas: Los usuarios pueden ser inducidos a realizar acciones que este no pretendía. Se emplean herramientas de línea de comandos o extensiones en los navegadores que generan páginas falsas [28].

Controles de accesos rotos: Implica que en algunos casos la aplicación no protege convenientemente el acceso a sus datos, provocando que un atacante pueda ver los datos confidenciales a través de la URL contenida en el servidor [28].

Los ataques cibernéticos cada día crecen y evoluciona más, por ende, las organizaciones tienen el privilegio de mejorar sus sistemas de seguridad para estar mejor preparados en caso de incidentes que puedan presentarse. Según el reporte de seguridad de OEA los ataques cibernéticos más frecuentes contra organizaciones son las siguientes:

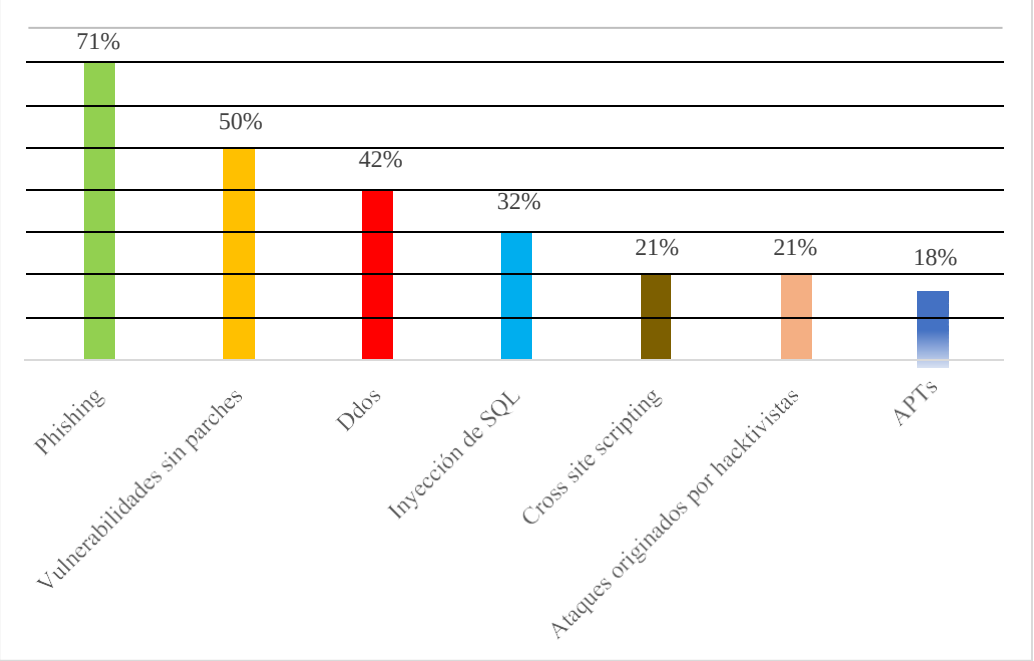


Tabla 10 Porcentaje de ataques cibernéticos contra organizaciones.

2.2.12 Pentesting para aplicaciones web

¿Qué es el pentesting?

"Pentesting o Penetration Testing (Test de penetración) es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas" [30].

El proceso de realización de un pentesting es llevado a cabo por profesionales que utilizan técnicas para identificar la clase de fallo de seguridad o vulnerabilidades que se encuentren dentro de un sistema. Uno de los mayores beneficios de un pentesting completo es que las técnicas hacen más riguroso el proceso de evaluación, para detectar de las posibles vulnerabilidades [26].

La ventaja principal de un Pentesting es que permite romper las barreras de seguridad que existen en numerosas aplicaciones web y con ayuda de esta metodología describir los fallos de seguridad, evaluarlos, explotarlos al máximo para continuar con la corrección de estos [26].

2.2.13 Importancia de un Pentesting

Las pruebas de Pentesting brindan una nueva perspectiva de que tipo de seguridad tiene el sistema y si se debe mejorar algún aspecto o si existen restricciones demás. Estas pruebas o ataques es conveniente realizarlos sin que la plantilla de trabajo sea consciente de que se van a realizar, para que la simulación de ataque sea lo más verídica posible [30]

Así mismo, en una empresa se verifica que la política de seguridad este bien orientada y aplicar algún tipo de sanción a quien se haya encontrado un

comportamiento indebido dentro del sistema de información. Normalmente al terminar una prueba de Pentesting el auditor realiza un informe con las vulnerabilidades encontradas y además añade las mejoras sugeridas para ser más seguro y fiable el sistema [30].

2.2.14 Importancia de la metodología OSSTMM en el pentesting

La investigación se orientó en la búsqueda de vulnerabilidades en la red con el fin de reducir los errores de seguridad y las vulnerabilidades a través de la utilización de una metodología OSSTMM y con plantillas SANS.

(Open Source Security Testing Methodology Manua) OSSTMM, es una metodología científica para pruebas de penetración de red y evaluación de vulnerabilidades para auditorias informáticas.

La metodología OSSTMM propone la optimización de la seguridad de los activos de información, con el objetivo de disminuir las limitaciones entre activos de información a proteger y las posibles brechas de seguridad, así como también la no espacio de activos de información y brechas de seguridad informática, dando como resultado la porosidad [31].

2.3 Marco Teórico

Para el desarrollo de este proyecto se consultaron proyectos similares con la finalidad de comprender el tema planteado. A continuación, se detallan los casos encontrados.

[32] "ANÁLISIS Y GESTIÓN DE LA SEGURIDAD EN LA RED DEL GAD MUNICIPIO DE RIOVERDE, MEDIANTE EL DISEÑO DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA, CSIRT".

Se realizo un proyecto de Análisis de Gestión de la Seguridad utilizando Kali Linux, para el Municipio de Rioverde con el objetivo de determinar las vulnerabilidades que existen en la red, para así dar una respuesta a incidentes informáticos que se puedan presencia en caso de un fallo en la Infraestructura de red.

[20] "EVALUACIÓN DE RIESGOS Y DESARROLLO DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES INFORMÁTICOS APLICADO AL CENTRO DE DATOS Y COMUNICACIONES DE LA UPSE".

El trabajo fue desarrollado para el área de informática en la Universidad Estatal Península de Santa elena, con el objetivo de implementar un plan de recuperación ante desastres informáticos, cumpliendo un conjunto de medidas técnicas, humanas y administrativas que permitan la continuidad de las operaciones y servicios en caso de desastres físicos o naturales.

2.3.1 Aplicación de la Metodología OSSTMM (Open Source Security Testing Methodology Manual)

La metodología OSSTMM se divide en cinco secciones o ambientes, las que permitirán identificar y enfocar los errores que tienen los sistemas operativos y tomar medidas para evitar posibles inconvenientes. Esta metodología abierta de testeo de seguridad OSSTMM se relaciona directamente con la identificación de errores y vulnerabilidades [33].

Fig. 13 Esquema de la metodología OSSTMM

Para llevar a cabo esta investigación, fue necesario escoger las secciones con mayor énfasis al proyecto como son Seguridad de la información, Seguridad en las tecnologías de Internet y Seguridad de los Procesos, todas estas secciones me permitirán medir la seguridad de la empresa al momento de realizar un Test de Penetración

2.3.2 Instituto de seguridad de la información (SANS)

Es la fuente más grande y confiable en proveer una buena certificación de seguridad de la información en el mundo. Este instituto brinda diferentes temas, políticas o controles disponibles en las tecnologías avanzadas, redactadas por excelentes especialistas en el ámbito de Sistemas, Auditoria, Redes y Seguridad. Cabe mencionar que Sans está encargado indispensablemente en desarrollar, mantener, actualizar y poner a disposición la mayor serie de documentos de investigación sin costo alguno. Esta institución orientada a la seguridad de la información ofrece además una certificación a través de GIAC, filial del Instituto SANS, que es un organismo de certificación que brinda más de 20 aspectos tecnológicos e incluye certificaciones técnicas en seguridad de la información, y programas de grado opcional a través del Instituto de Tecnología SANS, así como numerosos recursos de seguridad gratuitos, incluyendo boletines de noticias, documentos técnicos y transmisiones por Internet [20].

Los recursos de SANS Security Policy tienen como objetivo principal conceder plantillas y herramientas necesarias aproximadamente son 27 aspectos relacionados para la implementación de políticas de seguridad informática.

Según SANS, Una política es típicamente un documento que describe los requisitos o reglas específicas que se deben cumplir [20]

Esta documentación presentara un conjunto de estrategias reformadas y renovadas acorde a las necesidades reflejadas con las vulnerabilidades encontradas en el GAD Municipal. Entre las herramientas SANS más comunes que fueron utilizadas para la creación de políticas se distinguen las siguientes.

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las tecnologías de Internet

2.3.3 Fases del Pentest

Fase de Recolección de Información:
Para el proceso de recolección de información en la organización del GAD Municipal se las dividió en dos fases:

- External Footprinting.
- Internal Footprinting

External Footprinting

Esta recolección de información está estructurada en dos fases, a su vez las técnicas de recolección de datos desde el exterior están categorizadas en dos subcategorías denominadas Active Footprinting, que interactúa directamente con la infraestructura de la empresa consultando el DNS, analizando las cabeceras HTTP, enumeración de puertos y sus servicios. Por otro lado, se encuentra Passive Footprinting que recurre a la consulta de información por motores de búsqueda, registros públicos, y foros.

Passive Footprinting

El uso de Passive Footprinting es encontrar direcciones IP, rangos de direcciones de red y nombres de subdominios. Durante el proceso de recolección de datos se pueden descubrir algunos servicios (correo, web, DNS) proporcionados por los servidores.

2.4 Componentes de la Propuesta

2.4.1 Virtualización

Se implemento la virtualización del sistema operativo Kali Linux, que cuenta con una licencia de código abierto, el cual contiene los programas para la realización del pentesting informático.

2.4.2 Escenarios

Se realizaron diferentes configuraciones dentro del departamento de TIC como son los IP y proxys a continuación se detalla.

