UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"PROPUESTA DE MEJORA PARA LA IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD INFORMÁTICA EN LA DISTRIBUCIÓN DE UNA HERRAMIENTA PARA AUTODESK® AUTOCAD® UTILIZADA EN LA ELABORACIÓN DE DIAGRAMAS TÉCNICOS".

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

GERARDO NASSIR GUÍZAR GÓMEZ

Asesor: Dr. Modesto Javier Cruz Gómez

México D.F. 2012

Jurado Asignado

Profesores

Presidente:	Mtro. Juan José Carreón Granados
Vocal:	Dr. Modesto Javier Cruz Gómez
Secretario:	Fis. Raymundo Hugo Rangel Gutiérrez
1er. Suplente:	Ing. Gabriela Camacho Villaseñor
2do Suplente:	M.C. Cintia Quezada Reyes

ASESOR

_____

Dr. M. Javier Cruz Gómez

ASESOR TÉCNICO

_____

Ing. Julio César Velasco Martínez

SUSTENTANTE

_____

Gerardo Nassir Guízar Gómez

Agradecimientos:

A mis padres,
porque sin su gran apoyo y guía nada de esto hubiera sido posible, nunca hubo condiciones de ningún tipo, nunca se me negó nada, siempre obtuve lo que necesité y más, fueron incalculables horas de sacrificios, una inversión económica gigantesca, una cobertura de todo tipo de necesidades ininterrumpida, por eso nuevamente, les agradezco profundamente y espero algún día poder compensar de alguna manera todo lo que hicieron por mí.

A mis hermanos,
deseando que esto les sirva de un buen ejemplo para motivarlos a alcanzas sus metas y a continuar aprendiendo no solo en lo académico, sino en todos los aspectos que conforman la totalidad de un ser humano.

A Sandy,
porque junto con mis padres fue el otro pilar que me permitió lograr culminar la carrera, vio muchos de mis éxitos y fracasos, estuvo conmigo todo este camino, ayudándome incluso con algunos tópicos del plan de estudios de la carrera, dando todo el estilo visual a este trabajo. Por su valiosa compañía, ser la mejor pareja y por darme la motivación que necesitaba con su ejemplo, mi futuro, es para ella.

Al ingeniero Julio Cesar Velasco,
por ser un verdadero amigo, por haberme ayudado sin esperar nada a cambio, por todo el conocimiento que me ha aportado en mi desarrollo profesional y porque sin su ayuda, tiempo y asesoría técnica, este trabajo simplemente no hubiera sido posible, ¡Muchas gracias Julio! Fue una acción extraordinaria que valoro profundamente.

A mis amigos de la Torre de ingeniería,
Nayeli Andrade y Carlos Horta, que también me ayudaron y cubrieron cuando más lo necesité, los aprecio y respeto mucho, al igual que su carrera y el conocimiento técnico que poseen.

Al maestro Luis Fernando Pérez,
a quien también considero un gran amigo, un ejemplo a seguir y una persona que no ha hecho más que facilitar mi desarrollo profesional, intelectual y personal, jamás me limitó y al contrario, siempre me ha dado oportunidades y consideraciones de sobra, es un honor trabajar haciendo ingeniería con él y su grupo, ¡Gracias Ingeniero!.

Agradecimientos

A la ingeniera Mirian Guzmán,
quien siempre supo darme un buen consejo, escucharme y ayudarme con mi trabajo y muchos aspectos más, es una de las personas más nobles que he conocido en mi vida y solo le puedo desear mucho éxito profesional así como con su familia, ¡Gracias Mirian!

Al maestro Juan Carreón,
quien siempre estuvo al pendiente de mi situación académica, durante mi servicio social en LIDSOL y también con este trabajo de tesis, por su guía, su tutela y su amistad, ¡Gracias maestro!, siempre vio y continúa haciéndolo por todos los integrantes y ex integrantes de ese gran laboratorio.

A la maestra Cintia Quezada,
que se encargo de enseñarme las bases fundamentales de las especialidades a las que me dedicare el resto de mi vida profesional, las redes y la seguridad, por su paciencia, su apoyo, su tiempo, sus correcciones para esta tesis y todas las enseñanzas, ¡Gracias maestra!, un privilegio y un honor haber tomado la mitad de las materias de mi módulo con usted.

A la ingeniera Gabriela Camacho,
quien fue la primera en mostrarme el panorama de la programación y las redes de datos, siempre me oriento en lo académico, nunca estuvo demasiado ocupada para resolverme una duda y fomento en mi el habito de estar enterado del mundo de la T.I., lo cual ahora es parte de mi vida cotidiana, por esto y mucho más, ¡Gracias maestra!

Al físico Raymundo Rangel,
de quien aprendí grandes cosas sobre programación estructurada y orientada a objetos, fue él quien me enseño que es la ingeniería de software, y me ayudo a crear una estructura de pensamiento muy sistemática para atacar a los problemas, por todo esto y más, ¡Gracias maestro!

Al doctor Javier Cruz,
por su paciencia, apoyo y enseñanzas durante la elaboración de este trabajo, al igual que por haber aceptado ser mi director de tesis, ¡Gracias doctor!

A mis amigos de LIDSOL y la facultad,
Manuel López, Enrique Amaya, Andrés Hernández, Julio Cesar, Julio Adrian Rescalvo y Oscar Pacheco por compartir este reto conmigo, de quienes aprendí muchas cosas atraves de estos años, ¡Gracias a todos por su amistad!

ÍNDICE GENERAL

ÍNDICE DE TABLAS

Índice de tablas

Índice de tablas

Índice de tablas

INTRODUCCIÓN

Cuando se realizan ciertos tipos de proyectos de ingeniería, entre las diversas necesidades que surgen se encuentra la de representar instalaciones y sus diferentes niveles de información con dibujos técnicos. Diagramas que es posible realizar utilizando varios métodos distintos, uno ellos, es mediante el empleo de programas de *Diseño Asistido por Computadora* (Computer-Aided Design, CAD), ejemplos de este tipo de software son: *AutoCAD*®, *ArchiCAD*®, *CATIA*®, *QCAD*, entre otros. Al emplear este tipo de programas para realizar diagramas técnicos, es posible obtener varias ventajas importantes como: *mejores diseños; de forma más rápida y económica que los competidores, aumento en la velocidad para realizar dibujos técnicos, incremento en la productividad de los mismos, posibilidad de copiar, rotar y crear diseños espejo de instalaciones completas, al igual que de elegir entre varios tipos de letra, estilos, formatos, funciones de zoom, la capacidad de almacenar entidades para su posterior uso o manipulación, entre otras* (Bozdoc, M., 2003).

Sin embargo, al optar por la utilización de este tipo de programas para realizar los dibujos técnicos, surgen varias necesidades que deben ser cubiertas con el fin de lograr lo anterior, tales como: contar con personal especializado en el manejo óptimo de este tipo de programas (creación de geometría simple en dos dimensiones, manejo mínimo de *capas* (layers) y de *zoom*, impresión de formatos), capacitación, inversión económica, entre otras. Aún satisfaciendo las necesidades anteriores, la obtención de resultados desfavorables es frecuente; situación principalmente debida a la falta de especialización para ciertos tipos de proyectos de ingeniería por parte del personal señalado.

Conscientes de la problemática descrita y con el objetivo de mitigarla, algunas compañías de software CAD han abierto la posibilidad de crear herramientas de tipo *extensión/complemento,* denominadas también *plug-in(s)* (del idioma inglés “acoplable”) o *agregados* (Add-Ons) para sus programas.

Estas extensiones; son aplicaciones capaces de aportar nuevas funciones a sus productos (por ejemplo, AutoCAD®), y con frecuencia, se encuentran orientadas a la resolución de problemas particulares. La ejecución de estos complementos es llevada a cabo típicamente por el producto principal, mediante el uso y la interacción con la *Interface de Programación para Aplicaciones* (*Application Programming Interface, API*) de este último.

