EVALUACIÓN DEL NIVEL DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN PARA LAS SECRETARIAS DE PLANEACIÓN E INFRAESTRUCTURA DE LA ALCALDÍA DE TUNJA A TRAVÉS DE LA METODOLOGÍA STRIDE / DREAD.

PROPONENTE

JUAN SEBASTIAN QUINTANA CARBONELL

TRABAJO DE GRADO

UNIVERSIDAD SANTO TOMAS TUNJA

INGENIERIA DE SISTEMAS

2018

EVALUACIÓN DEL NIVEL DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN PARA LAS SECRETARIAS DE PLANEACIÓN E INFRAESTRUCTURA DE LA ALCALDÍA DE TUNJA A TRAVÉS DE LA METODOLOGÍA STRIDE / DREAD.

PROPONENTE

JUAN SEBASTIAN QUINTANA CARBONELL

CODIGO: 2103589

TUTOR:

INGENIERO IVAN FERNANDO LEAL RAMIREZ

TRABAJO DE GRADO

UNIVERSIDAD SANTO TOMAS TUNJA

INGENIERIA DE SISTEMAS

2018

AGRADECIMIENTOS

Agradezco a la Universidad Santo Tonás por abrirme las puertas en mi carrera profesional y guiarme en mi camino de una manera ética y moral, con un nivel de educación impecable, a todos los ingenieros que en mis años de estudio me ofrecieron sus conocimientos para llegar a una meta como ser Ingeniero de sistemas, a la alcaldía de Tunja por apoyar este proyecto y darme la confianza de realizarlo y medir mis capacidades, el ingeniero Alex Puertas Gonzales por tener la paciencia suficiente en este proyecto y siempre estar disponible para el apoyo que necesite, dándome sus mejores conocimientos y tiempo además de ser una persona tan paciente y siempre amable mostrando el complemento de un gran profesional, a todas las personas y amigos que me colaboraron siempre lo llevare en mi corazón, mil gracias, Dios los Bendiga, un abrazo fraterno.

Juan Sebastián Quintana Carbonell

DEDICATORIA

Primeramente a Dios por brindarme su bondad y sabiduría en estos años de formación, a mis amados y queridos Padres que lo dieron todo por verme aquí, sus esfuerzos y días difíciles ya han acabado, por ser ese apoyo incondicional que se lo sabre retribuir de mil maneras mis viejos, a mi hermana que con su apoyo aporto por este proyecto de mi vida, y a mis dos motores Martin y Thiago mis hijos , que siempre que caia el solo pensar en ellos me llenaron de fuerza y amor para seguir, Mis sobrinas que son como mis hermanas y estuvieron en todo mi proceso, a todos ellos gracias enormes por ser mi familia mi motivación.

A compañeros y amigos que siempre estuvieron a mi lado en este proceso también hay un espacio para ellos aquí, pues fueron apoyos que en su momento me llenaron de satisfacción y agrado, eternamente agradecidos y siempre estarán en mi corazón hermanos

Juan Sebastián Quintana Carbonell

.

CONTENIDO

1. ASPECTOS GENERALES

1.1 TITULO TRABAJO DE GRADO

- Evaluación del nivel del riesgo en seguridad de la información para las secretarias de planeación e infraestructura de la alcaldía de Tunja a través de la metodología STRIDE / DREAD.

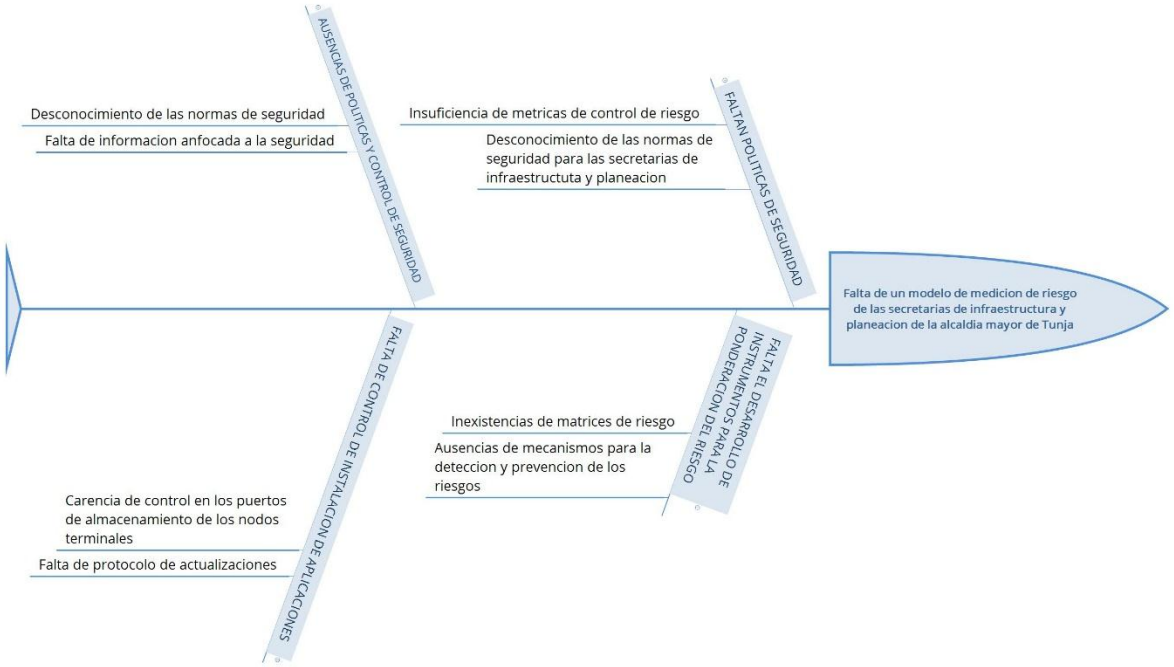
1.2 PLANTEAMIENTO DEL PROBLEMA

La información es lo más importante que tiene cualquier entidad y mucho más si es una entidad gubernamental como lo es la alcaldía de Tunja, que maneja su información en su gran mayoría de manera digital.

Esta información es de vital importancia debido a sus procesos en la alcaldía, es fundamental que esta información permanezca segura, prestando sus servicios correspondientes con las mejores medidas de seguridad. La información diariamente se encuentra expuesta a riesgos desde el momento en que se maneja hasta cuando esta almacenada, esto puede causar en la información diferentes situaciones tales como robo de la información , que seria algo que no se quiere, daño a la información, manejo no autorizado de la información y ataques informáticos.

Para evitar cualquier tipo de estas situaciones, se deben implementar controles y políticas de seguridad, que permitan lograr la prevención, detección y corrección de cualquier problema, con el objetivo de mantener la información segura.

Figura 1 Diagrama espina de pescado



Fuente : autor

1.3 ALCANCES

Para el presente trabajo se tendrán en cuenta los siguientes alcances:

- Se determinará mediante el modelo STRIDE las vulnerabilidades de los computadores de la secretaria de infraestructura y planeación se excluye las acciones correctivas.
- Se evaluará mediante el modelo DREAD el riesgo de las vulnerabilidades encontradas a través de la implementación de matrices relativas en los computadores de comunicación de la secretaria de infraestructura y planeación.
- Se realizará el diagnostico de riesgo en seguridad de la información de las secretarias de infraestructura y planeación de la alcaldía de Tunja basado en las metodología DREAD

1.4 JUSTIFICACIÓN

Buscando Soluciones ingenieriles que satisfagan la problemática actual de la secretaria de planeación e infraestructura de la alcaldía de Tunja, se determinan Proyectos de Seguridad de la información los cuales a través de procesos de ingeniería buscan fundamentar las propuestas a presentar y mejorar los procesos actuales de dicha entidad.

La Seguridad de la información para una entidad como la alcaldía de Tunja se convierte en un requisito de vital importancia, tener la información segura en una entidad tan importante es fundamental; luego de saber que actualmente no se manejan ningún requisito de seguridad de la información donde se evidencia la necesidad urgente de mejorar a partir de un diagnóstico de seguridad actual y a partir de este brindar soluciones a los posibles problemas encontrados, por lo cual se toma la decisión de realizar este proyecto.

1.5 OBJETIVOS

1.5.1 Objetivo General

Implementar el modelo STRIDE / DREAD para los computadores de la secretaria de infraestructura y planeación de la alcaldía de Tunja con el fin de determinar su nivel de riesgo respecto de la seguridad de la información.

1.5.2 Objetivos específicos

- Determinar mediante el modelo STRIDE las vulnerabilidades de los computadores de comunicaciones de la secretaria de infraestructura y planeación
- Evaluar, mediante la metodología DREAD, el nivel de riesgo de las vulnerabilidades encontradas a través de la implementación de matrices relativas al tema.