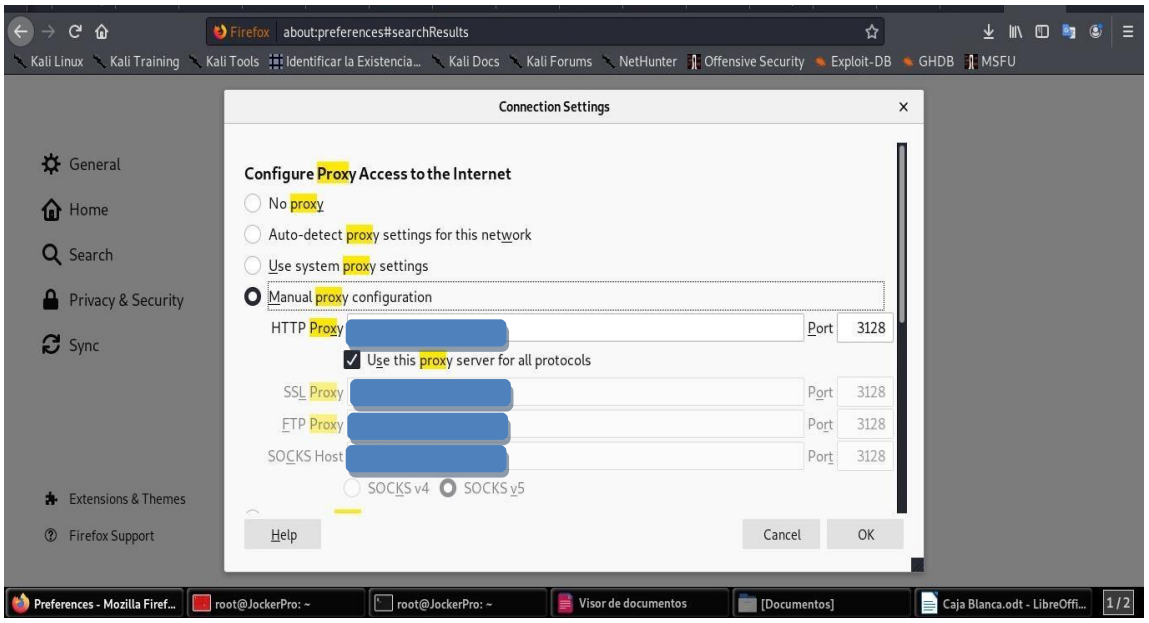


Fig. 14 Configuración del Proxy.

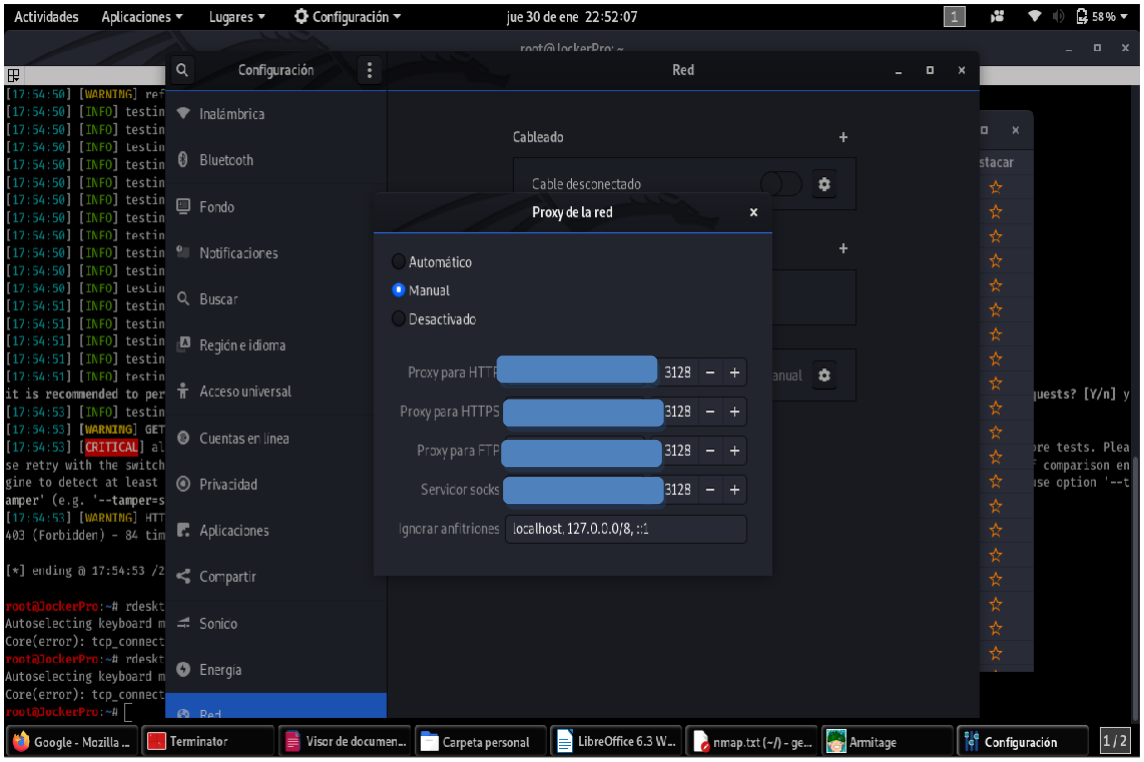


Fig. 15 Configuración de proxy y puertos.

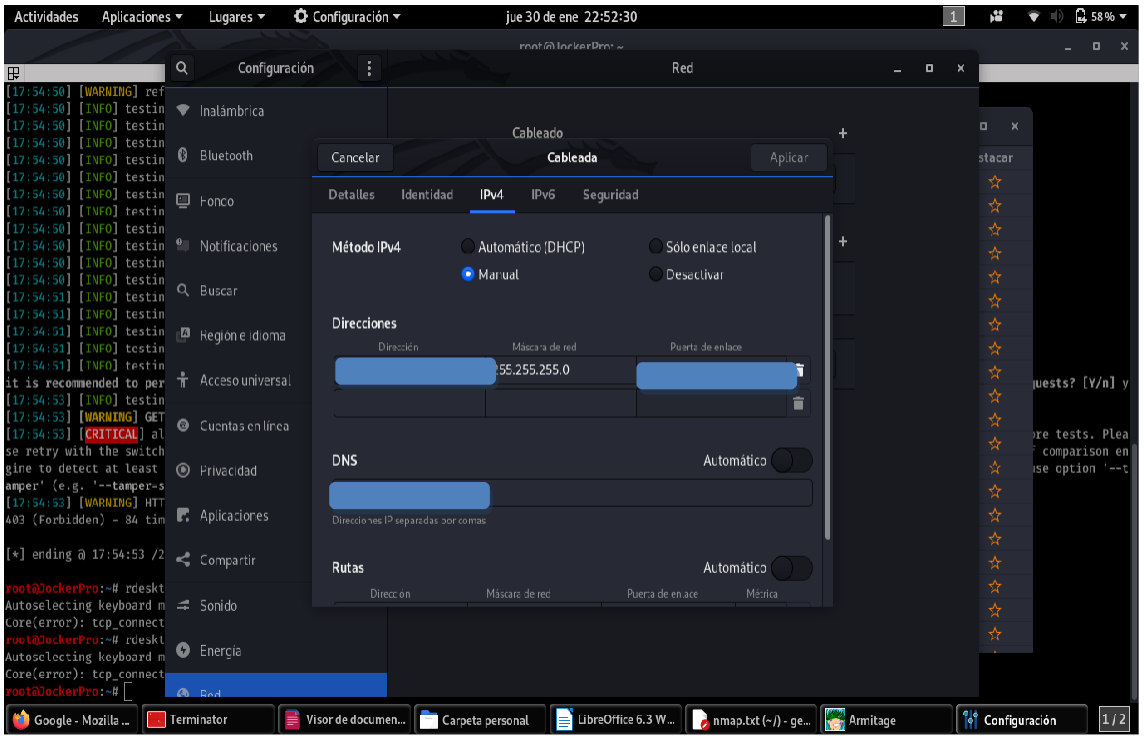


Fig. 16 Configuración de dirección IP Internamente.

Con el objetivo de realizar la fase de Passive Footprinting, se obtuvo mediante el rastreo de información de la empresa mediante el uso del buscador “Google” y obtuve los siguientes resultados.

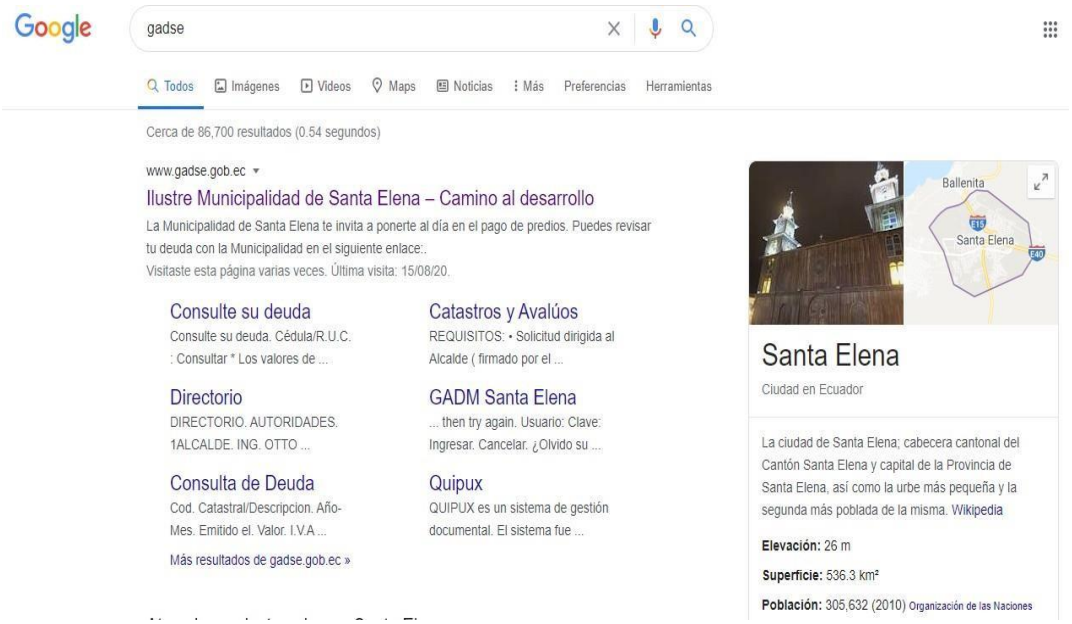


Fig. 17 Búsqueda sencilla en Google sobre la empresa

Se realizo un pentesting con herramientas online que nos brinda información importante de la empresa, por ende, se realizó una matriz detallando todos los datos recopilados, las herramientas que se usó son las siguientes:

- Netcraft.com
- Whatweb.net
- Nslookup
- Dmitry
- Dnsenum

Sitio	[redacted]
Dominio	[redacted]
Título de la Pagina	[redacted]
Dirección IP	[redacted]
Ubicación IP	Guayas – Naranjal – Nedetel Sa
ASN	AS264668 NEDETEL SA, EC (registrada el 15 de enero de 2016)
Historial de Alojamiento	3 cambios en 4 servidores de nombres únicos durante 6 años
Propietario de Netblock	NEDETEL SA
Nombre del Servidor	[redacted]
Administrador de DNS	fabianyagual@gmail.com
Tipo de Servidor	[redacted]
Código de Respuesta	200
Condiciones	284 (Único: 153, Vinculado: 136)
Imágenes	34 (faltan etiquetas Alt: 19)
Enlaces	91 (Interno: 56, Saliente: 15)
DNS inverso	host-157-100-54-163.ecua.net.ec
Organización de servidores de nombres	whois.PublicDomainRegistry.com
Compañía anfitriona	Ecuanet
Rango de IP del Propietario	[redacted]
Dirección del propietario:	Núñez De Vela Y Av. Atahualpa, E3-13, Edf. Torre D, 0000000 - Quito - 17
Teléfono del propietario:	[redacted]
Sitio web del propietario:	megadatos.net
Propietario CIDR:	[redacted]
Registro Whois creado:	08 julio 2005
Registro Whois actualizado:	15 jul 2010
Historial de cambios de dirección IP:	[redacted] web utiliza direcciones IP - [redacted] 3.68) utilizado el 30 de octubre de 2019 [redacted] sitio que usa esta dirección IP ahora
Servidores de Correo	[redacted]

Tabla 11 Recolección de Información de la Empresa.