Es importante resaltar que la construcción de complementos como éstos, solo es posible cuando existen sus correspondientes plataformas de desarrollo; las cuales son creadas y liberadas por las compañías de software CAD, para cada uno de sus productos, con estos fines específicos. Estas plataformas, ya traen integrados elementos como: la API del producto principal de las compañías, las funciones correspondientes para crear los complementos, que a su vez, son capaces de interactuar con alguno o varios lenguajes de programación compatibles. Las plataformas también, incluyen la documentación técnica de las mismas, al igual que la programación.

Un ejemplo real de un *plug-in* con características como las mencionadas, hecho para el software CAD de Autodesk®, AutoCAD®, es la *"QITDraw"* (acrónimo en el idioma inglés, derivado de la oración: *"Quick Intelligent Technical Drawing"*), herramienta inteligente y rápida para dibujo técnico. La QITDraw, es una barra (o paleta) de herramientas diseñada para dibujar diagramas técnicos y funcionar con AutoCAD® versión 2006 o posterior, dirigida principalmente a personas sin experiencia previa para realizar este tipo de diagramas con el programa de Autodesk® mencionado.

Esta barra de herramientas, tiene un objetivo específico, el cual es facilitar el proceso de dibujo de diagramas técnicos de isométricos de tuberías y equipos (tanques, torres de enfriamiento, calderas, etcétera), usados en proyectos de inspección técnica para el mantenimiento de instalaciones de PEMEX Refinación.

La QITDraw, fue creada dentro del CEASP^{4}A (Centro de Estudios para la Administración de la Seguridad de los Procesos Petroquímicos, Poliméricos y la Protección Ambiental), el cual es un grupo de trabajo perteneciente a la Facultad de Química de la UNAM. Fundado en 1997, con el único objetivo fundamental de lograr desarrollos tecnológicos y soluciones aplicables en el área de seguridad para los procesos en la industria química; con enfoque en la formación de estudiantes y profesionistas a través de su participación en proyectos de vinculación academia-industria.

La herramienta mencionada previamente (QITDraw), es uno de los varios desarrollos tecnológicos hechos por el grupo, el cual ha sido capaz de conseguir un aumento del 300% en la eficiencia del proceso de dibujo de diagramas técnicos, referencia basada en la experiencia obtenida durante la implementación de la misma. Este éxito, se debe principalmente a la utilización de métodos simplificados de dibujo por parte la QITDraw; los cuales permiten evitar la realización de procedimientos relativamente complejos, repetitivos y tediosos cuándo se dibujan diagramas técnicos en AutoCAD, por ejemplo: inserción y alineación de bloques, dibujo y recorte de polilíneas (líneas compuestas, capaces de cambiar de dirección), ajuste preciso de líneas, manejo de capas, etcétera.

La distribución y el mantenimiento de la QITDraw continúan llevándose a cabo debido a la continuación de los trabajos de dibujo de diagramas técnicos en PEMEX Refinación, necesidad que surgió a partir de los proyectos de colaboración que tiene esta entidad paraestatal con el CEASP^{4}A.

Para PEMEX Refinación, la herramienta es proporcionada de manera gratuita, sin embargo, resulta no ser la única entidad que requiere emplearla, lo anterior debido a causa de los objetivos y alcances de los proyectos mencionados que lleva a cabo esta institución. Por ello, se ha vuelto necesario que terceros utilicen también la paleta de dibujo, concretamente, dos entidades más: personal del CEASP^{4}A (en equipos de cómputo del grupo, tanto de escritorio como portátiles), así como una extensa variedad de contratistas externos al CEASP^{4}A y a PEMEX Refinación. Debido a las situaciones anteriores, la QITDraw tiene mecanismos de seguridad implementados que la protegen contra ataques cuando es distribuida, ataques como: copia, omisión de las restricciones de distribución, uso del producto sin la licencia correspondiente, uso del producto en lugares distintos a los autorizados en el convenio UNAM-PEMEX Refinación, extracción parcial y/o total de elementos no públicos y a los cuales el usuario no necesita tener acceso ni conocer para utilizar la herramienta adecuadamente.

a) Definición del problema

Los mecanismos de seguridad actualmente establecidos para la distribución de la herramienta de dibujo QITDraw, han funcionado de manera adecuada, y no se tienen registrados ataques o incidentes que indiquen algún compromiso a la seguridad de la misma. Sin embargo, ya han pasado varios años desde la implementación de estas protecciones, y no se han vuelto a revisar nuevamente, ni tampoco se les ha realizado o aplicado alguna actualización de seguridad. Aunado a lo anterior; un número cada vez mayor de personas utilizan la herramienta y la cantidad de escenarios donde se ejecuta a aumentado considerablemente.

Por lo anterior, es congruente suponer que los mecanismos de seguridad actualmente implementados para evitar ataques en la distribución de la QITDraw ya no son suficientes ni tan efectivos como lo eran al momento de su implementación.

b) Objetivo de la propuesta.

Construir y establecer una propuesta de mejora para la implementación de mecanismos de seguridad informática en la distribución de la herramienta QITDraw para Autodesk® AutoCAD®, empleada en la elaboración de diagramas técnicos. Propuesta que será construida en base a los resultados obtenidos de una metodología de análisis de riesgos informáticos generada, adaptada y aplicada a las necesidades del problema definido, así como a algunas referencias consideradas y tomadas de normatividad internacional para la seguridad de la información.

b.1) Objetivos específicos de la propuesta

Objetivo 1: Proponer, adaptar y aplicar una metodología de análisis de riesgos informáticos al proceso de distribución de la QITDraw, para identificar y evaluar los riesgos de seguridad que existen actualmente.

Objetivo 2: Tomar los resultados obtenidos en el análisis de riesgos informáticos y algunas referencias extraídas de la normatividad internacional para la seguridad de la información, como la base para construir e implementar una propuesta de mejora para los mecanismos de seguridad en el proceso de distribución de la QITDraw, que sea capaz de manejar los riesgos existentes y también proporcione tres servicios de seguridad: confidencialidad, integridad y disponibilidad.

Objetivo 3: Verificar que la propuesta de mejora es adecuada y capaz de manejar los riesgos de seguridad para el proceso de distribución de la QITDraw, que los primeros mecanismos de seguridad no lograron manejar.

c) Marco de desarrollo

La QITDraw fue desarrollada a mediados del año 2005 por el grupo CEASP^{4}A para PEMEX Refinación cuando se vio la necesidad de un aumento en la productividad de diagramas técnicos realizados en AutoCAD®, específicamente, diagramas de isométricos de tubería y dibujos de secciones de equipos para inspección técnica, lo anterior debido a la gran cantidad de información que era necesario procesar y digitalizar.

Los convenios de colaboración UNAM-PEMEX Refinación han continuado concretándose desde entonces, y con esto, la exigencia de una herramienta que realice cada vez más funciones, tenga soporte para las últimas versiones de AutoCAD® y sea segura cuando se distribuya, mientras los convenios sigan y permanezcan vigentes.

El trabajo de la siguiente tesis, se desarrollará dentro del instituto de ingeniería de la UNAM; en el ala norte del cuarto piso de la Torre de Ingeniería (TI), como una parte de los proyectos de actualización de la QITDraw en lo referente a la seguridad para su distribución, en colaboración con el grupo de desarrollo del CEASP^{4}A.

d) Metodología a utilizar

La primera parte de la metodología a utilizar es un *análisis de riesgos informáticos*, por ser una *herramienta* útil en: la identificación y evaluación de los riesgos existentes así como de los controles de seguridad existentes, que sistemáticamente conduce posteriormente a lograr un manejo adecuado de los mismos, tras la implementación nuevos controles de seguridad y el mantenimiento de los que ya están implementados para proporcionar un nivel de seguridad adecuado a los activos de interés, manteniendo un balance costo-beneficio.