- Realizar el diagnóstico de riesgo en seguridad de la información de las secretarias de infraestructura y planeación de la ciudad de Tunja, basado en las metodologías STRIDE / DREAD

1.6 MARCO REFERENCIAL

En el siguiente marco referencial se encontrará el marco teórico del trabajo realizado en donde se caracterizará la terminología utilizada para el desarrollo del trabajo, metodologías utilizadas directamente, para una mejor compresión del proyecto.

1.6.1 Marco teórico

En el marco teórico se definieron las terminologías utilizadas para contextualizar el proyecto investigado, antecedentes científicos que nos ayudan a tener un mejor resultado en el proyecto.

1.6.1.1 Metodología DREAD. Es un esquema de clasificación para cuantificar, comparar, y priorizar la cantidad del riesgo presentado por cada amenaza evaluada, el acrónimo DREAD se forma a partir de la primera letra de cada categoría a continuación **(OWASP, 2017)**

El valor del riesgo se calcula por la fórmula: Riesgo-DREAD = (Daño-potencial + Reproducibilidad + Explotabilidad + Usuarios afectados + Descubribilidad) / 5. **(Bertolín, 2012)**)

- **Damage potencial (Daño potencial):** ¿Cuál es el daño que puede originar la vulnerabilidad si llega a ser explotada?
- **Reproducibility (reproducibilidad):** ¿Es fácil reproducir las condiciones que propicien el ataque?
- **Explotability (Explotabilidad):** ¿Es sencillo llevar acabo el ataque?
- **Affected uses (Usuarios afectados)** ¿Cuántos usuarios se verían afectados?
- **Discoverability (Descubrimiento)** ¿Es fácil encontrar la vulnerabilidad? **(Barbara Olivares**)

1.6.1.2 Metodología STRIDE. Es un esquema de clasificación para caracterizar amenazas conocidas según los tipos de ataques, el acrónimo STRIDE se forma a partir de la primera letra de cada una de las siguientes categorías: **(Microsoft, 2009) (OWASP, 2017)**

Spoofing Identity (Suplantación de identidad): Esta categoría de amenazas indica básicamente que los usuarios no deberían ser capaces de hacerse pasar por otros usuarios. Es importante enfocarse en un adecuado sistema de autenticación y poner mucha atención en los temas de uso de sesión con el fin de evitar robos por medio del uso de éstas. **(Barbara Olivares)**

Tampering with Data (Manipulación de datos): Por la llegada de metodologías de desarrollo de software ágiles, es habitual que con el fin de cumplir con los tiempos se sacrifique la implementación de las medidas de seguridad Una de las primeras medidas preventivas que se suelen sacrificar, es el filtrado y la validación de los datos enviados y recibidos de los usuarios de la aplicación. En el caso específico de las aplicaciones desarrolladas para un entorno web, se puede dar a manera de ejemplo, las vulnerabilidades conocidas, tales como la inyección de sentencias SQL o el XSS; en general, en aquellos casos en los que las aplicaciones proporcionan al usuario, datos que no son obtenidos directamente de la propia aplicación, se realiza algún tipo de cálculo con ellos y posteriormente se almacenan, teniendo en cuenta que estos datos pueden ser susceptibles de una manipulación efectuada por un usuario malintencionado que disponga de las herramientas adecuadas. **(Barbara Olivares)**

Repudiation (Repudio): En esta categoría, se trata de establecer un nivel adecuado del seguimiento de las acciones realizadas por los usuarios de la aplicación; con el fin de evitar que aparezcan situaciones no deseadas se debe intentar garantizar él no repudio de los usuarios. Cada aplicación sobre la base de su funcionalidad, características y entorno, presenta diferentes riesgos y por lo tanto, las medidas de registro de las actividades que son efectuadas sobre los usuarios serán también diferentes… **(Barbara Olivares)**

Information Disclosure (Revelación de información): La existencia de vulnerabilidades en una aplicación que permitan extraer información sensible, es un factor claro de riesgo que en ocasiones puede derivar en pérdidas económicas, así como también, en la disminución de la confianza y reputación de cara a posibles o ya existentes usuarios, clientes, proveedores o inversores. **(Barbara Olivares)**

Denial of Service (Denegación de servicio): A la hora de diseñar una aplicación, o en el momento de añadir una nueva funcionalidad, es conveniente evitar aquellas situaciones que puedan devengar en la consecución de un ataque de denegación de servicio. **(Barbara Olivares)**

Elevation of Privilege (Elevación de privilegios): En el caso de que la aplicación o el sistema proporcionen diferentes niveles de privilegio en función de los distintos tipos de usuarios, todas las acciones que lleven al uso de privilegios deben ser filtradas a través de un mecanismo adecuado de autorización. Este método de validación de los privilegios deberá ser suficientemente robusto para impedir un posible escalamiento de privilegios. **(Barbara Olivares).**

1.6.1.3 Seguridad informática. La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y, que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de sus límites de su autorización **(DGTIC, direccion general de tecnologias de la informacion y comunicaciones , s.f., pág. 30)**

1.6.1.4 Vulnerabilidad. La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. **(protejete.wordpress., 2014)**

1.6.1.5 Amenaza. Una amenaza es una posible violación de la seguridad. La violación no necesita ocurrir realmente para una amenaza El hecho de que la violación pueda ocurrir significa que esas acciones que podría causar que ocurra debe ser protegido contra (o preparado para). Esas acciones se llaman ataques. Aquellos que ejecutan tales acciones, o hacen que sean ejecutados, son llamados atacantes.

Los tres servicios de seguridad-confidencialidad, integridad y disponibilidad- contra amenazas a la seguridad de un sistema. Se divide las amenazas en cuatro clases amplias: divulgación, o acceso no autorizado a la información; engaño o aceptación de datos falsos; interrupción, o interrupción o prevención del correcto funcionamiento; y usurpación, o control no autorizado de alguna parte de un sistema. Estos cuatro las clases amplias abarcan muchas amenazas comunes. Debido a que las amenazas son omnipresentes, una discusión introductoria de cada uno presentará temas que se repiten a lo largo del estudio de seguridad informática **(Bishop, Introduction to Computer Security, 2005)**

1.6.1.6 Riesgo. Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. **(Tarazona, 2007)**

1.6.1.7 Integridad. La integridad se refiere a la confiabilidad de los datos o recursos, y por lo general se expresa en términos de prevención de cambios indebidos o no autorizados La integridad incluye la integridad de los datos (el contenido de la información) y la integridad del origen (la fuente de los datos, a menudo llamada autenticación). La fuente de la información puede influir en su precisión y credibilidad y sobre la confianza que las personas depositan en la información. Esta dicotomía ilustra el principio de que el aspecto de integridad conocido como credibilidad es fundamental para el adecuado funcionamiento de un sistema. Volveremos a este tema cuando analicemos la lógica maliciosa**. (Bishop, Introducction to computer segurity, 2005)**

Los mecanismos de integridad se dividen en dos clases: mecanismos de prevención y detección mecanismos. 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 distinción entre estos dos tipos de intentos es importante. Lo primero ocurre cuando un usuario intenta cambiar datos a los que no tiene autoridad para cambio. Esto último ocurre cuando un usuario autoriza realizar ciertos cambios en los datos intenta cambiar los datos de otras maneras. Por ejemplo, supongamos que un sistema de contabilidad es en una computadora. Alguien irrumpe en el sistema e intenta modificar la contabilidad datos. Luego, un usuario no autorizado ha intentado violar la integridad de la contabilidad base de datos. Pero si un contador contratado por la empresa para mantener sus libros intenta malversar dinero enviándolo al extranjero y ocultando las transacciones, un usuario (el contador) ha intentado cambiar los datos (los datos contables) de forma no autorizada (moviéndolo a una cuenta bancaria suiza). La autenticación adecuada y los controles de acceso

generalmente detener el asalto desde el exterior, pero prevenir el segundo tipo de intento requiere controles muy diferentes **(Bishop, Introducction to computer segurity, 2005)**

1.6.1.8 Confidencialidad*.* La confidencialidad es la ocultación de información o recursos. La necesidad de mantener secreto de información surge del uso de computadoras en campos sensibles como el gobierno e industria.

