DETERMINACIÓN DEL NIVEL DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MAYOR DE TUNJA

PROPONENTE

LINA MARÍA WITTINGHAM JIMÉNEZ

PASANTÍA EMPRESARIAL

UNIVERSIDAD SANTO TOMÁS TUNJA

INGENIERÍA DE SISTEMAS

2018

DETERMINACIÓN DEL NIVEL DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA ALCALDÍA MAYOR DE TUNJA

PROPONENTE

LINA MARÍA WITTINGHAM JIMÉNEZ

CC 1.056.803.677 SAMACÁ

CÓDIGO: 2150600

DIRECTORES

Ingeniera Julieta Bernal

Alcaldía mayor de Tunja

Ingeniero Alex Puertas González
Universidad Santo Tomas Tunja

PASANTÍA EMPRESARIAL

UNIVERSIDAD SANTO TOMÁS TUNJA

INGENIERÍA DE SISTEMAS

2018

AGRADECIMIENTOS

Agradezco a todas las personas que directa o indirectamente me colaboraron para la elaboración de la pasantía empresarial, entre las cuales puedo nombrar: a la Ing. Julieta Bernal, Ingeniera del Área de Sistemas de la Alcaldía Mayor de Tunja, por abrirme las puertas de la entidad, la información, conocimiento y ayuda suministrada durante mi estadía dentro de la Alcaldía; a la Universidad Santo Tomás, por el nivel de educación implementado dentro de programa de Ingeniería de sistemas, el cual me permitirá ser una profesional integra y con valores demarcados; a todos los docentes que hicieron parte de mi formación durante todos estos años, ya que me compartieron sus valores y conocimientos, para así fortalecerme como estudiante y persona; a mis compañeros y personas que hicieron parte en mi vida, porque de ellos aprendí diversidad de aspectos necesarios para la profesión y la vida; a mis padres e hija por ser parte de mi vida darme lo mejor de cada uno de ellos y estar conmigo en todo momento; por último y no menos importante a mi director de pasantía empresarial, el Ing. Alex Puertas González, por aguantarme bastante durante todo este tiempo, por el aporte de sus conocimientos, experiencias y valores no solo en mi pasantía empresarial sino también en mi formación como profesional y como persona, del cual aprendí demasiado y estaré eternamente agradecida.

Lina María Wittingham Jiménez.

DEDICATORIA

A mis padres, por estar conmigo en cada paso de mi vida, por ser constantes, mi guía, por regalarme el milagro de la vida y permitirme luchar por mis sueños y metas. A mi mamá, por saber tener paciencia y ser incondicional conmigo, por estar en mis esfuerzos, en mis días buenos y malos, en mis logros y en toda mi vida. A mi papá por su apoyo, por estar conmigo siempre, a presar de la distancia. A mi hija por ser mi tesoro más preciado, mi fuerza, mis sonrisas en momentos que desfallecí y mayor inspiración para lograr todo lo que me he propuesto desde el momento en que llego a mi vida.

También a todos aquellos que son y serán mis pilares durante toda mi vida, les dedico este logro porque cada uno de ellos supo aguatarme y quererme a su manera. Infinitas gracias a todos los que creyeron en mí, incluso cuando ni yo misma lo hacía. Los llevo en mi corazón y sé que cada una de estas personas lo sabe.

Lina María Wittingham Jiménez.

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

1. ASPECTOS GENERALES

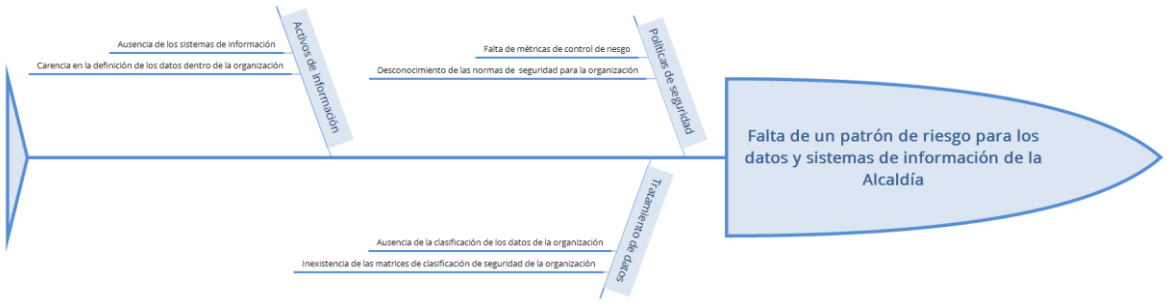
1.1. TÍTULO PASANTÍA

Determinación del nivel de seguridad de los sistemas de información de la Alcaldía mayor de Tunja.

1.2. PLANTEAMIENTO DEL PROBLEMA

Hoy en día, los sistemas de información son considerados como un activo tecnológico de gran importancia en los ámbitos institucionales; dado que representan la base de operaciones para los procesos de la organización. Esto reviste gran importancia debido a que, al presentarse alguna alteración sobre estos activos, se pueden detener o malograr las operaciones propias de la entidad, afectándose la disponibilidad, confidencialidad e integridad de la información, logrando la modificación y/o alteración, tanto de los datos necesarios para el funcionamiento de la entidad, como de los sistemas mismos. Tal es el caso de la Alcaldía Mayor de la Ciudad de Tunja, organización que al momento, no cuenta con un patrón de riesgo definido para el tratamiento de datos y sistemas de información, de acuerdo al Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, el cual se operativiza a través del manual de estrategia de gobierno en línea en su eje de seguridad y privacidad de la información. Así las cosas, no existe un estudio en donde se pueden encontrar las posibles vulnerabilidades que a este respecto, se encuentren en la Alcaldía. Debido a lo anterior es posible que puedan ocurrir robos, copias no autorizadas y revelación de información. Teniendo en cuenta que, con respecto a esto, se afecta el funcionamiento de la Alcaldía, presentándose fallas técnicas por falta de seguridad las cuales comprometen a toda la entidad.

Figura 1. Diagrama de causa y efecto



Fuente: Autor

1.3. ALCANCES

Para el presente trabajo se realizar los siguientes alcances.

- Se identificaran las características de los sistemas de información Tusig y Portal tributario, en la Alcaldía mayor de Tunja, teniendo en cuenta la descripción de los mismos, basada en los estándares establecidos por el MinTIC.

- Se implementará una matriz definida en la cual existan basada en las variables a evaluar y que cumpla los requerimientos dispuestos por el MinTIC, cuyo objetivo es describir los niveles de seguridad y la ponderación de las vulnerabilidades que se encuentren dentro de los sistemas de información. No se realizara ningún tipo de ataque pensando en el funcionamiento y operatividad adecuada de la alcaldía.

- En el plan de recomendaciones se darán a conocer los controles y acciones para notificar a la Alcaldía. Al igual, se generará un documento donde se describen los hallazgos, las vulnerabilidades, riesgos y grados afectación de los sistemas de información.

1.4. JUSTIFICACIÓN

En la actualidad, la implementación de análisis de seguridad dentro de un entorno empresarial, reviste especial importancia, debido a que, gracias a estos, es posible verificar el nivel de riesgo de la información dentro de la entidad, además de permitir una evaluación de las vulnerabilidades inherentes a los sistemas de información existentes en la organización, con lo cual se pueden elaborar contramedidas y planes de contingencia para salvaguardar los activos informáticos al interior de la dependencia; en este caso la sede central de la Alcaldía Mayor de Tunja.

Por otra parte, la aplicación de guías de seguridad, apoyadas en leyes de tipo nacional, reviste un valor especial en la dinámica del tratamiento de la información en entidades públicas, como lo es en este caso. Es así que, al implementar el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015 donde se menciona que la seguridad y privacidad de la información se debe regir teniendo en cuenta su correspondiente normatividad. Como por ejemplo la norma NTC-ISO-IEC 27001:2013, se da cumplimiento a los requerimientos gubernamentales en este aspecto.

Finalmente, con la aplicación de las técnicas de clasificación y medición de riesgo informático de este trabajo, se podrán generar indicadores que permiten ajustar los planes de compras y actualizaciones de los sistemas de información de la Alcaldía, en torno a la integridad, confidencialidad y disponibilidad de los datos dentro de la entidad y así, optimizar el funcionamiento, tanto de las plataformas de software de la entidad, como de la Alcaldía en sí misma.

1.5. OBJETIVOS

1.5.1. Objetivo General. Determinar el nivel de seguridad de los sistemas de información Tusig e Impuestos, finanzas plus y Portal tributario, en la Alcaldía mayor de Tunja, mediante matrices de clasificación y metodologías específicas, con el fin de verificar su nivel de riesgo en la organización.

1.5.2. Objetivos específicos. La descripción de los objetivos específicos se puede apreciar en la Tabla 1.

Tabla 1.Objetivos específicos

Nro.	Objetivo específico
1	Identificar las características de los sistemas de información de la alcaldía mayor de Tunja que serán objeto de estudio, a partir de la metodología propia del MinTIC, para el establecimiento de su nivel de relevancia y vulnerabilidad en la organización.
2	Determinar las matrices de clasificación de seguridad para los sistemas de información de la alcaldía mayor de Tunja, mediante metodologías de medición en seguridad, para la determinación de su nivel de riesgo.
3	Diseñar un plan de recomendaciones para las vulnerabilidades de los sistemas de información seleccionados, con base en los resultados de medición de riesgo.

Fuente: Autor

1.6. MARCO REFERENCIAL

Dentro del presente marco referencial se menciona la terminología, normas legales y metodologías las cuales se involucraron directa o indirectamente para el desarrollo de la pasantía, para así un mejor entendimiento de las consideraciones en general.

1.6.1. Marco Teórico. A continuación se describe la terminología necesaria con el objetivo de conceptualizar al lector.

1.6.1.1. Sistemas de información. Un sistema de información es un conjunto de elementos organizados, relacionados y coordinados entre sí, con una finalidad específica, tanto así que facilitan el funcionamiento de una empresa u organización. Los sistemas de información comparten una serie de propiedades las cuales son: proveer información, manejar una materia prima como los datos e información, con una organización interna que permite desempeñar funciones, tales como, captar datos, almacenarlos, procesarlos y entregar información. **(Aguilera López, 2010).**

Según Aguilera López, 2010 los elementos que interactúan dentro de un sistema de información son:

- Los recursos, estos pueden ser físicos como los computadores, componentes, periféricos y conexiones, recursos no informáticos y lógicos como sistemas operativos y aplicaciones informáticas.

- Equipo humano, el cual esta compuestos por las personas que trabajan para la empresa u organización.

- Información, esto representa el conjunto de datos organizados que tienen un significado, la cual puede estar contenida en todo tipo de soporte.

- Actividades que la organización, relacionadas o no con la información.

1.6.1.2. Activo informático o información. Un activo se define como aquel recurso de un sistema (informático o no) necesario para que una organización alcance los objetivos propuestos; o sea, todo aquello que tenga valor y que deba ser protegido frente a un posible percance, ya sea intencionado o no. Se considera como activos: los trabajadores, el software, los datos, el hardware, las comunicaciones, etc **(Escrivá Gascó, y otros, 2013).**

La seguridad informática tiene como objetivo proteger los activos, por lo que la primera labor es identificarlos para así establecer los mecanismos necesarios para su protección y analizar la relevancia de los mismos en la organización **(Escrivá Gascó, y otros, 2013)**.

Según Escrivá Gascó, y otros, 2013 algunos activos de los que se deben tratar son:

- **Información:** todo aquel elemento que contenga datos almacenados en cualquier soporte. Es decir documentos, libros, Patentes y datos almacenados en un sistema de información.

- **Software**: programas o aplicaciones que utilizan las entidades para su buen funcionamiento o para automatizar las actividades de la entidad.

- **Físico:** toda la infraestructura tecnológica que es utilizada por la entidad para almacenar, procesar, gestionar o trasmitir en función de las actividades que conciernen a la entidad. Dentro de esta categoría se encuentra incluida toda la infraestructura física, tales como armarios, sala de servidores, entre otros.

- **Personal de la entidad:** las personas que utilizan la estructura tecnológica, y de comunicación para el manejo de información, es decir funcionarios de la entidad, contratistas, etc.

1.6.1.3. Amenaza. Como amenaza se entiende una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produzca una violación de seguridad, afectando parte de la información y de la tecnología de la información de la organización **(Baca Urbina, 2016).**

Cuando la información, la tecnología de la información, o cualquier otro tipo de activo que pueda ser víctima de una amenaza, se ven afectados, no lo hacen en todas sus dimensiones ni en la misma cuantía. Por tanto, una vez que se determinar la amenaza que podría afectar a un activo, hay que estimar cuan vulnerables es dicho activo en dos sentidos, primero degradación, esto significa cuan perjudicado podría resultar el activo y el costo en su reparación o reposición, y segundo frecuencia, que significa cada cuando se materializa una amenaza. Después, se tiene que determinar en qué consisten las amenazas y en que pueden afectar a cada activo de la empresa y causar un daño considerable **(Baca Urbina, 2016)**. Las amenazas se suelen dividir en pasivas y activas según Baca Urbina, 2016, es decir en función de las acciones realizadas:

- Amenaza pasiva: también conocidas como “escuchas”. Su objetivo es obtener información relativa a una comunicación.

- Amenaza activa: que trata de realizar algún cambio no autorizado al sistema de información o activo, por eso son consideradas más peligrosas que las pasivas.

1.6.1.4. Vulnerabilidad. Una vulnerabilidad constituye un hecho o actividad que permite materializar una amenaza. Se considera vulnerable en la medida en que no hay suficiente protección como para que se evite que llegue a materializar la amenaza. Actualmente se contempla que hay ataques que son intencionados y no intencionados, aspecto que debe tenerse en cuenta a la hora de diseñar un sistema, ya que se deben prever todo tipo de amenazas existentes o que pueden existir en el futuro. **(Baca Urbina, 2016)**.

Con base a lo anterior, se puede distinguir las diferencias entre vulnerabilidad y amenaza, ya que una vulnerabilidad se refiere a las condiciones y características propias de los

sistemas de información o redes de comunicación, que los hacen susceptibles a sufrir una o varias amenazas **(Escrivá Gascó, y otros, 2013)**; en tanto que, una amenaza es toda acción que aprovecha una vulnerabilidad para poner en riesgo la seguridad de la información **(Baca Urbina, 2016)**.

1.6.1.5. Riesgo. En un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema **(Baca Urbina, 2016).** Es así que existen diversas definiciones para el término riesgo: entre todas se pueden destacar las siguientes **(Escrivá Gascó, y otros, 2013):**

- Según UNE-71504:2008, un riesgo es la estación del grado de exposición a que una amenaza pueda ser materializada sobre uno o más activos de información, causando daños o perjuicios a la entidad u organización.

- El CCN (Centro Cristológico Nacional de España) define el riesgo es la probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad y así causar un daño (impacto) en un proceso o un sistema.

Basado en lo anterior, el riesgo se define como una medida de la probabilidad de que se pueda materializar una amenaza, es decir, la ecuación **Riesgo = Probabilidad x Impacto**. Para poder establecer unos procedimientos de seguridad adecuados, será necesario realizar una clasificación de los datos y un análisis de riesgos con el fin de establecer prioridades y realizar una administración más eficiente de los recursos de la organización **(Escrivá Gascó, y otros, 2013).**

En los análisis de riesgos, se debe tener en cuenta que activos existen y se debe proteger, sus vulnerabilidades y amenazas, así como la probabilidad que produzca el impacto de las mismas; el análisis de riesgos permiten recomendar qué medidas se deberían tomar para conocer, prevenir, impedir, reducir o controlar los riesgos que ya habían sido identificados con anterioridad para así poder reducir al mínimo su potencialidad o posibles daños **(Escrivá Gascó, y otros, 2013).**

1.6.1.6. Ataque. Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema de información para causar un impacto sobre el, incluso tomar control sobre el mismo. Se trata de acciones tanto como intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema, de hecho se distingue entre ataques (acciones intencionadas) y errores (acciones fortuitas) (Escrivá Gascó, y otros, 2013).

Normalmente un ataque pasa por las siguientes fases según Escrivá Gascó, y otros, 2013:

- **Reconocimiento:** consiste en obtener toda la información que se considere necesaria de la víctima, ya sea una persona o una organización.

- **Explotación:** se trata de conseguir la información sobre el sistema a atacar, un ejemplo puede ser, la dirección IP, nombres de host, datos de autenticación, entre otros.

- **Obtención de acceso:** A partir de la información descubierta en la fase anterior, se intenta aprovechar alguna vulnerabilidad detectada en la victima para así llevar a cabo un ataque.

- **Mantenimiento del acceso:** Después de acceder al sistema, se busca la forma de implantar herramientas que permita un nuevo acceso al sistema en futuras ocasiones.

- **Borrado de huellas:** Por último, se intentaran borrar las huellas que se hayan podido dejar durante la intrusión así evitando ser detectado.

Hoy en día existen una gran variedad de herramienta de seguridad (como Nmap, Nessus, Wireshark, entre otras.) que permiten conseguir un buen nivel de seguridad, pero hay estrategias de ataque que se hacen orientadas a aprovechar las debilidades tanto de tipo informático como humano **(Escrivá Gascó, y otros, 2013)**.

1.6.1.7. Seguridad de la información. La seguridad informática, o de forma más global, la seguridad en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que involuntariamente no se exponga los datos y recursos (tanto físicos, lógicos y humanos) que permite el almacenamiento y transmisión de la información que se contiene. **(Raphaël RAULT, 2015).**

De la misma manera la seguridad informática y/o de la información es la disciplina que se encarga de diseñar y proporcionar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro. Los sistemas de información, no obstante a las medidas de seguridad que se les apliquen, no dejan de tener un margen de riesgo. Tanto así que se debe establecer un sistema de seguridad donde es necesario conocer los elementos que componen los sistemas de información, los peligros que afectan al sistema ya sean accidentales o provocados y las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Así mismo se encarga de preservar la confidencialidad, la integridad y la disponibilidad de la información; además, puede llegar a involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad **(Aguilera López, 2010).**

Existen tipos de seguridad, la **activa** donde se comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan los sistemas de información; la **pasiva** está conformada por medidas que se implantan cuando se llegue a producir un incidente de seguridad, para así minimizar su afectación y repercusión, al igual facilitar la recuperación del sistema de información; la **física** se asocia a la protección del sistema ante las posibles amenazas tales como incendios, robos, etc; la **lógica** son los mecanismos que protegen los datos, aplicaciones y sistemas operativos de un SI **(Escrivá Gascó, y otros, 2013).**

1.6.1.8. Integridad de la información. Según Bishop en Computer Security, de quien se extrae la información de este ítem, la integridad hace referencia a la veracidad de los datos o recursos, y que por lo general es expresada en términos de prevención de cambios impropios o no autorizados. La integridad incluye integridad de datos (es decir el contenido de la información) y la integridad de origen (la fuente de los datos, a menudo

también llamada autenticación). La fuente de la información puede influir en su credibilidad, precisión y la confianza que las personas depositan en la información. Esta dicotomía ilustra el principio de que el aspecto de integridad conocido como credibilidad, ya que es fundamental para el adecuado funcionamiento de un sistemas.

Los mecanismos de integridad se encuentran divididos en dos clases: mecanismos de prevención y mecanismo de detección. Los mecanismos de prevención buscan mantener la integridad de los datos bloqueando cualquier intento no autorizado de cambiar los datos o cualquier intento de cambiar los datos en formas no autorizadas. La diferencia entre estos dos tipos de intentos es importante. Debido a que, lo primero ocurre cuando un usuario intenta cambiar datos de los que no tiene autorización para cambiar. Lo segundo ocurre cuando un usuario autoriza realizar ciertos cambios en los datos o intenta cambiarlos de otras maneras. La autenticación y los controles de accesos adecuados generalmente detendrán los ataques desde el exterior, pero la prevención de cada intento requiere de diferentes controles.

Los mecanismos de detección no intentan prevenir las violaciones de la integridad; ellos simplemente informan que la integridad de los datos no es confiable. Los mecanismos de detección pueden analizar los eventos del sistema (acciones del usuario o del sistema) para detectar los posibles problemas o puede analizar los datos, para ver en si las restricciones requeridas o esperadas se mantienen. Los mecanismos pueden informar la causa real de la violación de integridad (se modificó una parte especifica de un archivo), o solo pueden informar que el archivo se encuentra dañado.

1.6.1.9. Confidencialidad de la información. Según Bishop en Computer Security, de quien se extrae la información de este ítem, la confidencialidad es la ocultación de información o recursos. La necesidad de mantener secreta la información surge del uso de computadores con información sensibles como las industrias y el gobierno. Por ejemplo, las instituciones gubernamentales de carácter militar y civil a menudo restringe el acceso a la información a quienes necesitan esa información.

Los mecanismos de control de acceso respaldan la confidencialidad. Un mecanismo de control de acceso para preservar la confidencialidad es la criptografía, que codifica datos para hacerlos incomprensibles. Una clave criptográfica controla el acceso a los datos que no se encuentran codificados, pero luego la clave criptográfica se convierte en un dato el cual se debe proteger.

El ocultamiento de recursos es otro aspecto importante de la confidencialidad. Los sitios a menudo desean ocultar su configuración y los sistemas que utilizan; las organizaciones pueden desear que otros no conozcan su información (porque se podría usar sin autorización o de maneras inapropiadas).

1.6.1.10. Disponibilidad de la información. Según Bishop en Computer Security, de quien se extrae la información de este ítem, La disponibilidad se refiere a la capacidad de usar la información o el recurso deseado. El aspecto de la disponibilidad que es relevante para la seguridad, es que alguien deliberadamente puede negar el acceso a los datos o un

servicio al hacerlo no disponible. Los diseños de sistemas usualmente asumen un modelo estadístico para analizar los patrones de uso esperados, y los mecanismos de seguridad aseguran la disponibilidad cuando se mantiene este modelo. Alguien puede manipular el uso (o los parámetros que controlan el uso, como el tráfico de red) para que las suposiciones de modelo estadístico no sean válidas, esto significa que los mecanismos para mantener los recursos o datos disponibles funcionan en un entorno para el que no fueron diseñados.

Los intentos de bloquear la disponibilidad, son llamados ataques de denegación de servicio, pueden ser los más difíciles de detectar, porque el análisis determina los patrones de accesos inusuales que son atribuibles a la manipulación deliberada de los recursos o del medio ambiente. Para complicar esta determinación en la naturaleza de los modelos estadísticos, incluso si el modelo describe con precisión el entorno, los eventos atípicos simples contribuyen a la naturaleza de las estadísticas.

1.6.1.11. SGSI (Sistema De Gestión De La Seguridad De La Información). ISMS es el concepto equivalente en inglés, a las siglas de Information Security Management System **(Blog especializado en Sistemas de Gestión , 2017).** Un SGSI seria, un conjunto de medidas de una entidad específica, destinadas para preservar la integridad, confidencialidad y disponibilidad de la información, independientemente del tipo, soporte, etc, de la misma **(Escrivá Gascó, y otros, 2013)**.

La norma NTC-ISO/IEC 27001 específica que, como cualquier otro sistema de gestión, el SGSI incluye tanto la entidad como las políticas, las responsabilidades, las actividades, los procedimientos y los recursos de la misma. Es decir, la documentación de soporte como las actividades u tareas que son realizadas. La norma ISO define que los sistemas de gestión siempre deben estar documentados, ya que, es una manera formalizar las normas e intrusiones y, también, son más fáciles de trasmitir y comunicar, como no sucede en la información verbal de tipo informal **(Gómez Fernández , y otros, 2012)**.

Una organización, empresa o entidad puede elegir implementar estas normas (SGSI e ISO) o decidir establecer su propia política para la gestión de seguridad **(Escrivá Gascó, y otros, 2013).**

1.6.1.12. Ciclo o formula PHVA (Planificar-Hacer-Verificar-Actuar). Las siglas del ciclo o formula PHVA forman un acrónimo por las iniciales de las palabras Planificar, Hacer, Verificar y Actuar. Cada uno de estos cuatro conceptos corresponde a una fase o etapa del ciclo **(ISOTools, 2015):**

- **Planificar:** En esta etapa se establecen los objetivos y se identifican los procesos necesarios para lograr ciertos resultados de acuerdo a las políticas que la organización maneja. En esta etapa se define también los parámetros de medición que se van a emplear para controlar y seguir el proceso.

- **Hacer:** Radica en la implementación de los cambios o acciones necesarias para lograr las mejoras ya planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente

los probables errores en la ejecución, normalmente se desarrolla en un plan piloto a modo de prueba.

- **Verificar:** Ya puesto en marcha el plan de mejoras, se establece un periodo de prueba para medir y valorar la capacidad y efectividad de los cambios. Se trata de una fase de regulación y ajuste.

- **Actuar:** Se realiza una vez ejecutadas las mediciones, dado el caso de que los resultados no se encuentren dentro las expectativas y objetivos predefinidos, se deberán realizar las correcciones y modificaciones que se consideren necesarias. Por otra parte, también se toman las decisiones y acciones pertinentes para la mejora continua en el desarrollo de los procesos.

Los resultados de la implementación de este ciclo permiten a las organizaciones o entidades una mejora integral de los productos y servicios, ayudando continuamente a la calidad, reduciendo costo, optimizando la productividad e incrementando la rentabilidad de la entidad y la organización **(ISOTools, 2015).**

1.6.1.13. Modelo de Seguridad y Privacidad de la Información (MSPI). El Modelo de Seguridad y Privacidad de la Información (MSPI), conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, tanto así que permite garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo **(MinTIC, 2016).**

El MSPI es el instrumento que se pone a disposición de las entidades con el fin de realizar el análisis de impacto que la información en la privacidad y la seguridad, que se pueda presentar a partir del desarrollo de funciones correspondiente a cada entidad, teniendo como referencia **(MinTIC, 2016):**

- Marco legal vigente.

- Las necesidades de los clientes internos y externos de la entidad.

- La identificación de los posibles problemas recurrentes relacionados con la privación y la seguridad.