Para generar la metodología de análisis de riesgos informáticos adaptada y aplicada a las necesidades del problema definido en esta tesis, se emplearán como referencia algunos de los pasos para la evaluación de riesgo descritos en el estándar para la seguridad de la información *ISO/IEC 27001:2005*, algunas de las directrices ofrecidas para la gestión del riesgo de seguridad de la información en la norma para la seguridad de la información *ISO/IEC 27002:2005*, y en lo descrito para el tema *Análisis del Riesgo* (López, M. J. y Quezada C., 2006, a).

Como partes complementarias a la construcción de la metodología adaptada de análisis de riesgos informáticos, se utilizarán también algunos de los conceptos para la administración del riesgo definidas en la *Metodología AVS, Metodología de Análisis de Vulnerabilidades De Seguridad* (Security Vulnerability Analysis Methodology, SVA Methodology), (CCPS, 2003).

También se hará uso de una matriz de riesgos construida con base en lo descrito por el método *Consideraciones Posteriores del Análisis*, (Analysis Follow-Up Considerations), (CCPS, 1992). Aunque las metodologías anteriores son aplicables para el estudio de riesgos en procesos industriales, tienen puntos en común con las metodologías de análisis de riesgos informáticos, por tal razón se considera que las metodologías de riesgos de procesos pueden complementar a las utilizadas para evaluación de riesgos de software, principalmente en la forma de manejar e interpretar los resultados, proceso para el cual, existe mayor experiencia en las metodologías de estudio de riesgos industriales.

En lo que respecta a la otra parte de la propuesta de mejora, la proporción de tres servicios de seguridad; se contemplarán los controles adicionales propuestos en base a los resultados del análisis de riesgos para determinar qué servicios de seguridad proporcionan. En caso de que los controles adicionales manejen adecuadamente los riesgos pero aún exista la ausencia de uno o más servicios de seguridad, se adecuarán controles adicionales para solucionar lo anterior. Para lograr esto, se emplearán los conceptos y los métodos indicados por López, M. J. y Quezada C. (2006, b); debido a que éstos últimos se encuentran basados en la norma ISO/IEC *27002*:2005, la cual contiene prácticas y métodos fundamentales de seguridad considerados como los mejores a nivel mundial, y porque además es un estándar que contempla los avances tecnológicos en lo referente a las T.I.

Para ofrecer los servicios de confidencialidad e integridad de contenido, se hará uso de algoritmos criptográficos simétricos y asimétricos según sea requerido. Cabe mencionar, que no se tratan a profundidad los tópicos correspondientes al funcionamiento de los algoritmos ni tampoco se programará o construirá ninguno de ellos, solo se emplearán según se requiera, los métodos y las funciones criptográficas existentes en el *Framework* (infraestructura digital) .NET versión 3.5 de Microsoft®. En lo referente al servicio de disponibilidad; se realizarán recomendaciones y aprovecharán las oportunidades de mejora sobre los procedimientos existentes para este servicio y se propondrán nuevos que ayuden a dar continuidad al proceso de distribución de la herramienta de dibujo QITDraw.

Cuando la propuesta de mejora se concrete, el siguiente paso que se llevará a cabo es el de su implementación, para lo cual se utilizarán técnicas de programación estructurada y orientada a objetos empleando el *entorno de desarrollo integrado* (IDE) de Microsoft®, Visual Studio 2008®, junto con el lenguaje de programación de alto nivel Visual Basic. La razón por la que estas herramientas fueron seleccionadas para la implementación de la propuesta, es porque cuentan con la plataforma .NET y un lenguaje de programación de alto nivel que resultan ser totalmente compatibles con la plataforma para desarrollo de aplicaciones de AutoCAD® (su API para .NET) y también porque la QITDraw está desarrollada en esta plataforma y con esta tecnología.

Por último, con el apoyo del jefe del grupo de soporte técnico, el del grupo de desarrollo y el director de proyectos del CEASP^{4}A, se verificará y realizará de manera formal; la evaluación de los casos del análisis de riesgo, la determinación de los casos de mayor riesgo, la implementación de la propuesta de mejora y las conclusiones sobre la misma (aplicando nuevamente los cuatro últimos pasos del análisis de riesgos informáticos adaptado).

e) Resultados esperados

Se espera que los resultados obtenidos del análisis de riesgos informáticos aplicado al proceso de distribución de la QITDraw, revelen las situaciones de riesgo más importantes y que requieran cubrirse de inmediato.

Se espera también que después de realizar la clasificación de los riesgos de seguridad, se pueda utilizar esa información para construir una propuesta de mejora adecuada para los mecanismos de seguridad actualmente implementados, que permita un manejo correcto de los riesgos de seguridad más elevados, que mantenga los riegos residuales a un nivel aceptable y simultáneamente se garanticen también los tres servicios que conforman la tríada de seguridad: confidencialidad, integridad y disponibilidad (López, M. J. y Quezada C., 2006, n).

CAPÍTULO 1

PROGRAMACIÓN PARA AUTOCAD 2010/2011

AutoCAD es un programa de Diseño Asistido por Computadora para el dibujo de precisión que ofrece herramientas para trabajar con sencillez, exactitud y rapidez. Es un programa líder a nivel mundial en la categoría de software CAD, el cual se ha vuelto una herramienta básica en el diseño mecánico e industrial (González, L., 2009).

Otra característica que posee AutoCAD es la de permitir su personalización mediante su API para .NET y la interacción de cuatro lenguajes de programación con la misma (AutoLISP, Visual LISP, Visual Basic (VBA) y C++ (ObjectARX/ObjectDBX) para realizar desde aplicaciones que resuelven tareas simples, repetitivas y tediosas, hasta complejas extensiones especializadas en cualquier campo del diseño asistido por computadora (Autodesk®, 2012).

1.1. Fundamentos de programación

Programar es crear (escribir en algún lenguaje de programación) un software de computadora (conjunto concreto de instrucciones que un equipo de cómputo puede ejecutar). Un programa normalmente se encarga de implementar un algoritmo (secuencia no ambigua, finita y ordenada de instrucciones que arroja un resultado) a un lenguaje de programación concreto para resolver uno o varios problemas específicos. Es posible definir un lenguaje de programación como un dialecto (conjunto de convenciones utilizadas para comunicarse), a través del cual el hombre puede comunicarse con las máquinas. La tendencia de la evolución de los lenguajes de programación se ha ido encaminando hacia la creación de lenguajes orientados a que las personas puedan interpretarlos de manera cada vez más natural, tal y como ocurre con el leguaje hablado; este tipo de lenguajes se les conoce como lenguajes de programación de alto nivel; ejemplos de este tipo de lenguajes son Visual Basic, C#, Phyton entre otros (Segura, J., 2005).

Es importante considerar que el desarrollo de programas, al igual que los lenguajes de programación, ha sufrido muchos cambios; los primeros programas enfocaban todo el esfuerzo en desarrollar y resolver todo tipo de cálculos algebraicos, después surgió el modelo relacional, constituido principalmente por una fuerte base algebraica (precursor del desarrollo y estructuración de las bases de datos) y posteriormente, el tercer gran cambio sobre el desarrollo de software fue la aparición del paradigma de programación, orientados a objetos. Con estos acontecimientos, la escritura de software pasa a ser una tarea no sólo de codificación algorítmica sino también de estructuración del problema; donde ahora la abstracción y el modelado de objetos adquieren una gran importancia para concretar correctamente la resolución de problemas (Segura, J., 2005).

Un programa tradicional, que sigue el paradigma estructurado (programación estructurada), se basa fundamentalmente en la ecuación de Wirth:

Programas = Algoritmos + Datos

De esta ecuación se deduce que los algoritmos y los datos se tratan por separado, de esta forma, las funciones o procedimientos que tratan estos datos los van procesando y pasando de unos a otros hasta obtener el resultado deseado.