Propietario de Netblock	Dirección IP	OS	Servidor web
NEDETEL SA Guayaquil	[redacted]	Linux	Apache / 2.2.15 CentOS
NEDETEL SA Guayaquil	[redacted]	Linux	Apache / 2.2.15 CentOS
CORPORACION NACIONAL DE TELECOMUNICACIONES - CNT EP Quito	[redacted]	Linux	Apache / 2.2.15 CentOS

Tabla 12 Servicios y Direcciones IP.

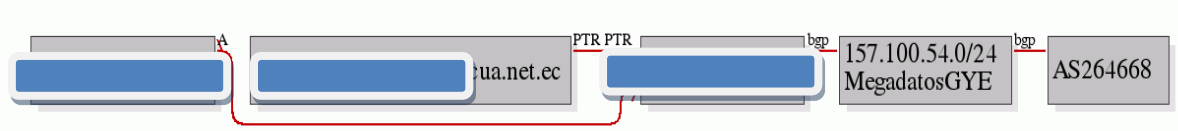


Fig. 18 Grafica de Distribución de Red.

Dmitry

Con la herramienta Dmitry se recolecto la información de los posible host y subdominios, así como correo electrónico, y puertos que puedan estar abiertos, los datos recolectados lo podemos guardar en un txt para mayor visibilidad.

La instrucción empleada para el uso de la herramienta es la siguiente:

dmitry -winsepf -t 9v-0 /Escritorio/dmitry/consulta.txt [redacted]

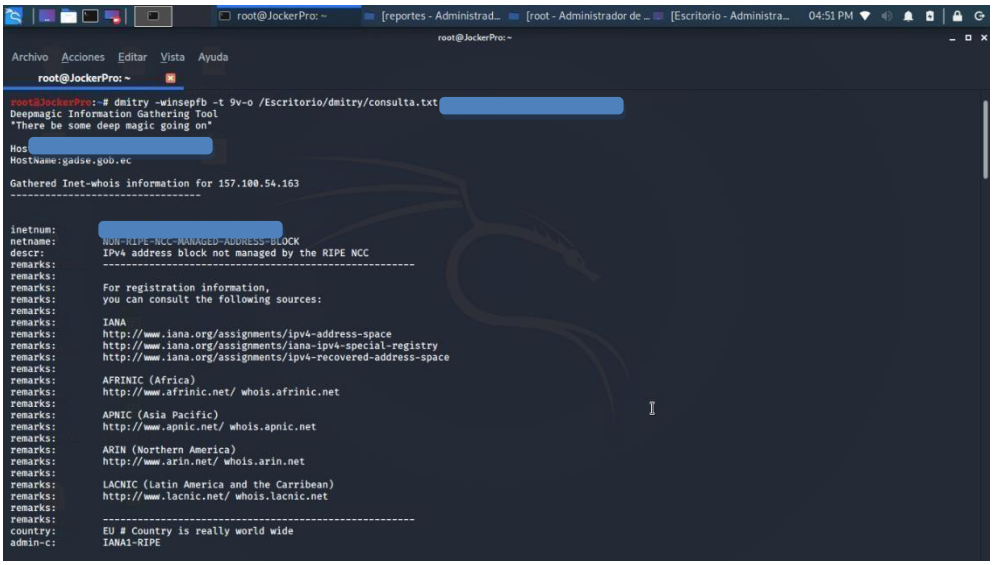


Fig. 19 Herramienta Dmitry

theHarvester

Esta herramienta permite recolectar información pública en la web, en la cual podemos conseguir información sobre emails, subdominios, hosts, nombres de empleados, puertos abiertos, banners, etc. Harvester es una secuencia de comandos Python simple que usa como motores de búsqueda a Google, Yahoo, Bing y muchos más.

La instrucción para una búsqueda de direcciones de correo es la siguiente:

~# theharvester -d [Dominio_Objetivo] -l 50 -b Google

La primera parte de los resultados con The Harvester expone un listado de las direcciones de correo electrónicos obtenidos desde Google, mientras que en la segunda parte se muestran los subdominios encontrados.

En la prueba que se realizó se encontró correos antiguos del personal que laboro anteriormente, se puede observar en la siguiente imagen:

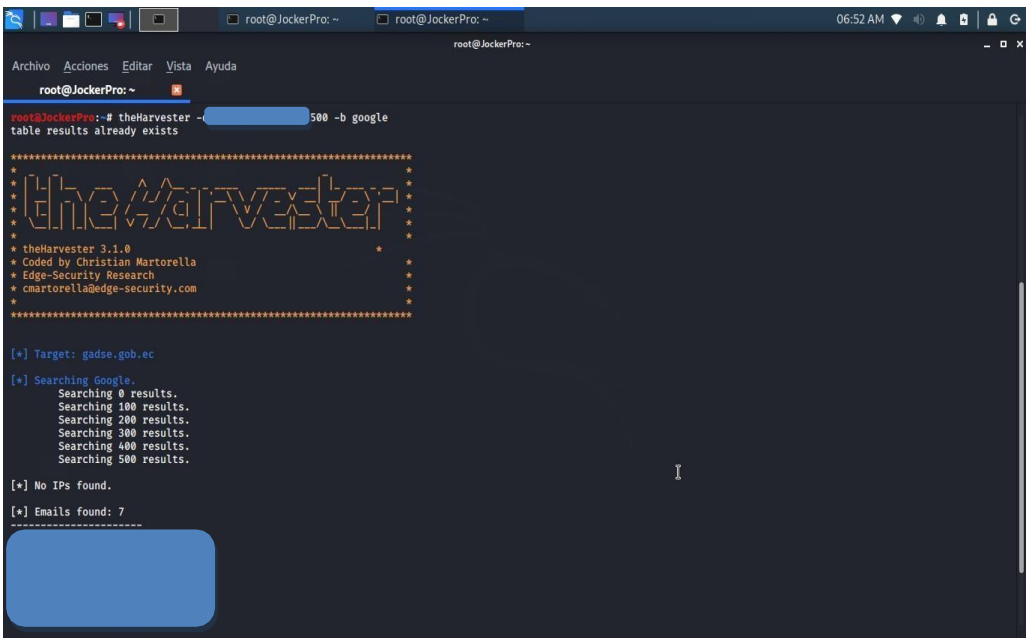


Fig. 20 Herramienta theHarvester

Direcciones de correo electrónico	Direcciones de Host
[redacted]	intranet [redacted]
[redacted]	quipux. [redacted] .100.54.164
[redacted]	[redacted] .100.54.163
[redacted]	
[redacted]	
[redacted]	
[redacted]	

Tabla 13 Direcciones de correo electrónico y IP.

Shodan

Shodan es un motor de búsqueda que permite encontrar iguales o diferentes tipos específicos de equipos conectados a internet a través de una variedad de filtros [34]. El resultado de la búsqueda de la IP [redacted] que corresponde al dominio de la empresa, se obtuvo la siguiente información donde se observa los puertos de dicha IP tiene abiertos, además información general del servidor que aloja el dominio.

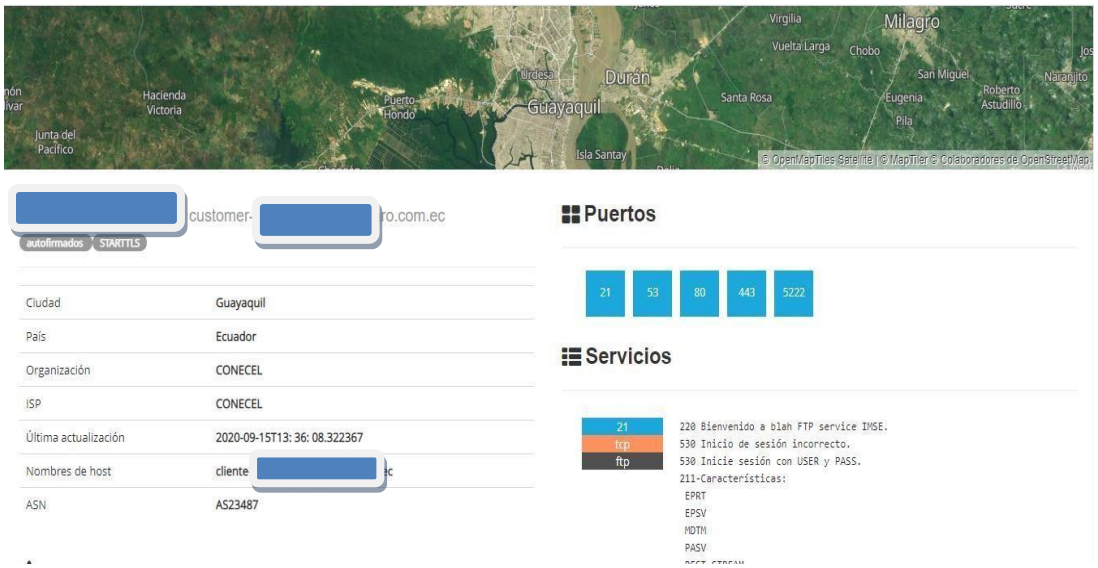


Fig. 21 Dirección IP y puertos abiertos.

Maltego

Maltego nos permitió la recolección de información de internet de forma gráfica, dado esto pudimos analizar y corroborar datos relevantes la cual podamos analizar para el respectivo pentesting.

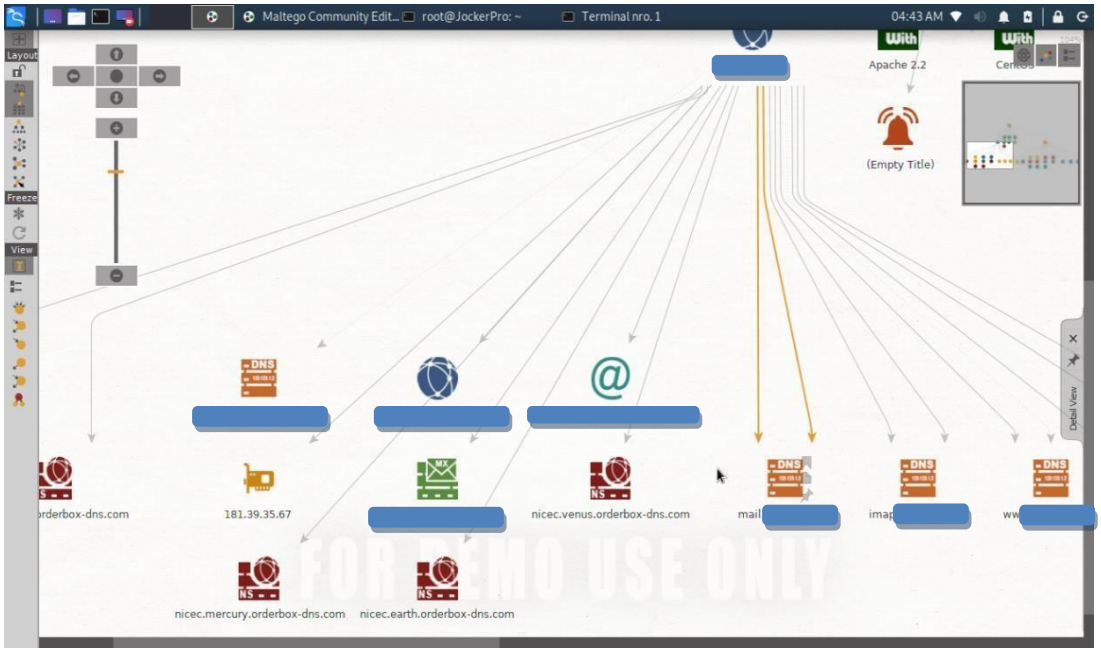


Fig. 22 Herramienta Maltego

Active Footprinting.