Los mecanismos de control de acceso respaldan la confidencialidad. Un mecanismo de control de acceso para preservar la confidencialidad es la criptografía, que codifica los datos para que sea incomprensible. Una clave criptográfica controla el acceso a los datos no codificados, pero entonces la clave criptográfica en sí misma se convierte en otro dato a proteger. **(Bishop, Introducction to computer segurity, 2005)**

1.6.1.9 Disponibilidad. La disponibilidad se refiere a la capacidad de usar la información o el recurso deseado. Disponibilidad es un aspecto importante de la fiabilidad, así como del diseño del sistema porque el sistema no disponible es al menos tan malo como ningún sistema en absoluto. El aspecto de la disponibilidad que es relevante para la seguridad es que alguien puede deliberadamente organizar denegar el acceso a datos o a un servicio haciendo que no esté disponible. Los diseños del sistema suelen suponer una estadística modelo para analizar los patrones de uso esperados y los mecanismos aseguran la disponibilidad cuando ese modelo estadístico se cumple. Alguien puede ser capaz de manipular el uso (parámetros que controlan el uso, como el tráfico de red) para que las suposiciones de la modelo estadístico ya no es válido. Esto significa que los mecanismos para mantener el recurso o datos disponibles están trabajando en un entorno para el que no estaban diseñado. Como resultado, a menudo fallan**. (Bishop, Introducction to computer segurity, 2005)**

1.6.1.10 Modelo de seguridad y privacidad de la información (MSPI). El “Instrumento de Evaluación MSPI” Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”. Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre sin fines lucrativos, por esta razón se prohíbe la comercialización y explotación de la misma. **(MINTIC, 2017)**

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. **(MINTIC, 2017)**

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información. **(MINTIC, 2017)**

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano. **(MINTIC, 2017)**

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad,

procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos. **(MINTIC, 2017).**

1.6.1.11 Everest ultímate

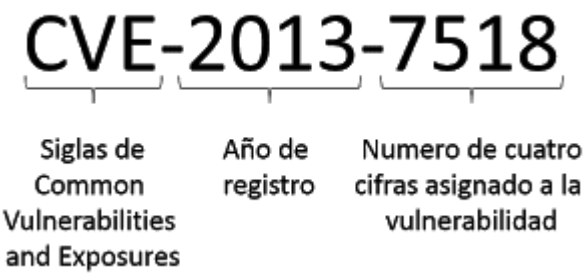
Everest Ultimate Edition es una herramienta que encontrará problemas de configuración en tu sistema, mostrará cada detalle de todos tus componentes hardware e información acerca del software que tengas instalado.

Desarrollado en una interfaz muy sencilla de usar, Everest Ultimate se convertirá en tu aliado para conocer todos los datos sobre los elementos de tu ordenador y sus características.El programa incluye un área de diagnósticos y puede elaborar informes sobre tu sistema. **(uptodown, 2008)**.

1.6.1.12 CVE Common Vulnerabilities and Exposures

CVE (Common Vulnerabilities and Exposures) es una lista de vulnerabilidades de seguridad de la información públicamente conocidas. Es quizás el estándar más usado. Permite identificar cada vulnerabilidad, asignando a cada una un código de identificación único. Se conoce como identificador CVE (CVE-ID) y está formado por las siglas de este diccionario seguidas por el año en que es registrada la vulnerabilidad o exposición y un número arbitrario de cuatro dígitos. Estos tres elementos van separados por un guion resultando un identificador con el siguiente formato: **(Eleven Patchs, 2014)**

Figura 2identificador de la vulnerabilidad



Fuente: Eleven patchs

Ventajas del CVE:

La utilidad de este catálogo es múltiple:

- Permite tener una base para la evaluación de las vulnerabilidades.
- Es un estándar muy adoptado para referirse a ellas. En la mayoría de las ocasiones, la asignación de un CVE permite diferenciar vulnerabilidades que, de otra forma, resultarían muy complejas de describir y diferenciar desde un punto de vista técnico.
- Realiza un proceso de actualización continua de las vulnerabilidades registradas en la lista.
- La posibilidad de monitorizar cambios o actualizaciones sobre la lista y los contenidos de las vulnerabilidades.
- Una revisión exhaustiva de las nuevas vulnerabilidades que podrán ser registradas en el diccionario. **(Eleven Patchs, 2014)**

2. DESARROLLO Y RESULTADOS

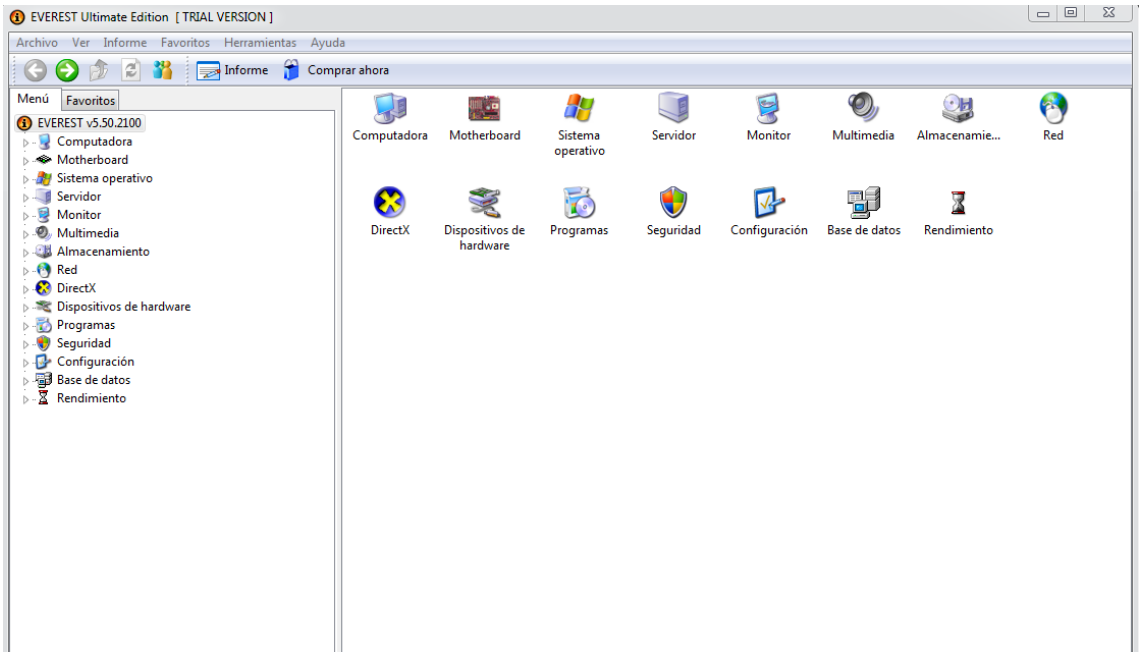
2.1 Desarrollo

A Continuación se explicara los pasos realizados para el desarrollo del proyecto, donde se especifican las tareas realizadas para la obtención de los resultados finales.

2.1.1 Extracción de datos en los computadores de las secretarias de infraestructura y planeación de la alcaldía de Tunja.

Para la obtención de los datos de los computadores fue necesario el uso de la herramienta Everest (demo), se llevó acabo la extracción de las aplicaciones instaladas, drivers utilizados, y sistema operativo de cada computador. Esta información recaudada es la base para la elaboración de las hojas de vida de los computadores y su respectiva caracterización.

Figura 3.Plataforma Everest



FUENTE AUTOR

2.1.2 Generación de reportes

Los archivos generados Everest (Demo) tienen una extensión .txt con la información de los computadores de las secretarias de planeación e infraestructura, en el cual se debe hacer la exportación al Excel donde se realiza las hojas de vida de los computadores.

2.1.3 Elaboración de las hojas de vida

Luego de tener los datos recolectados y agrupados por pc, procedemos a realizar las hojas de vida de cada computador, donde encontraremos: Fecha de evaluación, Elaborado por, nombre del equipo, Dirección Mac, Id Pc, aplicaciones, Origen APL, tipo de ataque, factor de riego, tipo de Riesgo, Impacto, Probabilidad, Zona de riesgo, CVE.

Figura 4 Hoja de vida computadores

	Matrices de seguridad Alcaldía Mayor de Tunja							
FECHAS DE EVALUACIÓN	28/10/2016							
ELABORADO POR	SEBASTIAN QUINTANA							
NOMBRE DEL EQUIPO	NERSA							
MAC	40-A8-F0-A8-A8-3C							
ID PC	PC1							
APLICACIONES	ORIGEN APL	TIPO DE ATAQUE	FACTOR RIESGO	TIPO DE RIESGO	IMPACTO	PROBABILIDAD	ZONA DE RIESGO	CVE
360 Total Security	360 Total Security es una aplicacion que no pertenece al SO	buffer overflow	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	2,5	20%	M	CVE-2017-8776 CVE-2017-8775 CVE-2017-8774
Archiv [TRIAL VERSION]	Archiv es una aplicacion que no pertenece al SO	cross-site scripting (XSS	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	1,5	43%	A	CVE-2008-0464
	AutoCA [TRIAL VERSION] es una aplicacion que no pertenece al SO	buffer overflow	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	4,9	20%	E	CVE-2018-1000042

Fuente autor

2.1.4 Hallazgo de las vulnerabilidades mediante CVE

A partir de obtener la información de los computadores y tener las hojas de vida establecidas procedemos a realizar el análisis de las vulnerabilidades mediante el CVE como se evidencia en la figura 4, encontrando las vulnerabilidades de las aplicaciones, Drivers y sistemas operativos de cada computador, extrayendo el Id de la vulnerabilidad y dejándola en la hoja de vida como se muestra en la Figura 5.