Por otro lado, la Programación Orientada a Objetos (POO) gira precisamente, en torno al concepto de objetos (entidades que tienen atributos particulares, datos y formas específicas de interactuar sobre ellos). Durante la ejecución del programa, los objetos reciben y envían mensajes a otros objetos que a su vez, realizan otras acciones (Segura, J., 2005).

1.2. Programación Orientada a Objetos (POO)

En la programación orientada a objetos existen dos elementos fundamentales; las clases (generalización de los objetos) y los objetos (concreción de la clase). La POO es un paradigma (esquema formal) que representa un cambio de perspectiva con respecto a la programación estándar por procedimientos (estructurada), donde cambia la idea de pensar en el flujo del programa desde el inicio hasta el fin del mismo, por la creación y el diseño de objeto; como los componentes independientes de una aplicación que tienen funcionalidad privada y funcionalidad que es posible exponer al usuario. Lo cual permite crear programas que se pueden mantener fácilmente, modificar cuando se requiera y reutilizar para la resolución de otros problemas (Microsoft® Corporation, 2012).

Aparte de las de las clases y los objetos, la POO envuelve otras cuatro propiedades fundamentales que es importante mencionar para el entendimiento cabal de la definición de este paradigma de programación.

A continuación se listan y explican brevemente las 4 propiedades de las que se menciono su existencia (Segura, J., 2005), posteriormente, se realiza una definición propia de POO:

1. Abstracción: Capacidad que posee un objeto para cumplir sus funciones independientemente del contexto en el que se le utilice, es decir, siempre expondrá sus mismas propiedades y arrojara los mismos resultados a través de sus eventos sin importar el ámbito donde sea creado.

2. Encapsulamiento: capacidad del objeto para responder a peticiones a través de sus métodos sin la necesidad de exponer sus propiedades o los medios utilizados para llegar a los resultados que arroja.
3. Herencia: característica por la cual los objetos se establecen a partir de una clase base de la que heredan todas sus propiedades, métodos y eventos (los cuales pueden o no ser implementados y/o modificados) al momento de su creación.
4. Polimorfismo: capacidad para que más de un objeto pueda ser creado mediante la utilización de la misma clase base.

Entonces, la programación orientada a objetos es un paradigma de programación donde se define una plantilla o clase que describe las características (atributos o propiedades) y el comportamiento (como proceden o cómo interactúan) un conjunto de objetos (instancias o representaciones concretas y especificas de la clase) similares para diseñar aplicaciones y programas informáticos.

1.3. El API para .NET de AutoCAD 2010/2011

La API para .NET es una es una fuente de código basado en la especificación destinada a ser utilizada como una interfaz de componentes de software para comunicarse entre sí. El API para .NET de AutoCAD 2010 y 2011 incluye especificaciones para varias rutinas, funciones y las librerías correspondientes que permiten añadir funcionalidad extendida al programa principal (Autodesk®, 2012).

El API para .NET de AutoCAD 2010 y 2011 permite manipular al propio programa, así como a los dibujos del mismo mediante los recursos de ensamblado y las librerías que están expuestas. La exposición de estos objetos permite el acceso a los mismos, por parte de una gran diversidad de lenguajes así como entornos de desarrollo de programación. Existen varias ventajas cuando el API para .NET de AutoCAD 2010 y 2011 es implementado (Autodesk®, 2012), por mencionar algunas:

- La apertura programática para los dibujos de AutoCAD en muchos entornos de desarrollo. Antes de la API para .NET, los desarrolladores se limitaban solo a programación con controles ActiveX® automatizados y a lenguajes de programación que soportaban COM, AutoLISP® y C++ con ObjectARX.
- La integración con otras aplicaciones para Windows como Microsoft® Excel® y Word® se hace considerablemente más fácil mediante la aplicación nativa del API para .NET o la librería expuesta ActiveX/COM.
- Un Framework .NET disponible para sistemas operativos de 32 y 64 bits.
- El acceso a interfaces de programación avanzadas, con una curva de aprendizaje más baja que la de los lenguajes de programación más tradicionales como C + +.

1.3.1. Librerías del API para .NET de AutoCAD 2010/2011

Las librerías del API para .NET de AutoCAD 2010/2011 es donde se encuentran todos los recursos (variedad de clases, estructuras, métodos, y eventos) que permiten la programación de las aplicaciones extendidas del propio software (Autodesk®, 2012). En el **Apéndice 1** de esta tesis, se muestra el código fuente de un programa que realiza la ejecución de comandos en AutoCAD a partir de una subrutina.

El API para .NET de AutoCAD está compuesto por tres diferentes librerías con extensión de archivo “DLL”, las cuales proveen acceso a los objetos hacia un archivo de dibujo o incluso hacia el propio AutoCAD. Cada archivo DLL define diferentes espacios de nombre, los cuales son utilizados para organizar los componentes de las librerías, esta organización se basa en la funcionalidad que cada uno de ellos es capaz de proveer (Autodesk®, 2012). Las tres librerías mencionadas en el API para .NET de AutoCAD son las siguientes:

- AcDbMgd.dll. Esta librería se utiliza cuando se trabaja con objetos en un archivo de dibujo.
- AcMgd.dll. Esta librería se utiliza cuando se trabaja directamente con el propio AutoCAD.
- AcCui.dll. Esta librería se utiliza cuando se trabaja con archivos de personalización del ambiente de trabajo.

1.3.2. Creación de archivos DWF

El nombre de este tipo de archivos viene del acrónimo en el idioma inglés de *Design Web Format*, o *Drawing Web File* (Formato de diseño Web o Archivo de Dibujo para la Web). Formato abierto (de código libre) y seguro, desarrollado específicamente para compartir datos complejos de CAD; la creación de archivos DWF está integrada nativamente (desde el diseño de la aplicación se contemplo esta característica) en AutoCAD así como en varios otros programas de diseño de Autodesk. Éste formato, es capaz de permitir a los usuarios publicar en internet datos de diseño complejos con un solo clic (Autodesk®, 2012).

CAPÍTULO 2

FUNDAMENTOS DE SEGURIDAD INFORMÁTICA

Antes de comenzar la definición de conceptos de seguridad informática necesarios para la estructuración de esta tesis, la primera pregunta que se planteará es: ¿Qué es? y ¿Por qué es importante la seguridad informática? Es posible definir a la seguridad informática (con base en la definición de diccionarios y conocimientos previos propios) como el área de la informática enfocada a proteger la integridad y privacidad de la infraestructura computacional y todo lo relacionado con ella (esto incluye la información), mediante diversas técnicas, aplicaciones y dispositivos.

Para responder la segunda cuestión de manera sencilla, se sabe que desde tiempos muy remotos el hombre ha resguardado y protegido sus conocimientos (información) debido a las ventajas y el poder que éstos son capaces de producir sobre otros hombres o sociedades, lo cual define la premisa de que el *saber es poder* (López, M. J. y Quezada C., 2006, c).

En la antigüedad surgen las bibliotecas, lugares donde se podía resguardar, transmitir o evitar que la información fuera obtenida por cualquiera, dando así unas de las primeras muestras de protección a la información. Con el paso del tiempo y el incremento de las T.I., el cuidado y la seguridad de la información se ha vuelto un elemento crucial para la humanidad. Por lo tanto y tomando en cuenta la premisa de que quien tiene la información tiene el poder; la seguridad informática (que entre sus actividades tiene la de proteger la información) es muy importante.

Lo siguiente a definir sería el significado de que un sistema sea seguro. De acuerdo con López, M. J. y Quezada C. (2006, d); un sistema o producto de Tecnología de la información (del idioma inglés, Information Technology, IT) es seguro si se puede confiar en que opere como se espera.

Por otra parte, WebFinance Inc. (2012), define a un sistema seguro como: un sistema de cómputo que se encuentra protegido a través de hardware y software especial, políticas, así como prácticas contra corrupción de información, destrucción, intercepción, pérdida o acceso no autorizado. Seis servicios esenciales provistos por un sistema seguro son: confidencialidad, integridad, autenticación, autorización, confidencialidad y no repudio.