Nmap

Es una herramienta de código abierto para exploración de red y auditoría de seguridad, utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red.

A continuación, se muestran los resultados obtenidos por nmap en el sistema web de la empresa utilizando el siguiente comando “nmap -T4 -F www.gadse.gob.ec”, donde se ven los puertos abiertos dentro del servidor de la empresa.

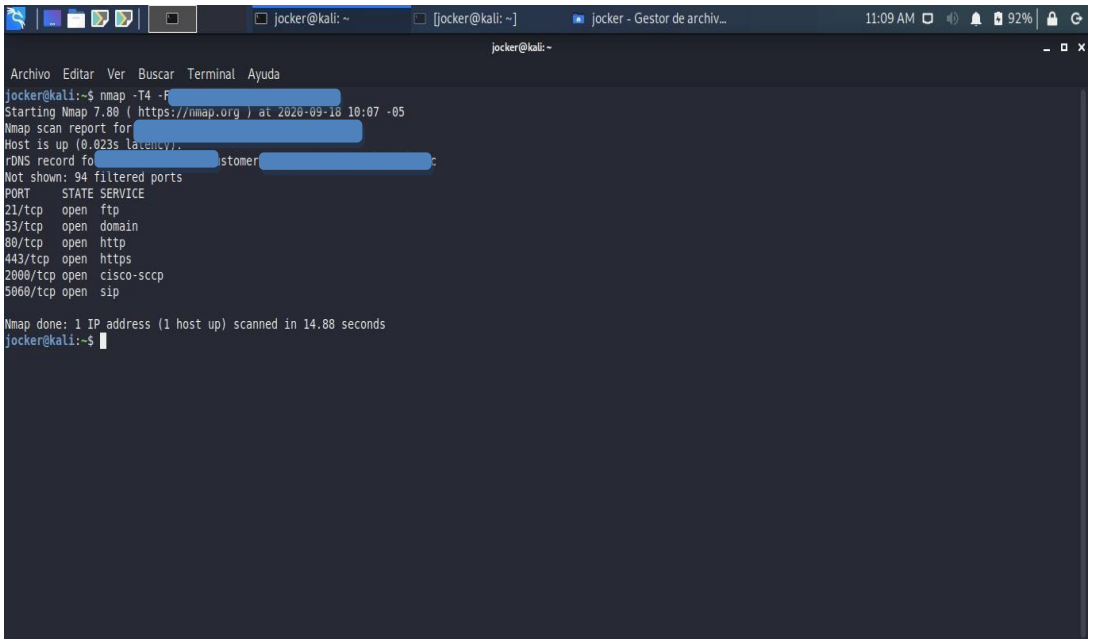


Fig. 23Resultado de análisis básico con nmap

Listado de puertos y su respectiva descripción.

- Puerto 21/tcp: FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) – control.
- Puerto 53/tcp: DNS Domain Name System (Sistema de Nombres de Dominio). Los Servidores DNS utilizan TCP y UDP, en el puerto 53 para responder las consultas.
- Puerto 80/tcp: El puerto por cual un servidor HTTP "escucha" la petición hecha por un cliente, es decir por una PC en específico.

Todas aquellas aplicaciones que funcionan en base a la IP (bien si son TCP o UDP) establecen comunicación con un servidor específico (puede ser SMTP, FTP, TELNET o HTTP, etc.) a través de un puerto, en el caso del HTTP, ese puerto es el 80. Así que mientras la PC de cada uno ocupa un puerto aleatorio, al momento de originar una petición al servidor, en el caso de HTTP siempre será, indistintamente el puerto 80, el que escuche o reciba la solicitud de servicio hecha por la PC cliente.

Puerto 443/tcp: HTTPS (Hypertext Transfer Protocol Secure) Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

Puerto 2000/tcp: CISCO- SCCP ()

Puero 5060/tcp: SIP

Enumeración

OWASP-ZAP

OWASP Zed Attack Proxy (ZAP) es una de las herramientas de seguridad gratuitas más populares del mundo.

Ayuda a encontrar automáticamente vulnerabilidades de seguridad en aplicaciones web mientras se desarrolla y prueban aplicaciones, además recopilar información de dominios. También es una gran herramienta para pentesters con experiencia para usar en pruebas de seguridad manual.

Esta herramienta localizada en el distro Kali Linux será utilizada para encontrar todos los archivos dentro del dominio de Dirsa, con el fin de un mayor acercamiento de cómo está constituido.

A2SV

Herramienta	**A2SV**
Descripción	Es una herramienta que sirve para hacer escaneo de una página web buscando vulnerabilidades SSL, esta herramienta está desarrollada en python por hahwul y la ofrece de forma gratuita en github.
Fecha de ejecución	11/07/2020
Aplicación	Web Page Institucional
Prioridad de vulnerabilidades	Alta/media/baja

Tabla 14 Herramienta A2SV, Vulnerabilidad #1.

Se realizo un escaneo con la herramienta A2SV, el cual nos dio como resultados 4 vulnerabilidades existente en la página web municipal, donde se redacta la descripción del problema y las posibles soluciones al problema encontrado

Vulnerabilidades Encontradas con A2SV	Vulnerabilidades Encontradas con A2SV
CVE: CVE-2007-1858: SSL Anonymous Cipher Suites Supported	CVE-2012-4929: vulnerabilidad de inyección SSL / TLS CRIME
Factor de Riesgo: Low	Factor de Riesgo: Low
Valor CVSS Base: 2.6	Valor CVSS Base: 4.3
Solución: Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados débiles.	Solución: S.O. WINDOWS: Aplicar configuraciones en el host afectado habilitando TLS 1.2, de igual manera se recomienda mantener en la última versión los navegadores desde los cuales se accede al servicio https.

Tabla 15 Herramienta A2SV, Vulnerabilidad #2.

Vulnerabilidades Encontradas con A2SV	Vulnerabilidades Encontradas con A2SV
CVE-2014-0224: Vulnerabilidad de inyección CCS	POODLE: vulnerabilidad SSLv3 (CVE-2014-3566)
Factor de Riesgo: Low	Factor de Riesgo: Medio
Valor CVSS Base: 5.8	Valor CVSS Base: 6.4
Solución: Para actualizar a la nueva versión de openssl con la solución, haga 'yum update openssl' desde la línea de comandos o realice una actualización desde la interfaz de usuario.	Solución: Desactivar el protocolo SSL 3.0 para protegerse contra este ataque.

Tabla 16 Herramienta A2SV, Vulnerabilidad #3.

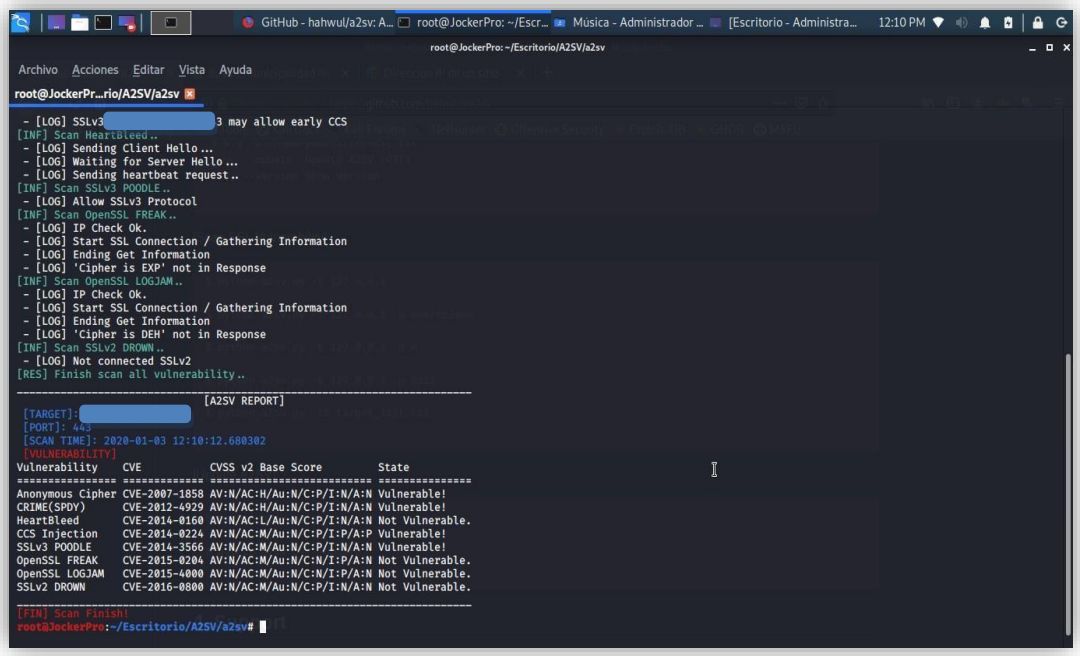


Fig. 24 Herramienta utilizada A2SV, con sus respectivas Vulnerabilidades

Acceso a máquina remota

Uno de los problemas más frecuentes que hay es el acceso remoto a maquinas no hay políticas establecidas que dictamen los pasos o herramientas a utilizar para mitigar el acceso a sus credenciales.

Esto no debería hacerse, la mejor opción para el acceso remoto es a través de VPN y dándole permiso con privilegios de seguridad, aplicando “Ingeniería social”, recolectamos información de alta procedencia como es que la máquina de la DBA que se puede acceder a ella esto porque para poder lograrlo deshabilita todos los firewalls posibles para acceder a ella, dejando a esta al asecho de los atacantes, expuesta al robo de información.