1.6.1.14. NTC-ISO/IEC 27001. ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa u organización. La versión más reciente publicada es la 2013 y cuyo nombre completo es ISO/IEC 27001:2013; la primera versión fue publicada en 2005 la cual fue desarrollada en base a la norma británica BS 7799-2 **(ISOTools, 2018).**

La norma ISO 27001, como el resto de normas aplicables a los sistemas de gestión, está pensada para que sea empleada en todo tipo de organizaciones (tales como, empresas privadas y públicas, entidades sin ánimo de lucro, entre otras), sin importar el tamaño o actividad **(Gómez Fernández , y otros, 2012).**

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente, teniendo en cuenta que, la aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un "enfoque basado en procesos" **(ISO27000, 2006).**

En esta norma se especifican los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad requeridos, de acuerdo a las necesidades que presenta la entidad **(Gómez Fernández , y otros, 2012).**

1.6.1.15. Metodología STRIDE. El término STRIDE es un esquema de clasificación de amenazas conocidas según los tipos de ataques que se utilizan (o motivaciones del atacante) **(Microsoft, 2009)**. STRIDE es el acrónimo que se forma a partir de la primera letra de cada una de las categorías, las cuales serían **(OWASP, 2018** y **microsoft, 2009):**

- **Spoofing (Suplantación de identidad):** Hace referencia al uso de técnicas de suplantación de identidad por lo general con usos maliciosos o de investigación. Un ejemplo de suplantación de identidad es el acceso ilegal, luego uso de la información de autenticación de otro usuario, ingresando así con el nombre de usuario de otra persona.

- **Tampering (Manipulación de datos):** Los usuarios puede potencialmente cambiar los datos de un sistema, retornarlos al SI y, de ese modo, manipular la información del cliente. Los ejemplos incluyen cambios no autorizados realizados en datos persistentes, como los que son guardados dentro de una base de datos y la alteración de datos que viajan entre dos computadores a través de internet.

- **Repudiation (Repudio):** Las amenazas de repudio están asociadas a usuarios que niegan el hecho de realizar una acción dentro de un SI, sin que otras partes tengan alguna forma de probar lo contrario; por ejemplo, un usuario realiza operaciones ilegales en un sistema, que carece de la capacidad de realizar un rastreo de las mismas.

- **Information Disclosure (Divulgación de información):** En este punto, se habla de la posibilidad de que un atacante revele de manera pública los datos de un usuario, ya sea de manera anónima o como un usuario autorizado, logrando una pérdida de confianza y reputación. Las amenazas de divulgación exponen la información de los usuarios a quienes no tienen acceso a ella. Por ejemplo, la capacidad de usuarios para leer un archivo en específico, se da por acceso que un administrador le da a este usuario, sobre el documento en cuestión. Si una tercera persona, está en capacidad de acceder a este recurso, sin los permisos correspondientes, bien sea de forma voluntaria o no, se dice que hay una revelación de información.

- **Denial of service (Denegación de servicio):** Los ataques de denegación de servicio (DoS) no permiten el acceso a los usuarios a una aplicación, componente o sistema de información, por ejemplo, el hacer que un servicio web no esté disponible o no se pueda utilizar por un periodo de tiempo, a través de la inundación de la tarjeta de red del servidor que los aloja.

- **Elevation of Privilege (Elevación de privilegios):** Si un sistema de información tiene funciones administrativas y roles de usuario definidos, es de vital importancia garantizar que el usuario no pueda usar funciones a las cuales no se le a otorgado el acceso correspondiente. Este tipo de amenaza, le da permisos suficientes a un usuario para comprometer el sistema. La elevación de privilegios incluye aquellas situaciones en que el atacante puede llegar a vulnerar eficazmente todas las defensas del sistema y se ha convertido en parte del mismo.

1.6.1.16. Base de datos de vulnerabilidades CVE. "The CVE List was launched by MITRE as a community effort in 1999, and the U.S. National Vulnerability Database (NVD) was launched by the National Institute of Standards and Technology (NIST) in 2005" **(CVE, 1999 - 2005)**.

CVE – "A list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including NVD" (CVE, 1999 - 2005)**.**

NVD – "A vulnerability database built upon and fully synchronized with the CVE List so that any updates to CVE appear immediately in NVD" **(CVE, 1999 - 2005).**

1.6.1.17. NIST. NIST por sus siglas en inglés, National Institute of Standards and Technology, en español Instituto Nacional de Normas y Tecnología, es una agencia de la Administración tecnológica del departamento de comercio de Estados Unidos, cuya misión es la de promover la innovación y competencia industrial en los Estados Unidos a través de metodologías normas y tecnologías de forma que mejoren la estabilidad económica y la calidad de vida de las personas **(NIST, 2015)**.

1.6.1.18. OWASP. OWASP (acrónimo de Open web application Security Project, en español proyecto abierto de seguridad de aplicaciones web) Es una organización benéfica sin fines de lucro, de nivel mundial, y que se enfoca en mejorar la seguridad informática, haciéndola visible para las personas, organizaciones y entidades interesadas en la toma de decisiones a este respecto, y de forma oficial. Está compuesta por una comunidad de profesionales, que emiten herramientas de software y documentación basada en conocimientos sobre seguridad de las aplicaciones y la información**.** Actualmente, los proyectos de OWASP son: Proyectos en documentación: Guía OWASP, OWASP top ten, métricas, proyecto legales, guía de pruebas de seguridad, AppSec FAQ, al igual proyectos en desarrollo: WebScarab, Filtros de validación, WebGoat, DotNet **(OWASP, 2001)**.

1.6.1.19. Atacante. A menudo se suele hablar de hacker de manera genérica para referirse a un individuo que vulnera las protecciones de un sistema. Es por eso que debe distinguir la diferencia entre diferentes tipos de atacantes **(Roa Buendía, 2013)**:

- **Hacker:** Es la persona que ataca la defensa informática de un sistema, solo para saber los vulnerabilidades que este tiene. Si tiene éxito, moralmente debe avisar a los administradores sobre los hallazgos en seguridad que ha encontrado.

- **Cracker:** Realiza el mismo ataque a la defensa informática, pero esta vez si quiere hacer daño, ya sea, robando datos, desactivar servicios, alterar información o permitiendo, lo cual es su mayor función, el acceso a aplicaciones o servicios a los cuales no es permitido entrar o usar.

- **Script Kiddie:** Son aprendices de hacker y cracker que, al encontrar en Internet cualquier ataque, lo lanzan sin conocer muy bien lo que están haciendo y sobre todo, las consecuencias derivadas de su actuación (esto se hace especialmente peligroso).

- **Programadores de malware:** Expertos en programación de sistemas operativos y aplicaciones, que son capaces de aprovechar las vulnerabilidades de alguna versión concreta de un software conocido para generar un programa que permite atacar o aprovechar un defecto, en función de materializar alguna amenaza conocida.

- **Sniffers:** Expertos en protocolos de comunicaciones, capaces de procesar una captura de trafico de red para localizar la información relevante dentro de una transmisión.

- **Ciberterrorista:** Cracker con intereses políticos y económicos a gran escala.

Se debe tener en cuenta que el atacante no siempre cumple fielmente con un ataque en específico, ya que, en la actualidad, se pueden usar ataques combinados, es decir, es posible encontrar una vulnerabilidad de un sistema de información para suplantar a un usuario y a partir de esta, también modificar los datos encontrados en un sitio específico de la aplicación.

1.6.1.20. Ataque de inyección de código arbitrario. El ataque de inyección de código, es el término general para el tipo de ataques que tratan de inyectar código que es interpretado o ejecutado por una aplicación. Este tipo de ataques explota el manejo pobre de la información que es verídica **(OWASP, 2015).** Este tipo de ataques son habitualmente posibles, debido a que se hace la validación apropiada en las entradas y salidas de datos, en lo que respecta a:

- Caracteres permitidos.

- Formato de datos.

- Cantidad de datos.

Los ataques de inyección de código arbitrario, difieren de los ataques de inyección de comandos, ya que en estos últimos, un atacante está limitado por las funcionalidades del lenguaje inyectado. Es decir si la aplicación utiliza PHP el atacante está limitado a solo hacer inyección de código PHP **(OWASP, 2015).**

1.6.1.21. Ataque de Denegación de Servicio (DOS). Nombrado también DoS por sus siglas en ingles Denial Off Service, tiene como objetivo la pérdida de acceso a un determinado software o aplicación **(Escrivá Gascó, y otros, 2013)**. Este ataque no está dirigido a obtener ningún tipo de acceso no autorizado, sino para no permitir el uso de un recurso en concreto, ya sea, un servidor, un enrutador, un computador, un sistema de información o una red. Comúnmente se logra sobrecargando el uso del recurso interno, comúnmente discos, tarjetas de red o anchos de ancha. **(Baca Urbina, 2016)**.

1.6.1.22. Ataque Spoofing. Un Spoofing, es un ataque el cual hace referencia al uso de técnicas de suplantación de identidad, es decir, un atacante falsifica el servidor o servicio de origen para que la víctima piense que estos son de la confianza o autorizados y evitar que su detección **(Garcia, 2018).**

En el Spoofing, se usa en un juego de tres actores, los cuales son: un atacante, un atacado, y un sistema o servidor suplantado que tiene alguna relación con el atacado. Para que el atacante logre realizar su objetivo se necesita por un lado establecer una comunicación con su víctima (u objetivo), y por otro lado evitar que el equipo (computador o servidor) suplantado interfiera en el ataque. **(Garcia, 2018).**

Por otra parte, existen diferentes tipos de Spoofing dependiendo de la tecnología que se esté usando al momento del ataque, por ejemplo, IP Spoofing, ARP Spoofing, DNS Spoofing, Web Spoofing, email Spoofing entre otros (**Garcia, 2018**)**.**

1.6.1.23. Ataque MITIM (man-in-the-middle). Es una situación donde un atacante observa (por lo general utilizando un rastreador de puertos) la comunicación entre dos partes y falsifica los intercambios de datos para hacerse pasar por una de estas. Un ataque MITM es efectivo debido a la naturaleza de la articulación de los intercambios de información (entre los clientes y los servidores) y la trasferencia de datos. De esta manera, es posible ver y obtener la información y/o los datos transferidos **(OWASP, 2015).**

1.6.1.24. Exploit. El ataque Exploit se realiza con un programa o código que “explota” una vulnerabilidad de un sistema o de parte de el, para que el atacante utilice esta deficiencia en su beneficio. Es decir, estos códigos son utilizados como un “componente” de otro malware ya que permiten explotar las vulnerabilidades de un sistema o equipo para así permitir hacer uso de funciones que no están permitidas **(Borghello, Cristian, 2000 - 2009).**

1.6.1.25. Ataque XSS (Cross-site scripting). Los ataques XSS (Cross-site Scripting) ya que son un tipo de inyección, en los cuales los scripts maliciosos se implantan en sitios web verídicos y legales. Los ataques de XSS suelen ocurrir cuando un atacante usa un sitio web (software o sistema de información) para enviar código malicioso, generalmente en la forma de un script (lo cual es un conjunto de órdenes guardadas en un archivo de texto) del

lado del navegador, a un usuario final distinto, estos ataques son demasiados comunes y ocurren en cualquier lugar en que un sitio web utiliza la información de entrada de un usuario (campo de texto) dentro de la salida que genera sin validarla ni codificarla **(OWASP, 2018).**

1.6.1.26. Ataque Buffer Overflow. Los ataques Buffer Overflow se caracterizan por la sobrescritura de fragmentos de memoria del proceso, que no deberían ser modificados, ya sea de manera intencional o no. Al sobrescribir los valores como los IP, BP y entre otros registros, se producen excepciones y fallas de segmentación. **(OWASP, 2014).**

En términos de seguridad, los Buffer Overflow se producen en una aplicación cuando no se cuenta con los controles necesarios en el código de programación. Cabe destacar que para realizar estos tipos de ataques se debe contar con conocimientos de programación, como también nociones básica de la arquitectura de los sistemas operativos. En algunos casos a través de un Buffer Overflow el atacante logra tomar el control del equipo de la víctima o ejecuta un ataque de DoS **(Pérez, 2014).**

1.6.1.27. Exploit de puertos. Uno de los métodos más utilizados por los atacantes es la búsqueda de puertos abiertos, acción que se efectúa al enviar mensajes a los puertos del equipo o aplicación con el propósito de localizar los puntos en donde se encuentran las vulnerabilidades. Se considera que el puerto que se encuentra abierto, si acepta paquetes de conexión que no sean confiables, al igual si envía paquetes de respuesta a una solicitud de un escáner o analizador de puertos **(Baca Urbina, 2016).** Ya teniendo un puerto abierto se procede a aprovechar la vulnerabilidad, donde puede usarse un Exploit o inyección de código, conexión contra el puerto etc… **(Angelfire, 2016).**

1.6.1.28. Ataque Tampering. Este ataque se refiere a la modificación sin autorización de los datos o el software instalado en el sistema que es víctima (incluyendo el eliminador de archivos). Son particularmente serios cuando quien que lo realiza ha obtenido derechos de administrador, con la capacidad de poder realizar cualquier comando y así alterar o borrar cualquier información, incluyendo la baja total del sistema **(Borghello, Cristian, 2000 - 2009).**

Existen diversidad de casos en los que utilizan este ataque: empleados bancarios (o externos) que crean cuentas para desviar fondos a otras cuentas, estudiantes que modifican sus calificaciones, o contribuyentes que pagan para que se les anulen una deuda. Otras veces se remplazan versiones de software por otros con el mismos nombre los cuales tienen incorporados malware (virus, troyanos, gusanos, etc.) **(Borghello, Cristian, 2000 - 2009).**

1.6.1.29. Ataque SQL injection. El ataque permite introducir código SQL en una aplicación en el nivel de validación de entradas, para realizar operaciones en una base de datos. El origen de la vulnerabilidad radica en que no se verifican de manera correcta las variables utilizadas en un programa que contiene o genera un código de tipo SQL **(Baca Urbina, 2016).**

Cuando un atacante logra inyectar el código SQL extra sobre la base de datos, lo hace para alterar o destruir la información alojada en la misma, lo cual se logra más fácilmente cuando

el programa se desarrolló sin darle importancia a este problema, así poniendo en riesgo la seguridad del sistema **(Baca Urbina, 2016).**

1.6.1.30. Ataque de inyección de comandos. La inyección de comandos es un ataque en el cual, el objetivo es la ejecución de comandos arbitrarios en el sistema operativo vía una aplicación vulnerable. Los ataques de inyección de comandos tienen la probabilidad de ocurrir cuando existe aplicación donde pasan datos inseguros proporcionados por el usuario. En este ataque, los comandos del sistema operativo suministrados por el atacante generalmente se ejecutan con los privilegios de la aplicación vulnerable. Los ataques de inyección de comandos son posibles en gran parte a la falta de validación de entrada en los campos de texto **(OWASP, 2016).**

1.6.1.31. Ataque Ip Spoofing. El ataque Spoofing, sucede cuando se suplanta (o altera) un elemento de un sistema o máquina para hacerse pasar por otra (**Garcia, 2018).** Uno de estos casos es el ataque de IP Spoofing, donde se hace referencia a la IP del servidor y/o servicio, donde el atacante hace una copia falsa de la dirección IP para ocultar la identidad de quien envía un mensaje o acceso y así poder lograr privilegios de entrada al sistema **(Díaz, y otros, 2004).** Dado que, el protocolo IP contiene la dirección fuente y la dirección destino expresadas en forma numérica, del paquete de datos que se envía, el atacante puede llegar a modificar los primeros números de la IP, de esta manera, el computador que recibe el paquete detecta que viene de un terminal distinto, respondiendo a una dirección falsa. De una forma común, el ataque sustituye la dirección IP origen del servidor por la dirección IP que se desea suplantar, con el fin de enviar y recibir paquetes a esta última **(Baca Urbina, 2016).**

1.6.2. Marco Legal. En este marco legal se mencionan las normas legales que involucradas indirectamente o directamente en el desarrollo de la pasantía.

1.6.2.1. Ley 1273 de 2009. "Por medio de la cual 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" **(LEY 1273 DE 2009, 2009)**.

En la ley 1273 de 2009 se clasifica y se sanciona los delitos informáticos, a través de dos capítulos y diez artículos los cuales son descritos a continuación **(LEY 1273 DE 2009, 2009)**:

Capitulo I. "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"

Artículo 269A: "Acceso abusivo a un sistema informático." El que sin autorización o por fuera de lo convenido, aceda a un sistema informático protegido o con medidas de seguridad, ya sea de manera general o parcial, incurrirá en pena de prisión por cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales vigentes **(LEY 1273 DE 2009, 2009)**.

Artículo 269B: "Obstaculización ilegítima de sistema informático o red de telecomunicación." Todo aquel, sin estar facultado para ello, impida u obstaculice el funcionamiento o acceso a un sistema de información, a los datos contenidos allí, o una red de comunicación, incurrirá en un pena de prisión de cuarenta y ocho (48) meses noventa y seis (96) meses y una multa de cien (100) a mil (1.000) salarios mínimos legales vigentes, siempre que la conducta no esté constituida en un delito con pena mayor **(LEY 1273 DE 2009, 2009).**

Artículo 269C: "Interceptación de datos informáticos". Aquel que sin una previa orden judicial, intercepte los datos informáticos en su origen, destino o el interior de un sistema de información, o las emisiones electromagnéticas provenientes de un sistema de información que los trasporte incurrirá en pena de prisión por treinta y seis (36) a setenta y dos (72) meses **(LEY 1273 DE 2009, 2009)**.

Artículo 269D: "Daño Informático". El que, sin estar facultado para ello, destruya, borre, deterioré, altere o suprima datos de información, o un sistema de tratamiento informático o sus partes o componentes lógicos, incurrirá en pena de prisión por cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales vigentes **(LEY 1273 DE 2009, 2009).**

Artículo 269E: "Uso de software malicioso". Aquella persona, que son estar facultada para ello, produzca, trafique, adquiera, distribuya, venda, envié, introduzca o extraiga del territorio nacional software malicioso y otros programas informáticos de efectos dañinos, incurrirá en pena de prisión por cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales vigentes **(LEY 1273 DE 2009, 2009).**

Artículo 269F: "Violación de datos personales". El que, sin estar facultado para ello, con interese propios o de un terceo, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos, datos personales contenidos en ficheros, archivos, bases de datos o medios equivalentes, incurrirá en pena de prisión por cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales vigentes **(LEY 1273 DE 2009, 2009).**

Artículo 269G: "Suplantación de sitios web para capturar datos personales". La persona con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, modifique el sistema de resolución de nombres de dominio, incurrirá en pena de prisión por cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales vigentes **(LEY 1273 DE 2009, 2009).**

Artículo 269H: "Circunstancias de agravación punitiva". Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere **(LEY 1273 DE 2009, 2009)**:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

- Por servidor público en ejercicio de sus funciones.

- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

- Revelando o dando a conocer el contenido de la información en perjuicio de otro.

- Obteniendo provecho para sí o para un tercero.

- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

- Utilizando como instrumento a un tercero de buena fe.

- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Capitulo II. "De los atentados informáticos y otras infracciones"

Artículo 269I: "Hurto por medios informáticos y semejantes". El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código **(LEY 1273 DE 2009, 2009)**.

Artículo 269J: "Transferencia no consentida de activos". El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa **(LEY 1273 DE 2009, 2009)**.

1.6.2.2. Ley 1712 de 2014. "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información púbica nacional y se dictan otras disposiciones" **(Ley 1712 de 2014, 2014).**

En la ley 1712 de 2017 sirve para el establecimiento de las normas de transparencia y del derecho de acceso a la información, a través de cinco títulos y treinta y tres artículos los cuales son descritos a continuación:

Título I. "Disposiciones generales"

Artículo 1. "Objeto". El objeto de la presente leyes regular el derecho de acceso a [1 la información pública, los procedimientos para el ejercicio y garantía del derecho y ~ las excepciones a la publicidad de información **(Ley 1712 de 2014, 2014)**.

Artículo 2. "Principio de máxima publicidad para titular universal". Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley **(Ley 1712 de 2014, 2014)**.

Artículo 3. "Otros principios de la transparencia y acceso a la información pública". En la interpretación del derecho de acceso a la información se deberá ti " adoptar un criterio de razonabilidad y proporcionalidad, así como aplicar. Los siguientes principios **(Ley 1712 de 2014, 2014):**

- Principio de transparencia.
- Principio de buena fe.
- Principio de facilitación.
- Principio de no discriminación.
- Principio de gratuidad.
- Principio de celeridad.
- Principio de eficacia.
- Principio de la calidad de la información.
- Principio de la divulgación proactiva de la información.
- Principio de responsabilidad en el uso de la información.

Artículo 4. "**Concepto del derecho".** En ejercicio del derecho fundamental de acceso a 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. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática **(Ley 1712 de 2014, 2014)**.

Artículo 5. "Ámbito de aplicación". Las disposiciones de esta ley serán aplicables a las siguientes personas en calidad de sujetos obligados **(Ley 1712 de 2014, 2014)**:

- Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital.
- Los órganos, organismos y entidades estatales independientes o autónomos y de control.
- Las personas naturales y jurídicas, públicas o privadas, que presten función pública, que presten servicios públicos respecto de la información directamente relacionada con la prestación del servicio público.

- Cualquier persona natural, jurídica o dependencia de persona jurídica que desempeñe función pública o de autoridad pública, respecto de la información directamente relacionada con el desempeño de su función.
- Los partidos o movimientos políticos y los grupos significativos de ciudadanos.
- Las entidades que administren instituciones parafiscales, fondos o recursos de naturaleza u origen público.

Artículo 6. "Definiciones". En esta sección de la ley se define Información, información pública, información pública clasificada, información pública reservada, publicar o divulgar, sujetos obligados, gestión documental, documento de archivo, archivo, datos abiertos, documento en construcción **(Ley 1712 de 2014, 2014)**.

Título II. "De la publicidad y del contenido de la información".

Artículo 7. "Disponibilidad de la Información". En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que **presten (Ley 1712 de 2014, 2014).**

Artículo 8. "Criterio diferencial de accesibilidad". Con el objeto de facilitar que las poblaciones específicas accedan a la información que particularmente las afecte, los sujetos obligados, a solicitud de las autoridades de las comunidades, divulgarán la información pública en diversos idiomas y lenguas y elaborarán formatos alternativos comprensibles para dichos grupos. Deberá asegurarse el acceso a esa información a los distintos grupos étnicos y culturales del país y en especial se adecuarán los medios de comunicación para que faciliten el acceso a las personas que se encuentran en situación de discapacidad **(Ley 1712 de 2014, 2014)**.

Artículo 9. Información mínima obligatoria respecto a la estructura del sujeto obligado. Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva en los sistemas de información del Estado o herramientas que lo sustituyan **(Ley 1712 de 2014, 2014)**:

- La descripción de su estructura orgánica, funciones y deberes, la ubicación de sus sedes y áreas, divisiones o departamentos, y sus horas de atención al público.
- Su presupuesto general, ejecución presupuestal histórica anual y planes de gasto público para cada año fiscal, de conformidad con el artículo 74 de la ley 1474 de 2011.
- Un directorio que incluya el, cargo, direcciones de correo electrónico y teléfono del despacho de los empleados y funcionarios y las escalas salariales correspondientes a las categorías de todos los servidores que trabajan en el sujeto ti obligado, de conformidad con el formato de información de servidores públicos y contratistas.

- Todas las normas generales y reglamentarias, políticas, lineamientos o manuales, las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos y los resultados de las auditorías al ejercicio presupuestal e indicadores de desempeño.

- Su respectivo plan de compras anual, así como las contrataciones adjudicadas para la correspondiente vigencia en lo relacionado con funcionamiento e inversión, las obras públicas, los bienes adquiridos, arrendados y en caso de los servicios de estudios o investigaciones deberá señalarse el tema específico, de conformidad con el artículo 74 de la ley 1474 de 2011. En el caso de las personas naturales con contratos de prestación de servicios, deberá publicarse el objeto del contrato, monto de los honorarios y direcciones de correo electrónico, de conformidad con el formato de información de servidores públicos y contratistas.

- Los plazos de cumplimiento de los contratos.

- Publicar el Plan Anticorrupción y de Atención al Ciudadano, de conformidad con el artículo 73 de la ley 1474 de 2011.

Artículo 10. "Publicidad de la contratación". En el caso de la información de contratos indicada en el artículo 9 literal e), tratándose de contrataciones sometidas al régimen de contratación estatal, cada entidad publicará en el medio electrónico institucional sus contrataciones en curso y un vínculo al sistema electrónico para la contratación pública o el que haga sus veces, a través del cual podrá accederse directamente a la información correspondiente al respectivo proceso contractual, en aquellos que se encuentren sometidas a dicho sistema, sin excepción **(Ley 1712 de 2014, 2014)**.

Artículo 11. "Información mínima obligatoria respecto a servicios, procedimientos y funcionamiento del sujeto obligado". Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva **(Ley 1712 de 2014, 2014)**:

- Detalles pertinentes sobre todo servicio que brinde directamente al público, incluyendo normas, formularios y protocolos de atención.

- Toda la información correspondiente a los trámites que se pueden agotar en la entidad, incluyendo la normativa relacionada, el proceso, los costos asociados y los distintos formatos o formularios requeridos.

- Una descripción de los procedimientos que se siguen para tomar decisiones en las diferentes áreas.

- El contenido de toda decisión Y/o política que haya adoptado y afecte al público, junto con sus fundamentos y toda interpretación autorizada de ellas.

- Todos los informes de gestión, evaluación y auditoría del sujeto obligado.

- Todo mecanismo interno y externo de supervisión, notificación y vigilancia pertinente del sujeto obligado.