Para esta tesis, se considerará que la herramienta de dibujo QITDraw es segura si los mecanismos de seguridad implementados que la protegen contra ataques cuando es distribuida funcionan como se espera.

Acorde con lo dicho por López, M. J. y Quezada C. (2006, c), el segundo activo más valioso después de los recursos humanos en las empresas es la información. Lo valioso de la información frecuénteme radica en quien la posee, y el principio para reducir la inseguridad de la misma es creando conciencia de la importancia que tiene la seguridad de la información, y que para ello es necesario proporcionar confidencialidad, integridad y disponibilidad. Teniendo conocimiento de lo anterior, lo siguiente que se debe conocer es el cómo lograr este objetivo, la seguridad de la información.

López, M. J. y Quezada C. (2006, e) sostienen que lograr la seguridad de la información requiere plantear y elegir cuál o cuáles son las mejores herramientas o el conjunto de ellas que sean capaces de proporcionarla. Llegar a este objetivo implica seguir una metodología secuencial que en general es capaz de dar respuesta a las siguientes tres cuestiones: ¿Qué?, ¿De qué?, y ¿Cómo? se va a proteger un activo al que se le pretende dar seguridad.

Para López, M. J. y Quezada C. (2006, f), un activo es todo aquello (bien tangible e intangible) que es importante y tiene valor para una organización o persona y que necesita protección (datos, infraestructura, hardware, software, personal, información, servicios, etc.).

Mientras que la norma ISO/IEC 27001:2005 toma un activo como: un objeto o recurso de valor empleado en una empresa u organización.

En la presente tesis, un activo es considerado; cada una de las partes que conforman a la herramienta de dibujo de diagramas técnicos (QITDraw), es decir, el código fuente de los comandos, los bloques y las plantillas. Esto se retomará en la sección 5.1.

Al plantear y dar respuesta a la cuestión ¿Qué se quiere proteger?, se identifican los recursos a los cuales se pretende brindar seguridad. Lo más adecuado es desarrollar esta identificación formal de los activos por un grupo de personas compuesto por individuos de cada área de la compañía (o de las áreas que se consideren necesarias) para obtener ventajas en este paso como: visión cabal del valor de los activos, consecuencias de pérdidas, entre otras (López, M. J. y Quezada C., 2006, e).

Al dar respuesta a la cuestión anterior, el siguiente paso es responder la segunda pregunta ¿De qué se quiere proteger?, con el fin de identificar las posibles amenazas, vulnerabilidades y riesgos a los cuales están expuestos los activos identificados en la incógnita anterior.

La seguridad se orienta a ofrecer protección en contra de riesgos; los cuales poseen muchas categorías al igual que las amenazas y se pueden considerar ambos tan exhaustivamente como se requiera. Sin embargo en el campo de la seguridad se otorga mayor atención a individuos relacionados con actividades maliciosas o de tipo humanas principalmente. La protección de los activos es responsabilidad de los dueños junto con especialistas de seguridad informática; que en conjunto pueden analizar todas las posibles amenazas que podrían presentarse. Pero siempre se terminan definiendo cuáles aplican realmente sobre los activos a proteger (López, M. J. y Quezada C., 2006, g).

Después se plantea y da respuesta a la tercera y última cuestión sobre los activos, ¿Cómo se van a proteger?, considerando siempre las respuestas a las preguntas previas, lo sucesivo es determinar la manera en que se protegerán los activos identificados en contra de las amenazas y vulnerabilidades de seguridad identificadas (López, M. J. y Quezada C., 2006, h).

En cuanto a la selección de las herramientas de seguridad necesarias para proteger la información, es correcto seguir algún esquema basado en normas o estándares internacionales, debido a que este tipo de acciones son capaces de brindar mayor confiabilidad, mantener un cierto nivel de garantía y holgura con las necesidades de seguridad. Cabe mencionar que para dar respuesta a las tres preguntas formuladas anteriormente, siempre existirá la aplicación de criterios objetivos y subjetivos, razón por la cual nunca existirán indicadores precisos ni universales para la seguridad IT (López, M. J. y Quezada C., 2006, h).

2.1. Normatividad de la seguridad informática

Las normas son documentos técnico-legales que contienen especificaciones técnicas de aplicación recomendada. Son elaborados por consenso de las partes interesadas y están basadas en los resultados de la experiencia y el desarrollo tecnológico de compañías, sociedades o instituciones especialistas en un área de conocimiento en particular. Para esta tesis, se utilizaron algunos aspectos, lineamientos, sugerencias, referencias y criterios de algunas de las normas internacionales que existen para la seguridad, por ello a continuación se describen brevemente en qué consiste cada una de ellas, un fragmento de su historia, así como los criterios tomados de cada una de ellas.

2.1.1. Estándar ISO/IEC 27001

Es un estándar internacional dirigido al manejo de la seguridad de la información en sistemas, parte de la familia de estándares ISO/IEC 27000, fue aprobado y publicado en octubre del año 2005 por la ISO, y la IEC. Esta norma se encarga de establecer, implementar, mantener y mejorar un “Sistema de Gestión de la Seguridad de la Información” (SGSI) basado en el “Ciclo de Deming”: PHVA (Planificar, Hacer, Verificar, Actuar), metodología nombrada en base al acrónimo en el idioma inglés: *Plan, Do, Check, Act*, (PDCA), es decir, establece los requerimientos y especificaciones de un SGSI, después proporciona los medios para medir, los métodos para realizar el seguimiento correspondiente, y dar control a la administración de seguridad. Su nombre completo es ISO/IEC 27001:2005 - Information security management systems - Requirements.

Esta norma especifica enfoques para varios temas mediante el empleo de la metodología PDCA, entre ellos se encuentra la gestión de riesgo, el cual es un proceso de identificación, análisis, cálculo, evaluación y reducción de riesgo hasta un nivel aceptable, además de la implementación de los mecanismos correctos de defensa para mantener un nivel de riesgo aceptable. Algunas de las acciones y actividades incluidas para esta gestión son:

- Identificación de los activos.
- Identificación de requisitos legales y de negocios, relevantes para lograr el paso anterior.
- Valoración de los activos identificados.
- Definición del impacto de una pérdida de confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades para los activos identificados.
- Evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cálculo del riesgo.
- Evaluación de los riesgos frente a una escala de riesgos.

Después de efectuar los pasos anteriores, se procede a determinar las acciones a tomar respecto a los riesgos identificados, es decir: controlar el riesgo; fortalecer los controles existentes y/o agregar nuevos controles, compartir el riesgo; mediante acuerdos contractuales parte del riesgo se traspasa a un tercero, aceptar el riesgo; se determina que el nivel de exposición es adecuado y por lo tanto se acepta. La norma también sostiene que la administración de riesgo es un proceso continuo que es necesario evaluar periódicamente. (ISO/IEC 27001:2005).

2.1.2. Estándar ISO/IEC 27002

Estándar internacional dirigido al manejo de la seguridad de la información; cuya precursora fue la norma BS 7799, originalmente publicada por el Grupo BSI en 1995, también conocido como la institución británica de estándares (Del idioma inglés: *The British Standards Institution*), organismo proveedor de servicios multinacionales de negocios, principalmente la construcción de estándares y todo lo relacionado con ellos, fundado en 1901 (British Standards Institution, 2012).

La norma BS 7799 fue escrita por el Departamento de Comercio e Industria (Del idioma inglés: *Department of Trade and Industry*, DTI) del gobierno del Reino Unido y estaba constituida por varias partes, la primera parte contenía las mejores prácticas para la administración de la seguridad de la información; revisada en 1998 y luego de largas discusiones con organizaciones mundiales de estándares fue eventualmente adoptada y lanzada por la ISO en diciembre del año 2000 como la ISO/IEC 17799:2000, Tecnología de la Información - Código de prácticas recomendadas para la gestión de la seguridad de la información (Del idioma inglés: *Information Technology - Code of practice for information security management*). Nuevamente en junio 2005 fue revisada y actualizada a ISO/IEC 17799:2005, para después cambiar de nombre e incorporarse a las series de estándares ISO 27000 en julio de 2007 como la ISO/IEC 27002:2005.