Fig. 25 Acceso remoto a otra maquina

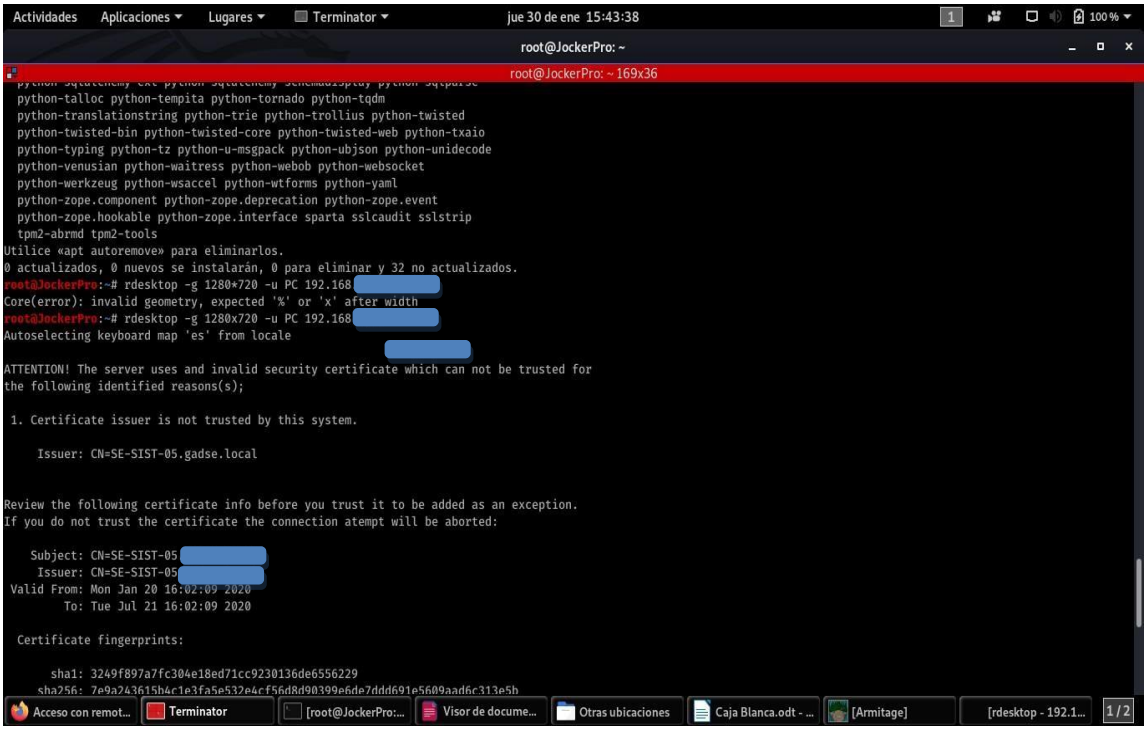


Fig. 26 Comandos usados para el acceso remoto

2.5 Requerimientos

2.5.1 Requerimientos para realización del pentesting

Para realizar la instalación de la máquina virtual se requiere de las siguientes características

Máquinas para pentesting
Ram: 3 GB **Disco Duro: 80 GB**

Tabla 17 Requerimientos Técnicos de las máquinas virtuales

2.5.2 Reconocimiento de servicios

Es necesario realizar el reconocimiento de los servicios que ofrece la empresa en las diferentes aplicaciones a escanear para así no corromper un DNS al momento del pentesting.

2.5.3 Habilitar puertos

Para que el escaneo del pentesting informático cumpla con los objetivos se tienen que habilitar ciertos puertos para tener una información más explícita de las vulnerabilidades encontradas.

2.5.4 Configuración de Proxy

La respectiva realización del proxy para las respectivas peticiones y acceso al internet para el escaneo de vulnerabilidades.

2.6 Diseño de la Propuesta

2.6.1 Arquitectura global

Para el proyecto de investigación se implementó un diseño de pentesting informático cumpliendo con las metodologías necesarias, con el fin de conocer los pasos que son necesarios para realizar los ataques, sus servidores y servicios que brinda para así poder usar las herramientas necesarias.

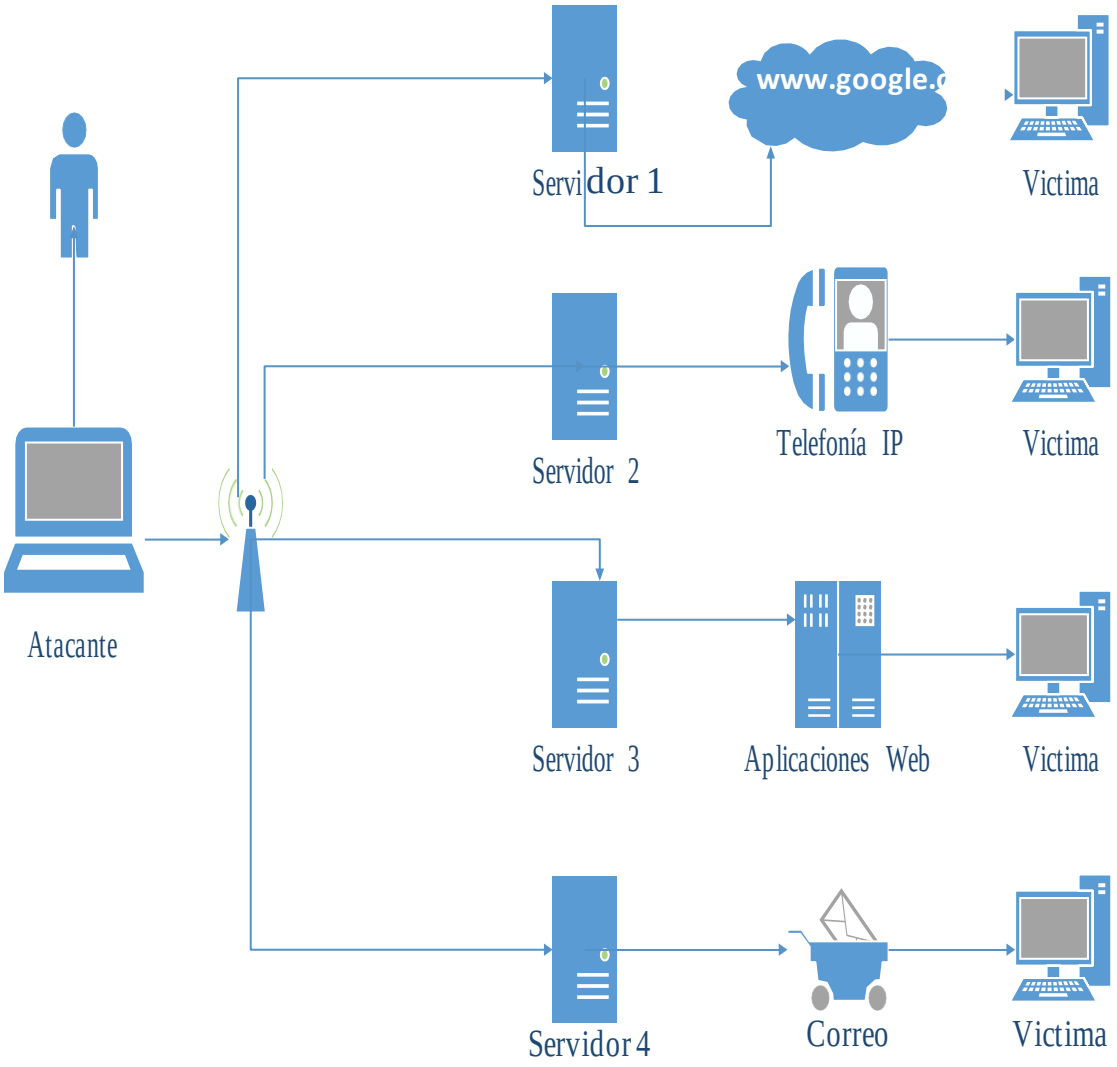


Tabla 18 Arquitectura del Pentesting informático.

2.7 Estudio de Factibilidad

2.7.1 Factibilidad Operativa

Para la implementación de las políticas de seguridad se necesitó de un personal técnico especializado en el área de redes y seguridad informática que se detalla a continuación:

Categorías	Componentes / Rubros	Cantidades
Recursos Humanos	Analista de seguridad Informática	1
Total		

Tabla 19 Recurso Humano

2.7.2 Factibilidad Técnica

En la factibilidad técnica se establecieron las herramientas de hardware y software de acuerdo con las metodologías usadas tanto en los análisis realizados.

Categorías	Componentes / Rubros	Cantidades
Recursos de Hardware	Laptop HP core i5	1
	Impresoras EPSON XP 440	1
	Partes y accesorios computacionales	-

Tabla 20 Recursos de Hardware

Categorías	Componentes / Rubros	Cantidades
Recursos de Software	Kali Linux	1
	Programa de análisis	1
	Programa de monitoreo	1

Tabla 21 Recursos de Software

Categorías	Componentes / Rubros	Cantidades
Recursos de Materiales	Suministros y accesorios	1
Total		

Tabla 22 Recursos de Materiales

2.7.3 Factibilidad Financiera

Categorías	Componentes / Rubros	Cantidades	Precio Unitario	Total
Recursos de Hardware	Laptop core i5	1	$800.00	$800.00
	Impresa Espon XP 440	1	$275.00	$275.00
				$1075.00
Recursos de Software	Kali Linux	1	$0.00	$0.00
	Programa de análisis	1	$0.00	$0.00
	Programa de monitoreo	1	$0.00	$0.00
				$0.00
Recursos Humanos	Analista de Seguridad Informática	6 (meses)	$2.400,00	$2.400,00
				$2.400,00
Recursos Materiales	Suministros y accesorios	-	$300.00	$300.00
				$300.00
Total				$3375.00

Tabla 23 Recursos Financieros del Proyecto

Costo Real del Proyecto

El presupuesto del hardware va a tener un costo cero porque la empresa cuenta con equipos que facilitan la ejecución del proyecto, poseen 5 laptops, donde se podrá realizar el pentesting informático, así como impresoras, UPS, etc. En software el presupuesto se torna a un costo cero, debido a que las herramientas para pentesting y análisis son de código abierto por ende tienen un coste de cero, A nivel operacional el costo también es cero ya que los recursos operaciones fueron abordados por quien ejecutara el proyecto. Este valor lo asumirá el operante del proyecto por tratarse de un tema de titulación, basado en el análisis realizo se concluye que el proyecto es factiblemente económico porque tiene un coste total de $300. Además, se posee las herramientas, equipos y personal necesario para la realización de la propuesta tecnológica. A continuación, se describe una tabla general del presupuesto

Categorías	Costos
Recursos de Hardware	$0.00
Recursos de Software	$0.00
Recursos Humanos	$0.00
Recursos Materiales	$300.00
Total	$300.00

Tabla 24 Financiamiento del proyecto en general

2.8 Resultados

Política de acceso remoto

1. Visión general

El acceso remoto a nuestra red corporativa es esencial para mantener la productividad de nuestro Equipo, pero en muchos casos este acceso remoto se origina en redes que ya pueden estar comprometidas o tienen una postura de seguridad significativamente menor que nuestra red corporativa. Si bien estas redes remotas están fuera del control de la política de Reacciones hiperbólicas, LLC, debemos mitigar estos riesgos externos lo mejor que podamos.

2. Propósito

El propósito de esta política es definir reglas y requisitos para conectarse a la red de Gobierno Autónomo Descentralizado Municipal de Santa Elena desde cualquier host. Estas reglas y requisitos están diseñados para minimizar la exposición potencial a Gobierno Autónomo Descentralizado [redacted] por daños que pueden resultar del uso no autorizado de los recursos de Gobierno Autónomo Descentralizado [redacted] Los daños incluyen la pérdida de datos confidenciales o confidenciales de la empresa, propiedad intelectual, daños a la imagen pública, daños a los sistemas internos críticos de Gobierno Autónomo Descentralizad[redacted] y multas u otras responsabilidades financieras incurridas como resultado de esas pérdidas.