Figura 5 Plataforma CVE

Vuln ID	Summary	CVSS Severity
CVE-2018-5165	In 32-bit versions of Firefox, the Adobe Flash plugin setting for "Enable Adobe Flash protected mode" is unchecked by default even though the Adobe Flash sandbox is actually enabled. The displayed state is the reverse of the true setting, resulting in user confusion. This could cause users to select this setting intending to activate it and inadvertently turn protections off. This vulnerability affects Firefox < 60. **Published:** June 11, 2018; 05:29:15 PM -04:00	(not available)
CVE-2016-10603	air-sdk is a NPM wrapper for the Adobe AIR SDK. air-sdk downloads binary resources over HTTP, which leaves it vulnerable to MITM attacks. It may be possible to cause remote code execution (RCE) by swapping out the requested binary with an attacker controlled binary if the attacker is on the network or positioned in between the user and the remote server. **Published:** June 01, 2018; 02:29:01 PM -04:00	(not available)
CVE-2018-4994	Adobe Connect versions 9.7.5 and earlier have an exploitable Authentication Bypass vulnerability. Successful exploitation could lead to sensitive information disclosure. **Published:** May 19, 2018; 01:29:01 PM -04:00	(not available)
CVE-2018-4992	Adobe Creative Cloud Desktop Application versions 4.4.1.298 and earlier have an exploitable Improper input validation vulnerability. Successful exploitation could lead to local privilege escalation. **Published:** May 19, 2018; 01:29:01 PM -04:00	(not available)
CVE-2018-4991	Adobe Creative Cloud Desktop Application versions 4.4.1.298 and earlier have an exploitable Improper certificate validation vulnerability. Successful exploitation could lead to a security bypass.	(not available)

Fuente autor

Figura 6 vulnerabilidad CVE

CVE
CVE-2017-8776
CVE-2017-8775
CVE-2017-8774
CVE-2018-4916
CVE-2018-4915
CVE-2018-4914
CVE-2018-4913

Fuente autor

2.1.5 Clasificación de las vulnerabilidades de los computadores mediante Stride

Teniendo las vulnerabilidades obtenidas mediante CVE, hacemos la clasificación de vulnerabilidades según STRIDE, caracterizando la amenaza encontrada en cada uno de los componentes del computador, así de esta manera tenemos como resultado el tipo de amenaza encontrada.

Figura 7 Clasificación STRIDE

FACTOR RIESGO
vulnerabilidad que facilita la Inyeccion de codigo arbitrario
vulnerabilidad que facilita la Inyeccion de codigo arbitrario
vulnerabilidad que facilita la Inyeccion de codigo arbitrario
Permite ataques remotos provocar una denegación de servicio

Fuente autor

2.1.6 *Determinación del impacto y probabilidad median CVE*

Para la determinación del impacto y la probabilidad se tienen en cuenta las vulnerabilidades encontradas en el CVE y por medio de la national vulnerability database donde se almacenan el impacto y la probabilidad, donde Impact Subscore corresponde a al impacto y Exploitability Subscore corresponde a la probabilidad. Como se muestra en la figura 7

Figura 8 Obtención de impacto y probabilidad

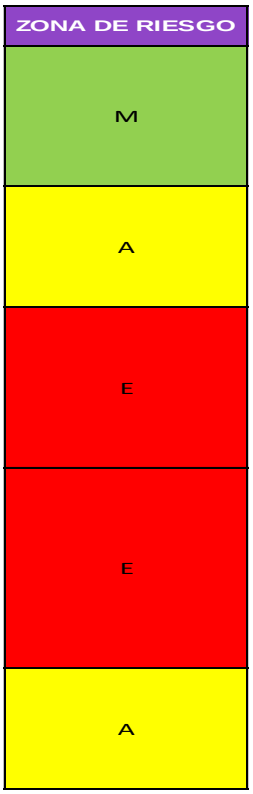
CVSS Base Score: 6.9
Impact Subscore: 10.0
Exploitability Subscore: 3.4
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 6.9

Fuente autor

2.1.7calculo de la zona del riesgo mediante DREAD y MSPI

Para la determinación del riesgo se tienen en cuenta la multiplicación de impacto por probabilidad, en el cual nos dará un valor que será escalado según el MSPI en la tabla de cálculos de valores, donde tenemos la zona de riesgo que puede ser zona extrema, zona alta, zona moderada y zona baja que se representa con su color representativo. Como se ve en la figura 8

Figura 9 Zona de riesgo



Fuente autor

2.1 Análisis de los computadores

En esta fase de desarrollo, se analizaron los computadores en los cuales se efectuara la evaluación del riesgo de las vulnerabilidades encontradas de las secretarias de planeación e infraestructura de la alcaldía mayor de Tunja.

2.1.1 Identificación de los NTD

Se identificaron los computadores activos e inactivos en los cuales se desarrolló la evaluación del riesgo de vulnerabilidades de las secretarias de infraestructura y planeación, como se muestra en la tabla 1.

Tabla 1. Descripción número de computadores

SECRETARIA	**CANTIDAD DE EQUIPOS**	**EQUIPOS ACTIVOS**	**EQUIPOS INACTIVOS**	**EQUIPOS EVALUADOS**
INFRAESTRUCTURA	19	17	2	17
PLANEACION	25	16	11	16

Fuente autor

2.1.3 Identificación de las aplicaciones, SO y drivers instalados de los NTD

Mediante la aplicación Everest (demo) se realizó la extracción de las aplicaciones, Sistemas operativos (SO) y Drivers instalados en los computadores de datos, así de esta manera se fue alimentado las hojas de vida de los equipos, ya que no se contaba con la información completa, así de esta manera se levantó la información base de los equipos de las secretarias de planeación e infraestructura.

2.1.4 Documentación del cuadro resumen de los NTD

Se levantaron las hojas de vida de todos los computadores luego de la extracción de la información, en donde se tuvieron en cuenta: Fecha de elaboración de la hoja de vida, Nombre de equipo, dirección Mac, Id del pc, Aplicaciones instaladas, origen APL, tipo de ataque, factor riesgo, impacto, probabilidad, valor de riesgo(DREAD), zona de riesgo(mintic) y CVE (Common Vulnerabilities and Exposures), utilizando las métricas de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html , y los cálculos de valores.

Figura 1. Instrumento de Caracterización de los equipos de infraestructura - instrumento de Caracterización de los equipos de planeacion - Anexo 1. Instrumento de Caracterización de los equipos de infraestructura

	Matrices de seguridad Alcaldía Mayor de Tunja							
FECHAS DE EVALUACIÓN	28/10/2016							
ELABORADO POR	SEBASTIAN QUINTANA							
NOMBRE DEL EQUIPO	NERSA							
MAC	40-A8-F0-A8-A8-3C							
ID PC	PC1							
APLICACIONES	ORIGEN APL	TIPO DE ATAQUE	FACTOR RIESGO	TIPO DE RIESGO	IMPACTO	PROBABILIDAD	ZONA DE RIESGO	CVE
360 Total Security	360 Total Security es una aplicacion que no pertenece al SO	buffer overflow	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	2,5	20%	M	CVE-2017-8776 CVE-2017-8775 CVE-2017-8774
Archiv [TRIAL VERSION]	Archiv es una aplicacion que no pertenece al SO	cross-site scripting (XSS	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	1,5	43%	A	CVE-2008-0464
	AutoCA [TRIAL VERSION] es una aplicacion que no pertenece al SO	buffer overflow	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	4,9	20%	E	CVE-2018-1000042

FUENTE. AUTOR

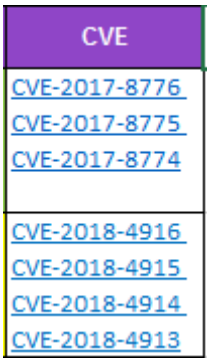
2.2 Determinación del modelo STRIDE

Mediante el Modelo STRIDE se hizo la clasificación de las vulnerabilidades encontradas en los diferentes equipos de las áreas de Infraestructura y planeación, tomando los cálculos de valores del modelo de seguridad de Min Tic para hallar el valor del riesgo y la metodología STRIDE para la clasificación de las vulnerabilidades.

2.2.1 Determinación de vulnerabilidades

En esta fase se establecerá el procedimiento para la obtención de la vulnerabilidades encontradas en los COMPUTADORES de datos, teniendo como herramienta CVE de donde extraemos las vulnerabilidades encontradas en su base de datos national vulnerability database (NVS) por cada aplicación, Driver y Sistema operativo, obteniendo de esta manera las vulnerabilidades encontradas.