Esta norma está constituida a partir de varios conceptos cuyo objetivo central es manejar o administrar la seguridad de la información mediante elementos y clausulas enfocadas a prácticas y métodos fundamentales de seguridad, contemplando siempre los avances tecnológicos, y es uno de los estándares de seguridad de la información más reconocido a nivel mundial (López, M. J. y Quezada C., 2006, i).

El ISO/IEC 27002:2005 define a la información como un activo o recurso de valor que existe en varias formas dentro de una organización que independientemente a lo anterior siempre debe estar propiamente protegida. El objetivo principal de la seguridad de la información es proteger este recurso de una forma oportuna y conveniente de un amplio rango de vulnerabilidades; asegurando la continuidad del negocio, minimizando los daños y maximizando las ganancias de inversión así como de las oportunidades de negocio. (López, M. J. y Quezada C., 2006, i).

En la sección 9 de esta norma; adquisición, desarrollo y mantenimiento de sistemas de información, se pretende asegurar que los controles apropiados del sistema de información se incorporen y mantengan. Algunos de los objetivos de esta sección son:

- Aseguramiento de la construcción de sistemas operacionales.
- Prevención de modificaciones, mal uso o pérdida de los datos en sistemas o aplicaciones.
- Mantenimiento de la Triada de la Seguridad para la información.
- Mantenimiento de la seguridad del software, el sistema y los datos.

Tales objetivos de la sección anterior, son un punto más de referencia para constituir la seguridad de la información. (ISO/IEC 27002:2005).

En conclusión, estas dos normas son parte de la familia de estándares para la gestión o administración de la seguridad de la información. Familia de normas de seguridad de la información publicada conjuntamente por la Organización Internacional de Normalización (*International Organization for Standardization*, ISO) y la Comisión Electrotécnica Internacional (*International Electrotechnical Commission*, IEC). El estándar ISO/IEC 27001 provee los requerimientos para los sistemas de gestión para la seguridad de la información, mientras que el estándar ISO/IEC 27002 es un código de prácticas para la administración de la seguridad de la información.

2.2. Amenazas y vulnerabilidades

De acuerdo con López, M. J. y Quezada C. (2006, j), una amenaza es representada a través de una persona, una circunstancia, un evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación de la seguridad. Por lo tanto, una amenaza es todo aquello que pretende o intenta destruir.

Con base en la definición anterior, se puede considerar una amenaza como una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, al darse una oportunidad, podría dar lugar a una violación de la seguridad (ya sea en la confidencialidad, integridad, disponibilidad).

Para la presente tesis, una amenaza es cualquier persona, evento o circunstancia que intenta, pretende o tiene la posibilidad de ocasionar algún daño o la perdida de los activos de interés de la QITDraw.

López, M. J. y Quezada C. (2006, k) definen vulnerabilidad como un punto del sistema que es susceptible a ser atacado o a dañar la seguridad del mismo, es decir, son las debilidades o aspectos que pueden ser explotados para quebrantar la seguridad del sistema informático.

Paralelamente, la ISO/IEC 27001:2005, define una vulnerabilidad como una debilidad o condición de debilidad que puede ser explotada con la materialización de una o varias amenazas para un activo.

En esta tesis, una vulnerabilidad es una condición de debilidad o deficiencia en los mecanismos de protección para la distribución de la herramienta, que puede ser aprovecha o explotada por alguna amenaza, generando así, una brecha en la seguridad.

2.2.1. Clasificación general de amenazas

Las amenazas de seguridad tienen su origen de diversas fuentes; entre ellas, se consideran cinco: Fuentes de amenazas de humanos, errores de hardware, errores de la red, problemas de tipo lógico y desastres. A continuación se describe cada una de ellas (López, M. J. y Quezada C., 2006, j).

1. **De Humanos:** la amenaza surge por ignorancia, descuido, negligencia o inconformidad cuando se maneja la información. En lo que respecta a esta fuente de amenaza, en la presente tesis se realizan varias consideraciones que se emplean durante el análisis de riesgos; con el fin de concretar la propuesta de mejora que permita cumplir los objetivos de la misma; para las consideraciones posteriores se tomó en cuenta aparte de las definiciones previas, lo descrito por un artículo sobre las amenazas internas de una empresa (Symantec® Corporation., 2011), lo que sostiene un artículo sobre el perfil psicológico de ladrones de datos empresariales (Computerworld., 2011), lo que refiere un artículo sobre considerar a los jefes de las empresas como amenazas (O'Connell, P., 2002) y lo que explican las respuestas a preguntas frecuentes en seguridad en cómputo (Andrade, J., 2011).

a) **Ingeniería social:** ejecutada por una manipulador, es un acto mediante el cual personal sin acceso o con acceso parcial a la herramienta (QITDraw) manipulan a otras personas con el fin de convencerlas para de ejecutar acciones que normalmente no realizan, con el fin de obtener la herramienta de una forma no controlada.

b) **Robo:** ejecutado por ladrones, es un acto en el cual personal que sustrae la herramienta (QITDraw) de su fuente original cuando se distribuye, esto incluye: obtener el código fuente, los bloques, las plantillas o la herramienta completa (sección 5.1 de esta tesis).

c) **Fraude:** ejecutado por fraudulentos, es un acto mediante el cual personal que tiene acceso a la herramienta (QITDraw), realiza distribuciones no controladas de la misma.

d) **Sabotaje:** ejecutado por saboteadores, es un acto mediante el cual personal que tiene acceso a la herramienta (QITDraw), realiza actos deliberados enfocados en dañar la integridad de la misma en sus procesos de distribución.

e) **Negligencia:** llevado a cabo por personas negligentes, ocurre cuando el personal provoca daño de manera no intencionada en el proceso de distribución de los activos por causa de falta de conocimientos o descuidos.

f) **Empleados:** personal interno que labora en la organización, pueden llegar a cometer una violación a la seguridad por desconocimiento o inexistencia de normas básicas de seguridad, aunque también pueden cometer tal acción de manera intencional, afectando así alguna parte del proceso de distribución de la QITDraw.

g) **Ex empleado:** personas interesadas en violar la seguridad de la empresa para la que laboraban, resentidas e inconformes. Poseen conocimiento suficiente sobre los procedimientos de uso y distribución de la herramienta (QITDraw).

h) **Intrusos remunerados:** atacantes poco habituales pero extremadamente peligrosos, son *crackers* (*hackers black hat*) con grandes conocimientos y experiencia en computación, pagados por una tercera parte realizar algún daño al proceso de distribución de la QITDraw. También existen los *hackers gray hat*, que tienen habilidades equiparables a las de un cracker, así como una ética ambigua en lo referente al acceso a información y sistemas para los cuales no tienen la autorización correspondiente (TechTarget., 2003).