3. Alcance

Esta política se aplica a todos los empleados, contratistas, proveedores y agentes de Gobierno Autónomo Descentralizado [redacted] con una computadora o estación de trabajo de propiedad o propiedad personal de Gobierno Autónomo Descentralizado Municipal de Santa Elena utilizada para conectarse a la

red Gobierno Autónomo Descentralizado Municipal de Santa Elena. Esta política se aplica a las conexiones de acceso remoto que se utilizan para trabajar en nombre de Gobierno Autónomo Descentralizado , incluida la lectura o el envío de correos electrónicos y la visualización de recursos web de la intranet. Esta política cubre todas y cada una de las implementaciones técnicas de acceso remoto utilizadas para conectarse a redes de Gobierno Autónomo Descentralizado

4. Política

Es responsabilidad de los empleados, contratistas, vendedores y agentes de Gobierno autónomo Descentralizado con privilegios de acceso remoto a la red corporativa de Gobierno Autónomo Descentralizado asegurarse de que su conexión de acceso remoto tenga la misma consideración que la conexión del usuario en el sitio al Gobierno Autónomo Descentralizado

El acceso general a Internet para uso recreativo a través de la red Gobierno autónomo Descentralizado está estrictamente limitado a empleados, contratistas, vendedores y agentes de Gobierno autónomo Descentralizado (en adelante, los "Usuarios autorizados"). Al acceder a la red Gobierno autónomo Descentralizado una computadora personal, los Usuarios autorizados son responsables de evitar el acceso a los recursos o datos de la computadora Gobierno autónomo Descentralizado por parte de Usuarios no autorizados. Se prohíbe la realización de actividades ilegales a través de la red Gobierno autónomo Descentralizado Municipal de Santa Elena por parte de

cualquier usuario (autorizado o no). El usuario autorizado tiene la responsabilidad y las consecuencias del mal uso del acceso del usuario autorizado. Para obtener más información y definiciones, consulte la Política de uso aceptable.

Los usuarios autorizados no utilizarán redes de Gobierno autónomo Descentralizado Municipal de [redacted] para acceder a Internet para intereses comerciales externos.

Para obtener información adicional sobre las opciones de conexión de acceso remoto de Gobierno autónomo Descentralizado [redacted] incluido cómo obtener un inicio de sesión de acceso remoto, software antivirus gratuito, solución de problemas, etc., visite el sitio web de Servicios de acceso remoto (URL de la empresa).

4.1 Requisitos

4.1.1 El acceso remoto seguro debe controlarse estrictamente con cifrado (es decir, redes privadas virtuales (VPN)) y frases de contraseña fuertes. Para obtener más información, consulte la Política de cifrado aceptable y la Política de contraseña.

4.1.2 Los usuarios autorizados protegerán su nombre de usuario y contraseña, incluso de miembros de la familia.

4.1.3 Al usar una computadora propiedad de Gobierno autónomo Descentralizado [redacted] para conectarse de forma remota a la red corporativa de Gobierno autónomo Descentralizado [redacted] los Usuarios autorizados deben asegurarse de que el host remoto no esté conectado a ninguna otra red al mismo tiempo, con la excepción de las

redes personales que bajo su control total o bajo el control completo de un usuario autorizado o un tercero.

4.1.4 El uso de recursos externos para realizar negocios de Gobierno autónomo Descentralizado Municipal [redacted] debe ser aprobado previamente por InfoSec y el gerente de la unidad de negocios correspondiente.

4.1.5 Todos los hosts que están conectados a las redes internas de Gobierno autónomo Descentralizado Municipal [redacted] a través de tecnologías de acceso remoto deben usar el software antivirus más actualizado (coloque la URL del sitio del software corporativo aquí), esto incluye las computadoras personales. Las conexiones de terceros deben cumplir con los requisitos establecidos en el Acuerdo de terceros.

4.1.6 El equipo personal utilizado para conectarse a las redes de Gobierno autónomo Descentralizado Municipal [redacted] debe cumplir con los requisitos de los equipos propios de Gobierno autónomo Descentralizado Municipal de [redacted] para acceso remoto como se establece en las Normas de configuración de hardware y software para Acceso remoto a Gobierno autónomo Descentralizado Municipal de [redacted] Redes.

5. Cumplimiento de la política

5.1 Medida de cumplimiento

El equipo de seguridad de información verificará el cumplimiento de esta política a través de varios métodos, que incluyen, entre otros, visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas e inspección, y proporcionará comentarios al propietario de la política y al negocio correspondiente. gerente de la unidad.

5.2 Excepciones

Cualquier excepción a la política debe ser aprobada por los Servicios de acceso remoto y el Equipo de seguridad de información por adelantado.

5.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

5.4 Estándares, políticas y procesos relacionados

Revise las siguientes políticas para obtener detalles sobre la protección de la información al acceder a la red corporativa a través de métodos de acceso remoto y el uso aceptable de la red de Gobierno autónomo Descentralizado Municipal de [redacted]

- Política de cifrado aceptable
- Política de uso aceptable
- Política de contraseñas
- Acuerdo de terceros
- Estándares de configuración de hardware y software para acceso remoto a redes de Gobierno autónomo Descentralizado Municipal de [redacted]

6 revisión histórica

Fecha de revisión	Responsable	Problema Encontrado	Posible Solución	Factor de riesgo
14/02/2020	Abel Ramírez Borbor	Acceso remoto dentro del departamento de informática a la PC del DBA de la Institución.	La mejor opción para el acceso remoto es a través de VPN y	Alto

14/02/2020	Abel Ramírez Borbor	Acceso remoto a la máquina del Ingeniero a cargo de la programación y cambio del sistema.	dándole permiso con privilegios de seguridad	Alto

Tabla 25 Revisión histórica

Política de protección de contraseña

1. Visión general

Las contraseñas son un aspecto importante de la seguridad informática. Una contraseña mal elegida puede resultar en acceso no autorizado y / o explotación de nuestros recursos. Todo el personal, incluidos los contratistas y proveedores con acceso a los sistemas de Gobierno Autónomo Descentralizado Municipal [redacted] es responsable de tomar las medidas adecuadas, como se describe a continuación, para seleccionar y proteger sus contraseñas.

2. Propósito

El propósito de esta política es establecer un estándar para la creación de contraseñas seguras y la protección de esas contraseñas.

3. Alcance

El alcance de esta política incluye todo el personal que tiene o es responsable de una cuenta (o cualquier forma de acceso que admita o requiera una contraseña) en cualquier sistema que resida en cualquier instalación de Gobierno Autónomo Descentralizado Municipal de [redacted] tenga acceso a Gobierno Autónomo Descentralizado Municipal de [redacted]red, o almacena cualquier información no pública de Gobierno Autónomo Descentralizado Municipal de [redacted]

4. Política

4.1 Creación de contraseña

4.2 Todas las contraseñas de nivel de usuario y nivel de sistema deben cumplir con las Pautas de construcción de contraseña.

4.2.1 Los usuarios deben usar una contraseña única y separada para cada una de sus cuentas relacionadas con el trabajo. Los usuarios no pueden usar contraseñas relacionadas con el trabajo para sus propias cuentas personales.

4.2.2. Las cuentas de usuario que tienen privilegios de nivel de sistema otorgados a través de membresías de grupo o programas como sudo deben tener una contraseña única de todas las otras cuentas que posee ese usuario para acceder a privilegios de nivel de sistema. Además, se recomienda encarecidamente utilizar alguna forma de autenticación multifactor para cualquier cuenta privilegiada

4.3 Cambio de contraseña

4.4 Las contraseñas deben cambiarse solo cuando existan motivos para creer que una contraseña se ha visto comprometida.

4.5 El equipo de Infosec o sus delegados pueden realizar descifrados o suposiciones de contraseñas de forma periódica o aleatoria. Si se adivina o se descifra una contraseña durante uno de estos escaneos, el usuario deberá cambiarla para cumplir con las Pautas de construcción de contraseña.

4.6 Protección de contraseña

4.7 Las contraseñas no deben compartirse con nadie, incluidos supervisores y compañeros de trabajo. Todas las contraseñas deben tratarse como información

confidencial y confidencial de Gobierno Autónomo Descentralizado Municipal de [redacted] Corporate Information Security reconoce que las aplicaciones heredadas no son compatibles con los sistemas proxy existentes. Consulte la referencia técnica para obtener detalles adicionales.

4.8 Las contraseñas no deben insertarse en mensajes de correo electrónico, casos de Alliance u otras formas de comunicación electrónica, ni revelarse por teléfono a nadie.

4.9 Las contraseñas solo se pueden almacenar en "administradores de contraseñas" autorizados por la organización.

4.10 No utilice la función "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web).

4.11 Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe informar el incidente y cambiar todas las contraseñas.

4.12 Desarrollo de aplicaciones

4.13 Los desarrolladores de aplicaciones deben asegurarse de que sus programas contengan las siguientes precauciones de seguridad:

4.14 Las aplicaciones deben admitir la autenticación de usuarios individuales, no de grupos.

4.15 Las aplicaciones no deben almacenar contraseñas en texto claro o en cualquier forma fácilmente reversible.

4.16 Las aplicaciones no deben transmitir contraseñas en texto claro a través de la red.

4.17 Las aplicaciones deben proporcionar algún tipo de gestión de roles, de modo que un usuario pueda hacerse cargo de las funciones de otro sin tener que conocer la contraseña del otro.

4.18 Autenticación multifactorial

4.19 Se recomienda encarecidamente la autenticación multifactor y debe usarse siempre que sea posible, no solo para cuentas relacionadas con el trabajo sino también para cuentas personales.

5. Cumplimiento de la política

5.1 Medida de cumplimiento

El equipo de Infosec verificará el cumplimiento de esta política a través de varios métodos, que incluyen, entre otros, visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas, y comentarios al propietario de la política.

5.2 Excepciones

Cualquier excepción a la política debe ser aprobada por el Equipo de Infosec con anticipación.

5.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

5.4 Estándares, políticas y procesos relacionados

- Pautas de construcción de contraseña

6. Revisión histórica

Fecha de revisión	Responsable	Problema Encontrado	Posible Solución	Factor de riesgo
14/02/2020	Abel Ramírez Borbor	Control de un pc dentro del departamento de informática, por medio de fuerza bruta, a través de un diccionario de datos.	La mejor opción para mejorar la seguridad en las contraseñas es usar caracteres y símbolos, entre más larga sea la contraseña, más dificultoso será para el atacante penetrar la seguridad del usuario.	Alto

Tabla 26 Revisión Histórica

Política de seguridad de aplicaciones web

1. Visión general

Las vulnerabilidades de las aplicaciones web representan la mayor parte de los vectores de ataque fuera del malware. Es crucial que se evalúe cualquier aplicación web para detectar vulnerabilidades y se corrija cualquier vulnerabilidad antes del despliegue de producción.

2. Propósito

El propósito de esta política es definir evaluaciones de seguridad de aplicaciones web dentro de Gobierno Autónomo Descentralizado Municipal de [redacted]. Las evaluaciones de aplicaciones web se realizan para identificar debilidades potenciales o realizadas como resultado de una configuración incorrecta involuntaria, autenticación débil, manejo de errores insuficiente, fuga de información confidencial, etc. El descubrimiento y la subsiguiente mitigación de

estos problemas limitarán la superficie de ataque de Gobierno Autónomo Descentralizado Municipal [redacted] servicios disponibles tanto interna como externamente, así como satisfacer el cumplimiento de las políticas vigentes.