- Sus procedimientos, lineamientos, políticas en materia de adquisiciones y compras, así como todos los datos de adjudicación y ejecución de contratos, incluidos concursos y licitaciones.
- Todo mecanismo de presentación directa de solicitudes, quejas y reclamos a disposición del público en relación con acciones u omisiones del sujeto obligado. Junto con un informe de todas las solicitudes, denuncias y los tiempos de respuesta del sujeto obligado.
- Todo mecanismo o procedimiento por medio del cual el público pueda participar en la formulación de la política o el ejercicio de las facultades de ese sujeto obligado.
- Un registro de publicaciones que contenga los documentos publicados de conformidad con la presente ley y automáticamente disponibles, así como un Registro de Activos de Información.
- Los sujetos obligados deberán publicar datos abiertos, para lo cual deberán contemplar las excepciones establecidas en el titulo 3 de la presente ley. Adicionalmente, para las condiciones técnicas de su publicación, se deberán observar los requisitos que establezca el gobierno nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones o quien haga sus veces.

Artículo 12. "Adopción de esquemas de publicación". Todo sujeto obligado deberá adoptar y difundir de manera amplia su esquema de publicación, dentro de los seis meses siguientes a la entrada en vigencia de la presente ley. El esquema será difundido a través de su sitio Web, y en su defecto, en los dispositivos de divulgación existentes en su dependencia, incluyendo boletines, gacetas y carteleras **(Ley 1712 de 2014, 2014)**.

Artículo 13. "Registros de Activos de Información". Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de **(Ley 1712 de 2014, 2014):**

- Todas las categorías de información publicada por el sujeto obligado.
- Todo registro publicado.
- Todo registro disponible para ser solicitado por el público.

Artículo 14. "Información publicada con anterioridad". Los sujetos obligados deben garantizar y facilitar a los solicitantes, de la manera más sencilla posible, el acceso a toda la información previamente divulgada. Se publicará esta información en los términos establecidos **(Ley 1712 de 2014, 2014)**.

Artículo 15. "Programa de Gestión Documental". Dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente ley, los sujetos obligados deberán adoptar un Programa de Gestión Documental en el cual se establezcan los procedimientos y lineamientos necesarios para la producción, distribución, organización, consulta y conservación de los documentos públicos. Este Programa deberá integrarse con las funciones administrativas del sujeto obligado. Deberán observarse los lineamientos y

recomendaciones que el Archivo General de la Nación y demás entidades competentes expidan en la materia **(Ley 1712 de 2014, 2014)**.

Artículo 16. "Archivos". En su carácter de centros de información institucional que contribuyen tanto a la eficacia y eficiencia del Estado en el servicio al ciudadano, como a la promoción activa del acceso a la información pública, los sujetos obligados deben asegurarse de que existan dentro de sus entidades procedimientos claros para la creación, gestión, organización y conservación de sus archivos. Los procedimientos adoptados deberán observar los lineamientos que en la materia sean producidos por el Archivo General de la Nación **(Ley 1712 de 2014, 2014)**.

Artículo 17. Sistemas de información. Para asegurar que los sistemas de información electrónica sean efectivamente una herramienta para promover el acceso a la información pública, los sujetos obligados deben asegurar que estos **(Ley 1712 de 2014, 2014)**:

- Se encuentren alineados con los distintos procedimientos y articulados con los lineamientos establecidos en el Programa de Gestión Documental de la entidad;
- Gestionen la misma información que se encuentre en los sistemas administrativos del sujeto obligado;
- En el caso de la información de interés público, deberá existir una ventanilla en la cual se pueda acceder a la información en formatos y lenguajes comprensibles para los ciudadanos;
- Se encuentren alineados con la estrategia de gobierno en línea o de la que haga sus veces.

Título III. "Excepciones acceso a la información".

Artículo 18. "Información exceptuada por daño de derechos a personas naturales o jurídicas". Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos **(Ley 1712 de 2014, 2014)**:

- El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.
- El derecho de toda persona a la vida, la salud o la seguridad.
- Los secretos comerciales, industriales y profesionales, así como los estipulados en el parágrafo del artículo 77 de la Ley 1474 de 2011.

Artículo 19. "Información exceptuada por daño a los intereses públicos". Es toda aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional **(Ley 1712 de 2014, 2014)**:

- La defensa y seguridad nacional.
- La seguridad pública.
- Las relaciones internacionales.
- La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.
- El debido proceso y la igualdad de las partes en los procesos judiciales.
- La administración efectiva de la justicia.
- Los derechos de la infancia y la adolescencia.
- La estabilidad macroeconómica y financiera del país.
- La salud pública.

Artículo 20. "**Índice de Información clasificada y reservada".** Los sujetos obligados deberán mantener un índice actualizado de los actos, documentos e informaciones calificado como clasificado o reservado, de conformidad a esta ley. El índice incluirá sus **denominaciones, la motivación y la individualización del acto en que conste tal calificación (Ley 1712 de 2014, 2014)**.

Artículo 21. "Divulgación parcial y otras reglas". En aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción contenida en la presente ley, debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable. La información pública que no cae en ningún supuesto de excepción deberá ser entregada a la parte solicitante, así como ser de conocimiento público. La reserva de acceso a la información opera respecto del contenido de un documento público pero no de su existencia **(Ley 1712 de 2014, 2014)**.

Artículo 22. "Excepciones temporales". La reserva de las informaciones amparadas por el artículo 19 no deberá extenderse por un período mayor a quince (15) años **(Ley 1712 de 2014, 2014).**

Título IV. "De las garantías al ejercicio del derecho de acceso a la información"

Artículo 23. "Funciones del Ministerio Público". El Ministerio Público será el encargado de velar por el adecuado cumplimiento de las obligaciones estipuladas en la presente ley. Para tal propósito, la Procuraduría General de la Nación en un plazo no mayor a seis meses establecerá una metodología para que aquel cumpla las siguientes funciones y atribuciones **(Ley 1712 de 2014, 2014)**:

- Desarrollar acciones preventivas para el cumplimiento de esta ley.
- Realizar informes sobre el cumplimiento de las decisiones de tutelas sobre acceso a la información.

- Publicar las decisiones de tutela y normatividad sobre acceso a la información pública.
- Promover el conocimiento y aplicación de la presente ley y sus disposiciones entre los sujetos obligados, así como su comprensión entre el público, teniendo en cuenta criterios diferenciales para su accesibilidad, sobre las materias de su competencia mediante la publicación y difusión de una guía sobre el derecho de acceso a la información.
- Aplicar las sanciones disciplinarias que la presente ley consagra.
- Decidir disciplinariamente, en los casos de ejercicio de poder preferente, los casos de faltas o mala conducta derivada del derecho de acceso a la información.
- Promover la transparencia de la función pública, el acceso y la publicidad de la información de las entidades del Estado, por cualquier medio de publicación.
- Requerir a los sujetos obligados para que ajusten sus procedimientos y sistema de atención al ciudadano a dicha legislación.
- Realizar, directamente o a través de terceros, actividades de capacitación de funcionarios públicos en materia de transparencia y acceso a la información.
- Efectuar estadísticas y reportes sobre transparencia y acceso a la información de los órganos de la administración del Estado y sobre el cumplimiento de esta ley.
- Entregar en debida forma las respuestas a las peticiones formuladas con solicitud de identificación reservada a las que se refiere el parágrafo del artículo 4° de la presente ley.
- Implementar y administrar los sistemas de información en el cumplimiento de sus funciones, para lo cual establecerá los plazos y criterios del reporte por parte de las entidades públicas que considere necesarias.

Artículo 24. "Del Derecho de acceso a la información". Toda persona tiene derecho a solicitar y recibir información de cualquier sujeto obligado, en la forma y condiciones que establece esta ley y la Constitución **(Ley 1712 de 2014, 2014)**.

Artículo 25. "Solicitud de acceso a la Información Pública". Es aquella que, de forma oral o escrita, incluida la vía electrónica, puede hacer cualquier persona para acceder a la información pública **(Ley 1712 de 2014, 2014)**.

Artículo 26. "Respuesta a solicitud de acceso a información". Es aquel acto escrito mediante el cual, de forma oportuna, veraz, completa, motivada y actualizada, todo sujeto obligado responde materialmente a cualquier persona que presente una solicitud de acceso a información pública. Su respuesta se dará en los términos establecidos **(Ley 1712 de 2014, 2014).**

Artículo 27. "Recursos del solicitante". Cuando la respuesta a la solicitud de información invoque la reserva de seguridad y defensa nacional o relaciones internacionales, el solicitante podrá acudir al recurso de reposición, el cual deberá interponerse por escrito y

sustentando en la diligencia de notificación, o dentro de los tres (3) días siguientes a ella **(Ley 1712 de 2014, 2014)**.

Negado este recurso corresponderá al Tribunal administrativo con jurisdicción en el lugar donde se encuentren los documentos, si se trata de autoridades nacionales, departamentales o del Distrito Capital de Bogotá, o al juez administrativo si se trata de autoridades distritales y municipales, decidir en única instancia si se niega o se acepta, total o parcialmente, la petición formulada **(Ley 1712 de 2014, 2014)**.

Para ello, el funcionario respectivo enviará la documentación correspondiente al tribunal o al juez administrativo en un plazo no superior a tres (3) días. En caso de que el funcionario incumpla esta obligación el solicitante podrá hacer el respectivo envío de manera directa **(Ley 1712 de 2014, 2014)**.

El juez administrativo decidirá dentro de los diez (10) días siguientes. Este término se interrumpirá en los siguientes casos **(Ley 1712 de 2014, 2014)**:

Cuando el tribunal o el juez administrativo solicite copia o fotocopia de los documentos sobre cuya divulgación deba decidir, o cualquier otra información que requieran, y hasta la fecha en la cual las reciba oficialmente.

Cuando la autoridad solicite, a la sección del Consejo de Estado que el reglamento disponga, asumir conocimiento del asunto en atención a su importancia jurídica o con el objeto de unificar criterios sobre el tema. Si al cabo de cinco (5) días la sección guarda silencio, o decide no avocar conocimiento, la actuación continuará ante el respectivo tribunal o juzgado administrativo.

Artículo 28. "Carga de la prueba". Le corresponde al sujeto obligado aportar las razones y pruebas que fundamenten y evidencien que la información solicitada debe permanecer reservada o confidencial. En particular, el sujeto obligado debe demostrar que la información debe relacionarse con un objetivo legítimo establecido legal o constitucionalmente. Además, deberá establecer si se trata de una excepción contenida en los artículos 18 y 19 de esta ley y si la revelación de la información causaría un daño presente, probable y específico que excede el interés público que representa el acceso a la información **(Ley 1712 de 2014, 2014)**.

Artículo 29. "Responsabilidad Penal". Todo acto de ocultamiento, destrucción o alteración deliberada total o parcial de información pública, una vez haya sido objeto de una solicitud de información, será sancionado en los términos del artículo 292 del Código Penal **(Ley 1712 de 2014, 2014)**.

Título V. "Vigencia y medidas de promoción"

Artículo 32. "Política Pública de acceso a la información". El diseño, promoción e implementación de la política pública de acceso a la información pública, estará a cargo de la Secretaría de Transparencia de la Presidencia de la República, el Ministerio de Tecnología de la Información y Comunicaciones, el Departamento Administrativo de la Función Pública (DAFP), el Departamento Nacional de Planeación (DNP), el Archivo

General de la Nación y el Departamento Administrativo Nacional de Estadística (DANE) **(Ley 1712 de 2014, 2014)**.

Artículo 33. "Vigencia y derogatoria". La presente ley rige a los seis (6) meses de la fecha de su promulgación para todos los sujetos obligados del orden nacional. Para los entes territoriales la ley entrará en vigencia un año después de su promulgación. La presente ley deroga todas las disposiciones que le sean contrarias **(Ley 1712 de 2014, 2014)**.

1.6.2.3. Decreto 1078 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" **(Decreto 1078 de 2015, 2015)**.

Para este decreto se enfocó en el titulo número nueve en el capítulo uno, las secciones uno y dos donde se reglamenta las políticas, lineamientos e instrumentos con respecto a la tecnología de la información.

Título 9. "Políticas y lineamientos de tecnologías de la información"

Capítulo 1. "Estrategia de Gobierno en Línea"

SECCIÓN 1. "Objeto, Ámbito de Aplicación, Definiciones, principios y Fundamentos"

Artículo 2.2.9.1.1.1. "*Objeto".* Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y 18.s Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad **(Decreto 1078 de 2015, 2015).**

Artículo 2.2.9.1.1.2. "*Ámbito de aplicación".* Serán sujetos obligados de las disposiciones contenidas en el presente capítulo las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas **(Decreto 1078 de 2015, 2015)**.

Artículo 2.2.9.1.1.3. "*Definiciones".* Para la interpretación del presente capítulo, las expresiones aquí utilizadas deben ser entendidas con el significado que a continuación se indica (**Decreto 1078 de 2015, 2015)**:

Arquitectura empresarial: Es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria.

Marco de referencia de arquitectura empresarial para la gestión de tecnologías de la información: El Marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información.

Artículo 2.2.9.1.1.4. "*Principios y fundamentos de la Estrategia de Gobierno en línea".* La Estrategia de Gobierno en línea se desarrollará conforme a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad consagrados en los artículos 209 de la Constitución Política **(Decreto 1078 de 2015, 2015)**.

Así mismo, serán fundamentos de la Estrategia los siguientes **(Decreto 1078 de 2015, 2015)**:

Excelencia en el servicio al ciudadano: Propender por el fin superior de fortalecer la relación de los ciudadanos con el Estado a partir de la adecuada atención y provisión de los servicios, buscando la optimización en el uso de los recursos, teniendo en cuenta el modelo de Gestión Pública Eficiente al Servicio del Ciudadano y los principios orientadores de la Política Nacional de Eficiencia Administrativa al Servicio del Ciudadano.

Apertura y reutilización de datos públicos: Abrir los datos públicos para impulsar la participación, el control social y la generación de valor agregado.

Estandarización: Facilitar la evolución de la gestión de TI del Estado colombiano hacia un modelo estandarizado que aplica el marco de referencia de arquitectura empresarial para la gestión de TI.

Interoperabilidad: Fortalecer el intercambio de información entre entidades y sectores.

Neutralidad tecnológica: Garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, emplear contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones, así como garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

Innovación: Desarrollar nuevas formas de usar las Tecnologías de la Información y las Comunicaciones para producir cambios que generen nuevo y mayor valor público.

Colaboración: Implementar soluciones específicas para problemas públicos, mediante el estímulo y aprovechamiento del interés y conocimiento de la sociedad, al igual que un esfuerzo conjunto dentro de las propias entidades públicas y sus servidores.

Sección 2. "Componentes, instrumentos y responsables".

Artículo 2.2.9.1.2.1. *Componentes.* Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea.

- **TIC para Servicios.** Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo.

- **TIC para el Gobierno abierto.** Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones.

- **TIC para la Gestión.** Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno.

- **Seguridad y privacidad de la Información.** Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Artículo 2.2.9.1.2.2. "*Instrumentos".* Los instrumentos para la implementación de la estrategia de Gobierno en línea serán los siguientes **(Decreto 1078 de 2015, 2015)**:

Manual de Gobierno en Línea. Define las acciones que corresponde ejecutar a las entidades del orden nacional y territorial respectivamente.

Marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información. Establece los aspectos que los sujetos obligados deberán adoptar para dar cumplimiento a las acciones definidas en el Manual de Gobierno en Línea.

Artículo 2.2.9.1.2.3. "*Responsable de coordinar la implementación de la Estrategia de Gobierno en línea en los sujetos obligados".* El representante legal de cada sujeto obligado, será el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en línea **(Decreto 1078 de 2015, 2015).**

Artículo 2.2.9.1.2.4. "*Responsable de orientar la implementación de la Estrategia de Gobierno en línea".* En las entidades del orden nacional, el Comité Institucional de Desarrollo Administrativo de que trata el artículo 6 del Decreto 2482 de 2012, o las normas que lo modifiquen o sustituyan, será la instancia orientadora de la implementación de la Estrategia de Gobierno en línea al interior de cada entidad. Los sujetos obligados deberán incluir la estrategia de Gobierno en línea de forma transversal dentro de sus planes estratégicos sectoriales e institucionales, y anualmente dentro de los planes de acción de acuerdo con el Modelo Integrado de Planeación y Gestión de qué trata el Decreto 2482 de 2012 o las normas que lo modifiquen o sustituyan. En estos documentos se deben definir las actividades, responsables, metas y recursos presupuestales que les permitan dar cumplimiento a los lineamientos que se establecen.

1.6.2.4. Decreto 1499 de 2017. En el cual se estable y se reglamenta el alcance del sistema de gestión y su articulación con el Sistema de Control Interno, de tal manera permita el fortalecimiento de los mecanismos, métodos y procedimientos de gestión y control al

interior de los organismos y entidades del Estado. De igual manera se actualiza el Modelo Integrado de Planeación y Gestión **(Decreto 1499 de 2017, 2017)**.

Título 22. "Sistema de gestión"

Capítulo 1. "Objeto e instancias de dirección Y coordinación del sistema de gestión".

Artículo 2.2.22.1.1. "Sistema de Gestión". El Sistema de Gestión, creado en el artículo 133 de la Ley 1753 de 2015, que integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, es el conjunto de entidades y organismos del Estado, políticas, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad **(Decreto 1499 de 2017, 2017)**.

Artículo 2.2.22.1.2. "Dirección y Coordinación del Sistema de Gestión". El Presidente de la República dirigirá el Sistema de Gestión, con el apoyo del Consejo para la Gestión y el Desempeño Institucional **(Decreto 1499 de 2017, 2017)**.

Artículo 2.2.22.1.3. "**Consejo para la Gestión y el Desempeño Institucional".** El Consejo para la Gestión y el Desempeño Institucional, presidido por Función Pública. Estará conformado por las entidades y organismos que, por su misión, tienen a cargo funciones transversales de gestión y desempeño a nivel nacional y territorial, así **(Decreto 1499 de 2017, 2017):**

- Ministerio de Hacienda y Crédito Público.
- Ministerio de las Tecnologías de la Información y las Comunicaciones.
- Departamento Administrativo de la Presidencia de la República.
- Departamento Nacional de Planeación.
- Departamento Administrativo Nacional de Estadística.
- Departamento Administrativo de la Función Pública.
- Archivo General de la Nación.
- Agencia Nacional de Contratación Pública -Colombia Compra Eficiente
- Agencia Nacional de Defensa Jurídica del Estado
- Contaduría General de la Nación

Artículo 2.2.22.1.4. "Funciones del Consejo para la Gestión y el Desempeño Institucional". El Consejo para la Gestión y el Desempeño Institucional cumplirá las siguientes funciones **(Decreto 1499 de 2017, 2017):**

- Coordinar y gestionar las actividades necesarias para el correcto funcionamiento del Sistema de Gestión.

- Proponer políticas, normas, herramientas, métodos y procedimientos en materia de gestión y desempeño institucional.

- Definir los criterios de evaluación y seguimiento de las políticas de gestión y desempeño institucional, buscando la simplificación y racionalización de reportes de información y requerimientos para su implementación y operación.

- Adoptar los criterios diferenciales para la operación de las políticas de gestión y desempeño.

- Proponer estrategias de articulación y coordinación de las entidades que lo integran, con el fin de fortalecer el Modelo Integrado de Planeación y Gestión -MIPG Y evitar la colisión de competencias y la duplicidad de funciones.

- Presentar al Consejo de Ministros, por lo menos una vez al año o cuando el Presidente de la República lo solicite, los resultados de la evaluación de la gestión y el desempeño de las entidades.

- Presentar al Gobierno Nacional recomendaciones para la adopción de políticas, estrategias o acciones para mejorar la gestión y el desempeño institucional de las entidades y organismos del Estado.

- Proponer estrategias para la debida operación del Modelo Integrado de Planeación y Gestión -MIPG.

- Evaluar el logro de los objetivos del Modelo Integrado de Planeación y Gestión MIPG Y del cumplimiento permanente de sus principios.

- Promover la investigación en materia de gestión institucional y la identificación de buenas prácticas susceptibles de ser replicables en las entidades y organismos públicos.

- Cumplir las funciones de la Comisión Intersectorial del Servicio al Ciudadano de que trata el Decreto 2623 de 2009.

- Cumplir las funciones del Grupo de Racionalización y Automatización de Trámites GRAT, establecidas en el artículo 2.2.24.4 del presente Decreto.

- Adoptar su reglamento de funcionamiento.

Artículo 2.2.22.1.5. "Articulación y complementariedad con otros sistemas de gestión". El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información **(Decreto 1499 de 2017, 2017)**.

Capítulo 2. "Políticas de gestión y desempeño institucional"

Artículo 2.2.22.2.1. "Políticas de Gestión y Desempeño Institucional". S e denominarán políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes **(Decreto 1499 de 2017, 2017)**:

- Planeación Institucional.
- Gestión presupuestal y eficiencia del gasto público.
- Talento humano.
- Integridad
- Transparencia, acceso a la información pública y lucha contra la corrupción
- Fortalecimiento organizacional y simplificación de procesos
- Servicio al ciudadano
- Participación ciudadana en la gestión pública
- Racionalización de trámites
- Gestión documental
- Gobierno Digital, antes Gobierno en Línea
- Seguridad Digital
- Defensa jurídica
- Gestión del conocimiento y la innovación
- Control interno
- Seguimiento y evaluación del desempeño institucional

Capítulo 3. "Modelo integrado de planeación y gestión"

Artículo 2.2.22.3.1. "Actualización del Modelo Integrado de Planeación y Gestión". Para el funcionamiento del Sistema de Gestión y su articulación con el Sistema de Control Interno, se adopta la versión actualizada del Modelo Integrado de Planeación y Gestión MIPG **(Decreto 1499 de 2017, 2017)**.

Artículo 2.2.22.3.2. "Definición del Modelo Integrado de Planeación y Gestión MIPG". El Modelo Integrado de Planeación y Gestión -MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio **(Decreto 1499 de 2017, 2017)**.

Artículo 2.2.22.3.3. "Objetivos del Modelo Integrado de Planeación y Gestión –MIPG". El Modelo Integrado de Planeación y Gestión -MIPG, tendrá como objetivos **(Decreto 1499 de 2017, 2017)**:

- Fortalecer el liderazgo y el talento humano bajo los principios de integridad y legalidad, como motores de la generación de resultados de las entidades públicas

- Agilizar, simplificar y flexibilizar la operación de las entidades para la generación de bienes y servicios que resuelvan efectivamente las necesidades de los ciudadanos.

- Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación para la toma de decisiones la mejora continua.

- Facilitar y promover la efectiva participación ciudadana en la planeación, gestión y evaluación de las entidades públicas.

- Promover la coordinación entre entidades públicas para mejorar su gestión y desempeño.

Artículo 2.2.22.3.4. "Ámbito de Aplicación". El Modelo Integrado de Planeación y Gestión -MIPG se adoptará por los organismos y entidades de los órdenes nacional y territorial de la Rama Ejecutiva del Poder Público. En el caso de las entidades descentralizadas con capital público y privado, el Modelo aplicará en aquellas en que el Estado posea el 90% o más del capital social **(Decreto 1499 de 2017, 2017).**

Artículo 2.2.22.3.5. "Manual Operativo del Modelo". El Consejo para la Gestión y Desempeño Institucional adoptará y actualizará el Manual Operativo del Modelo Integrado de Planeación y Gestión -MIPG, cuyo proyecto será presentado por la Función Pública **(Decreto 1499 de 2017, 2017).**

Artículo 2.2.22.3.6. "Comités Sectoriales de Gestión y Desempeño". Estarán integrados por el ministro o director de departamento administrativo, quien lo presidirá, y por los directores, gerentes o presidentes de las entidades y organismos adscritos o vinculados al respectivo sector y cumplirán las siguientes funciones **(Decreto 1499 de 2017, 2017):**

- Dirigir y orientar la planeación estratégica del sector.

- Dirigir y articular a las entidades del sector administrativo en la implementación, desarrollo y evaluación del Modelo Integrado de Planeación y Gestión -MIPG.

- Hacer seguimiento a la gestión y desempeño del sector y proponer estrategias para el logro de los resultados, por lo menos una vez cada semestre.

- Hacer seguimiento, por lo menos una vez cada semestre, a las acciones y estrategias sectoriales adoptadas: para la operación y evaluación del Modelo Integrado de Planeación y Gestión, y proponer los correctivos necesarios.

- Dirigir y articular a las entidades del sector administrativo en la operación de las políticas de gestión y desempeño y de las directrices impartidas por la Presidencia de la República y el Ministerio· de Tecnologías de la Información y las Comunicaciones en materia de Gobierno y Seguridad Digital.

- Las demás que tengan relación directa con la implementación, operación, desarrollo y evaluación del Modelo en su integridad, en el respectivo sector.

Artículo 2.2.22.3.7. "Comités departamentales, distritales y municipales de Gestión y Desempeño". A nivel departamental, municipal y distrital habrá Comités Departamentales, Distritales y Municipales de Gestión y Desempeño los cuales estarán integrados por el gobernador o alcalde, quienes los presidirán, los miembros de los consejos de gobierno y por los gerentes, presidentes o directores de las entidades descentralizadas de la respectiva jurisdicción territorial **(Decreto 1499 de 2017, 2017).**

Los Comités Departamentales, Distritales y Municipales de Gestión y Desempeño cumplirán las siguientes funciones **(Decreto 1499 de 2017, 2017)**:

- Orientar la implementación, operación, seguimiento y evaluación del Modelo Integrado de Planeación y Gestión en el departamento, distrito o municipio y sus entidades descentralizadas.

- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación y desarrollo del Modelo, en el respectivo departamento, distrito o municipio.

- Impulsar mecanismos de articulación administrativa entre las entidades del respectivo departamento, distrito o municipio para el diseño, implementación, seguimiento y evaluación del Modelo Integrado de Planeación y Gestión.

- Presentar los informes que el Gobierno Nacional y los organismos de control requieran sobre la gestión y el desempeño en el respectivo departamento, distrito o municipio.

- Dirigir y articular a las entidades del departamento, distrito o municipio en la implementación y operación de las políticas de gestión y desempeño y de las directrices

impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de Gobierno y Seguridad Digital.