2. **Errores de hardware:** la amenaza se origina por fallas físicas presentadas por cualquier elemento de los dispositivos de hardware de la computadora. Los problemas más comunes y frecuentes respecto al suministro de energía son: bajo voltaje, alto voltaje, ruido electromagnético, variación de frecuencia, etc. Igualmente se considera el deterioro o incorrecto funcionamiento, así como cargas estáticas, sobrecalentamiento, y otros más.
3. **Errores de la red:** se presenta una amenaza cuando el flujo de información que va a circular por el canal de comunicación se calcula inadecuadamente, provocando la no disponibilidad de la red. Otro factor importante y que muchas veces no se considera, puede ser la desconexión del canal. En cuanto al aspecto lógico existen diversas amenazas como: monitoreo, escaneo, obtención de contraseñas, denegación de servicio, entre otras. En lo referente al aspecto físico se pueden mencionar amenazas como: interferencia, cables con daños o cortados que pueden afectar la integridad de los datos o la información.
4. **Problemas de tipo lógico:** en esta fuente, la amenaza logra presentarse cuando un diseño bien elaborado de un mecanismo de seguridad se implementa erróneamente (falla al cumplir con las especificaciones de diseño). Otra amenaza de tipo lógico puede ser la comunicación entre procesos si un intruso utiliza una herramienta que le permite el envío y la recepción de información. Cualquier malware que entra a un sistema de cómputo sin ser invitado e intenta romper las reglas se considera una amenaza y entre en el rubro de esta fuente.
5. **Desastres:** estas amenazas surgen de las fuerzas naturales (también conocidas como *Acts of God*, actos de dios, por tratarse de eventualidades que están fuera del control humano), tales como: inundaciones, terremotos, fuego, viento, etcétera. Tales eventos generan amenazas directas que repercuten de manera directa en el funcionamiento de los equipos de cómputo, las redes de datos, instalaciones eléctricas, líneas de comunicación, entre otras.

2.2.2. Clasificación general de vulnerabilidades

Las vulnerabilidades de seguridad se pueden clasificar en seis tipos: físicas, naturales, de hardware, de software, de red y humanas. A continuación se describe cada una de ellas (López, M. J. y Quezada C., 2006, k).

1. **Físicas:** se localizan en el edificio o propiamente en el entorno físico del sistema. Frecuentemente esta vulnerabilidad es relacionada con la posibilidad de acceder físicamente al lugar o donde se encuentran los activos que se quieren modificar, vulnerar o destruir. Este tipo de vulnerabilidad hace referencia a los controles de acceso para un sistema. Para equipos de cómputo se pueden plantear mecanismos de seguridad, lo cual no siempre es suficiente, sin embargo, siempre existe la posibilidad de echar mano de medidas en forma de software que eviten el robo de información (Gómez, A., 2011, a).
2. **Naturales:** se refiere a la magnitud en la que el sistema puede verse afectado por desastres naturales o del ambiente. Ejemplos de este tipo de vulnerabilidades son: no contar con servidores espejo del sistema en otros lugares geográficos en caso de terremotos, inundaciones u otros fenómenos naturales. No disponer de equipos UPS (ver glosario) ni plantas de energía eléctrica alternas; instalaciones eléctricas defectuosas, sistemas de ventilación y de enfriamiento inadecuados, entre otros.
3. **De hardware:** esta vulnerabilidad existe cuando se omitió la verificación de las características técnicas y las especificaciones de los dispositivos físicos, lo cual resulta en incertidumbre sobre la confiabilidad de los mismo, la falta de mantenimiento es otra vulnerabilidad, junto con la adquisición de equipo de mala calidad o el mal uso del mismo, etcétera.

4. **De software:** fallas o debilidades del software del sistema hacen que sea menos confiable. Este tipo de vulnerabilidades abarca los errores de programación del sistema operativo o las aplicaciones, ya sean programas comerciales o hechos por el usuario.
5. **De red:** la interconexión de equipos de cómputo a la red de datos supone un incremento elevado de las vulnerabilidades de los mismos, debido al aumento de la cantidad de gente que puede o intenta tener acceso. Fallas debidas a una mala estructura y diseño del cableado estructurado también entran en esta categoría, al igual que no contar con plantas emergentes para la red o dispositivos de intercambio de placas de cableado estructurado completo.
6. **Humanas:** en lo que respecta a esta clasificación de vulnerabilidad, se tomó en cuenta lo descrito por López, M. J. y Quezada C. (2006, l), junto con un artículo sobre el tema, ingeniería social (Sandoval, E., 2011). Ser susceptible a ingeniería social e inversa, la contratación de personal sin un perfil psicológico adecuado y con poca ética, falta de personal para cumplir cabalmente con las tareas requeridas en la organización, descuidos, cansancio, maltrato del personal, un servicio técnico poco confiable, pocos controles de acceso, no contar con registro del personal, personal no autorizado, etcétera. Son algunas de las vulnerabilidades que se encuentran dentro de esta clasificación.

2.3. Métodos de ataque

Gómez Vieites, define un ataque como la conclusión o la culminación de una amenaza, que origina pérdidas totales o parciales (Gómez, A., 2011, b).

La metodología AVS define a un atacante como: una persona mal intencionada que desea hacer algún tipo de daño sobre los activos a proteger, varios sinónimos son utilizados para referirse a estas personas, entre ellos; perpetradores, los enemigos a vencer, aquel que convierte las amenazas en vulnerabilidades (CCPS, 2003).

Para esta tesis, un atacante es cualquier persona que representa una amenaza para los activos a proteger durante el proceso de distribución de la herramienta.

López, M. J. y Quezada C. (2006, m)**,** proponen una división de tres etapas para un ataque a un sistema de cómputo, las cuales son:

1. **La preparación y el planteamiento:** etapa en la que se definen los objetivos que se desean lograr con el ataque, se realiza la recolección de información útil para los propósitos previamente establecidos, se define el método de ataque que será utilizado, la fecha y el lugar en que se realizará, así como para quien va dirigido.
2. **La activación:** es la segunda etapa del ataque, se realiza de tres formas principales; ocurre una interrupción el sistema y si no es factible, entonces se utiliza un programa que lleve a cabo la misión de manera directa. Un ataque más sofisticado implica un retardo entre la preparación y la activación. Y finalmente, otra forma de activación puede ser una bomba de tiempo lógico.
3. **La ejecución o culminación:** es la última etapa y aquí se identifican los daños y las pérdidas (parciales o totales) que causó el atacante. En la tercera etapa, las misiones del ataque adquieren gran diversidad, a continuación se me mencionan algunas.

- Mal uso activo: Se afecta directamente la integridad de la información o la disponibilidad de los servicios.
- Mal uso pasivo: Se afecta directamente la confidencialidad, pero el estado del sistema no es afectado.
- Denegación de servicio: Son los más fáciles de realizar, la red es saturada con tráfico, es cualquier situación que niega el servicio.
- Robo del servicio: Los atacantes roban los servicios de cómputo y de comunicación de los sistemas que logran perpetrar.
- Ataques a los escudos: Pueden clasificarse en tres tipos y son técnicas avanzadas
- Autenticación: El intruso es capaz de pasar los controles de conexión, y utilizar una contraseña para autenticarse.
- Ataques por debajo del nivel del escudo: Cuando existen controles de acceso antes de los activos de interés, lo que se ataca no son los controles, sino las transacciones que llaman a estos.
- Compromiso del cifrado: Algunos métodos de este tipo son efectivos con las claves de cifrado pertinentes, si no lo son, el método de cifrado puede comprometerse, y con ello, la información. Existen problemas cuando los métodos de cifrado son mal implementados o mal diseñados.
- Destrucción de evidencia: Ocurre cuando los registros de eventos, sucesos o monitoreo son alterados, destruidos o desviados.
- Subversión de los controles de aplicación: cuando los escudos operan en el nivel de aplicación, se pueden explotar las debilidades de estos controles para ganar acceso a la información que se desea proteger.

2.4. Servicios de seguridad

Un servicio de seguridad es el segundo aspecto más importante a considerar en la seguridad informática (el primero es un ataque); un servicio de seguridad es aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización. Estos servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad lograrlo (López, M. J. y Quezada C., 2006, n).

López, M. J. y Quezada C. (2006, o) definen control como: los protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de una organización.

Por otro lado, el estándar ISO/IEC 27001:2005, define control como: un mecanismo de seguridad de prevención y corrección empleado para disminuir las vulnerabilidades. Para esta tesis, un control es un mecanismo de protección para los activos que contrarresta a las amenazas y disminuye las vulnerabilidades que afectan a las mismas.