3. Alcance

La política cubre todas las evaluaciones de seguridad de aplicaciones web solicitadas por cualquier individuo, grupo o departamento con el fin de mantener la postura de seguridad, el cumplimiento, la gestión de riesgos y el control de cambios de las tecnologías en uso en Gobierno Autónomo Descentralizado Municipal [redacted]

Las evaluaciones de seguridad de la aplicación web serán realizadas por personal de seguridad delegado, ya sea empleado o contratado por Gobierno Autónomo Descentralizado Municipal [redacted] Todos los hallazgos se consideran confidenciales y se deben distribuir a las personas sobre la base de "necesidad de saber". La distribución de cualquier hallazgo fuera de Gobierno Autónomo Descentralizado Municipal [redacted] está estrictamente prohibida a menos que lo apruebe el director de información.

Las relaciones dentro de las aplicaciones de varios niveles encontradas durante la fase de determinación del alcance se incluirán en la evaluación a menos que se limiten explícitamente. Las limitaciones y la justificación posterior se documentarán antes del inicio de la evaluación.

3. Política

Las aplicaciones web están sujetas a evaluaciones de seguridad basadas en los siguientes criterios:

a) Lanzamiento de aplicación nueva o importante: estará sujeto a una evaluación completa antes de la aprobación de la documentación de control de cambios y / o lanzamiento al entorno en vivo.

b) Aplicación web adquirida o de terceros: estará sujeta a una evaluación completa, después de lo cual estará sujeta a los requisitos de la política.

c) Versiones puntuales: estarán sujetas a un nivel de evaluación apropiado en función del riesgo de los cambios en la funcionalidad y / o arquitectura de la aplicación.

d) Lanzamientos de parches: estarán sujetos a un nivel de evaluación apropiado en función del riesgo de los cambios en la funcionalidad y / o arquitectura de la aplicación.

e) Liberaciones de emergencia: se permitirá que una liberación de emergencia renuncie a las evaluaciones de seguridad y asuma el riesgo asumido hasta el momento en que se pueda realizar una evaluación adecuada. Los comunicados de emergencia serán designados como tales por el director de información o un gerente apropiado a quien se le haya delegado esta autoridad.

Todos los problemas de seguridad que se descubren durante las evaluaciones deben mitigarse en función de los siguientes niveles de riesgo. Los niveles de riesgo se basan en la metodología de calificación de riesgo de OWASP. Se requerirán pruebas de validación de remediación para validar las estrategias de

reparación y / o mitigación para cualquier problema descubierto de nivel de riesgo medio o mayor.

a) Alto - Cualquier problema de alto riesgo se debe solucionar de inmediato o se deben implementar otras estrategias de mitigación para limitar la exposición antes del despliegue. Las aplicaciones con problemas de alto riesgo están sujetas a ser desconectadas o denegadas su liberación al entorno en vivo.
b) Medio - Los problemas de riesgo medio deben revisarse para determinar qué se requiere para mitigar y programar en consecuencia. Las aplicaciones con problemas de riesgo medio se pueden desconectar o denegar su lanzamiento al entorno en vivo en función de la cantidad de problemas y si varios problemas aumentan el riesgo a un nivel inaceptable. Los problemas deben solucionarse en una versión de parche / punto a menos que otras estrategias de mitigación limiten la exposición.
c) Bajo - El problema debe revisarse para determinar qué se requiere para corregir el problema y programarlo en consecuencia.

Los siguientes niveles de evaluación de seguridad serán establecidos por la organización InfoSec u otra organización designada que realizará las evaluaciones.

a) Una evaluación completa se compone de pruebas para todas las vulnerabilidades de aplicaciones web conocidas utilizando herramientas automáticas y manuales basadas en la Guía de pruebas de OWASP. Una evaluación completa utilizará técnicas de prueba de penetración manual para validar las vulnerabilidades descubiertas para determinar el riesgo general de todos y cada uno descubierto.

b) Una evaluación rápida consistirá en un escaneo automatizado (típicamente) de una aplicación para los riesgos de seguridad de la aplicación web OWASP Top Ten como mínimo.

c) Se realiza una evaluación específica para verificar los cambios de corrección de vulnerabilidad o la nueva funcionalidad de la aplicación.

Las herramientas de evaluación de seguridad de aplicaciones web aprobadas actualmente en uso que se utilizarán para las pruebas son:

- <A2SV>
- <NESSUS>

Se pueden utilizar herramientas y / o técnicas dependiendo de lo que se encuentre en la evaluación predeterminada y la necesidad de determinar la validez y el riesgo están sujetos a la discreción del equipo de Ingeniería de Seguridad.

4. Cumplimiento de la política

4.1. Medida de cumplimiento

El equipo de seguridad de información verificará el cumplimiento de esta política a través de varios métodos, que incluyen, entre otros, visitas periódicas, monitoreo de video, informes de herramientas comerciales, auditorías internas y externas, y comentarios al propietario de la política.

4.2. Excepciones

Cualquier excepción a la política debe ser aprobada por el equipo de seguridad de información con anticipación.

4.3. Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

Las evaluaciones de la aplicación son un requisito del proceso de control de cambios y deben cumplir con esta política a menos que se encuentre exento. Todas las versiones de la aplicación deben pasar por el proceso de control de cambios. Cualquier aplicación web que no cumpla con esta política se puede desconectar hasta el momento en que se pueda realizar una evaluación formal a discreción del Director de Información.

5. Estándares, políticas y procesos relacionados

- OWASP Top Ten Project
- OWASGuía de prueba de P
- OWASP Metodología de calificación de riesgo

6. Revisión histórica

Fecha de revisión	Responsable	Problema Encontrado	Posible Solución	Factor de riesgo
14/02/2020	Abel Ramírez Borbor	Utilización de correos personales, para el alojamiento de hosting o dominios de la empresa, esto causa que el atacante use esta información para realizar ingeniera social y para posibles divulgaciones de datos confidenciales.	Utilizar correos institucionales para el registro de procesos o creaciones de alojamientos, etc.	Alto

Tabla 27 Revisión Histórica

Conclusiones

- Las empresas a medida que van creciendo su información de datos se vuelve más frágil y tienden a ser atacados, por personas externas, por motivos de extorción, robo de información, etc., Por ende, la seguridad informática es la mayor prioridad que se debe tener en toda entidad.
- Las herramientas de pentesting informático son seleccionadas, basados en las necesidades para la obtención de información, el cual debe cumplir con parámetros establecidos para su manejo.
- Los reportes generados en el sistema operativo Kali Linux, muestran el comportamiento e información de vulnerabilidades que puede estar expuesto la empresa, estos datos permitirán realizar un estudio riguroso para la elaboración de posibles soluciones, en base a políticas de seguridad.
- Cada una de las fases del proyecto nos aportó varias maneras de alcanzar con los objetivos planteados, y la obtención de conocimientos.
- Las políticas de seguridad SANS, no son usadas con mucha frecuencia por las empresas debido al bajo conocimiento de información que se posee, estas plantillas ayudan a una mejor administración y toma de decisiones en caso de ataques.

Recomendaciones

- Se recomienda realizar VPN para el manejo de computadoras personales usadas remotamente por el usuario debido a que son fáciles de hackear.
- El personal que realice el escaneo de vulnerabilidades en la red deberá ser una persona externa que no conozca la estructura organizacional de la empresa, con el fin de ser más efectivo en la obtención de datos.
- En base a este proyecto y por los reportes generados, se podrían realizar investigaciones de análisis forense, ataques cibernéticos entre otras.
- Analizar y verificar rigurosamente la compatibilidad de las herramientas a emplear al momento de realizar el escaneo de vulnerabilidades, la mayoría son realizadas por terceros y estas poseen puertas traseras que ocasionarían un DNS en la empresa

Bibliografía

[1] J. Urquijo Valdivielso, "Sociedad y nuevas tecnologías: ventajas e inconvenientes," Almenara Rev. Extrem. ciencias Soc., no. 9, pp. 5–45, 2017.

[2] R. De Referencia, "Anticipa ndo lo desconocido," 2019.

[3] El comercio, "Simpatizantes de Assange han dirigido ataque a las web de varias entidades. Se indagan las actividades de Ola Bini," 16 abril, 2019. https://www.pressreader.com/ (accessed Jul. 31, 2019).

[4] C. T. C. HERIBERTO, "SISTEMA DE DETECCIÓN DE INTRUSOS EN REDES MEDIANTE EL MÉTODO HEURÍSTICO PARA EL GOBIERNO MUNICIPAL DE LA CIUDAD DE OTAVALO.," UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES "UNIANDES - IBARRA," 2016.

[5] Antonia Laborde, "'Robin Hood', el pirata cibernético que tiene paralizada la Administración de Baltimore | Tecnología | EL PAÍS," 24 Mayo, 2019. https://elpais.com/tecnologia/2019/05/23/actualidad/1558646983_883457.html (accessed Jul. 31, 2019).

[6] eltelégrafo, "Ecuador registra 40 millones de ataques cibernéticos desde fin de asilo a Assange," 15 de abril, 2019. https://www.eltelegrafo.com.ec/noticias/politica/3/ecuador-ataquesciberneticos-assange (accessed Jul. 31, 2019).

[7] "MAPA | Mapa en tiempo real de amenazas cibernéticas Kaspersky." https://cybermap.kaspersky.com/es (accessed Sep. 24, 2019).

[8] S. N. de la A. Publica, Esquema Gubernamental de Seguridad de la Información (EGSI). Ecuador: Secretaria Nacional de la Administracion.

[9] J. L. F. López, "ANALISIS Y GESTION DE VULNERABILIDADES DE SISTEMAS INFORMATICOS CON SOFTWARE LIBRE (AGVISL)," Catalunya, 2017. [Online]. Available:

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72567/6/jlopezfernanTFG0118memoria.pdf.

[10] Tarazona T César H., "AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN," Bogóta, 2015. [Online]. Available: https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/.

[11] J. Creasey, "A guide for running an effective Penetration Testing programme," Crest, no. April, pp. 1–64, 2017.

[12] "CWE - Common Weakness Enumeration." https://cwe.mitre.org/index.html (accessed Sep. 18, 2019).

[13] CISCO, "Tabla de contenido," 2018. [Online]. Available: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf.

[14] Prof. Ing. Luis Velazquez-Araque PhD., "Metodología de la investigación," Metodol. la Investig., vol. 1, no. 1, pp. 1–5, 2010, doi: 10.1007/s13398-014-0173-7.2.

[15] SANS, "Information Security Training | SANS Cyber Security Certifications & Research." https://www.sans.org/ (accessed Jul. 31, 2019).

[16] D. V. Prieto et al., "Impacto de las tecnologías de la información y las comunicaciones en la educación y nuevos paradigmas del enfoque educativo," Rev. Cuba. Educ. medica Super., vol. 25, no. 1, pp. 95–102, 2011, [Online]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21412011000100009.

[17] Plan Nacional de Desarrollo 2017-2021, "Gobierno Nacional del Ecuador," Proc. IEEE Conf. Decis. Control, pp. 3757–3764, 2017, doi: 10.1109/CDC.2014.7039974.