- Las demás que tengan relación directa con la implementación, operación, desarrollo y evaluación del Modelo en su integridad, en la respectiva jurisdicción.

Artículo 2.2.22.3.8. "Comités Institucionales de Gestión y Desempeño". En cada una de las entidades se integrará un Comité Institucional de Gestión y Desempeño encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión MIPG, el cual sustituirá los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal **(Decreto 1499 de 2017, 2017)**.

Los Comités Institucionales de Gestión y Desempeño cumplirán las siguientes funciones **(Decreto 1499 de 2017, 2017):**

- Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión -MIPG.

- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión -MIPG.

- Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión -MIPG.

Artículo 2.2.22.3.9. "Implementación del Modelo Integrado de Planeación y Gestión en entidades autónomas, con regímenes especiales y en otras ramas del poder público". Las entidades y organismos del Estado sujetos a régimen especial en los términos del artículo 40 de la Ley 489 de 1998, las Ramas Legislativa y Judicial, la Organización Electoral, los organismos de control y los institutos científicos, que decidan adoptar el Modelo, determinarán las instancias que consideren necesarias para su implementación y evaluación **(Decreto 1499 de 2017, 2017).**

Artículo 2.2.22.3.10. "Medición de la Gestión y Desempeño Institucional". La recolección de información necesaria para dicha medición se hará a través del Formulario Único de Reporte y Avance de Gestión -FURAG. La medición de la gestión y desempeño institucional se hará a través del índice, las metodologías o herramientas definidas por la Función Pública, sin perjuicio de otras mediciones que en la materia efectúen las entidades del Gobierno (**Decreto 1499 de 2017, 2017**)**.**

Artículo 2.2.22.3.11. "Criterios Diferenciales". La implementación y desarrollo del Modelo Integrado de Planeación y Gestión MIPG en las entidades del orden territorial, tal como lo prevé el artículo 133 de la Ley 1753 de 2015, se hará con criterios diferenciales atendiendo sus características y especificidades que definirán los líderes de política **(Decreto 1499 de 2017, 2017).**

Artículo 2.2.22.3.12. "Certificación de Calidad". Las entidades y organismos públicos, que lo consideren pertinente, podrán certificarse bajo las normas nacionales e internacionales de calidad (**Decreto 1499 de 2017, 2017).**

Artículo 2.2.22.3.13. "Programas de capacitación para la implementación y desarrollo del Modelo Integrado de Planeación y Gestión". La Escuela Superior de Administración Pública -ESAP, bajo los lineamientos técnicos del Departamento Administrativo de la Función Pública, diseñará y ofrecerá programas o estrategias de capacitación, formación y desarrollo de competencias laborales dirigidas a los servidores públicos, con el fin de fortalecer la gestión y el desempeño en las entidades públicas **(Decreto 1499 de 2017, 2017)."**

Título 23. "Articulación del sistema de Gestión con los sistemas de control interno".

Artículo 2.2.23.1. "Articulación del Sistema de Gestión con los Sistemas de Control Interno". Se articulará al Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión -MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades.

El Control Interno es transversal a la gestión 'Y desempeño de las entidades Y se implementa a través del Modelo Estándar de Control Interno –MECI **(Decreto 1499 de 2017, 2017).**

Artículo 2.2.23.2. "Actualización del Modelo Estándar de Control Interno". La actualización del Modelo Estándar de Control Interno para el Estado Colombiano -MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación Y Gestión MIPG **(Decreto 1499 de 2017, 2017).**

Artículo 2.2.23.3. "Medición del Modelo Estándar de Control Interno". Los jefes de control interno o quienes hagan sus veces realizarán la medición de la efectividad de dicho Modelo. La Función Pública establecerá la metodología, la periodicidad y demás condiciones necesarias para tal medición y recogerá la información a través del Formulario Único de Reporte y Avance de Gestión –FURAG **(Decreto 1499 de 2017, 2017).**

ARTICULO 2.2.23.4. "Seguimiento a la implementación y operación del Modelo Integrado de Planeación y Gestión –MIPG". La Procuraduría General de la Nación podrá hacer seguimiento a la implementación y operación del Modelo Integrado de Planeación y Gestión -MIPG en las entidades del orden nacional y territorial **(Decreto 1499 de 2017, 2017)."**

Artículo 2.2.21.3.14. "Comités Departamentales, Municipales y Distritales de Auditoría". A nivel departamental habrá un Comité de Auditoría del cual harán parte los jefes de control interno o quienes hagan sus veces de las entidades pertenecientes al sector central y descentralizado del departamento, así como por los de las entidades que no hagan parte de la rama ejecutiva del orden departamental, previa solicitud de éstos; el Comité estará presidido por el jefe de control interno o quien haga sus veces de la respectiva gobernación y la secretaría técnica será ejercida por el jefe de control interno elegido por mayoría simple de los miembros del Comité **(Decreto 1499 de 2017, 2017)**.

1.6.2.5. Documento CONPES 3701 de 2011. “Busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema” **(Conpes 3701 de 2011, 2011)**.

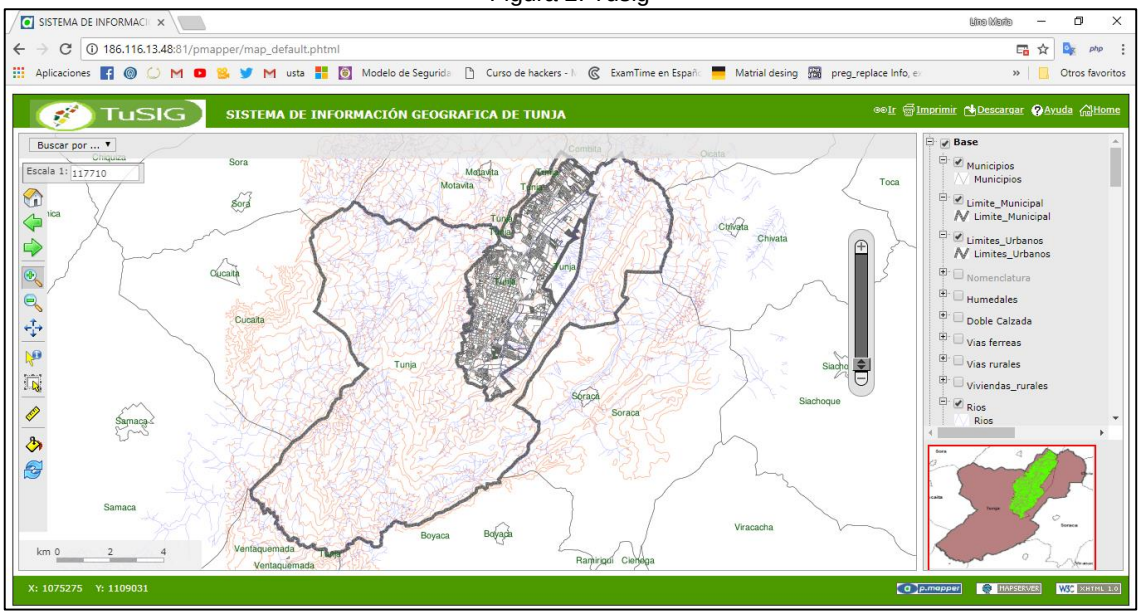
Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema **(Conpes 3701 de 2011, 2011)**.

La problemática central se fundamenta en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 “Prosperidad para Todos”, como parte del Plan Vive Digital **(Conpes 3701 de 2011, 2011)**.

2. DESARROLLO Y RESULTADOS

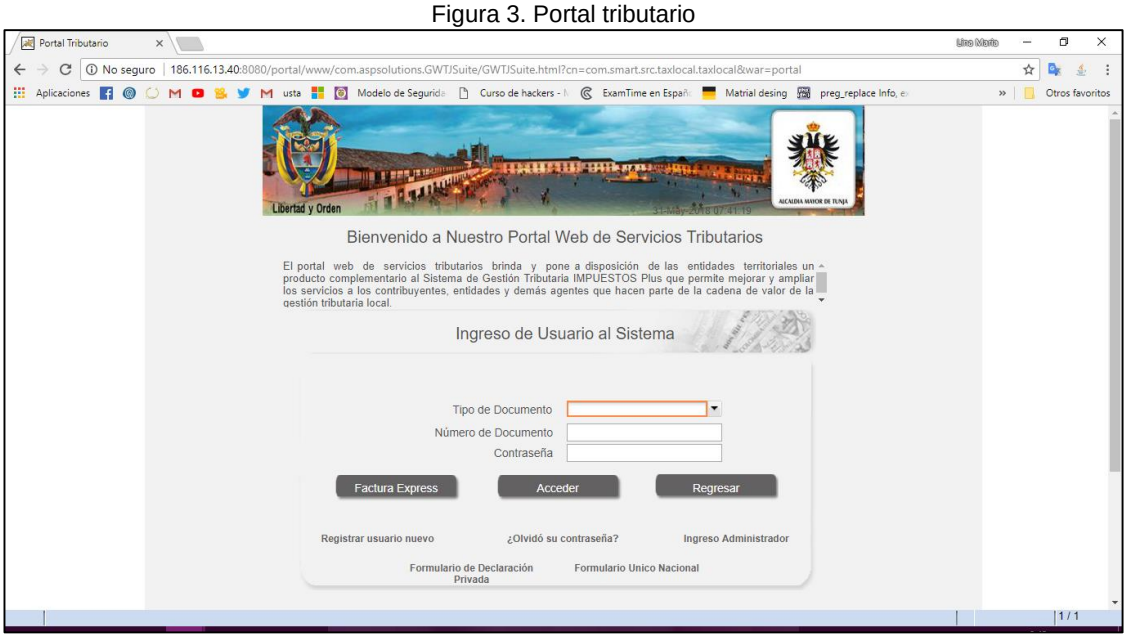
Los sistemas de información analizados para el proyecto fueron Tusig (figura 2) y Portal tributario (figura 3).

Figura 2. Tusig



Fuente: Alcaldía Mayor de Tunja - http://186.116.13.48:81/pmapper/map_default.phtml

Figura 3. Portal tributario



Fuente: Alcaldía Mayor de Tunja - http://186.116.13.40:8080/portal/www/com.aspsolutions.GWTJSuite/GWTJSuite.html?cn=com.smart.src.taxlocal.taxlocal&war=portal

Dentro del presente capitulo se encuentran, representadas cada una de las actividades que se desarrollaron y los resultados obtenidos durante el proyecto (pasantía).

2.1. Identificación y clasificación de los Sistemas de Información.

Dentro del desarrollo de la caracterización de los sistemas de información, se determinaron las siguientes variables:

Tabla 2. Clasificación de los sistemas de información

Nombre del sistema de información	Nombre de Variable de clasificación	Descripción
Descripción	Sistema Operativo Servidor	Se especifica la plataforma base de cada uno de los sistemas de información.
	Ruta Interna Servidor	Se muestra la dirección IP interna del servidor.
	Ruta URL	Se encuentra la URL (Para internet) de ingreso a cada sistema de información.
	Versión	Se encuentra especificado la versión en la que se encuentra actualmente el sistema de información.
	Fecha de Instalación	Se describe la fecha en que se instaló cada sistema de información en cuestión.
	Base de Datos	Se describe el tipo de base de datos y versión correspondiente.
	Componentes	Se identifica el software adicional utilizado como parte de cada uno de los sistemas de información (Php).
	Documentación	Se describe si el sistema de información posee documentación, tal como, manual de usuario, diseño de software, código fuente, entre otros
	Tipo de Aplicación	Se especifica si el sistema de información es de tipo local o web.
	Tipo de Acceso	Se tipifica si el sistema de información es de acceso local o a través de internet.
	Actualizado	Se especifica si el sistema de información se encuentra en la actualidad con parches o actualizaciones pertinentes.
	Desarrollador / Entidad	Se describe el nombre de las personas y la entidad, que

Nombre del sistema de información	Nombre de Variable de clasificación	Descripción
Descripción		realizó desarrollo del sistema de información.
	Procesos	Se especifica que actividad institucional soporta el sistema de información.
	Funciones	Detalla lo que realiza el sistema de información dentro de la entidad.
	Dependencia	Describe la sección de la entidad a la cual se encuentra asociado.
	Usuarios	Especifica los usuarios a los cuales se encuentra dirigidos los sistemas de información.

Fuente: Autor

A continuación se encuentra aplicadas los campos donde se caracteriza los sistemas de información Tusig y Portal tributario como se encuentra representado en la figura 4, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información.

Figura 4. Instrumento de Caracterización de los Sistemas Información [1] - Anexo 2. Caracterización Sistemas de Información

Caracterización de los sistemas de información															
ENTIDAD EVALUADA	Alcaldía Mayor de Tunja														
FECHAS DE EVALUACIÓN	13/6/2019														
CONTACTO	Ing. Julieta Bernal, Area de Sistemas, 318 5356831, sistemas@tunja-boyaca.gov.co														
ELABORADO POR	Lina Maria Wittingham Jiménez														
Descripción															
Nombre del sistema de información	Sistema Operativo Servidor	Ruta Interna Servidor	Ruta URL	Versión	Fecha de Instalación	Base de Datos	Componentes	Documentación	Tipo de Aplicación	Tipo de Acceso	Actualizado	Desarrollador / Entidad	Procesos	Funciones	Dependencia	Usuarios
Tusig	Windows Server 2008 standard-Service Pack 2	10.52.0.13	http://186.116.134.81:81/pmapper/map_default.phtml	1.0	Julio de 2015 (Aproximadamente)	No tiene	Php 5.4.3, lenguaje de etiquetas de Mapserver, JavaScript (jQuery 1.5.1)	Si tiene	Web/Aplicacion de transformación	Público	No	Marilyni Esperanza Moreno Ramos, Manuel Arcadio Rodriguez Cervantes / Universidad Santo Tomas-Tunja	Misionales	Sistema de Información Geográfica de Tunja. En esta aplicación web está contenida la información geográfica del municipio, disponible para libre consulta por los ciudadanos.	Oficina Asesora de Planeación	Todas las oficinas, curadurías urbanas, secretarías del municipio y ciudadanía (Sin roles definidos)
Portal Tributario	Linux 2.6.x - Linux 3.x	10.25.1.8	http://186.116.140.88/0/portal/www/com.aspsolutions.GWTJSuite/GWTJSuite.html?cn=com.smart.src.tools.cal.tax/calificaciones/portal	-	-	Oracle 11 g	Apache Tomcat 4.1+, Java, ExtJS, SWFObject	-	-	-	-	-	Apoyo	Sistema local que tiene como función almacenar la información referente al impuesto predial, las finanzas del municipio y un módulo de gestión de activos del Almacén General.	Secretaría de Hacienda	Funcionarios Secretaría de Hacienda, ciudadanía

Fuente: Autor

[1] En el instrumento de Caracterización de los Sistemas de Información se encuentran unos campos vacíos debido a que no se otorgó acceso de la Información del Portal Tributario, a partir de que una de las dependencias de la Alcaldía Mayor de Tunja, a pesar de que se solicitó tanto verbal como por escrito y a la fecha no fue posible acceder a ella.

2.2. Determinación de los instrumentos de seguridad y niveles de riesgo

En el presente numeral se establecen los instrumentos de clasificación de los Sistemas de Información, al igual que la determinación de los niveles de seguridad y riesgo de los mismos.

2.2.1. Variables de seguridad. Para medir el índice de inseguridad de los SI de la alcaldía, se tendrán en cuenta la implementación de las variables Integridad, disponibilidad y confidencialidad de la información. Esta selección de variables se hace con base en los conceptos de bicho para la seguridad informática, permiten agrupar las posibles vulnerabilidades que se presentan en una aplicación en producción. Además de lo anterior, es posible combinar los resultados obtenidos con metodologías de vulnerabilidades existentes en el mercado, Tal como STRIDE, que es la utilizada en este proyecto.

Para realizar la medición correspondiente a este punto, en los SI de la alcaldía Mayor de Tunja, se tendrá en cuenta la implementación de las siguientes variables relativas a la seguridad de la información tabla 3:

Tabla 3. Variables

Variable	Control NIST
Integridad de la información	(Control NIST SI-7 Special Publication 800-53 (Rev. 4))[2]
Disponibilidad de la información	(Control NIST SC-14 Special Publication 800-53 (Rev. 4))[3]
Confidencialidad en la transmisión	(Control NIST SC-8 Special Publication 800-53 (Rev. 4))[4]

Fuente: Autor

Esta selección de variables se hace con base en los conceptos presentados en el marco teórico del presente trabajo y las definiciones que Bishop hace en este aspecto, en lo relativo a clasificarlas como las métricas más importantes, en lo referente a la seguridad de un sistema. De la misma forma, el Ministerio de las TIC propone estas tres métricas para medición, desde la dimensión operativa, de su modelo MEMSI: **Modelo Estratégico de Métricas en Seguridad de la Información (MinTIC, 2016)**, definido en la guía de auditoría No 15 para seguridad y privacidad de la información, Estos datos sirven de base para todo el estudio, ya que se seleccionan para tener en cuenta el cumplimiento de la normativa nacional en términos de mediciones en seguridad de la información

Adicionalmente, para el marco de aplicación, y las medidas de la seguridad de la información de un SI, se tiene en cuenta lo desarrollado por NIST (National Institute of Standards and Technology) en Security Measurement NIST SP 800-55 en el apartado 3.5.1 en lo que atañe a los sistemas de información individuales, y a la implementación de

[2] Tomado de: National Vulnerability Database, NIST, 2018 disponible en: https://nvd.nist.gov/800-53/Rev4/control/SI-7#enhancement-1 (25-05-2018)
[3] Tomado de: National Vulnerability Database, NIST, 2018 disponible en: https://nvd.nist.gov/800-53/Rev4/control/SC-14 (25-05-2018)
[4] Tomado de: National Vulnerability Database, NIST, 2018 disponible en: https://nvd.nist.gov/800-53/Rev4/control/SC-8?baseline=moderate#enhancement-1 (25-05-2018)

metodologías de medida (**Information Security Measurement Program Implementation Process**), del sexto numeral, del mismo documento, haciendo la salvedad, de acuerdo a este estándar NIST, del desarrollo de las fases uno (**Prepare for data collection**) y dos (**Collect Data and Analyze Results**) para esta pasantía **(Chew, 2008)**

Para concluir este párrafo, cabe anotar que las variables seleccionadas, permiten agrupar las posibles vulnerabilidades que se presentan en una aplicación en producción, tanto mediante el uso de metodologías de evaluación como STRIDE, como con la aplicación de patrones de medición de riesgo, que para el caso de este estudio sería OWASP.

2.2.2. Ponderación de valores. Para realizar la ponderación de los valores se tuvieron en cuenta la probabilidad, impacto, establecimiento de la zona de riesgo como valores principales. Para complementar la información se calculó la prioridad de los componentes de los sistemas de información, en función de su pertinencia y aplicación de medidas correctivas.

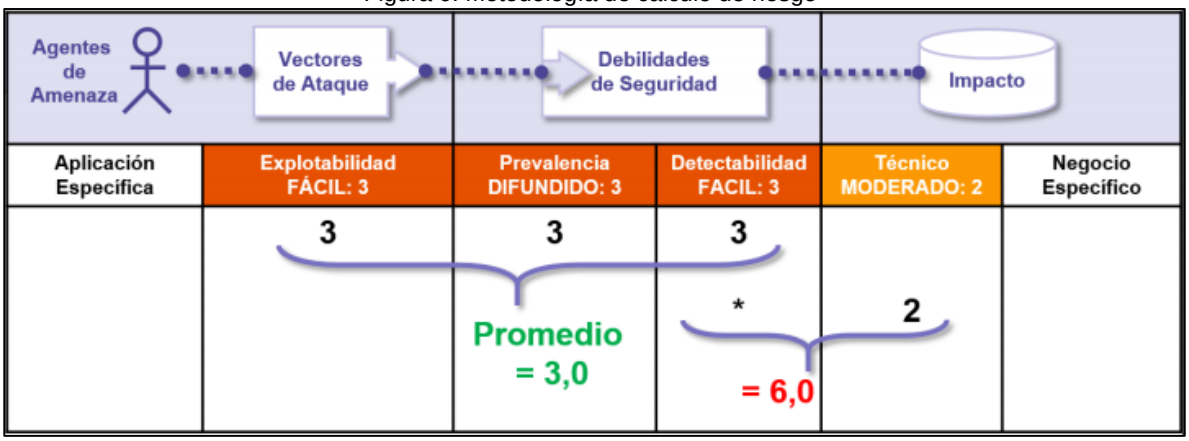
Figura 5. Detalle de la aplicación de variables en el instrumento generalidades Anexo 3. Instrumento Hallazgos Generalidades Componentes Puertos- Sección generalidades y puertos

Clasificación			
Explotabilidad	Prevalencia	Detectabilidad	Impacto técnico

Fuente: Autor

El establecimiento del riesgo se realiza mediante la ponderación de los valores de la explotabilidad, prevalencia, detectabilidad e impacto técnico, usando la metodología de OWASP top 10 como puede verse en OWASP Top 10 - 2017.

Figura 6. Metodología de cálculo de riesgo



Fuente: OWASP Top 10 – 2017 - https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Cabe anotar que estos valores están escalados desde el valor 1 hasta el valor 3 de forma descendente, tal como se puede observar en la figura 7.

Figura 7. Valores generalidades y puertos

Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico
Fácil 3	Difundido 3	Fácil 3	Severo 3
Promedio 2	Común 2	Promedio 2	Moderado 2
Difícil 1	Poco Común 1	Difícil 1	Mínimo 1

Fuente: OWASP Top 10 – 2017 - https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Análogamente, para medir el **riesgo** se utilizó la ponderación establecida por OWASP con valores desde 0 hasta 9, con una escala accedente, tal como puede observase en la figura 8.

Figura 8.Riesgo generalidades y puertos

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Fuente: OWASP - https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

A continuación se describen cada uno de los valores de ponderación para el instrumento de componentes de los sistemas de información, los cuales se encuentran definidos en la Guía de Riesgos DAFP como puede verse en Guía para la administración del riesgo - Función Pública.

Probabilidad para la medición de este indicador se tiene en cuenta la figura 9, que establece una escala ascendente de 1 hasta 5 como base de operación.

Figura 9. Probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

Fuente: Guía de Riesgos DAFP - http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Impacto para la medición de este indicador se tiene en cuenta la figura 10, que establece una escala ascendente de 1 hasta 5 como base de operación.

Figura 10.Impacto componentes

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Fuente: Guía de Riesgos DAFP - http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Para el establecimiento de este indicador se elabora la siguiente tabla con los base en los indicadores de riesgo implementados en ISO27000, como a continuación se detalla (figura 11).

Figura 11. Prioridad

PRIORIDAD		
PRIORIZACIÓN DEL RIESGO	**TIPO DE RIESGO**	**DESCRIPCIÓN DEL RIESGO**
PRIORIDAD A	ALTO	Requiere la aplicación de contra medidas a muy corto plazo.
PRIORIDAD B	MEDIO	Requiere la aplicación de contra medidas a mediano plazo.
PRIORIDAD C	BAJO	Requiere la aplicación de contra medidas a largo plazo.
PRIORIDAD D	MINIMO	Requiere la aplicación de contra medidas y de observación no imediatas.

Fuente: Autor

Para el caso de la **zona de riesgo** representada en la figura 12, la cual contempla un análisis cualitativo para representar la magnitud de las consecuencias potenciales (impacto) y las posibilidades de ocurrencia (probabilidad), donde se tiene en cuenta el siguiente esquema como a continuación se detalla.

Figura 12. Zona de riesgo

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP - http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

2.2.3. Elaboración de instrumentos. Los instrumentos fueron elaborados con los estándares establecidos por el MinTIC en el MSPI, tales como, Modelo de Seguridad y Privacidad de la Información, Guía de Procedimientos de Seguridad de la Información y Guía de Gestión de Riesgo. Para la implementación de estos instrumentos se incluyeron las variables anteriormente mencionadas, teniendo en cuenta, su especificación (seguridad, inventario, instrumentos, entre otros) tal como aparece en la figura 13 y figura 14.

Figura 13. Portada variables de medición

	Variables de seguridad	
ENTIDAD EVALUADA	Alcaldía Mayor de Tunja	
FECHAS DE EVALUACIÓN	fecha de entrega	
CONTACTO	contacto de la entidad	
ELABORADO POR	Lina Maria Wittingham Jiménez	

Fuente: Autor

Figura 14. Portada instrumentos de seguridad

	Instrumento de seguridad	
ENTIDAD EVALUADA	Alcaldía Mayor de Tunja	
FECHAS DE EVALUACIÓN	fecha de entrega	
CONTACTO	contacto de la entidad	
ELABORADO POR	Lina Maria Wittingham Jiménez	

Fuente: Autor

2.2.3.1. Instrumento generalidades. En este instrumento se detallan los hallazgos encontrados en los sistemas de información, así como la cuantificación de los mismos, su impacto y STRIDE correspondiente, como puede verse en la tabla 4.

Tabla 4. Descripción instrumento generalidades

Nombre del Campo	Descripción
Sistema de Información	Se especifica el nombre del sistema de información al que se realiza el análisis.
N°	Se enumera el hallazgo encontrado dentro del sistema de información.
Hallazgo	Se describe la generalidad hallada dentro del sistema de información.
Vulnerabilidad	Es la debilidad encontrada dentro del sistema de información.
Ataque	Los tipos de ataques que pueden llegar a suceder con el hallazgo descubierto en el sistema de información.
STRIDE	Se especifica dentro de la metodología STRIDE la categoría a la que afecta el hallazgo.
Clasificación	Se encuentra constituido por explotabilidad, prevalencia, detectabilidad e impacto técnico.
Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Se especifica las variables de seguridad afectadas a partir de la implicación de los sistemas de información.
Riesgo	Describe la ecuación de riesgo propiamente de OWASP para determinar el valor y el nivel que se encuentra el sistema de información.