Figura 2 vulnerabilidades extraídas del CVE



CVE
CVE-2017-8776
CVE-2017-8775
CVE-2017-8774
CVE-2018-4916
CVE-2018-4915
CVE-2018-4914
CVE-2018-4913

Fuente autor

2.2.2 Clasificación de las vulnerabilidades según STRIDE

La determinación de las vulnerabilidades se estableció por medio de la metodología STRIDE y el Modelo de seguridad y privacidad de la información (MSPI). Teniendo en cuenta esta ultima ya que fue implementada por el MINTIC a mitad del segundo periodo del 2017, por esta razón fue tenida en cuanta para la estandarización de la medición del riesgo.

STRIDE, Este término es el acrónimo “Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege". Para seguir el método STRIDE, se descompone el sistema en diferentes componentes, seguido de analizar cada uno, con el objetivo de comprobar si es susceptible de sufrir amenazas; después se proponen acciones que traten de mitigarlas y se repite el proceso hasta llegar a una situación cómoda con las amenazas restantes. **(Barbara Olivares)**

- Spoofing Identity (Suplantación de identidad)
- Tampering with Data (Manipulación de datos)
- Repudiation (Repudio)
- Information Disclosure (Revelación de información)
- Denial of Service (Denegación de servicio)
- Elevation of Privilege (Elevación de privilegios)

De esta manera logramos por medio de STRIDE identificar el factor del riesgo identificando los riesgos relacionados en cada elemento del equipo.

Figura 3 Factor del riesgo según STRIDE

FACTOR RIESGO
vulnerabilidad que facilita la Inyeccion de codigo arbitrario
Permite ataques remotos provocar una denegación de servicio

Fuente autor

2.2.3 Ponderación de valores

Para ponderar los valores fue necesario tener en cuenta dos variables importantes, como es el impacto del riesgo y la probabilidad del riesgo, esto para hallar la zona del riesgo del equipo, multiplicando impacto por probabilidad, de esta manera se halla la zona del riesgo.

Figura 7 Detalle de las variables de impacto y probabilidad en el instrumento de generalidades. Anexo1 anexo1.Instrumento Hallazgos Generalidades aplicaciones

IMPACTO	PROBABILIDAD	ZONA DE RIESGO

Fuente autor

A. Impacto

En la tabla 3 IMPACTO. Se evidencio el indicador de medición con una valoración de 1 a 5, donde 1 es el valor despreciable en el cual no tiene mayor impacto en el riesgo y 5 es el valor critico donde tiene mayor impacto de riesgo.

Tabla 2 Impacto. anexo3.Calculo de valores

IMPACTO		
IMPACTO	**VALORACIÓN**	**CRITERIO**
Despreciable	1	No Hay impacto
Leve	2	Hay un impacto leve
Moderado	3	Rendimiento moderado, pero se mantiene su desarrollo
Significativo	4	Rendimiento medio, pero funcional.

Crítico	5	Retrasos inminentes, incumplimiento con los requerimientos del impuesto

Fuente Modelo de Seguridad y Privacidad de la Información MSPI

http://www.mintic.gov.co/gestionti/615/articles5482_Instrumento_Evaluacion_MSPI.xlsx

B. Probabilidad, para la medición de este indicador se tiene en cuenta la tabla 3,, que establece una escala ascendente de 1 hasta 5 como base de operación, donde 1 es la probabilidad más baja con efecto raro que ocurra y 5 la probabilidad más alta que transcurra.

Tabla 4 Probabilidad. anexo3.Calculo de valores

PROBABILIDAD		
EFECTO	**VALORACIÓN**	**CRITERIO**
Raro	1	Falla probable
Improbable	2	Probable ocasionalmente
Posible	3	Probabilidad casos extremos
Probable	4	Fallos moderables
Casi seguro	5	Alto riesgo de ocurrencia de fallas

Fuente Modelo de Seguridad y Privacidad de la Información MSPI

http://www.mintic.gov.co/gestionti/615/articles5482_Instrumento_Evaluacion_MSPI.xlsx

C. Prioridad, se tuvo en cuenta la prioridad , para ponderar la zona del riesgo donde se tuvo en cuenta la tabla 5 , en el cual la prioridad A hace referencia a una zona de riesgo muy grave y la prioridad D con un riesgo menor que tendrá medidas correctivas con mas baja prioridad que las demás.

Tabla 3 PRIORIDAD

PRIORIDAD	
PRIORIZACIÓN DEL RIESGO	**DESCRIPCIÓN DEL RIESGO**
PRIORIDAD A	RIESGO MUY GRAVE: Requiere de medidas preventivas urgentes.
PRIORIDAD B	RIESGO IMPORTANTE: Requiere medidas preventivas obligatorias.
PRIORIDAD C	RIESGO MODERADO: Requiere medidas preventivas .
PRIORIDAD D	RIESGO MENOR: Se vigilará aunque no requieren medidas preventivas iniciales.

Fuente Modelo de Seguridad y Privacidad de la Información MSPI http://www.mintic.gov.co/gestionti/615/articles5482_Instrumento_Evaluacion_MSPI.xlx

D. Zona de riesgo, teniendo los datos de probabilidad e impacto se procedió a multiplicarlos para tener como resultado la zona del riesgo de las aplicaciones, driver y sistema operativo, utilizando la tabla 6.

Tabla 4. 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 Modelo de Seguridad y Privacidad de la Información MSPI http://www.mintic.gov.co/gestionti/615/articles5482_Instrumento_Evaluacion_MSPI.xlx

2.3 Caracterización del riesgo

En la fase de caracterización del riesgo tendremos la elaboración de las matrices, con su respectiva ponderación, corrección de la matriz a partir de la estandarización de MSPI establecido por MINTC.

2.3.1 Elaboración de la matriz de riesgo

- La elaboración de las matrices se realizaron teniendo como base lo establecido por la estandarización realizada en el modelo de seguridad y privacidad de la información (MSPI) de MinTic y guía de gestión del riesgo.

Tabla 5. CARACTERIZACION MATRIZ Instrumento de Caracterización de los equipos de infraestructura - Anexo 1. Instrumento de Caracterización de los equipos de infraestructura

Campo	Descripción
Fecha evaluación	Fecha en el cual se a efectuado la evaluación
Elaborado por	Persona encargada de realizar la matiz
Nombre del Equipo	Nombre de equipo con el que se cuenta actualmente
Dirección Mac	Numero de dirección Mac con el que el nodo terminal de datos cuenta.
Id de pc	Se establece un Id del pc para el control del número de COMPUTADORES de datos
Aplicaciones	Aplicaciones instaladas en el equipo
Origen APL	Origen de la aplicación en el quipo
Tipo de ataque	Tipo de ataque al que se encuentra expuesto cada aplicación, driver o sistema operativo
Factor de riesgo	Específica a donde está enfocado el riesgo encontrado
Tipo de riesgo	Tipo de riesgo al que se encuentra expuesto cada aplicación, driver o sistema operativo
Impacto	Se especifica los valores extraídos de la base de datos del CVE en una escala de 1 a 5
Probabilidad	Se especifica la probabilidad que ocurra esta vulnerabilidad extraída de CVE
Zona de riesgo	La zona de riesgo se halla cruzando el impacto por probabilidad y se estandariza según MinTic, asignándole colores según su zona de riesgo
CVE	Id de las vulnerabilidades encontradas en NVD

Fuente [Instrumento de Caracterización de los equipos de infraestructura](#) - Anexo 1. Instrumento de Caracterización de los equipos de infraestructura

Figura 8 Potada hoja de vida de equipos

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Matrices de seguridad Alcaldía Mayor de Tunja	vive digital para la gente
FECHAS DE EVALUACIÓN		
ELABORADO POR		
NOMBRE DEL EQUIPO		
DIRECCION MAC		
ID PC		

Fuente autor

Figura 8 instrumento Hallazgos Generalidades aplicaciones

TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN MINTIC	Matrices de seguridad Alcaldía Mayor de Tunja					vive digital para la gente		
FECHAS DE EVALUACIÓN								
ELABORADO POR								
NOMBRE DEL EQUIPO								
DIRECCION MAC								
ID PC								
APLICACIONES	ORIGEN APL	TIPO DE ATAQUE	FACTOR RIESGO	TIPO DE RIESGO	IMPACTO	PROBABILIDAD	ZONA DE RIESGO	CVE

Fuente autor

2.3.2 Corrección de la Matriz de riesgo

Inicialmente se empezó con una matriz con diferentes parámetros y características que a la actual, su corrección de la matriz se basó a la estandarización realizada por MinTic en donde formaliza una matriz estándar para la realización de las hojas de vida de los computadores como se muestra a continuación

Figura 9 MATRIZ INICIAL

UNIVERSIDAD SANTO TOMÁS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
TUNJA
Experiencia y Calidad