[18] P. Problema, "Instituto politécnico nacional," 2010.

[19] B. C. N. Geovanna, “Año: 2019,” p. 77, 2019, [Online]. Available: NARVÁEZ NARVÁEZ, Á. E. (2019). ANALISIS DE VULNERABILIDADES PARA LA RED LAN DE LA EMPRESA “HIDROMAG”, BAJO LA METODOLOGIA “OSSTMM” (Bachelor’s thesis, Quito).

[20] C. D. E. Inf, E. T. D. E. Titulaci, P. Tecnol, I. E. N. Sistemas, and I. E. N. Electr, “Península De Santa Elena Facutad De Sistemas Y,” 2015.

[21] D. Alimentos, “Seguridad de la Comida,” p. 80.

[22] Ing. Alvaro Arrieta, “Políticas Y Normas De Seguridad Informática,” 2010.

[23] J. Veloz, A. Alcivar, G. Salvatierra, and C. Silva, “Informática Y Sistemas,” vol. 1, pp. 1–12, 2017, [Online]. Available: https://doi.org/10.33936/isrtic.v1i1.194.

[24] D. Édison Flórez Vergara, F. Camilo Castro Riveros, R. Andrés Castillo Estepa Víctor Daniel Gil Vera, and J. Carlos Gil Vera, “Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas Informatic organizational security: a simulation model based on systems dynamic,” Sci. Tech. Año XXII, vol. 22, no. 2, 2017.

[25] “What is Kali Linux? | Kali Linux Documentation.” https://www.kali.org/docs/introduction/what-is-kali-linux/ (accessed Sep. 03, 2020).

[26] M. D. E. Sistemas, “Universidad autónoma de baja california sur,” 2018.

[27] A. R. M. y Terán and M. A. V. Martínez, “Aspectos Básicos de la Seguridad en Aplicaciones Web,” Universidad Nacional Autónoma de México. pp. 1–8, 2016, [Online]. Available: http://www.seguridad.unam.mx/.

[28] D. Stuttard and M. Pinto, The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, vol. 7. 2011.

[29] “About Us | The OWASP Foundation.” https://owasp.org/about/ (accessed Sep. 15, 2020).

[30] "Qué es el Pentesting | OpenWebinars." https://openwebinars.net/blog/que-es-el-pentesting/ (accessed Sep. 15, 2020).

[31] "Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de Educación Superior." https://www.redalyc.org/jatsRepo/5122/512255650001/html/index.html (accessed Oct. 12, 2020).

[32] R. Fonseca, "Universidad Politécnica Salesiana Sede Quito," Tesis, pp. 1–100, 2017, [Online]. Available: http://dspace.ups.edu.ec/bitstream/123456789/5081/1/UPS-CYT00109.pdf.

[33] Y. Gavilánez Cruz, "Metodología Osstmm Para La Detección De Errores Operativos De 64 Bits a Nivel De Usuario Final," pp. 31–43, 2016, [Online]. Available: http://dspace.espoch.edu.ec/bitstream/123456789/4598/1/20T00676.pdf.

[34] "Shodan." https://www.shodan.io/ (accessed Sep. 16, 2020).

ANEXOS

Anexo 1 Encuesta De Seguridad Informática Dirigida Al Área De Sistemas.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

ESCUELA DE INFORMÁTICA

Encuesta de Seguridad Informática dirigida al área de Sistemas

Objetivo: Con el principal objetivo de obtener información de forma personalizada acerca de los mecanismos de seguridad, de los sistemas de información y servidores que posee la empresa.

Nombre de la Institución: xxxxxxxxxxxxxxx

Nombre de Dirigente Encargado: xxxxxxxxxxxxxxx

Nota: Marcar con una **X** sus respuestas

1. ¿Existe un área o persona responsable de seguridad informática y seguridad de la información en la empresa?

   Sí ○ No ○

2. ¿Qué software utiliza en la empresa para controlar software malicioso? (se puede seleccionar varias alternativas)

   Antivirus ☐
   Anti-Spam ☐
   Antispyware ☐
   Cortafuegos/firewall ☐
   Otros, indique cuáles ☐ _____

3. ¿Cuáles de los siguientes mecanismos de autenticación utiliza en la empresa? (se puede seleccionar varias alternativas)

   Firma electrónica digital ☐
   Clave de Acceso ☐
   No tiene ☐
   Otros ☐

4. ¿Cuál es el tipo de backup que realiza a los servidores de la empresa?

Backup completo	☐
Backup diferencial	☐
Backup incremental	☐
Backup espejo	☐

5. ¿Qué servicios y sistemas considera más críticos en términos de disponibilidad? (se puede seleccionar varias alternativas)

De almacenamiento de datos	☐
Servicios de comunicación	☐
Sistemas de procesamiento de datos	☐
Otros	☐

6. ¿Existe el apoyo necesario de las máximas autoridades en temas de tecnología?

Sí ○ No ○

7. ¿Ha tenido algún incidente de seguridad en el último periodo laboral?

Sí ○ No ○

8. ¿Conocen que son los CSIRT?

Sí ○ No ○

9. ¿Le gustaría implementar un sistema de Incidente de Seguridad Informática?

Sí ○ No ○

Anexo 2 Ventajas y Desventajas de herramientas utilizadas en la detección de vulnerabilidades

Nombre de la Herramienta	Característica	Tipo	Ventajas	Desventajas
Herramientas online (netcraft)	Permiten obtener información a través de publicaciones en Internet sobre una empresa.	Online	• Fácil manejo • Da reportes muy detallados de las IP, dominios, host, etc. de la página web a escanear.	• No da reportes en xml o pdf
Maltego	Permite recolección de información y minería de datos, además enumera información relacionada con elementos de red	Open Source	• Fácil manejo • Da resultados en de forma detallada de los servidores y DNS. • Tiene una versión gratis.	• Sus funciones más potentes son de paga. • Delimitaciones en las transformadas.
Nmap	Descubrimiento de servidores Identifica puertos abiertos en un host objetivo. Determina qué servicios está ejecutando un host. Determinar qué sistema operativo y versión utiliza un host. Obtiene algunas características del hardware de la máquina objeto de la prueba	Open Source	• Facilidad de guardar los resultados en formato xml, o txt. • Puede detectar sin falta la mayor parte de los equipos conectados a una red.	• Esta herramienta utiliza el programa “ping” para realizar su escaneo y este tiene la desventaja de que hace mucho ruido en la red, lo cual puede ser detectado fácilmente por un sniffer o bien un equipo o computadora puede permanecer sin detectarse si bloquea el “ping” por medio de un

				firewall.
OpenVas Scanner	Escaneo de varios hosts simultáneamente Soporte SSL para OTP Soporte de WMI (opcional)Gestión de notas para resultados de escaneo Gestión de falsos positivos Escaneos programados Gestión de usuarios	Open Source	• Obtención rápida de información • Facilita el trabajo para gente poco experimentada	• Limitados a la información de los plugins y firmas que dispongan en el momento de análisis • Pueden producir falsos positivos.
Nslookup	es una herramienta que permite consultar un servidor de nombres y obtener información relacionada con el dominio o el host y así diagnosticar los eventuales problemas de configuración que pudieran haber surgido en el DNS.	Open Source	• Tiene un parámetro que al escribir en minúscula o mayúscula no tiene relevancia	• Sus resultados pueden ser complejos de entender
A2SV	Es una herramienta que sirve para hacer escaneo de una página web buscando vulnerabilidades SSL.	Open Source	• Fácil manejo en su instalación. • Sus resultados son en formato (Common Vulnerabilities and Exposures)	• No se puede exportan en formatos pdf • Y solo está disponible para Linux.

Dmitry	Es un programa en línea de comando para UNIX/GNU/Linux, escrita completamente en C, la cual proporciona la capacidad de obtener tanta información como sea posible sobre un host objetivo.	Open Source	• Hace una recogida de información más extensa y sus resultados se pueden guardar en xml.	• Encontramos que solo es posible contar con la versión en inglés de la herramienta y que el escaneo de puertos utiliza TCP lo que implica una comunicación de tres pasos que puede dejar huellas en el log del servidor o ser detectado por un sistema de detección de intrusos.
DNsenum	El propósito de DNSenum es capturar tanta información como sea posible sobre un dominio.	Open Source	• Buena organización de los resultados que nos pueden ayudar en el reconocimiento que se está realizando.	• Solo está disponible para Linux.
theHarvester	TheHarvester: Esta herramienta permite realizar una búsqueda en internet de direcciones de correos electrónicos a partir de un dominio.	Open Source	• La recolección de información la podemos exportar en xml.	• Solo está disponible para Linux.
OWASP ZAP	Es un escáner de seguridad web de código abierto. Pretende ser	Open Source	• Posee un interfaz gráfico de gran uso.	• El escaneo puede demorar, según la velocidad del internet.

	utilizado como una aplicación de seguridad y como una herramienta profesional para pruebas de penetración.		• Los resultados se pueden exportan en formato xml, pdf.	
Vega		Open Source.	• Encontrar fallos de seguridad y corregirlos y los datos pueden ser extraídos en formato xml, pdf.	Otros pueden encontrar los fallos y pueden cambiar toda la página.

Anexo 3 Certificado de aprobación de la Empresa

[redacted]

[redacted]

EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SANTA ELENA

HACE CONSTAR

Que el Señor Abel **Fabricio Ramirez Borbor** con Cédula de Identidad **2450629940,** egresado de la **Facultad de sistemas y telecomunicaciones Carrera de Ingeniera en sistemas,** quien realizo un reporte de vulnerabilidades encontradas en el GAD Municipal con sus respectivas políticas de seguridad, como tema de su propuesta tecnológica "ANÁLISIS PROACTIVO DE AMENAZAS DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN PARA LA INFRAESTRUCTURA DE SERVIDORES Y RED DE LA DIRECCIÓN DE TIC DE UN GAD MUNICIPAL" , cumple a cabalidad todos los **requerimientos** emitidos por nosotros.

Esta constancia se expide a solicitud del interesado **para anexar** a su documentación de su propuesta tecnológica.

[redacted]

Ing. Fabián Rolando Yagual del Pezo
Director de Informática y Tecnología
GOBIERNO MUNICIPAL DE [redacted]

Anexo 4 Certificado Antiplagio

La Libertad, 20 de octubre del 2020.

Ing. Freddy Villao S.
Director (E) de Carrera En su despacho.

Por medio de la presente me es muy grato saludarle y poner a su disposición el resultado del análisis del software anti-plagio URKUND del documento con el tema de titulación **"Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de TIC de un Gad Municipal"**, correspondiente a la Sr. Ramírez Borbor Abel Fabricio, estudiante de la Carrera de Ingeniería en Sistemas.

URKUND

Document Information

Analyzed document	PropuestaTecnologicaAbelRamirez.docx (D82236706)
Submitted	10/20/2020 9:15:00 PM
Submitted by	DANIEL IVAN QUIRUMBAY YAGUAL
Submitter email	dquirumbay@upse.edu.ec
Similarity	4%
Analysis address	dquirumbay.upse@analysis.urkund.com

Lsi. Daniel Quirumbay Yagual, MSIA

Docente Tutor

C.C.: Dirección Carrera Informática, Archivo