Fuente: Autor

A su vez, el campo de clasificación de este instrumento se subdivide en explotabilidad, prevalencia, detectabilidad e impacto técnico como se muestra en la tabla 5.

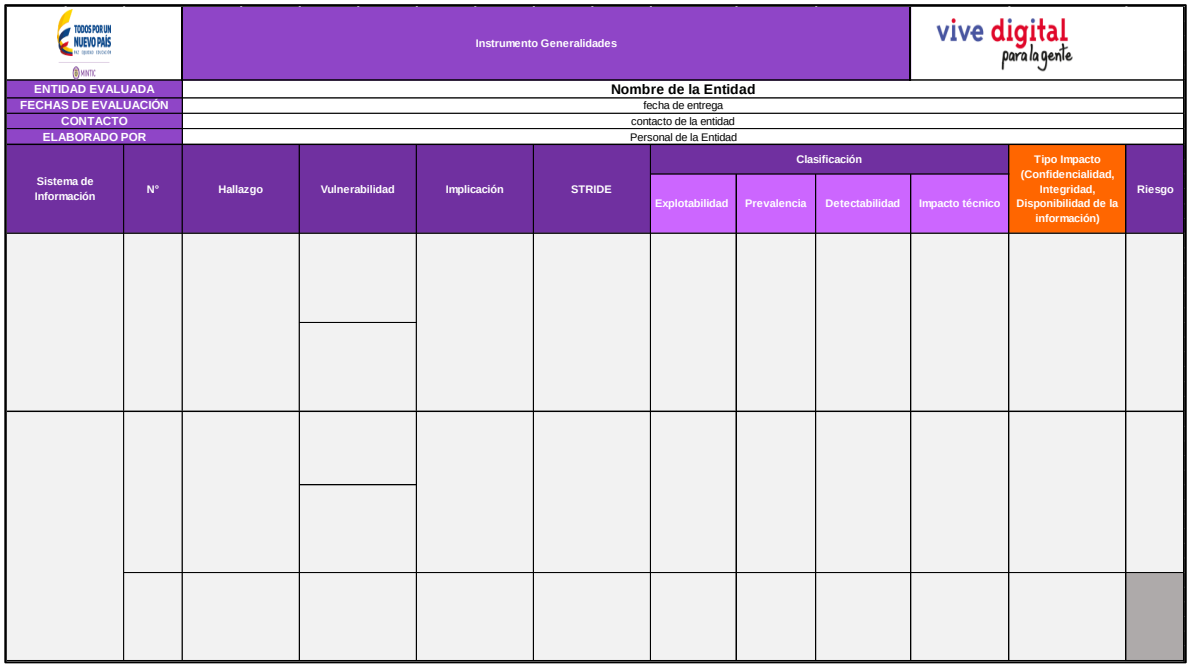
Tabla 5. Descripción de la clasificación del instrumento SI

Nombre del Campo		Descripción
Clasificación	**Explotabilidad**	Representa el vector de ataque donde se especifica si se puede encontrar o explotar una vulnerabilidad.
	Prevalencia	Representa que tan detectable son las debilidades de seguridad dentro del sistema de información.
	Detectabilidad	Es donde se observa que tipo de controles deben existir y son necesarios para las vulnerabilidades posibles.
	Impacto técnico	Es una estimación de cualquier brecha de seguridad existente.

Fuente: Autor

La implementación final de ese instrumento se puede observar en la figura 15 la cual se encuentra a continuación.

Figura 15.Instrumento generalidades Anexo 3. Instrumento Hallazgos Generalidades Componentes Puertos Sección Generalidades



TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento Generalidades								vive digital para la gente		
ENTIDAD EVALUADA	Nombre de la Entidad										
FECHAS DE EVALUACIÓN	fecha de entrega										
CONTACTO	contacto de la entidad										
ELABORADO POR	Personal de la Entidad										
Sistema de Información	N°	Hallazgo	Vulnerabilidad	Implicación	STRIDE	Clasificación				Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Riesgo
						Explotabilidad	Prevalencia	Detectabilidad	Impacto técnico		

Fuente: Autor

2.2.3.2. Instrumento componentes. Para este instrumento se detallan los hallazgos encontrados en los sistemas de información para los componentes, así como la cuantificación de los mismos, su impacto y STRIDE correspondiente, como puede verse en la tabla 6:

Tabla 6. Descripción Instrumento de componentes

Nombre del Campo	Descripción
Sistema de Información	Se especifica el nombre del sistema de información al que se realiza el análisis de componentes.
N°	Se enumera el hallazgo encontrado dentro del componente del sistema de información.
Hallazgo	Se describe el tipo componente y si es utilizado o implementado hallado dentro del sistema de información.
Componente	Se encuentra el nombre del componente que ya anteriormente descrito en el hallazgo.
Versión	Se especifica la versión del componente que se utiliza dentro del sistema de información.
Implicación	Son los tipos de ataques que pueden llegar a suceder con el hallazgo descubierto en los componentes del sistema de información.
STRIDE	Se especifica dentro de la metodología STRIDE la categoría a la que afecta la implicación

Nombre del Campo	Descripción
Clasificación	Se encuentra constituido por la probabilidad, el impacto, el valor entre la probabilidad y el impacto, la prioridad.
Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Se especifica las variables de seguridad afectadas a partir de la implicación de los componentes.
Evaluación	Se encuentra la zona de riesgo la cual especifica el valor ponderado en el que se encuentra el componente del sistema de información.
Base de datos de vulnerabilidades CVE	en este último campo se encuentra las vulnerabilidades de los componentes de los sistemas de información traídas directamente de CVE

Fuente: Autor

A su vez, el campo de clasificación de este instrumento se subdivide en la probabilidad, el impacto, el valor entre la probabilidad y el impacto, la prioridad como se muestra en la tabla 7.

Tabla 7. Descripción de la clasificación del instrumento de componentes

Nombre del Campo		Descripción
Clasificación	**Probabilidad**	Se especifica que tan posible es la afectación que pueda tener el componente del sistema de información
	Impacto	Describe el tipo de afectación que produce el hallazgo.
	Valor	Describe la ecuación de riesgo la cual es **Riesgo = Probabilidad X Impacto**
	Prioridad	Se especifica el tipo de prioridad para así después poder tomar las medidas necesarias.

Fuente: Autor

Para los sub campos de la clasificación se encuentra otra subdivisión en dos columnas, de acuerdo a la implantación del cálculo de vulnerabilidades CVE de NVD. Para este caso particular, se toman en cuenta el vector base y el vector medioambiental, como se representa en la tabla 8.

Tabla 8. Vector base y el vector medioambiental

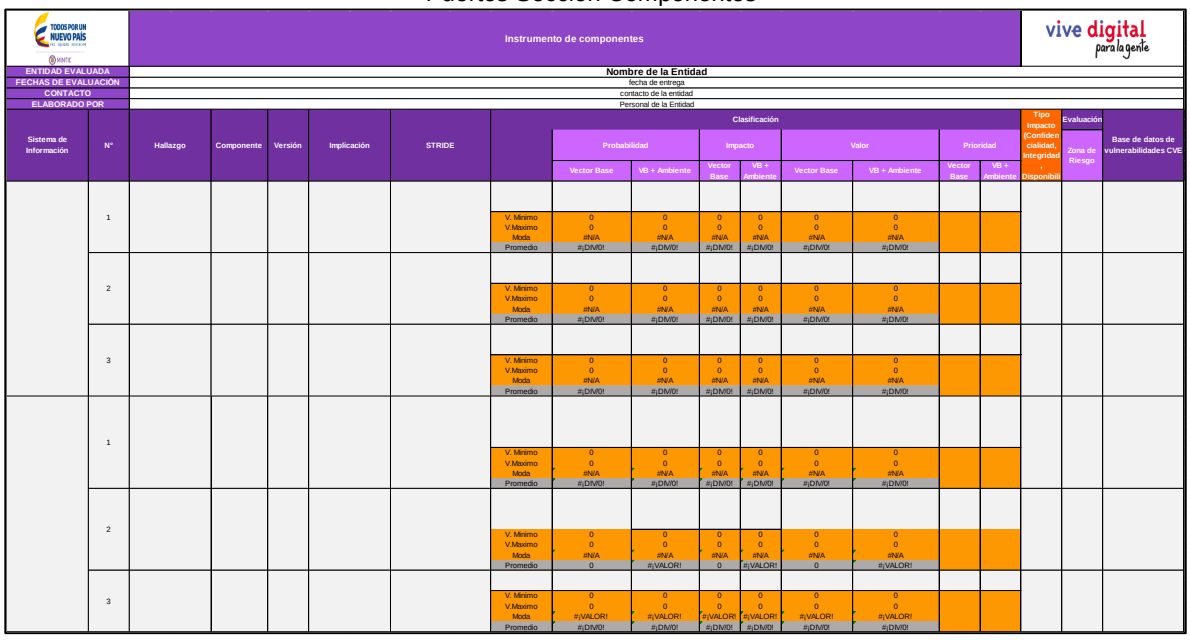
Nombre del Campo	Descripción
Vector Base	“The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it.” (FIRST.org, 2018)

Nombre del Campo	Descripción
VB + Ambiente	“Different environments can have an immense bearing on the risk that a vulnerability poses to an organization and its stakeholders. “ (FIRST.org, 2018)

Fuente: Autor

La implementación final de ese instrumento se puede observar en la figura 16 la cual se encuentra a continuación.

Figura 16. Instrumento de componentes Anexo 3. Instrumento Hallazgos Generalidades Componentes Puertos Sección Componentes



Fuente: Autor

2.2.3.3. Instrumento puertos. En este instrumento se detallan los hallazgos encontrados en los sistemas de información para los puertos, así como la cuantificación de los mismos, su impacto y STRIDE correspondiente, como puede verse en la tabla 9.

Tabla 9. Descripción Instrumento puertos

Nombre del Campo	Descripción
Sistema de Información	Se especifica el nombre del sistema de información al que se realiza el análisis.
N°	Se enumera el hallazgo encontrado dentro del sistema de información.
Hallazgo	Se describe el puerto y si está abierto o cerrado hallado dentro del sistema de información.
Vulnerabilidad	Es la debilidad encontrada dentro de los puertos del sistema de información.
Servicio	El nombre del servicio que provee el puerto para el sistema de información.

Nombre del Campo	Descripción
Ataque	Los tipos de ataques que pueden llegar a suceder con el hallazgo descubierto para los puertos del sistema de información.
STRIDE	Se especifica dentro de la metodología STRIDE la categoría a la que afecta el hallazgo del puerto.
Clasificación	Se encuentra constituido por explotabilidad, prevalencia, detectabilidad e impacto técnico de los puertos.
Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Se especifica las variables de seguridad afectadas a partir del hallazgo y ataque de los puertos de los sistemas de información.
Riesgo	Describe la ecuación de riesgo propiamente de OWASP para determinar el valor y el nivel que se encuentra en los puertos del sistema de información.

Fuente: Autor

A su vez, el campo de clasificación de este instrumento se subdivide en explotabilidad, prevalencia, detectabilidad e impacto técnico como se muestra en la tabla 10.

Tabla 10. Descripción de la clasificación del instrumento puertos

Nombre del Campo		Descripción
Clasificación	**Explotabilidad**	Representa el vector de ataque donde se especifica si se puede encontrar o explotar una vulnerabilidad.
	Prevalencia	Representa que tan detectable son las debilidades de seguridad dentro del sistema de información.
	Detectabilidad	Es donde se observa que tipo de controles deben existir y son necesarios para las vulnerabilidades posibles.
	Impacto técnico	Es una estimación de cualquier brecha de seguridad existente.

Fuente: Autor

La implementación final de ese instrumento se puede observar en la figura 17 la cual se encuentra a continuación.

Figura 17. Instrumento puertos Anexo 3. Instrumento Hallazgos Generalidades Componentes Puertos Sección Puertos

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Instrumento puertos									vive digital para la gente		
ENTIDAD EVALUADA	Nombre de la Entidad											
FECHAS DE EVALUACIÓN	fecha de entrega											
CONTACTO	contacto de la entidad											
ELABORADO POR	Personal de la Entidad											
Sistema de Información	N°	Hallazgo	Servicio	Vulnerabilidad	Implicación	STRIDE	Clasificación				Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Riesgo
							Explotabilidad	Prevalencia	Detectabilidad	Impacto técnico		
	1											
	2											
	3											
	1											
	2											
	3											

Fuente: Autor

2.2.4. Niveles de seguridad. Los niveles de seguridad fueron determinados a partir de las metodologías **OWASP** y **STRIDE**, de la base de datos de vulnerabilidades de **NVD**, teniendo en cuenta la cuantificación de los datos de **CVE** y la normativa propia de **MinTIC** como se explicara a continuación.

Para calcular el nivel de seguridad de las generalidades y puertos de cada sistema de información se realizó el siguiente procedimiento:

- Caracterización de las generalidades y puertos utilizados por los sistemas de información.
- Determinación de vulnerabilidades para las generalidades y puertos de información de los sistemas de información, vía OWASP.
- Cuantificación de valores OWASP para las vulnerabilidades encontradas
- Clasificación y categorización de las vulnerabilidades a través de STRIDE.
- Determinación de variables de seguridad mediante referencia OWASP.
- Escalamiento de datos teniendo como base la documentación MinTIC.

Para calcular el nivel de seguridad de los componentes de cada sistema de información se realizó el siguiente procedimiento:

- Caracterización de los componentes utilizados por los sistemas de información.

- Determinación de vulnerabilidades para los componentes de los SI, vía NVD.
- Cuantificación de vectores CVE para las vulnerabilidades encontradas
- Clasificación y categorización de las vulnerabilidades a través de STRIDE.
- Determinación de variables de seguridad mediante referencia cruzada STRIDE - CVE
- Escalamiento de datos teniendo como base la documentación MinTIC.

2.2.5. Niveles de riesgo. Los niveles de riesgo fueron obtenidos a partir de la normativa propia del **MinTIC** y las metodologías **OWASP** y **STRIDE**, la cual se explicará a continuación.

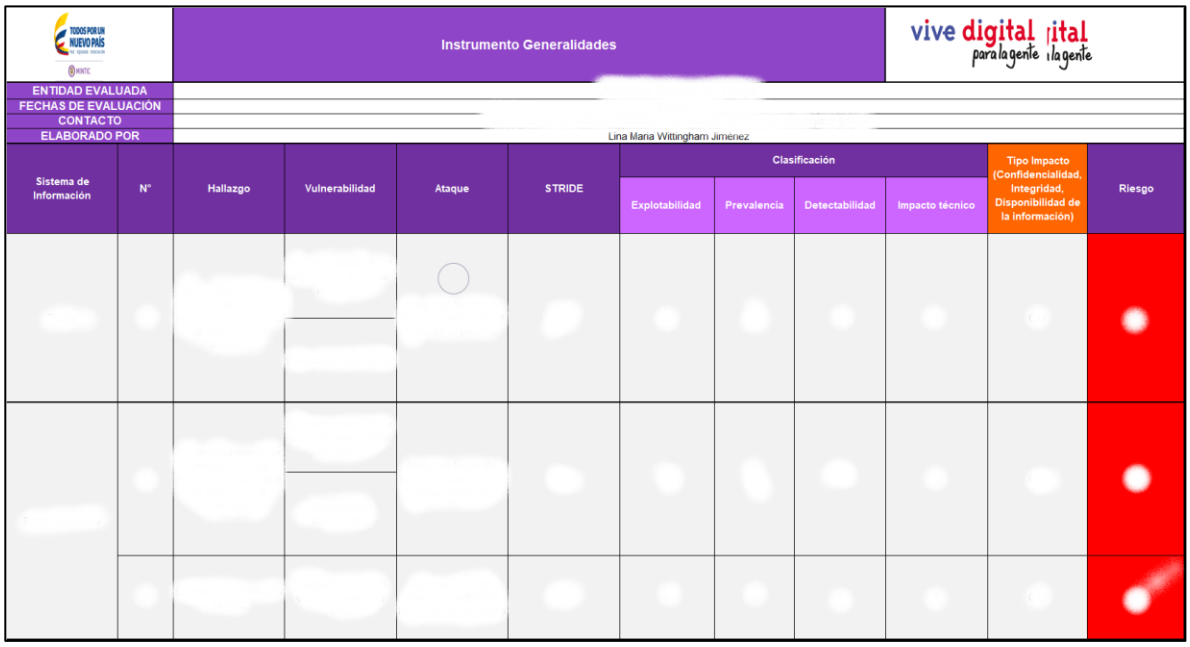
Para calcular el nivel de riesgo de las generalidades, componentes y puertos de cada sistema de información se realizó el siguiente procedimiento:

- Caracterización de las generalidades, componentes y puertos utilizados por los sistemas de información.
- Determinación de vulnerabilidades para las generalidades y puertos vía OWASP, para los componentes vía NVD.
- Ejecución un conteo de los datos y valores de seguridad de las generalidades, componentes y puertos.
- Escalamiento propio de MinTIC una vez obtenidos todos los datos y valores de seguridad para las generalidades, componentes y puertos.
- Cuantificación de los datos y los valores para las generalidades, componentes y puertos se realiza las gráficas de niveles de seguridad y riesgo.
- Generación de reportes gráficos demuestran las veces en que se repite la clasificación y categorización de las vulnerabilidades a través de STRIDE. Al igual las veces en que se repite el tipo de impacto CID (Confidencialidad, Integridad, Disponibilidad) dentro de cada generalidad, componente y puerto.
- Realización conteo total de la clasificación y categorización de las vulnerabilidades a través de STRIDE, y tipo de impacto CID.

2.2.6. Aplicación de instrumentos. Los instrumentos fueron aplicados a partir del análisis de cada sistema de información, donde se implementa la caracterización de los componentes, generalidades y puertos de los mismos.

En la figura 18, se observa la aplicación del instrumento de generalidades para los sistemas de información (Tusig y Portal tributario).

Figura 18. Aplicación instrumento de generalidades

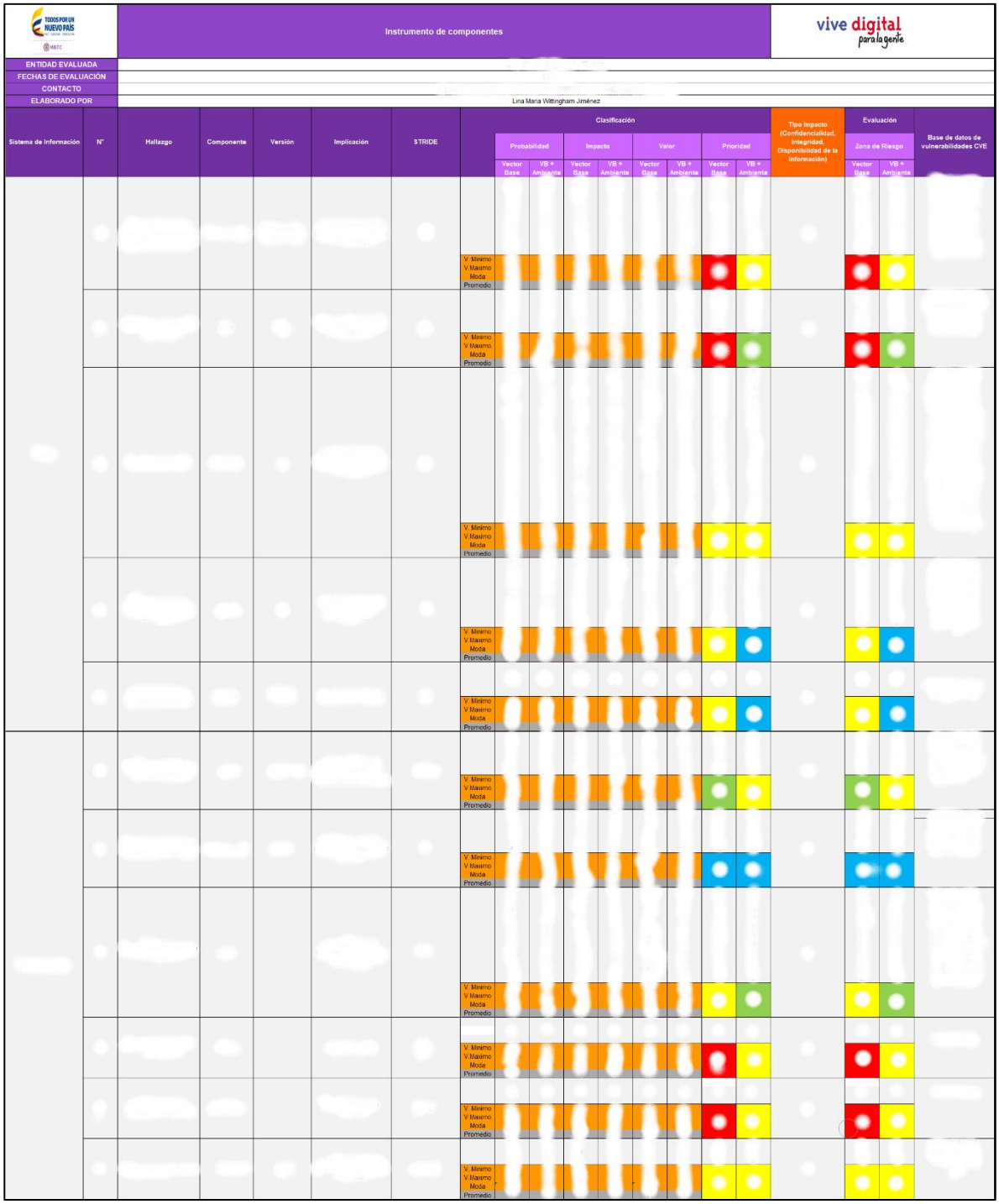


Instrumento Generalidades											
ENTIDAD EVALUADA											
FECHAS DE EVALUACIÓN											
CONTACTO											
ELABORADO POR	Lina Maria Wittingham Jiménez										
Sistema de Información	N°	Hallazgo	Vulnerabilidad	Ataque	STRIDE	Clasificación				Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Riesgo
						Explotabilidad	Prevalencia	Detectabilidad	Impacto técnico		

Fuente: Autor

En la figura 19 se observa la aplicación del instrumento de componentes para los sistemas de información (Tusig y Portal tributario).

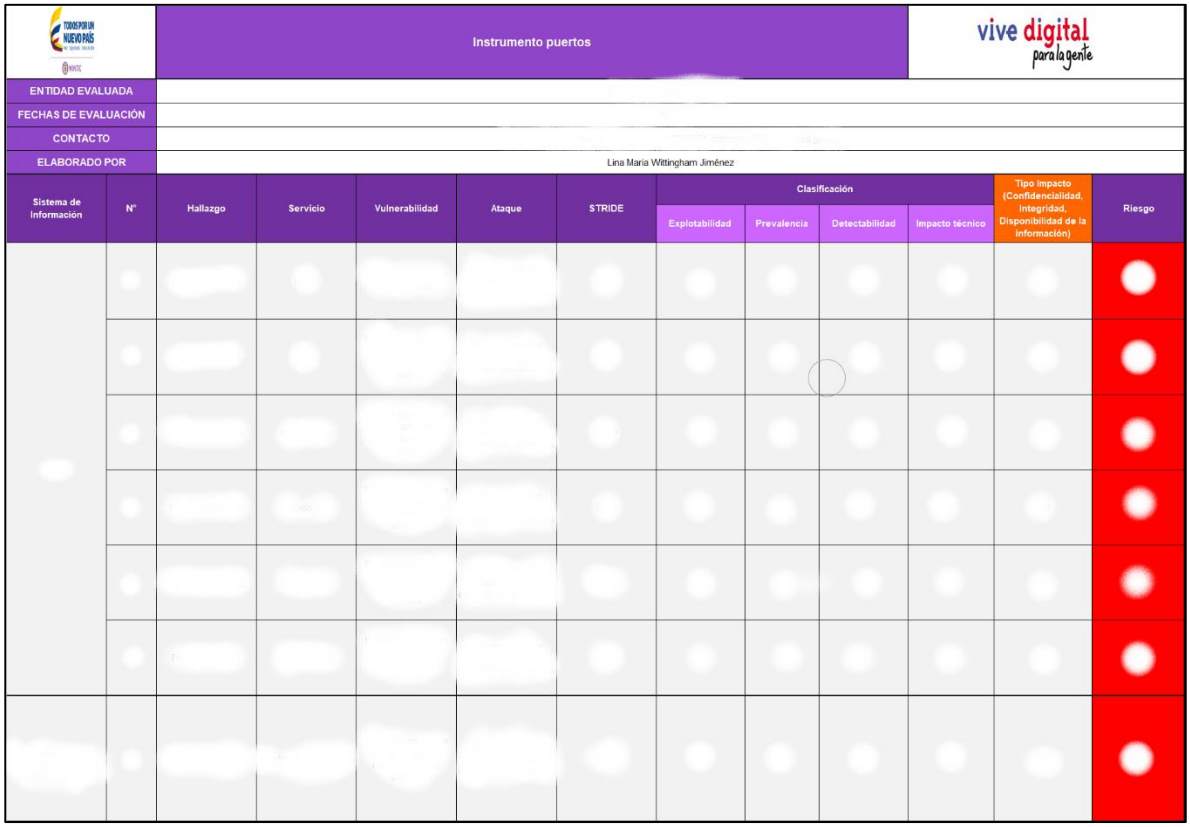
Figura 19. Aplicación Instrumento de componentes



Fuente: Autor

En la figura 20 se observa la aplicación del instrumento de puertos para los sistemas de información (Tusig Portal tributario).

Figura 20.Aplicación del instrumento de puertos



Instrumento puertos												
ENTIDAD EVALUADA												
FECHAS DE EVALUACIÓN												
CONTACTO												
ELABORADO POR	Lina Maria Wittingham Jiménez											
Sistema de Información	N°	Hallazgo	Servicio	Vulnerabilidad	Ataque	STRIDE	Clasificación				Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Riesgo
							Explotabilidad	Prevalencia	Detectabilidad	Impacto técnico		

Fuente: Autor

2.2.6. Obtención de datos y cuantificación. En este apartado se explicarán cada uno de los pasos metodológicos anteriormente diseñados, teniendo en cuenta su correspondiente aplicación en los instrumentos de medición, tanto para niveles de seguridad, como para niveles de riesgo en los sistemas de información Tusig y Portal Tributario.