ID PC	PC16
NOMBRE DE EQUIPO	ESTHER
RESPOSABLE DE EQUIPO	ESTHER ESCOBAR
ELABORO	SEBASTIAN QUINTANA
REVISO	
FECHA ELABORACIO	28/10/2016
MAC	78-E3-B5-96-2F-63

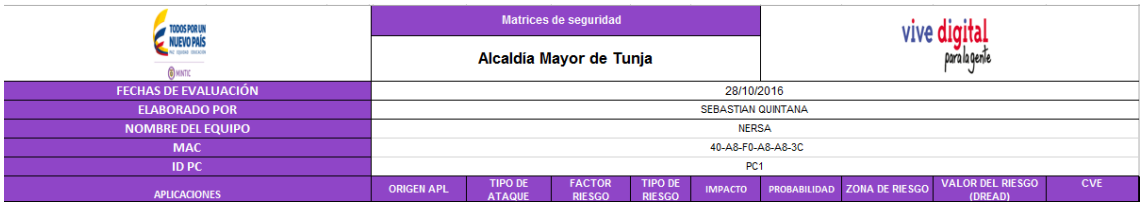
APLICACIONES	ORIGEN APL	TIPO DE ATAQUE	FACTOR RIESGO	TIPO DE RIESGO	IMPACTO	PROBABILIDAD	RIESGO	CVE

Fuente autor

En la figura 9 se muestra la prime matriz implementada para las dos secretarias, infraestructura y planeación, donde evidenciamos que no se manejaba ningún tipo de

estandarización ni normativa, a diferencia de la actualización de la nueva matriz como se muestra a continuación.

Figura 10. Matriz estandarizada



Matrices de seguridad								
Alcaldía Mayor de Tunja								
FECHAS DE EVALUACIÓN	28/10/2016							
ELABORADO POR	SEBASTIAN QUINTANA							
NOMBRE DEL EQUIPO	NERSA							
MAC	40-A8-F0-A8-A8-3C							
ID PC	PC1							
APLICACIONES	ORIGEN APL	TIPO DE ATAQUE	FACTOR RIESGO	TIPO DE RIESGO	IMPACTO	PROBABILIDAD	ZONA DE RIESGO	VALOR DEL RIESGO (DREAD)	CVE

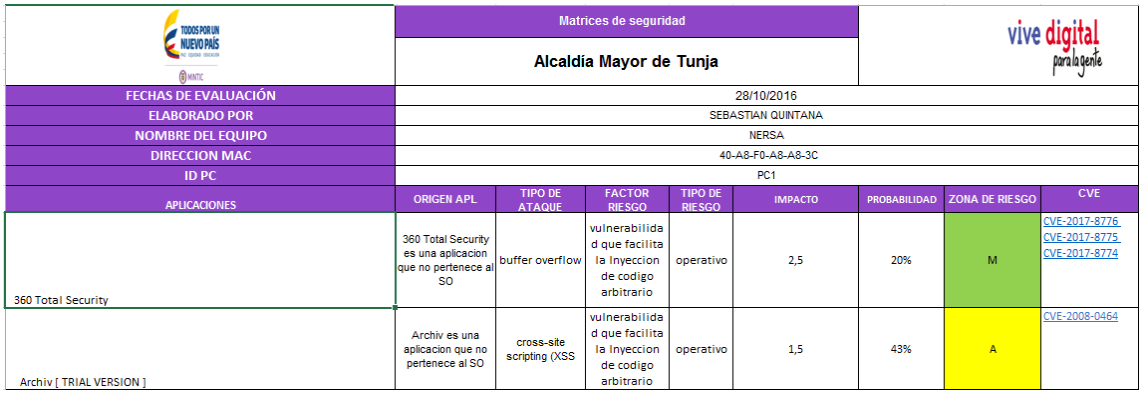
Fuente autor

En la figura10 Matriz estandarizada, tenemos la modificación establecida por el MinTic en el cual se agrega una característica, zona de riesgo en el cual se hace la ponderación (baja, moderada, alta, extrema) con sus colores establecidos para cada zona de riesgo hallada

2.3.3 Aplicación de la matriz de riesgo

Las matrices de riesgo fueron aplicadas a las secretarias de infraestructura y planeación de la alcaldía de Tunja donde se caracterizaron los computadores, extrayendo su impacto y probabilidad para hayar su zona de riesgo en cada uno de ellos. Como se puede evidenciar en la figura 11

Figura 11 aplicacion matriz de riesgo - Instrumento de Caracterización de los equipos de infraestructura - Instrumento de Caracterización de los equipos de planeacion - anexo5 y anexo4



Matrices de seguridad								
Alcaldía Mayor de Tunja								
FECHAS DE EVALUACIÓN	28/10/2016							
ELABORADO POR	SEBASTIAN QUINTANA							
NOMBRE DEL EQUIPO	NERSA							
DIRECCION MAC	40-A8-F0-A8-A8-3C							
ID PC	PC1							
APLICACIONES	ORIGEN APL	TIPO DE ATAQUE	FACTOR RIESGO	TIPO DE RIESGO	IMPACTO	PROBABILIDAD	ZONA DE RIESGO	CVE
360 Total Security	360 Total Security es una aplicacion que no pertenece al SO	buffer overflow	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	2,5	20%	M	CVE-2017-8776 CVE-2017-8775 CVE-2017-8774
Archiv [TRIAL VERSION]	Archiv es una aplicacion que no pertenece al SO	cross-site scripting (XSS	vulnerabilidad que facilita la Inyeccion de codigo arbitrario	operativo	1,5	43%	A	CVE-2008-0464

Fuente autor

2.4 Implementación del diagnostico

En esta fase se realizaron los diagnósticos que dejan evidenciado los resultados de la medición en los computadores de las secretarias de infraestructura y planeación de la

alcaldía de Tunja, haciendo énfasis a las zonas de riesgo, de cada nodo terminal y cada secretaria en general, como se mostrara a continuación.

2.4.1 Elaboración de los estadísticos

La elaboración de datos estadísticos que se mostraran a continuación, tiene como base los datos anteriormente obtenidos del cve en el cual se analiza la vulnerabilidad y se obtuvo su respectivo impacto y probabilidad del riesgo, para hallar la zona del riesgo respectiva a cada computador y al total de las secretarias de infraestructura y planeación.

- **Datos estadísticos secretaria de infraestructura**

Tabla 6 PONDERACION DE RIESGO INFRAESTRUCTURA

PC	EXTREMO	ALTO	MEDIO	BAJO
PC1	88	36	71	58
PC2	29	40	18	33
PC5	56	54	26	47
PC6	30	45	21	56
PC7	30	45	21	56
PC8	30	45	21	56
PC9	41	35	15	43
PC10	38	46	21	46
PC11	38	44	22	53
PC12	35	49	19	34
PC13	35	49	19	34
PC14	55	59	23	69
PC15	47	41	25	44
PC16	38	45	45	19
PC17	40	51	18	64
PC18	38	49	20	63
PC19	36	46	19	59
	704	779	424	834

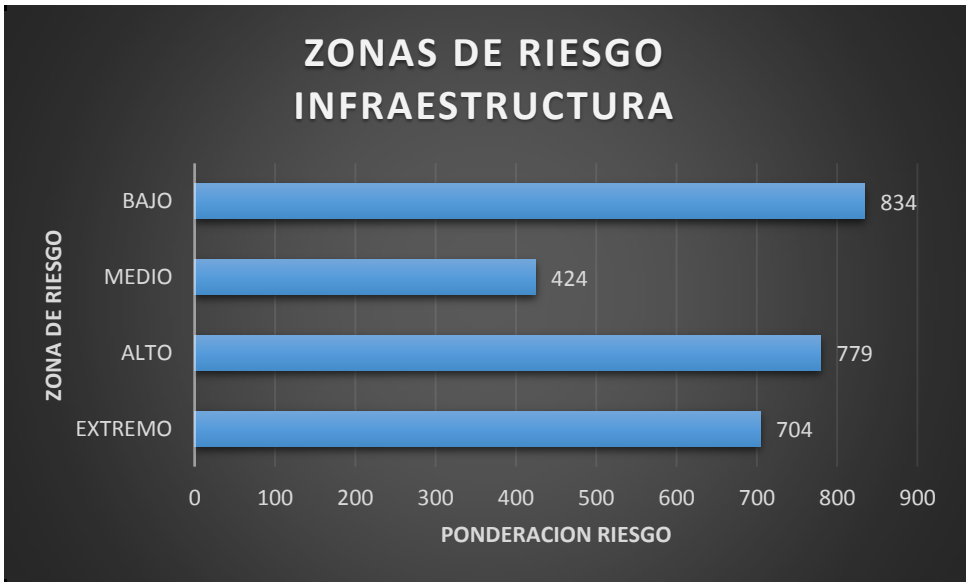
Fuenteautor

En la tabla 9 ponderación de riesgo infraestructura obtenemos las zonas de riesgo de los computadores del departamento de infraestructura es su totalidad. En donde encontramos en la secretaria en general un hallazgo de 704 zonas de riesgo extremas

que exponen la seguridad de la información de manera alarmante, 779 zonas de riesgo alto, 424 zonas de riesgo moderadas y 834 zonas de riesgo bajas.