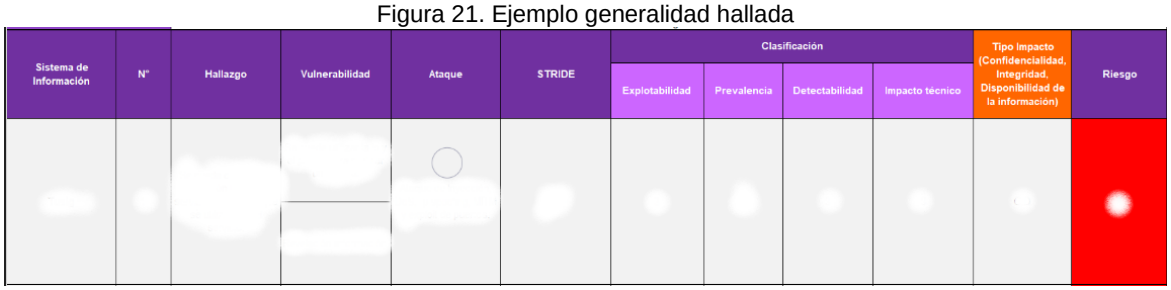
2.2.6.1. Instrumento generalidades. Según la metodologías descritas en el aparatados **2.2.4** y **2.2.5**, como se observó el siguiente desarrollo para la implantación del instrumento.

Metodología para el cálculo de los niveles de seguridad

- **Caracterización de las generalidades utilizadas por los sistemas de información.**

Para hacer claridad en la obtención y cuantificación de los datos, se usa como ejemplo una de las generalidades halladas, la cual se observa en la figura 21. En esta pueden verse los campos del instrumento en su versión final, con la cual se explicará el desarrollo de los pasos de esta sección.

Figura 21. Ejemplo generalidad hallada



Fuente: Autor

- **Determinación de vulnerabilidades para las generalidades de los sistemas de información, vía OWASP.**

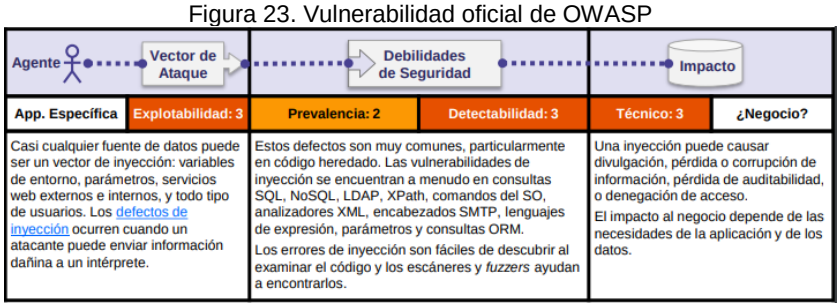
A través de los conocimientos adquiridos en clases y métodos de investigación (buenas prácticas de seguridad informática) para seguridad informática, se encontraron los hallazgos correspondientes a las vulnerabilidades de las generalidades del sistema, tal como se puede apreciar en la figura 22.

Figura 22. Ejemplo hallazgo generalidades

Fuente: Autor

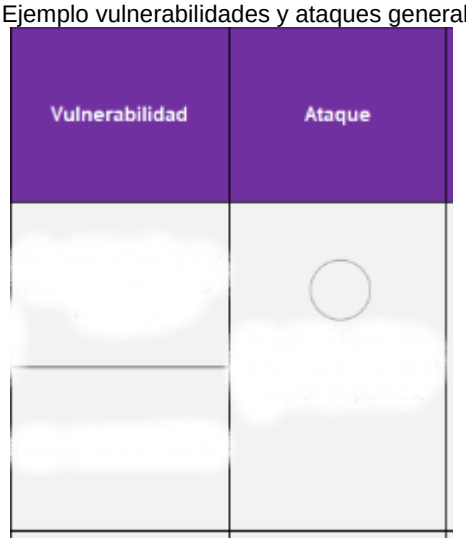
Vía OWASP se determinaron las vulnerabilidades a través de la búsqueda de las mismas dentro del OWASP TOP 10 Para dar un ejemplo de esto se observa la figura 23 donde se encuentra la vulnerabilidad oficial de OWASP. Con base en la información de la figura 23, se relacionan los ataques a las vulnerabilidades encontradas en el instrumento de generalidades del sistema de información, tal como se puede observar en la figura 24.

Figura 23. Vulnerabilidad oficial de OWASP



Fuente: OWASP Top 10 – 2017 - https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Figura 24. Ejemplo vulnerabilidades y ataques generalidades

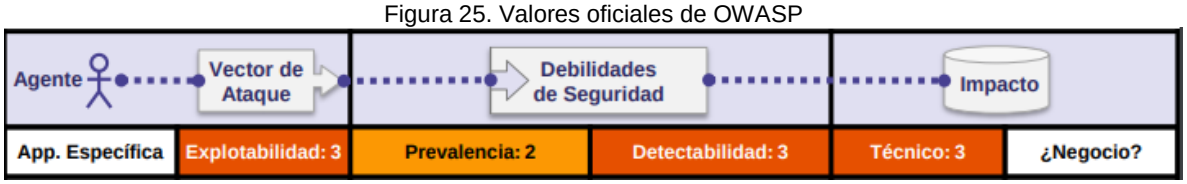


Fuente: Autor

- **Cuantificación de valores OWASP para las vulnerabilidades encontradas.**

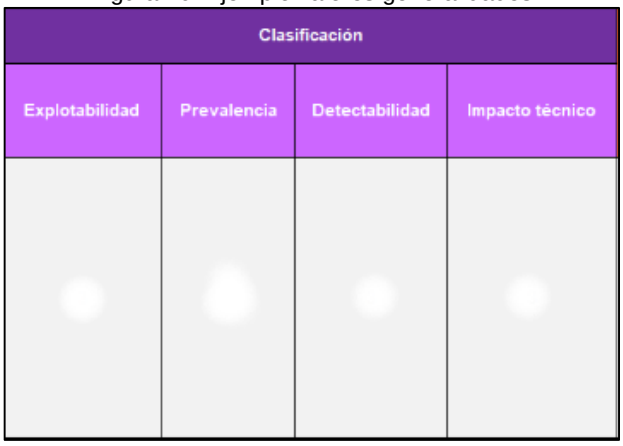
Se cuantifica los valores a través del OWASP TOP 10, para dar un ejemplo de esto se observa la figura 25 donde se encuentra los valores oficiales de OWASP. Con base en la información de la figura 25, se relacionan los valores de las vulnerabilidades encontradas en el instrumento de generalidades del sistema de información tal como se puede observar en la figura 26.

Figura 25. Valores oficiales de OWASP



Fuente: OWASP Top 10 – 2017 - https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Figura 26. Ejemplo valores generalidades

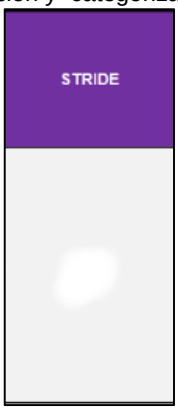


Fuente: Autor

- **Clasificación y categorización de las vulnerabilidades a través de STRIDE.**

A partir de las vulnerabilidades a través de la base documental de OWASP, se determinó la clasificación y categoría STRIDE en la que se encuentra dicha vulnerabilidad, como se puede observar en la figura 27.

Figura 27. Ejemplo clasificación y categorización STRIDE generalidades

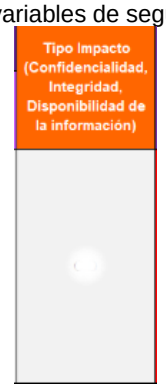


Fuente: Autor

- **Determinación de variables de seguridad mediante referencia OWASP.**

Una vez obtenidos las vulnerabilidades, ataques, valores y clasificación STRIDE para las generalidades de los sistemas de información a través de la referencia OWASP para cada caso, se determinan las variables de seguridad que se ven afectadas por la misma, como se observa en la figura 28.

Figura 28. Ejemplo variables de seguridad generalidades

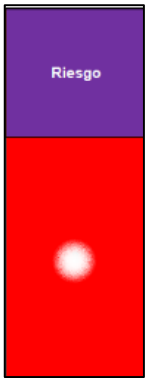


Fuente: Autor

- **Escalamiento de datos teniendo como base la documentación MinTIC.**

Como se puede apreciar en el numeral **2.2.2. Ponderación de valores,** se realiza el cálculo del riesgo de la vulnerabilidad hallada en el sistema información, como se representa en la figura 29.

Figura 29. Ejemplo escalamiento de datos generalidades



Fuente: Autor

Metodología para el cálculo de los niveles de riesgo

- **Caracterización de las generalidades utilizadas por los sistemas de información.**
- **Determinación de vulnerabilidades para las generalidades vía OWASP.**
- **Ejecución un conteo de los datos y valores de seguridad de las generalidades.**
- **Escalamiento propio de MinTIC una vez obtenidos todos los datos y valores de seguridad para las generalidades.**

Se encuentra directamente asociado al análisis de seguridad, expuesto anteriormente, como se puede observar en el presente documento.

- **Cuantificación de los datos y los valores para las generalidades se realiza las gráficas de niveles de seguridad y riesgo.**

Se cuantifica los datos y valores de las generalidades de los sistemas de información a través del análisis de seguridad anteriormente expuesto, para así realizar el conteo total de los niveles de seguridad y riesgo.

- **Generación de reportes gráficos demuestran las veces en que se repite la clasificación y categorización de las vulnerabilidades a través de STRIDE. Al igual las veces en que se repite el tipo de impacto CID (Confidencialidad, Integridad, Disponibilidad) dentro de cada generalidad.**

Las gráficas se realizaron a partir de los datos que se cuantificaron de los niveles de seguridad y riesgo de los hallazgos en los sistemas de información. Estas gráficas sirven para realizar un análisis estadístico descriptivo, usando estructuras de barras y diagramas porcentuales circulares.

- **Realización conteo total de la clasificación y categorización de las vulnerabilidades a través de STRIDE, y tipo de impacto CID.**

A través de la cuantificación de los datos, teniendo en cuenta los valores obtenidos, se determina el nivel total de afectación dentro de las generalidades de cada sistema de información, donde entre más alto sea el valor mayor la afectación.

2.2.6.2. Instrumento componentes. Según la metodologías descritas en el aparatados **2.2.4** y **2.2.5**, como se observó el siguiente desarrollo para la implantación del instrumento.

Metodología para el cálculo de los niveles de seguridad

- **Caracterización de los componentes utilizados por los sistemas de información.**

Para hacer claridad en la obtención y cuantificación de los datos, se usa como ejemplo uno de los componentes hallados, la cual se observa en la figura 30. En esta pueden verse los campos del instrumento en su versión final, con la cual se explicará el desarrollo de los pasos de esta sección.

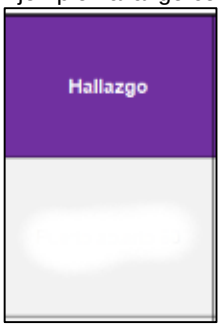
Figura 30. Ejemplo componente hallado

Fuente: Autor

- **Determinación de vulnerabilidades para los componentes de los SI, vía NVD.**

A través de los conocimientos adquiridos en clases y métodos de investigación (buenas prácticas de seguridad informática) para seguridad informática, se encontraron los hallazgos correspondientes a las vulnerabilidades de los componentes del sistema, tal como se puede apreciar en la figura 31.

Figura 31. Ejemplo hallazgo componentes

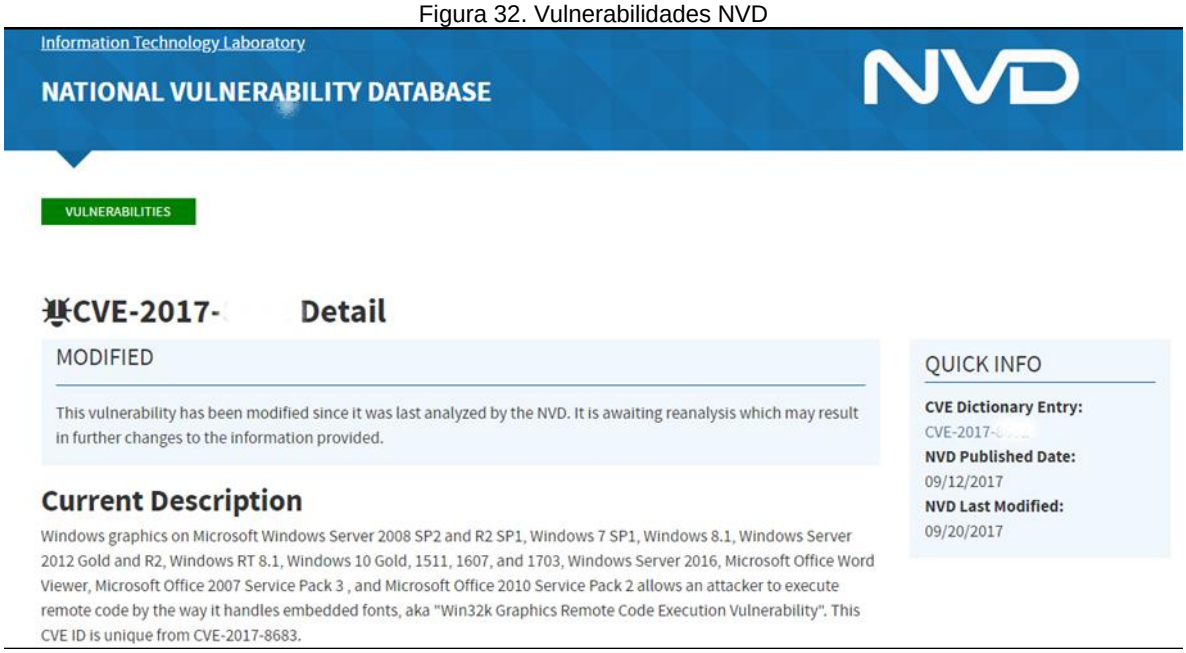


Fuente: Autor

Vía NVD se determinó las vulnerabilidades a través de la búsqueda de las mismas, para dar un ejemplo de esto se observa la figura 32 donde se encuentra la vulnerabilidad oficial en NVD. Con base en la información de la figura 32, se relacionan los ataques a las

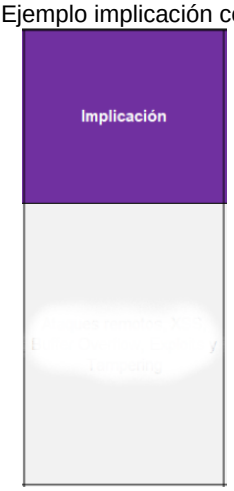
vulnerabilidades encontradas en el instrumento de componentes del sistema de información tal como se puede observar en la figura 33.

Figura 32. Vulnerabilidades NVD



Fuente: NVD - https://nvd.nist.gov/vuln/detail/CVE-2017-8682

Figura 33. Ejemplo implicación componentes

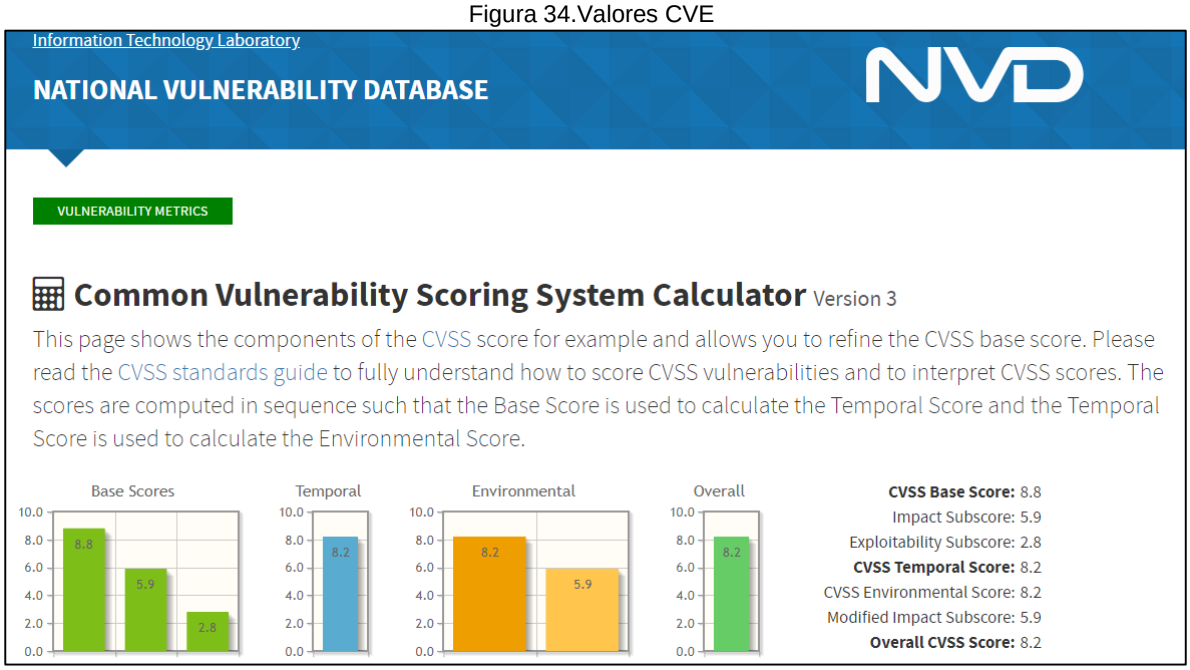


Fuente: Autor

- **Cuantificación de vectores CVE para las vulnerabilidades encontradas.**

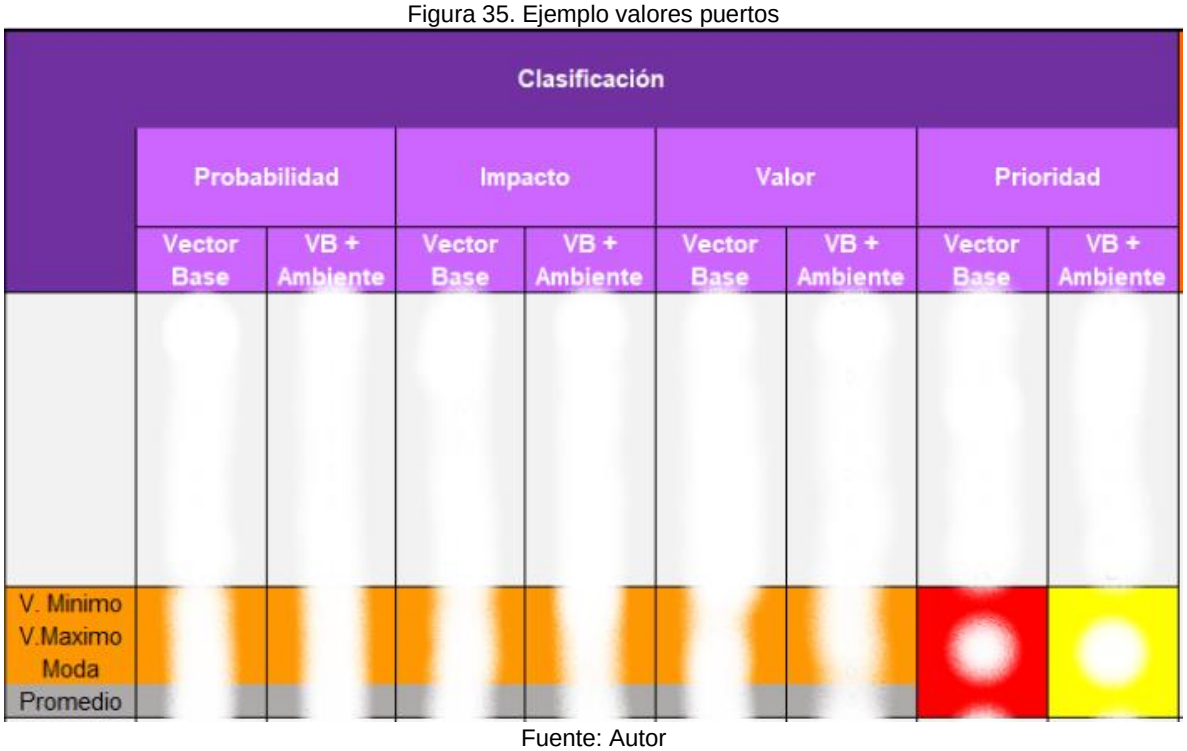
Se cuantifica los valores a través de Common Vulnerability Scoring System Calculator, para dar un ejemplo de esto se observa la figura 34 donde se encuentra los valores oficiales de NVD para CVE. Con base en la información de la figura 34, se relacionan los valores de las vulnerabilidades encontradas en el instrumento de componentes del sistema de información tal como se puede observar en la figura 35.

Figura 34.Valores CVE



Fuente: Common Vulnerability Scoring System Calculator / NVD para CVE

Figura 35. Ejemplo valores puertos

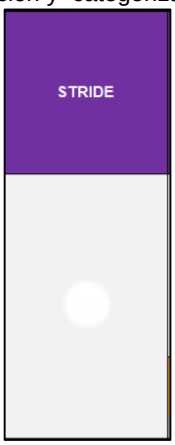


Fuente: Autor

- **Clasificación y categorización de las vulnerabilidades a través de STRIDE.**

A partir de las vulnerabilidades a través de la base documental de OWASP, se determinó la clasificación y categoría STRIDE en la que se encuentra dicha vulnerabilidad, como se puede observar en la figura 36.

Figura 36. Ejemplo clasificación y categorización STRIDE componentes



Fuente: Autor

- **Determinación de variables de seguridad mediante referencia cruzada STRIDE – CVE.**

Una vez obtenidos las vulnerabilidades, implicaciones, valores y clasificación STRIDE para los componentes de los sistemas de información a través de la referencia CVE para cada caso, se determinan las variables de seguridad que se ven afectadas por el mismo, como se observa en la figura 28.

Figura 37. Ejemplo variables de seguridad componentes

Fuente: Autor

- **Escalamiento de datos teniendo como base la documentación MinTIC.**

Como se puede apreciar en el numeral **2.2.2. Ponderación de valores,** se realiza el cálculo del riesgo de la vulnerabilidad hallada en el sistema información, como se representa en la figura 29.

Figura 38. Ejemplo escalamiento de datos componentes

Fuente: Autor

Metodología para el cálculo de los niveles de riesgo

- **Caracterización de los componentes utilizados por los sistemas de información.**
- **Determinación de vulnerabilidades para los componentes vía OWASP.**
- **Ejecución un conteo de los datos y valores de seguridad de los puertos.**
- **Escalamiento propio de MinTIC una vez obtenidos todos los datos y valores de seguridad para los componentes.**

Se encuentra directamente asociado al análisis de seguridad, expuesto anteriormente, como se puede observar en el presente documento.

- **Cuantificación de los datos y los valores para los componentes se realiza las gráficas de niveles de seguridad y riesgo.**

Se cuantifica los datos y valores de los componentes de los sistemas de información a través del análisis de seguridad anteriormente expuesto, para así realizar el conteo total de los niveles de seguridad y riesgo.

- **Generación de reportes gráficos demuestran las veces en que se repite la clasificación y categorización de las vulnerabilidades a través de STRIDE. Al igual las veces en que se repite el tipo de impacto CID (Confidencialidad, Integridad, Disponibilidad) dentro de cada puerto.**

Las gráficas se realizaron a partir de los datos que se cuantificaron de los niveles de seguridad y riesgo de los hallazgos en los sistemas de información. Estas gráficas sirven para realizar un análisis estadístico descriptivo, usando estructuras de barras y diagramas porcentuales circulares.

- **Realización conteo total de la clasificación y categorización de las vulnerabilidades a través de STRIDE, y tipo de impacto CID.**

A través de la cuantificación de los datos, teniendo en cuenta los valores obtenidos, se determina el nivel total de afectación dentro de los componentes de cada sistema de información, donde entre más alto sea el valor mayor la afectación.

2.2.6.3. Instrumento puertos. Según la metodologías descritas en el aparatados **2.2.4** y **2.2.5**, como se observó el siguiente desarrollo para la implantación del instrumento.

Metodología para el cálculo de los niveles de seguridad

- **Caracterización de los puertos utilizados por los sistemas de información.**

Para hacer claridad en la obtención y cuantificación de los datos, se usa como ejemplo una de los puertos hallados, la cual se observa en la figura 39. En esta pueden verse los campos del instrumento en su versión final, con la cual se explicará el desarrollo de los pasos de esta sección.

Figura 39. Ejemplo puerto hallado

N°	Hallazgo	Servicio	Vulnerabilidad	Ataque	STRIDE	Clasificación				Tipo Impacto (Confidencialidad, Integridad, Disponibilidad de la información)	Riesgo
						Explotabilidad	Prevalencia	Detectabilidad	Impacto técnico		

Fuente: Autor

- **Determinación de vulnerabilidades para los puertos de los sistemas de información, vía OWASP.**

A través de los conocimientos adquiridos en clases y métodos de investigación (buenas prácticas de seguridad informática) para seguridad informática, se encontraron los hallazgos correspondientes a las vulnerabilidades de los puertos y servicios del sistema, tal como se puede apreciar en la figura 40.

Figura 40. Ejemplo hallazgo generalidades

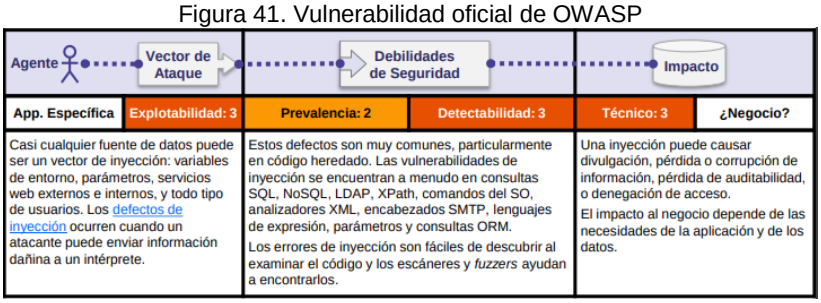
Hallazgo	Servicio

Fuente: Autor

Vía OWASP se determinaron las vulnerabilidades a través de la búsqueda de las mismas dentro del OWASP TOP 10 Para dar un ejemplo de esto se observa la figura 41 donde se encuentra la vulnerabilidad oficial de OWASP. Con base en la información de la figura 41,

se relacionan los ataques a las vulnerabilidades encontradas en el instrumento de puertos del sistema de información, tal como se puede observar en la figura 42.

Figura 41. Vulnerabilidad oficial de OWASP



Fuente: OWASP Top 10 – 2017 - https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

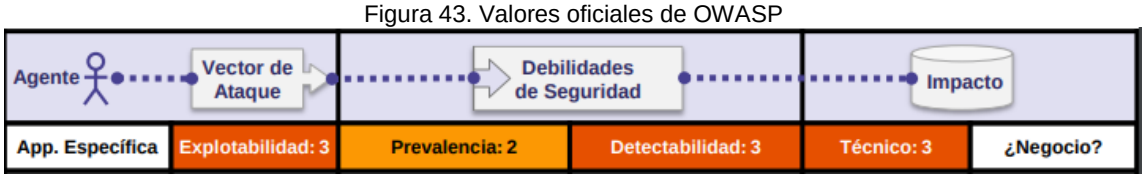
Figura 42. Ejemplo vulnerabilidades y ataques puertos

Fuente: Autor

- **Cuantificación de valores OWASP para las vulnerabilidades encontradas.**

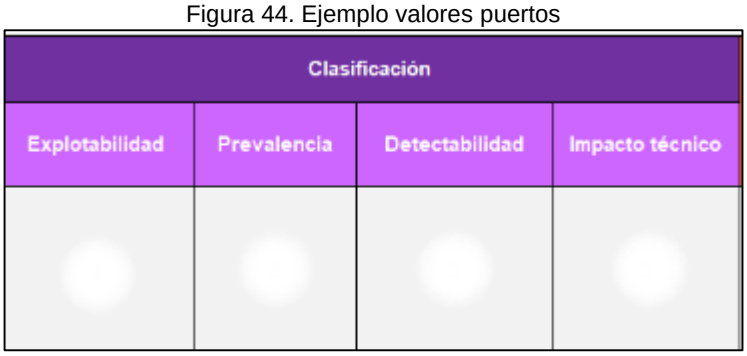
Se cuantifica los valores a través del OWASP TOP 10, para dar un ejemplo de esto se observa la figura 43 donde se encuentra los valores oficiales de OWASP. Con base en la información de la figura 43, se relacionan los valores de las vulnerabilidades encontradas en el instrumento de puertos del sistema de información tal como se puede observar en la figura 44.

Figura 43. Valores oficiales de OWASP



Fuente: OWASP Top 10 – 2017 - https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Figura 44. Ejemplo valores puertos

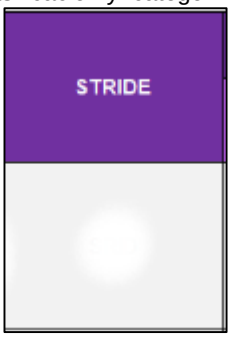


Fuente: Autor

- **Clasificación y categorización de las vulnerabilidades a través de STRIDE.**

A partir de las vulnerabilidades a través de la base documental de OWASP, se determinó la clasificación y categoría STRIDE en la que se encuentra dicha vulnerabilidad, como se puede observar en la figura 45.

Figura 45. Ejemplo clasificación y categorización STRIDE puertos

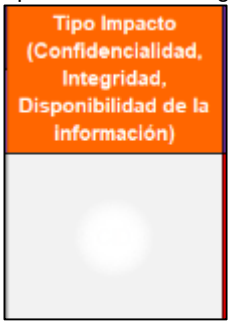


Fuente: Autor

- **Determinación de variables de seguridad mediante referencia OWASP.**

Una vez obtenidos las vulnerabilidades, ataques, valores y clasificación STRIDE para los puertos de los sistemas de información a través de la referencia OWASP para cada caso, se determinan las variables de seguridad que se ven afectadas por la misma, como se observa en la figura 46.

Figura 46. Ejemplo variables de seguridad puertos



Fuente: Autor

- **Escalamiento de datos teniendo como base la documentación MinTIC.**

Como se puede apreciar en el numeral **2.2.2. Ponderación de valores,** se realiza el cálculo del riesgo de la vulnerabilidad hallada en el sistema información, como se representa en la figura 47.

Figura 47. Ejemplo escalamiento de datos puertos

Fuente: Autor

Metodología para el cálculo de los niveles de riesgo

- **Caracterización de los puertos utilizados por los sistemas de información.**
- **Determinación de vulnerabilidades para los puertos vía OWASP.**
- **Ejecución un conteo de los datos y valores de seguridad de los puertos.**
- **Escalamiento propio de MinTIC una vez obtenidos todos los datos y valores de seguridad para los puertos.**

Se encuentra directamente asociado al análisis de seguridad, expuesto anteriormente, como se puede observar en el presente documento.

- **Cuantificación de los datos y los valores para los puertos se realiza las gráficas de niveles de seguridad y riesgo.**

Se cuantifica los datos y valores de los puertos de los sistemas de información a través del análisis de seguridad anteriormente expuesto, para así realizar el conteo total de los niveles de seguridad y riesgo.

- **Generación de reportes gráficos demuestran las veces en que se repite la clasificación y categorización de las vulnerabilidades a través de STRIDE. Al igual las veces en que se repite el tipo de impacto CID (Confidencialidad, Integridad, Disponibilidad) dentro de cada puerto.**

Las gráficas se realizaron a partir de los datos que se cuantificaron de los niveles de seguridad y riesgo de los hallazgos en los sistemas de información. Estas gráficas sirven para realizar un análisis estadístico descriptivo, usando estructuras de barras y diagramas porcentuales circulares.

- **Realización conteo total de la clasificación y categorización de las vulnerabilidades a través de STRIDE, y tipo de impacto CID.**

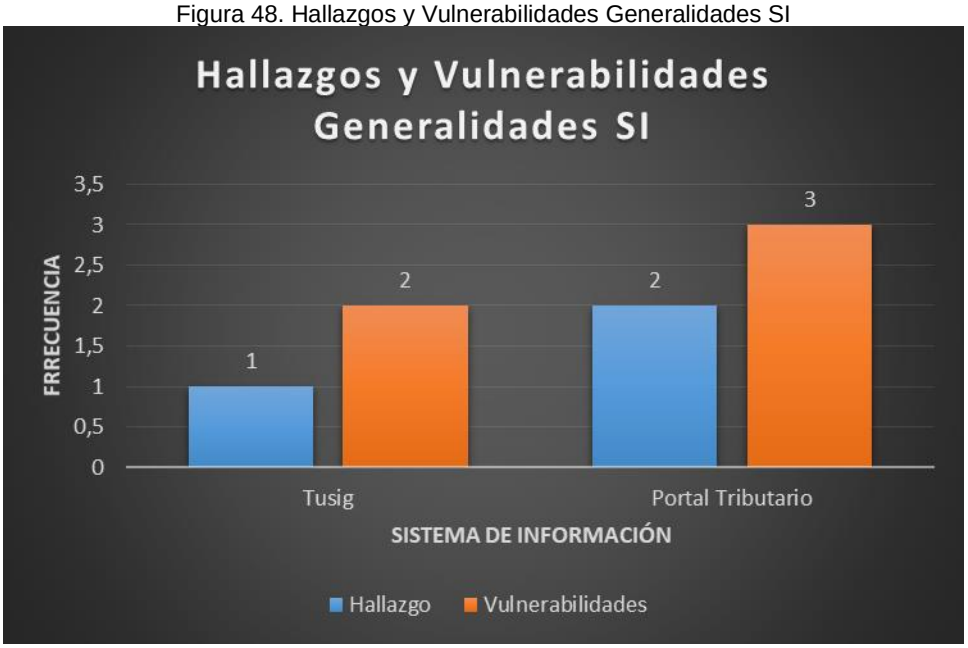
A través de la cuantificación de los datos, teniendo en cuenta los valores obtenidos, se determina el nivel total de afectación dentro de los puertos de cada sistema de información, donde entre más alto sea el valor mayor la afectación.

2.3. Resultados de medición y Recomendaciones

En el presente numeral se encuentra los resultados de medición en los sistemas de información Tusig y Portal tributario, tanto para la categorización de vulnerabilidades a través de STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of Privilege) como para las variables de seguridad, usando CID (Confidencialidad, Integridad y Disponibilidad). También se cuenta con las determinaciones del nivel de seguridad y riesgo de los sistemas de información de la Alcaldía mayor estudiados, teniendo en cuenta el descubrimiento de vulnerabilidades y clasificación vía CVE/NVD. Para tal efecto se muestran, tanto los resultados de cada SI por aparte, como los resultados globales del análisis de datos.

A continuación en la figura 48, donde se especifica los hallazgos y las vulnerabilidades para las generalidades en los sistemas de información.

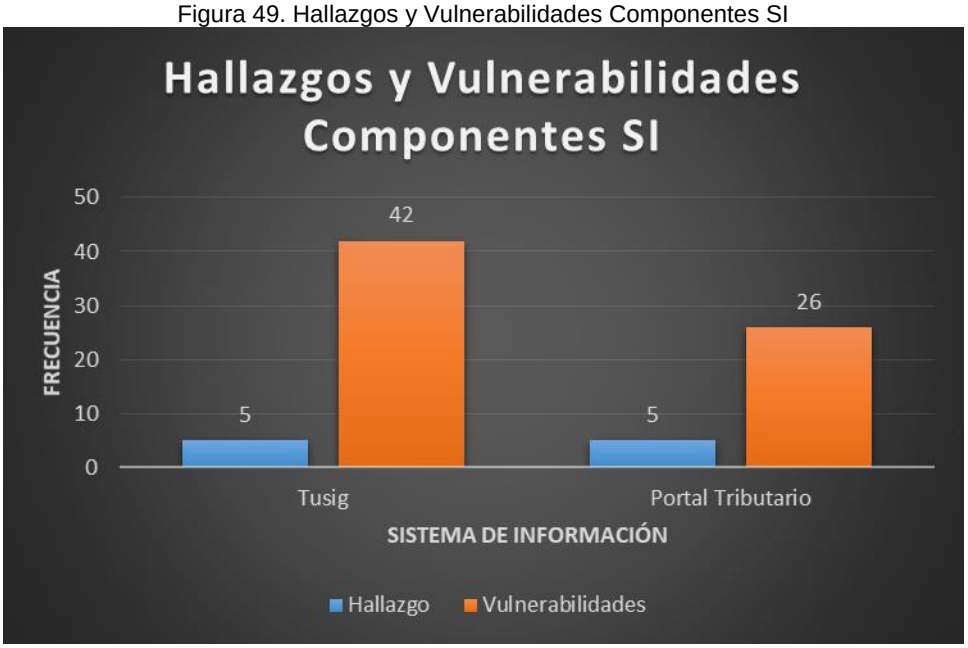
Figura 48. Hallazgos y Vulnerabilidades Generalidades SI



Fuente: Autor

En la figura 49, donde se especifica los hallazgos y las vulnerabilidades para los componentes en los sistemas de información.

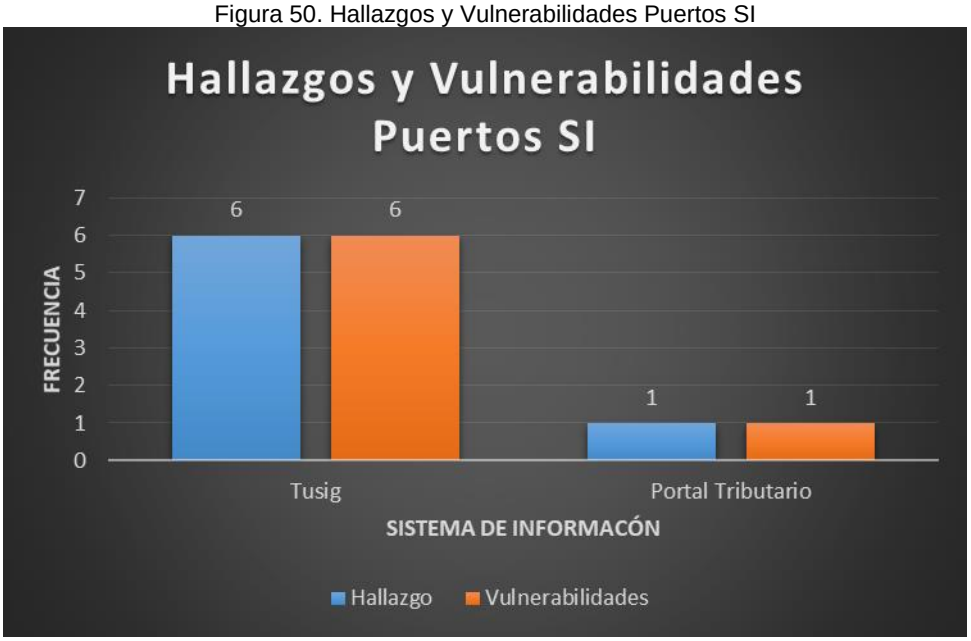
Figura 49. Hallazgos y Vulnerabilidades Componentes SI



Fuente: Autor

A continuación en la figura 50, donde se especifica los hallazgos y las vulnerabilidades para los puertos en los sistemas de información.

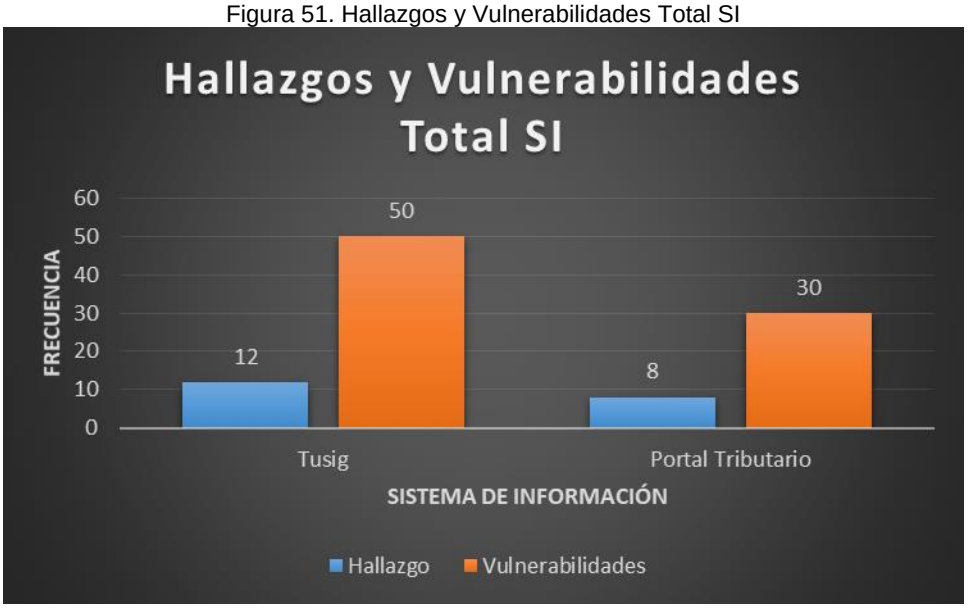
Figura 50. Hallazgos y Vulnerabilidades Puertos SI



Fuente: Autor

En la figura 51, donde se especifica los hallazgos y las vulnerabilidades para los totales en los sistemas de información.

Figura 51. Hallazgos y Vulnerabilidades Total SI



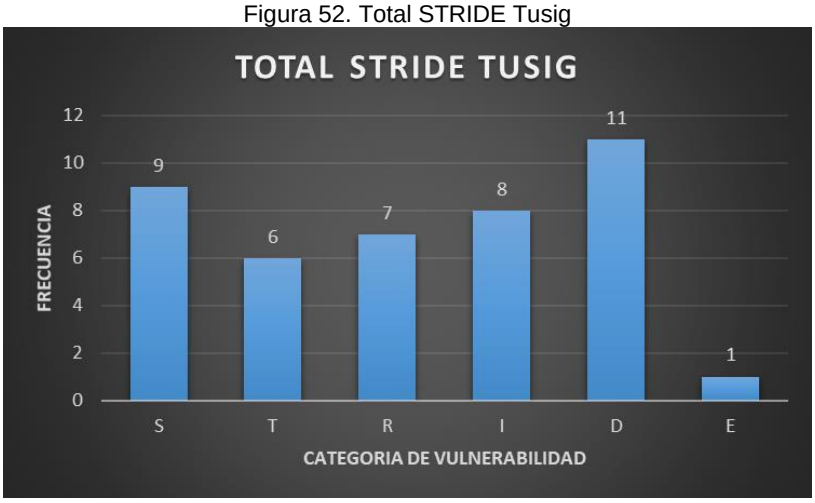
Fuente: Autor

2.3.1. Resultados Tusig.

- **Resultados Totales:**

Para los resultados totales del sistema, en términos de vulnerabilidades STRIDE, se obtuvieron a partir de la cuantificación de todos los índices, en todos los instrumentos asociados al Sistema de Información objeto de estudio, tal y como puede apreciarse en la figura 52.

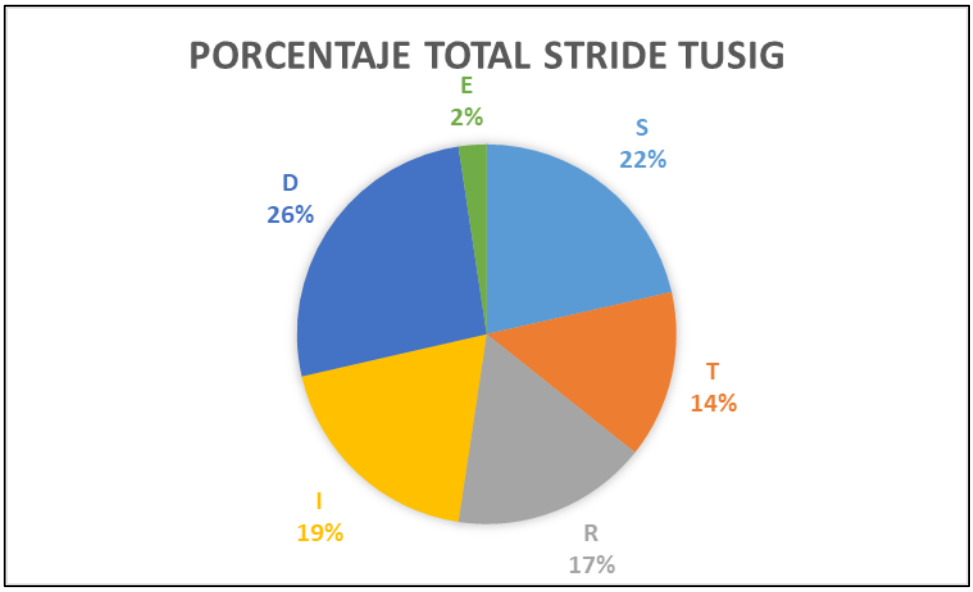
Figura 52. Total STRIDE Tusig



Fuente: Autor

En la figura 53 se muestran las incidencias porcentuales de las vulnerabilidades encontradas.

Figura 53. Porcentaje Total STRIDE Tusig

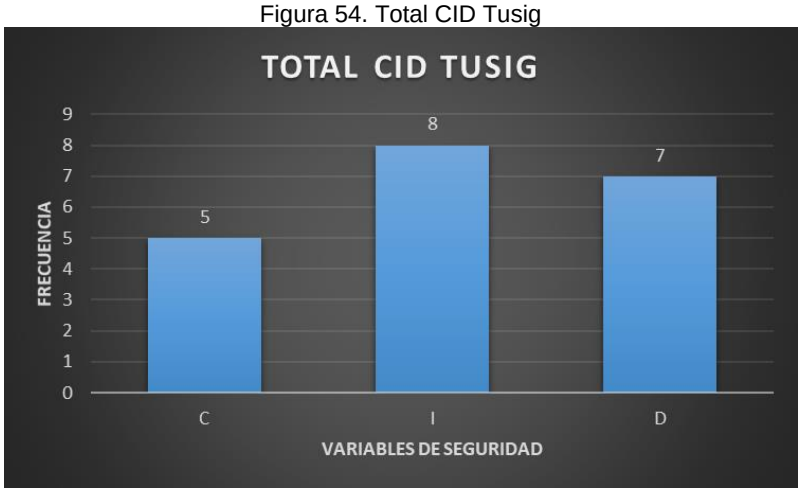


Fuente: Autor

Como puede apreciarse, para los grandes totales de las vulnerabilidades STRIDE, las mayores frecuencias están asociadas a Denial of Service (D) y a Spoofing (S) Sin embargo, los demás índices, con la excepción de Elevation of Privilege (E) se encuentran relativamente cerca a estos valores, lo cual aumenta el nivel de vulnerabilidad de la aplicación.

En cuanto a los resultados para el nivel de seguridad CID de la Alcaldía, realizando un proceso análogo al de la cuantificación del STRIDE, se obtuvieron los siguientes resultados, tal y como puede observarse en la figura 54.

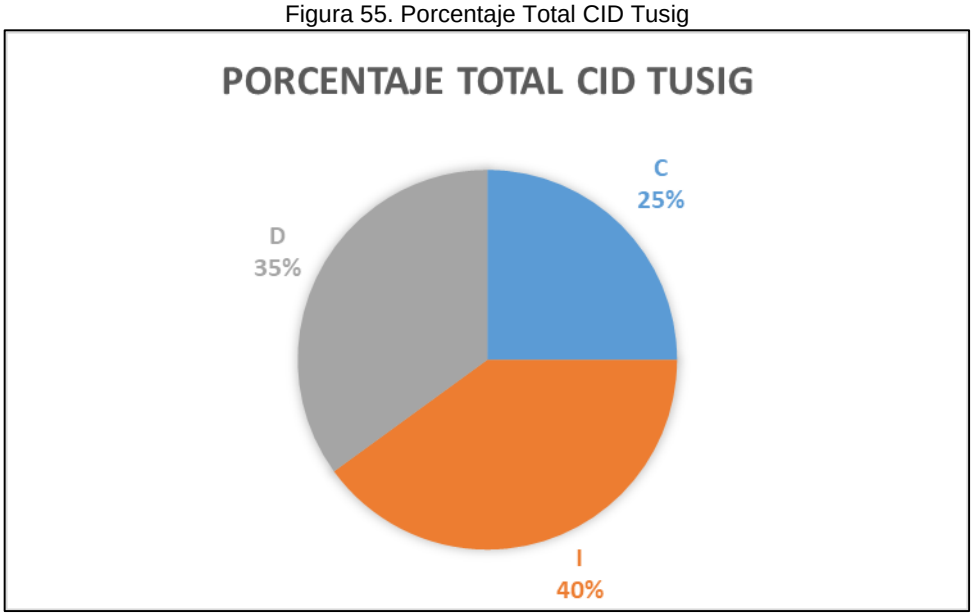
Figura 54. Total CID Tusig



Fuente: Autor

En la figura 55 se muestran las incidencias porcentuales de las vulnerabilidades encontradas

Figura 55. Porcentaje Total CID Tusig

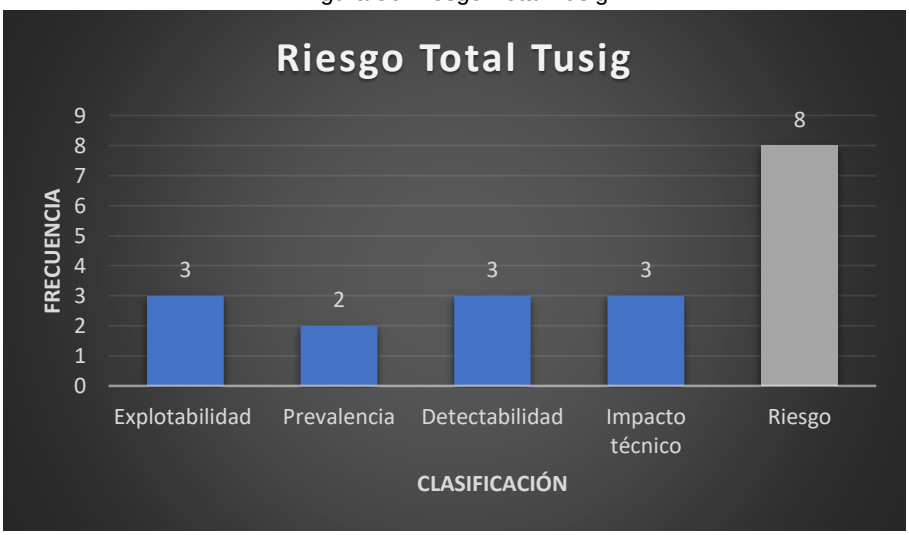


Fuente: Autor

Como es visible en las dos últimas gráficas, el porcentaje total de los niveles de seguridad, muestra una vulneración de la integridad del sistema en un 40% la más afectada.