- Donde las **zonas de riesgo extremas** tienen una **prioridad A (riesgo muy grave),** que requiere medidas preventivas de manera urgente en un periodo de tiempo no mayor a seis meses.
- **Zonas de riesgo altas** tienen una **prioridad B (riego importante),** que requiere medidas preventivas obligatorias en un periodo de tiempo no mayor a 8 meses
- **Zonas de riesgo moderadas** tienen una **prioridad C (riego moderado),** que requiere medidas preventivas en un periodo no mayor a 10 meses.
- **Zonas de riesgo baja,** tienen una **prioridad D (riesgo menor),** no se requieren medidas preventivas iniciales pero se tendrá vigilado.

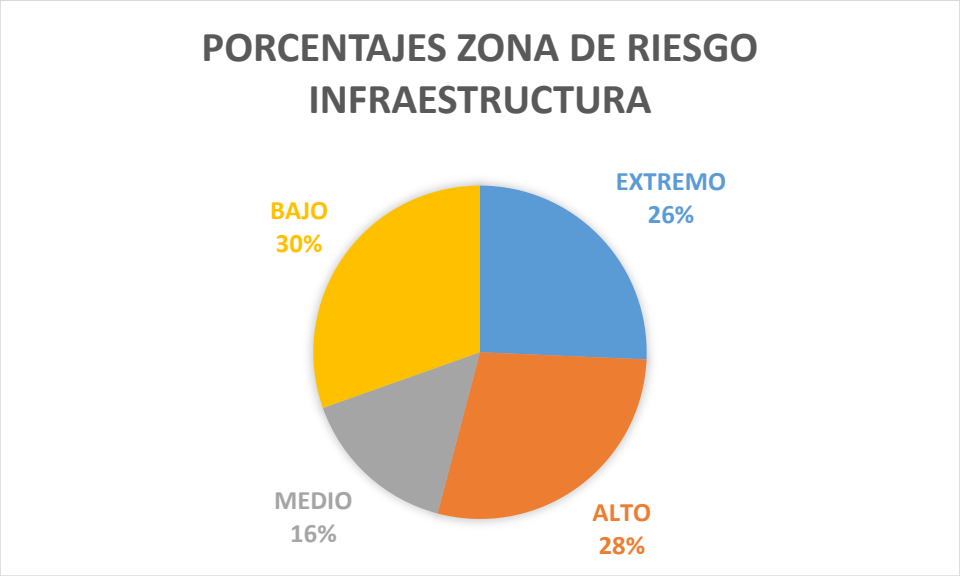
Figura 12. Gráfico de barras infraestructura



Fuente autor

Con los datos recaudados en la tabla 9 PONDERACION DE RIESGO INFRAESTRUCTURA , realizamos el diagrama de barras de la figura 12 grafico de barras infraestructura, donde tenemos los datos ponderados de todos los nodos activos de datos de este departamento, teniendo como resultado las zonas de riesgo totales de toda la secretaria, obteniendo como resultado un total de 704 zonas de riesgo en zona extrema, 779 zonas de riesgo altas, 724 zonas de riego moderadas y 834 zonas de riego bajas.

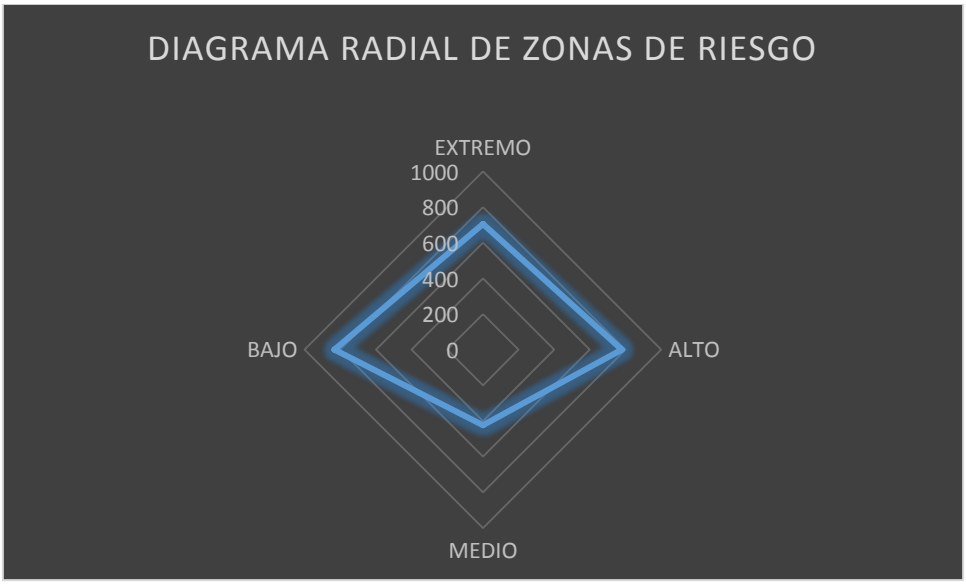
Figura 13 diagrama circular porcentajes de riesgo



Fuente autor

En la figura 13 diagrama circular porcentajes de riesgo tenemos los porcentajes de la zona de riesgo donde se evidencia que la zona de riesgo bajo tiene un 30%, luego zona de riesgo alto con un 28%, zona de riesgo extremo 26% y zona de riesgo medio en un 16%.

Figura 14 diagrama radial de zonas de riesgo



Fuente autor

En la Figura 14diagrama radial de zonas de riesgo, podemos observar nuestras cuatro zonas de riesgo en donde vemos la tendencia hacia donde se inclina la zona de riesgo la secretaria de infraestructura.

- **Datos estadísticos secretaria de planeación**

Tabla 7 PONDERACION DE RIESGO PLANEACION

PC	EXTREMO	ALTO	MEDIO	BAJO
PC1	54	57	19	50
PC3	56	67	34	81
PC4	55	68	27	55
PC8	35	49	19	34
PC9	37	42	19	44
PC10	29	40	18	33
PC12	30	45	21	56
PC13	39	34	14	41
PC14	36	44	17	39
PC16	38	44	22	53
PC17	56	54	26	47
PC19	47	41	24	44
PC20	47	41	24	44
PC22	55	58	20	50
PC23	52	57	19	62
PC24	39	32	14	43
totales	705	773	337	776

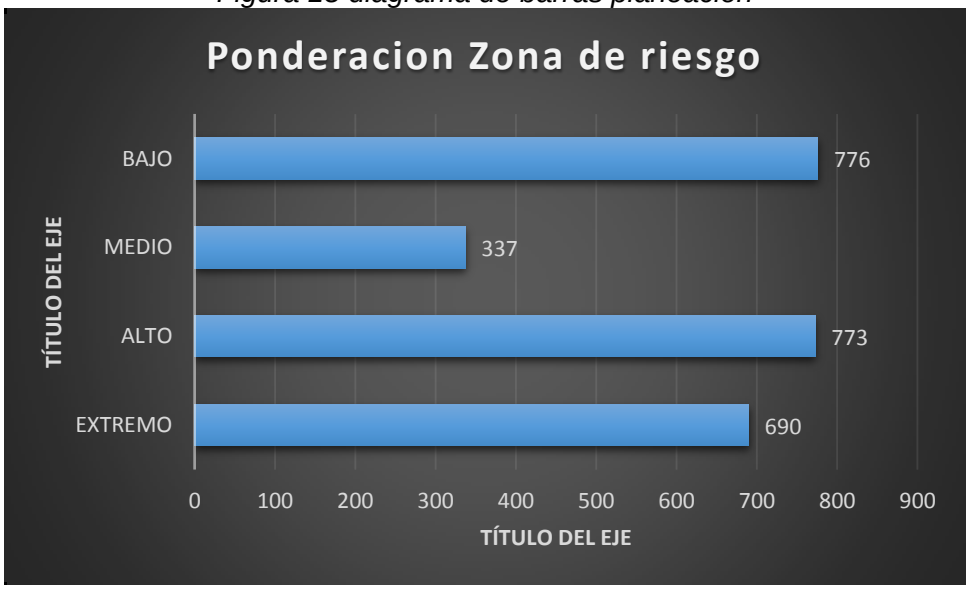
Fuente Autor

En la tabla 10 ponderación de riesgo planeación obtenemos las zonas de riesgo de los computadores del departamento de infraestructura es su totalidad. En donde encontramos en la secretaria en general un hallazgo de 705 zonas de riesgo extremas que exponen la seguridad de la información de manera alarmante, 773 zonas de riesgo alto, 337 zonas de riesgo moderadas y 776 zonas de riesgo bajas.