Para la ponderación del riesgo, se tienen en cuenta las dos estructuras. Por un lado, el promedio total de los ponderados para los instrumentos, puertos y generalidades del sistema de información, ya que estos utilizan métrica OWASP para el desarrollo de sus escalas. En este orden de ideas, se muestra el promedio total en la siguiente figura:

Figura 56.Riesgo Total Tusig



Fuente: Autor

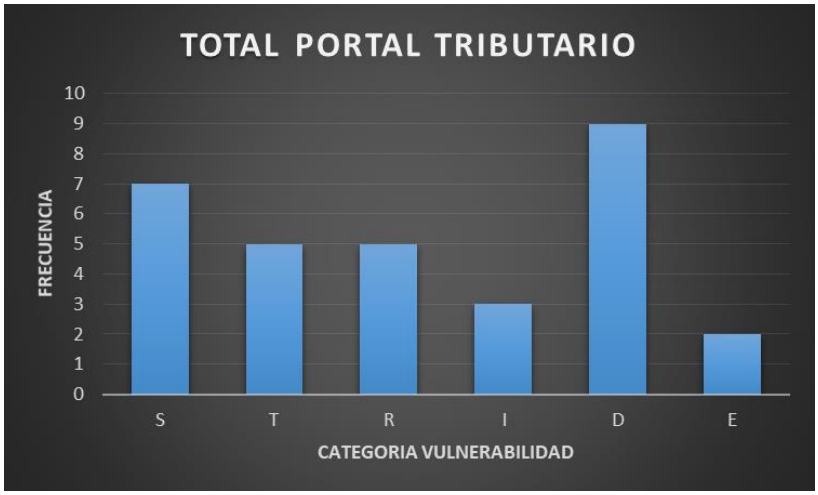
Respecto de lo anterior debe realizarse una revisión de la estructura de la red de datos, teniendo en cuenta todas las capas del modelo OSI, con el fin de poder establecer, mediante un esquema de cruce de datos, contra metodologías como NIST, los planes de acción y mejora en función de la seguridad de la información. También, deben observarse estructuras de control de flujo y tráfico de puertos, usando protocolos de monitoreo de red, como SNMP y correlacionadores de eventos, además de establecer de forma clara, las reglas del cortafuego de la institución, con el fin de optimizar los accesos.

2.3.2. Resultados Portal tributario. Para la presentación de resultados del portal tributario se sigue el mismo orden de los resultados presentados para Tusig.

Resultados Totales:

Para hacer la generalidad del STRIDE de la aplicación, se tienen los datos de la figura 57 los cuales, se muestran a continuación, teniendo en cuenta un proceso análogo de cuantificación, análogo al utilizado para Tusig.

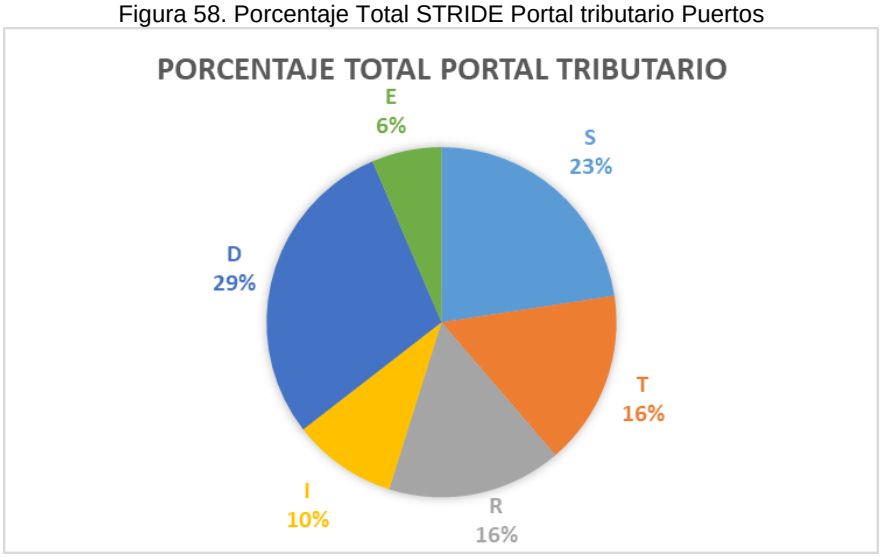
Figura 57. Total STRIDE Portal tributario Puertos



Fuente: Autor

En la figura 58 se muestran las incidencias porcentuales de las vulnerabilidades encontradas

Figura 58. Porcentaje Total STRIDE Portal tributario Puertos

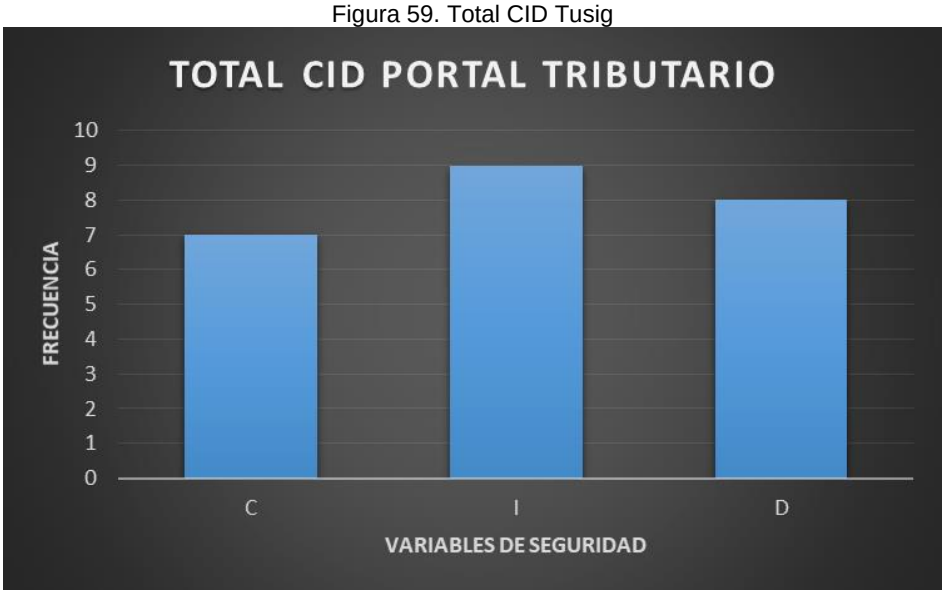


Fuente: Autor

La visión general del STRIDE muestra una inclinación hacia las denegaciones de servicio (D) ya que presenta la frecuencia más alta de todas las encontradas, y por ende una incidencia porcentual del 29% del total del análisis de vulnerabilidades, lo cual precisa de la toma de medidas para evitar caídas del sistema, como las mencionadas anteriormente en este mismo capítulo.

En cuanto a la determinación del nivel de seguridad total del Sistema de Información, los datos estadísticos pueden observarse en la figura 59.

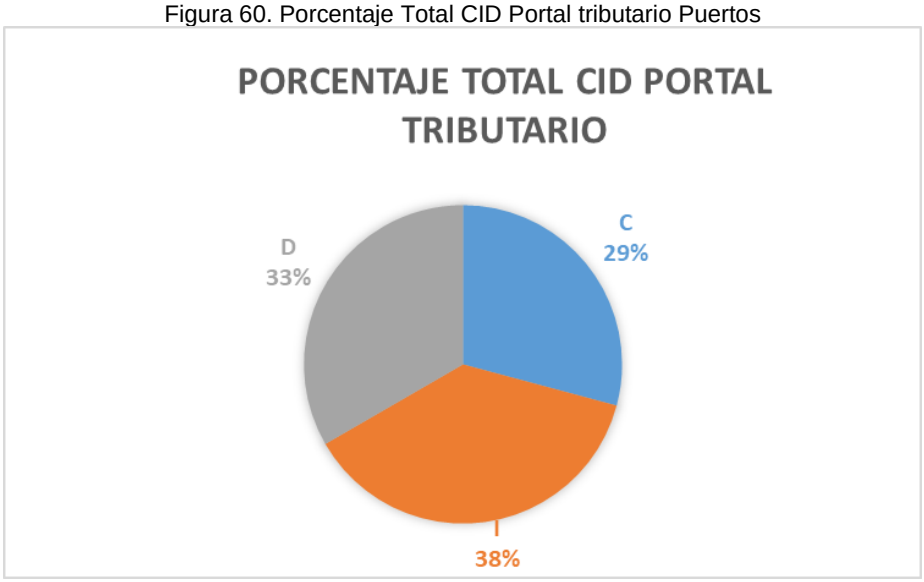
Figura 59. Total CID Tusig



Fuente: Autor

En la figura 60 se muestran las incidencias porcentuales de las vulnerabilidades encontradas.

Figura 60. Porcentaje Total CID Portal tributario Puertos

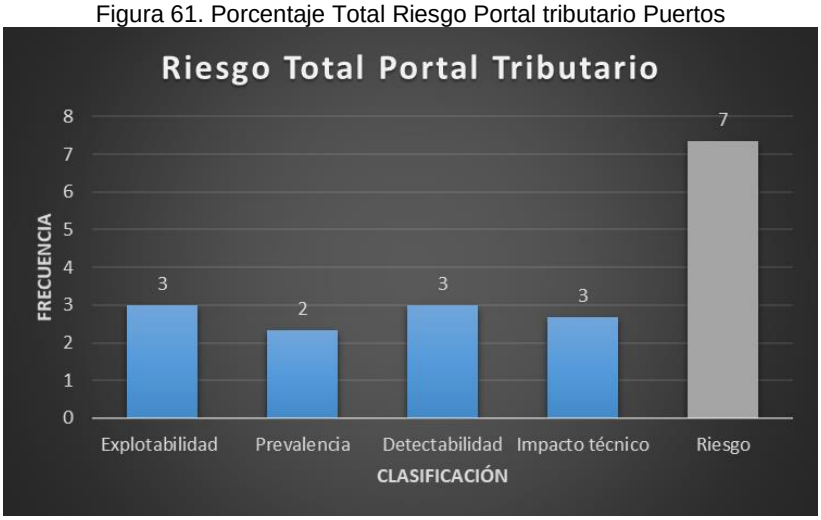


Fuente: Autor

En este punto, la recomendación es la misma, se debe reformular la seguridad de la red de comunicaciones de la Alcaldía, desde intranet e internet.

En cuanto a la ponderación del riesgo general de la aplicación, los resultados OWASP para puertos y generalidades, pueden observarse en la figura 61.

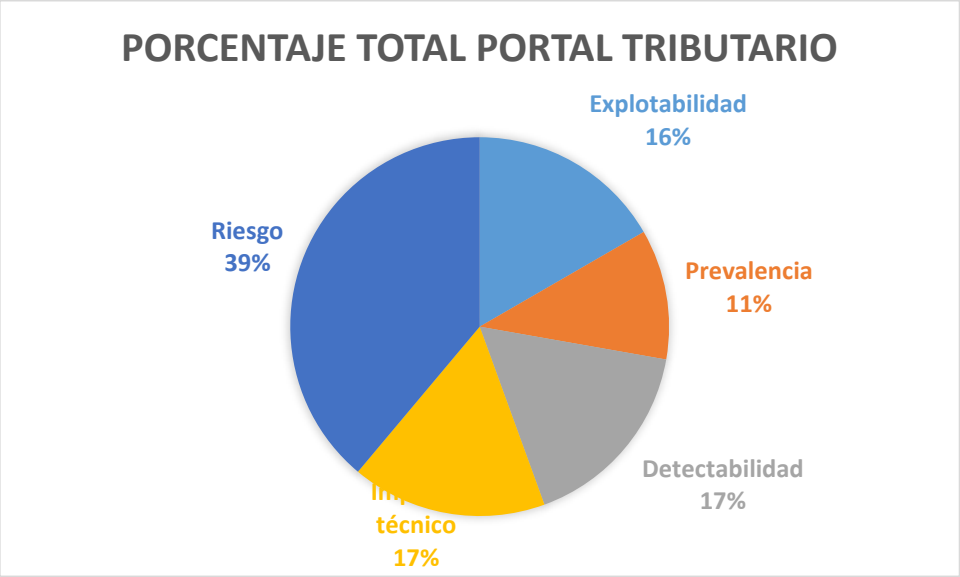
Figura 61. Porcentaje Total Riesgo Portal tributario Puertos



Fuente: Autor

En cuanto al riesgo de los componentes, definido vía CVE, se obtienen los resultados enunciados en la siguiente figura:

Figura 62. Porcentaje Total Riesgo Portal tributario Puertos



Fuente: Autor

En cuanto al riesgo total del Sistema de Información, teniendo en cuenta sus generalidades, componentes y puertos, es importante decir que es necesaria la reestructuración de la aplicación, los programas que utiliza para su funcionamiento, el hardware y demás elementos físicos del centro de datos asociados a la misma. Así mismo, debe hacerse la evaluación de políticas de acceso y monitorización de tráfico, análogamente a Tusig. Sin embargo, de forma puntual, es relevante realizar un test de penetración sobre la aplicación y una revisión del código fuente de la misma.

2.3.3. Plan de Recomendaciones. A continuación se encontraran las recomendaciones correspondientes a los resultados obtenidos del levantamiento de datos para los sistemas de información Tusig y Portal tributario.

- **Recomendaciones generales**

- Es importante realizar un proceso de reingeniería sobre las maquinas servidor y la red de comunicaciones de la Alcaldía Mayor de Tunja, más específicamente habría que hacer una revisión de los servidores de manera física y lógica, en búsqueda de posibles hallazgos que materialicen vulnerabilidades. Además, en este mismo aspecto, se deben implementar servicios SNMP (como por ejemplo Pandora FMS, Nagios, Zabbix, GroudWork, Zenoss, Monitis, Icinga, MRTG, PRTG, entre otros) para la monitorización de la red de comunicaciones y de las aplicaciones implementadas sobre los nodos terminales de datos de la entidad. Así mismo, se necesita la estructuración de

arquitecturas de control de acceso, asignación de permisos y generación de perfiles de acuerdo a normas como NIST o ISO27000, las cuales pueden sistematizarse usando por ejemplo, aplicaciones de directorios activos en los servidores Windows. Esto para suplir los hallazgos encontrados en el numeral 2.3 de este documento.

- Se recomienda la actualización de software base, incluyendo la aplicación de parches y/o reinstalación de aplicaciones para Tusig y Para el Portal, ya que en los resultados obtenidos en el numeral 2.3 se encuentran afectaciones de tipo Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service y Elevation of Privilege asociadas a versiones antiguas instaladas dentro de la entidad. Este proceso, que bien puede manejarse a través de la instalación y manejo de un servicio de actualizaciones, deberá realizarse en función de las listas de los fabricantes exclusivamente y no con base en parches de terceros, esto en función de garantizar aplicaciones sin la posibilidad de ejecutar código arbitrario embebido.

- Se recomienda la implementación de medidas preventivas, tales como, Sistemas de Detección de Intrusos, detección de intrusiones o actividad maliciosa y, en general, las consignadas en la guía de controles **NIST e ISO 27000 de manera de internacional y DAFP, MSPI** y en especial la **Guía 15 de Auditoria** de MinTIC de manera nacional, esto para tener una base documental para la aplicación de controles, que permitan mecanismos de clasificación de acceso a los archivos y sistemas de información de forma nominal, estándar, individual o de doble intervención, para ser aplicados de forma preventiva, defectiva, correctiva y disuasiva sobre el universo de la entidad.

- Se recomienda la unificación de sistemas operativos y bases de datos para los sistemas de información analizados, vía inventario de hardware y software del armario de servicios cruzado con análisis de depreciación de activos tecnológicos y ciclos de vida de las aplicaciones. Esto para favorecer la disponibilidad de los datos, el gobierno del núcleo de sistemas y mejora la aplicación de políticas de seguridad, dada una unicidad del software.

- Se recomienda actualizar e implementar las políticas de seguridad la información para la Alcaldía, según la normatividad establecida por MinTIC e ISO 27001, para así poder minimizar los riesgos dentro de la entidad en función de garantizar la confidencialidad, integridad y disponibilidad de la información. Para esto es especialmente importante, disponer y asignar a un encargado del SGSI dentro de la entidad, para el cumplimiento de requisitos legales, gestión de incidencias de seguridad e informar a los funcionarios de las novedades de seguridad con respecto a los sistemas de información (Tusig y Portal tributario para este caso) realizar capacitaciones con respecto a la seguridad de la información, y quien debería ser responsable de actualizar anualmente las políticas de seguridad, realizando la documentación de un manual de seguridad, en función de socializarlo con todos los funcionarios de la entidad y así tener un mejor funcionamiento a la hora de proteger la información.

3. CONCLUSIONES

- Dentro de la implementación de un diagnóstico de seguridad, es especialmente relevante establecer la relación de todos los agentes involucrados con el contexto de investigación (personal de la entidad, hardware, software, entre otros) con los datos e información de la entidad, teniendo en cuenta para ello los procesos de parametrización, clasificación y asignación de activos de información, dado que cualquier posible afectación en este esquema relacional puede perjudicar el funcionamiento correcto de la organización y conllevando a la posibilidad de generar costos económicos considerables.

- La utilización de métricas de parametrización de seguridad para las entidades y organizaciones son importantes, debido a que estas deben tener directrices de seguridad claras respecto al manejo de sus activos de información, en función de la integridad, disponibilidad y confidencialidad de los datos que manejan, a las vulnerabilidades a las que están sujetas en términos de la seguridad de la información y a las mejores prácticas que se puedan generar, para lograr una implementación segura en términos de factor humano, hardware y software logrando una solución que satisfaga las necesidades de la entidad.

- La implementación y aplicación de instrumentos de medición, que permitan recopilar datos en crudo de un entorno de investigación, resulta ser una medida notable dentro del desarrollo de esta clase de trabajos, ya que, por una parte ofrece documentos tangibles, con información histórica de la organización, que pueden ser analizados desde el punto de vista ingenieril a través del uso de herramientas de estadística descriptiva (como es este caso) y por otro lado permiten ofrecer una fuente de evidencias del trabajo, en procesos propios de una determinada institución, como lo es un análisis de vulnerabilidades sobre dos servicios en la Alcaldía Mayor de Tunja.

- Gracias a La aplicación de documentación propia de MinTIC (MSPI) para manejo de riesgos y auditoría de sistemas y metodologías de vulnerabilidades como STRIDE, fue posible observar la existencia de evidencias de riesgo informático, dentro de los sistemas de información Tusig y Portal Tributario de la Alcaldía Mayor de Tunja, teniendo como variables de medición, la Integridad, Disponibilidad y Confidencialidad de los datos, parámetros adoptados por las directivas nacionales, como fuentes de medición en un análisis de seguridad informática, debido a su validación en este trabajo, desde un punto de vista científico, usando un cruce de fuentes de datos utilizadas (CVE/NVD) para los datos de entrada a los instrumentos, con los procedimientos mencionados al comienzo de este párrafo.

- Se debe crear conciencia de la importancia de la aplicación de mediciones de seguridad en cualquier tipo de organización, teniendo en cuenta los aspectos mencionados en este trabajo. Ya que es una opción de poder definir un nivel de afectación dentro de la entidad, y por ende, sirve de trabajo base para la implantación de contramedidas en el

entorno de trabajo, disminuyendo la brecha de riesgo al interior de la organización, propendiendo por salvaguardar los datos de los usuarios y logrando crear responsabilidad social sobre el manejo seguro de la información que se brinda, circula y se entrega en un proceso empresarial.

- Los procesos de evaluación de seguridad informática, dentro de una organización, deben ser entendidos desde varios puntos de vista, no solamente desde el código fuente que se utiliza en una aplicación; ya que existen elementos asociados a la dinámica del servicio (Redes de comunicaciones, Hardware de Servidores, políticas de acceso de la entidad….) que intervienen en la evaluación y obtención de resultados, alterando las mediciones correspondientes. Es así, que debería favorecerse una integración de conocimientos, con el fin de lograr resultados, más fieles a la realidad y que toquen al sistema como un todo, dentro del ámbito organizacional objeto de estudio.

2. INFOGRAFÍA Y BIBLIOGRAFÍA

OWASP. 2001. OWASP. *OWASP.* [En línea] 1 de Diciembre de 2001. https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.

Advisera. Advisera. *Advisera.* [En línea] https://advisera.com/27001academy/es/que-es-iso-27001/.

Aguilera López, Purificación . 2010. *Seguridad informática.* s.l. : EDITEX, 2010.

Angelfire. 2016. Angelfire. *Angelfire.* [En línea] 2016. http://www.angelfire.com/droid/irra_b/html/exploit.htm.

Baca Urbina, Gabriel . 2016. *Introducción a la seguridad informática.* s.l. : Grupo Editorial Patria, 2016.

Bishop, Matt. 2005. *Introduction to Computer Security.* s.l. : Addison-Wesley Professional, 2005.

Blog especializado en Sistemas de Gestión . 2017. SGSI Blog especializado en Sistemas de Gestión . [En línea] 06 de Julio de 2017. https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/.

Borghello, Cristian. 2000 - 2009. Seguridad de la Informacion. *segu-info.* [En línea] 2000 - 2009. https://www.segu-info.com.ar/malware/exploit.htm.

—. 2000 - 2009. Seguridad de la Informacion. *segu-info.* [En línea] 2000 - 2009. https://www.segu-info.com.ar/ataques/ataques_modificacion.htm.

Conpes 3701 de 2011. 2011. Conpes 3701 de 2011. [En línea] 14 de Julio de 2011. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

Costas Santos, Jesús . 2014. *Seguridad informática.* s.l. : RA-MA Editorial, 2014.

CVE. 1999 - 2005. CVE Common Vulnerabilities and Exposures. *CVE Common Vulnerabilities and Exposures.* [En línea] 1999 - 2005. https://cve.mitre.org/index.html.

Decreto 1078 de 2015. 2015. Decreto 1078 de 2015. *Decreto 1078 de 2015.* Bogota : s.n., 2015.

Decreto 1499 de 2017. 2017. Decreto 1499 de 2017. *Decreto 1499 de 2017.* Bogota : República de Colombia, 2017.

Díaz, Gabriel , Mur, Francisco y Sancristóbal, Elio . 2004. *Seguridad en las comunicaciones y en la información.* s.l. : UNED - Universidad Nacional de Educación a Distancia, 2004.

Escrivá Gascó, Gema, Romero Serrano, Rosa María y Ramada, David Jorge. 2013. *Seguridad informática.* s.l. : Macmillan Iberia, S.A, 2013.

FIRST.org. 2018. FIRST.org. *FIRST.org.* [En línea] 2018. https://www.first.org/cvss/v2/guide#2-1-Base-Metrics.

Garcia, Carlos . 2018. Hacking Etico. *Hacking Etico.* [En línea] 17 de Enero de 2018. https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/.

Gómez Fernández , Luis y Andrés Álvarez, Ana . 2012. *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* s.l. : AENOR - Asociación Española de Normalización y Certificación, 2012.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). 2006. Norma Técnica Colombiana NTC-ISO/IEC 27001. *Norma Técnica Colombiana NTC-ISO/IEC 27001.* Bogota, Colombia : ICONTEC, 2006.

ISO27000. 2006. ISO27000. *Articulo.* s.l. : ISO, 2006.

ISOTools. 2018. ISOTools. *ISOTools.* [En línea] 2018. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001.

—. 2015. ISOTools. *ISOTools.* [En línea] 20 de Febrero de 2015. https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/.

LEY 1273 DE 2009. 2009. LEY 1273 DE 2009. *LEY 1273 DE 2009.* Bogota : República de Colombia, 2009.

Ley 1712 de 2014. 2014. Ley 1712 de 2014. *Ley 1712 de 2014.* Bogoota : República de Colombia, 2014.

Luz, Sergio De. 2010. redeszone. *redeszone.* [En línea] 03 de Noviembre de 2010. https://www.redeszone.net/2010/11/03/ataques-a-las-redes-listado-de-diferentes-ataques-a-las-redes-de-ordenadores/.

Microsoft. 2009. Microsoft. *Microsoft.* [En línea] 11 de Diciembre de 2009. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20).

Ministerio de Tecnologías de la Información y las Comunicaciones Colombia. Manual Gobierno en línea. Bogota : Ministerio de Tecnologías de la Información y las Comunicaciones .

—. Modelo de Seguridad y Privacidad de la Información. *Ministerio de Tecnologías de la Información y las Comunicaciones.* Bogota : Ministerio de Tecnologías de la Información y las Comunicaciones.

Ministerio de Tecnologías de la Información y las Comunicaciones. 2011. Ministerio de Tecnologías de la Información y las Comunicaciones. *Ministerio de Tecnologías de la Información y las Comunicaciones.* [En línea] 2011. http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

MinTIC. 2016. Ministerio de Tecnologías de la Información y las Comunicaciones. *Ministerio de Tecnologías de la Información y las Comunicaciones.* [En línea] 29 de Julio de 2016.

http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

NIST. 2015. National Institute of Standards and Technology. *National Institute of Standards and Technology.* [En línea] 2015. https://www.nist.gov/.

OWASP. 2018. OWASP. *OWASP.* [En línea] 22 de Enero de 2018. https://www.owasp.org/index.php/Threat_Risk_Modeling#STRIDE.

—. 2015. OWASP. *OWASP.* [En línea] 31 de Agosto de 2015. https://www.owasp.org/index.php/Man-in-the-middle_attack.

—. 2018. OWASP. *OWASP.* [En línea] 6 de Marzo de 2018. https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).

—. 2016. OWASP. *OWASP.* [En línea] 7 de Agosto de 2016. https://www.owasp.org/index.php/Command_Injection.

—. 2015. OWASP. *OWASP .* [En línea] 30 de Julio de 2015. https://www.owasp.org/index.php/Inyecci%C3%B3n_de_C%C3%B3digo.

—. 2014. OWASP. *OWASP.* [En línea] 03 de Septiembre de 2014. https://www.owasp.org/index.php/Buffer_overflow_attack.

Pérez, Ignacio. 2014. welivesecurity. *welivesecurity.* [En línea] 05 de Noviembre de 2014. https://www.welivesecurity.com/la-es/2014/11/05/como-funcionan-buffer-overflow/.

Raphaël RAULT, Laurent SCHALKWIJK, ACISSI, Marion AGÉ, Nicolas CROCFER, Robert CROCFER, David DUMAS, Franck EBEL, Guillaume FORTUNATO, Jérôme HENNECART, Sébastien LASSON. 2015. *Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa.* Barcelona : Ediciones ENI, 2015. 3ª edición.

Roa Buendía, José Fabián. 2013. *Seguridad informática.* s.l. : McGraw-Hill España, 2013.

Universidad Nacional Autónoma De México. 2015. Concepto de Criptografía. 2015.