- Donde las **zonas de riesgo extremas** tienen una **prioridad A (riesgo muy grave),** que requiere medidas preventivas de manera urgente en un periodo de tiempo no mayor a seis meses.
- **Zonas de riesgo altas** tienen una **prioridad B (riego importante),** que requiere medidas preventivas obligatorias en un periodo de tiempo no mayor a 8 meses
- **Zonas de riesgo moderadas** tienen una **prioridad C (riego moderado),** que requiere medidas preventivas en un periodo no mayor a 10 meses.

- **Zonas de riesgo baja,** tienen una **prioridad D (riesgo menor),** no se requieren medidas preventivas iniciales pero se tendrá vigilado.

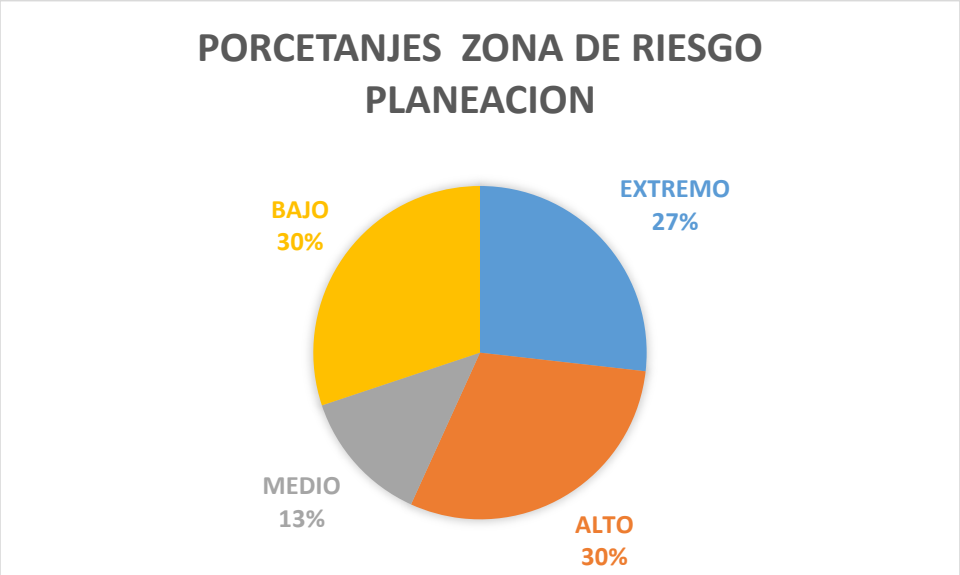
Figura 15 diagrama de barras planeación



Fuente autor

Con los datos recaudados en la tabla 10 ponderación de riesgo planeación, realizamos el diagrama de barras de la figura 15 grafico de barras planeación, donde tenemos los datos ponderados de todos los nodos activos de datos de este departamento, teniendo como resultado las zonas de riesgo totales de toda la secretaria, obteniendo como resultado un total de 690 zonas de riesgo en zona extrema, 773 zonas de riesgo altas, 337 zonas de riego moderadas y 775 zonas de riego bajas.

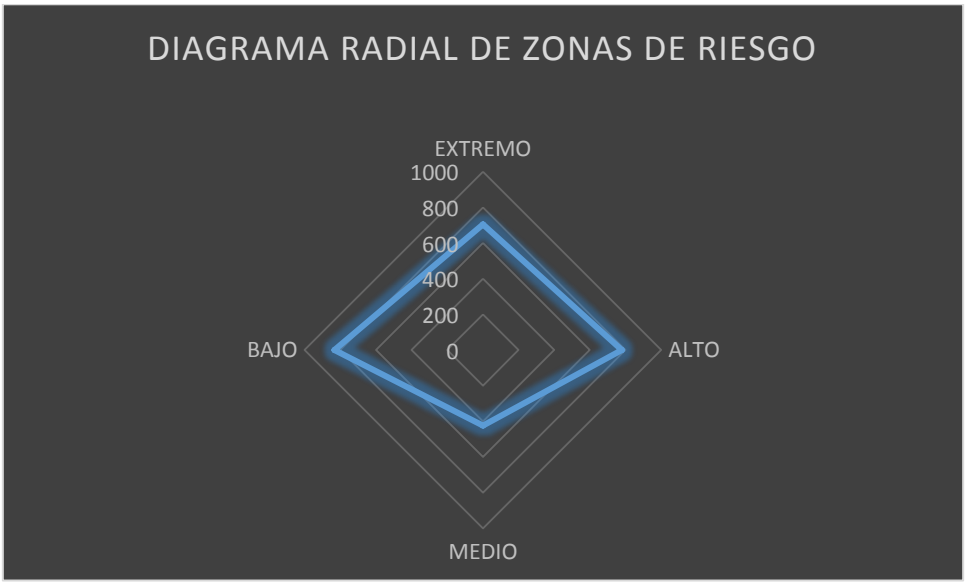
Figura 16 diagrama circular porcentajes de riesgo



Fuente autor

En la Figura 16 diagrama circular porcentajes de riesgo tenemos los porcentajes de la zona de riesgo donde se evidencia que la zona de riesgo bajo tiene un 30%, luego zona de riesgo alto con un 30%, zona de riesgo extremo 27% y zona de riesgo medio en un 13%.

Figura 17 diagrama radial de zonas de riesgo



Fuente autor

En la Figura 17 diagrama radial de zonas de riesgo, podemos observar nuestras cuatro zonas de riesgo en donde vemos la tendencia hacia donde se inclina la zona de riesgo la secretaria de planeación .

3. Recomendaciones

Luego del análisis de los riesgos de las vulnerabilidades de las secretarias de planeación e infraestructura, en base a los resultados obtenidos del levantamiento de la información se hacen las siguientes recomendaciones:

1. Diseñar un instrumento que contenga la información de cada uno de los equipos de las secretarias de planeación e infraestructura, donde figure la versión, fecha de actualización de los programas instalados.

2. Establecer restricciones para la instalación de software en cada uno de los equipos.

3. Diseñar planes de capacitación del buen uso de los quipos.

4. Plantear procedimientos para copias de seguridad periódicas
5. Agregar políticas para el manejo de la información con criterios de seguridad como claves para el acceso.

6. Crear programas de capacitación y concientización al personal en cuanto a políticas personales de seguridad

7. Mantener y controlar los software actualizados y licenciados
8. Actualizar los sistemas operativos mas antiguos a la ultima versión de Windows
9. Bajar los niveles de riego extremo y alto de manera inmediata en la secretarias de planeación e infraestructura

3. CONCLUSIONES

- La determinación de las vulnerabilidades de los computadores de las secretarias de planeación e infraestructura fue expresa gracias al modelo STRIDE utilizado para la clasificación de vulnerabilidades encontradas obteniendo de esta manera el factor del riesgo que puede afectar los computadores de las secretarias de infraestructura y planeación de la alcaldía mayor de Tunja.

- Los procesos de evaluación para evaluar los niveles de riesgo de las vulnerabilidades, fueron hallados mediante la metodología DREAD y Modelo de seguridad y privacidad de la información (MSPI) implementado por MINTIC en el cual se hallaron los niveles de riesgo y su respectiva zona de riesgo en cada aplicación encontrada en los equipos.

- Teniendo en cuenta el análisis de datos obtenidos en el proceso de evaluación se llevaron a cabo datos estadísticos donde se encontraron porcentajes de ponderación extremos y altos en las secretarias de planeación e infraestructura

4. INFOGRAFIA Y BIBLIOGRAFIA

Barbara Olivares, G. E. (s.f.). MODELADO DE AMENAZAS, UNA TÉCNICA. *Universidad Piloto de Colombia*, 12.

Bertolín, D. J. (2012). *Gestión de riesgos de seguridad y privacidad de la información.*

Bishop, M. (2005). Introducction to computer segurity. 785.

Bishop, M. (2005). *Introduction to Computer Security.*

DGTIC, direccion general de tecnologias de la informacion y comunicaciones . (s.f.). *http://dgtic.tabasco.gob.mx*.

***Eleven Patchs*. (2014).** Obtenido de http://blog.elevenpaths.com/2014/01/ocho-siglas-relacionadas-con-las.html

Microsoft. (2009).

MINTIC. (2017). *Fortalecimiento de la gestion TI del estado* . Obtenido de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

OWASP. (13 de Julio de 2017). *owasp.org*.

protejete.wordpress. (2014). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com

Tarazona, C. (2007). AMENAZAS INFORMÁTICAS Y.

***uptodown*. (2008)**. Obtenido de https://everest-ultimate-edition.uptodown.com/windows