2.4.1. Clasificación de los servicios de seguridad

Los servicios de seguridad se pueden clasificar en seis: confidencialidad, integridad, disponibilidad, autenticación, control de acceso y no repudio. A continuación se describe cada uno de ellos (López, M. J. y Quezada C., 2006, p).

1. **Confidencialidad:** capacidad de asegurar que solo el personal autorizado tiene acceso a algo, es un aspecto primario de la seguridad, su principal objetivo es mantener la información secreta para proteger los recursos y la información contra el descubrimiento intencional o accidental por personal no autorizado. La posesión de una llave permite la autenticación y la autorización, por consiguiente, la confidencialidad. Existen personas que desean tener acceso a la información no autorizada y a los recursos por varias razones como: adquirir ventajas competitivas, publicidad, venganza, entre otras. La criptografía es utilizada para proveer los servicios de confidencialidad. Todos los métodos de cifrado basados en la criptografía son los mecanismos de seguridad para proporcionar este servicio.
2. **Autenticación:** es un servicio que se encarga de verificar la identidad, trata siempre de asegurar una comunicación autentica. Su objetivo principal es asegurar al receptor que el mensaje proviene una fuente autentica (de la fuente de la que se espera el mensaje). La autenticación es realizada principalmente por medio de; algo que se sabe (contraseñas, números identificadores, etc.), algo que se tiene (tarjetas, chips, etc.), algo que se es (la voz, la retina, huellas digitales, entre otras.
3. **Integridad:** es aquel servicio que provee controles que aseguran que el contenido de los datos no haya sido modificado. Si no existe la integridad cualquier persona puede manipular los datos según su conveniencia. Existen dos distinciones del servicio; con recuperación y sin recuperación. Ya que es un servicio orientado a contrarrestar ataques activos, el sistema detecta las intrusiones y si tiene recuperación corregirá automáticamente la falla, de lo contrario una intervención humana seria requerida. Los servicios de integridad se pueden ofrecer mediante varios mecanismos de seguridad, dos ejemplos son: el código de detección de modificación; que es una suma de comprobación de los datos, generada utilizando algún algoritmo criptográfico y la firma digital; una pieza de información asociada con los datos que únicamente puede ser creada por el firmante y puede ser verificada por cualquier persona.

4. **No repudio:** es un servicio que previene a los emisores o a los receptores de negar un mensaje transmitido. Las firmas digitales también son utilizadas por tener la propiedad de que pueden ser creadas únicamente por los firmantes y verificadas por cualquiera.
5. **Control de acceso:** servicio que se encarga de identificar y autenticar a una persona o entidad de manera exitosa para conceder acceso.
6. **Disponibilidad:** este servicio ocurre cuando las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces como sea necesario. Únicamente se refiere al tiempo para obtener la información, no importa si la información es correcta o no. Para ello siempre deben existir soluciones alternas, como respaldos actualizados, de servicios propios o externos, y planes de continuidad.

2.5. Análisis de riesgos

De acuerdo con López, M. J. y Quezada C. (2006, f), no existe la seguridad total, por lo tanto las medidas y los mecanismos de seguridad no pueden asegurar el 100% de la protección contra las vulnerabilidades, por ello en cualquier es imprescindible para cualquier organización realizar periódicamente un análisis de riesgos con el fin de identificar las consecuencias probables o los riesgos asociados a las vulnerabilidades, para así lograr un manejo adecuado de los mismos tras la implementación y el mantenimiento de los controles de seguridad que reduzcan los efectos negativos a un nivel aceptable.

Un análisis de riesgos es un procedimiento para estimar el riesgo de los activos de cómputo relacionados y la pérdida debido a la manifestación de las amenazas (López, M. J. y Quezada C., 2006, f).

La fórmula para determinar el riesgo total es:

Riesgo = (Clasificación de frecuencia / probabilidad) x (Daño del acontecimiento)

Por otra parte, la norma ISO/IEC 27001:2005 sostiene que un análisis de riesgos es una metodología que permite el uso sistemático de la información disponible. Para dar al manejo del riesgo la información necesaria para formular juicios de valor sobre la seguridad de la información de la organización. Este procedimiento identifica los controles de seguridad existentes, calcula las vulnerabilidades y evalúa la relación amenaza-vulnerabilidad en cada área de estudio. Buscando siempre la relación costo-beneficio sobre las soluciones de seguridad destinadas a manejar el riesgo.

2.5.1. Definición de conceptos básicos

En esta sección se establecen conceptos considerados fundamentales para comenzar a describir la metodología de análisis de riesgos (López, M. J. y Quezada C., 2006, q):

- Riesgo: Posibilidad de ocurrencia de algún daño o perdida. Probabilidad de ocurrencia de un evento desfavorable que puede ocasionar un daño potencial a servicios, recursos o sistemas de una empresa. (ISO/IEC 27001:2005).
- Impacto: Perdidas como resultado de la manifestación de una amenaza Evaluación del riesgo: comparación de los resultados de un análisis de riesgos con criterios estándares u otros criterios de decisión.

- Manejo del riesgo: identificación, control y minimización o eliminación de riesgos de seguridad por un costo aceptable.
- Aceptación del riesgo: decisión para aceptar cierto riesgo.
- Perdida esperada: impacto anticipado y negativo sobre los activos debido a una amenaza materializada.
- Riesgo residual: nivel de riesgo que sobra después de considerar todas las amenazas, vulnerabilidades y las medidas necesarias de seguridad, este se acepta o si es muy alto se busca reducirlo.
- Recomendación: Es la identificación de controles adicionales después de haberse identificado un riesgo residual.

2.5.2. Tipos de análisis de riesgos

El proceso para determinar los controles de seguridad más apropiados y rentables es frecuentemente una cuestión complicada y subjetiva. Por ello metodologías sistemáticas como el análisis de riesgo adecuan estas cuestiones sobre una base más objetiva. A continuación se definen los dos tipos esenciales de análisis de riesgos (López, M. J. y Quezada C., 2006, r):

- Análisis cuantitativo: en este tipo de análisis todos los activos, recursos y controles, se identifican y evalúan en términos económicos. Todas las amenazas potenciales se identifican y se estima la frecuencia de ocurrencia, para posteriormente compararlas con las vulnerabilidades con el fin de identificar las áreas más sensibles.

- Análisis cualitativo: en vez de establecer valores exactos se dan notaciones como alto, bajo, medio, etc. Que representan la frecuencia de ocurrencia y el valor de los activos. Uno de los problemas de este tipo de análisis son los consensos y las jerarquizaciones que deben realizarse con la información, los controles y las decisiones sobre su valor. A pesar de ello, este método siempre es más recomendable cuando no se cuenta con una forma precisa de determinar tiempos de frecuencia o causas económicas de los activos.

Un ejemplo de una escala de riesgo, útil para el análisis cualitativo es que se presenta en la tabla 1.

Tabla 1. Escala de riesgo (López, M. J. y Quezada C., 2006, q)**.**

Cálculo del riesgo de incidencias por año	Clasificación
0	Ninguna
1-3	Baja
4-7	Media
8-14	Alta
15-19	Crítica
20-30	Extrema

Otras escalas para el uso sistemático de la información, también útiles para describir el riesgo son las contenidas en la tabla 2 y en la 3.

Tabla 2. Impacto del acontecimiento (López, M. J. y Quezada C., 2006, q)**.**

Daño del acontecimiento	Grado del daño	Clasificación
Insignificante	Sin Impacto	0
Menor	No se requiere un esfuerzo extra para reparar	1
Significante	Daño tangible, esfuerzo extra requerido para reparar	2
Dañino	Gasto significante requerido de recursos Daño a la reputación y a la confianza	3
Serio	Perdida de la conexión compromiso de grandes cantidades de datos o servicios	4
Grave	Apagado permanente, compromiso total	5

Tabla 3. Frecuencia de ocurrencia de un acontecimiento (López, M. J. y Quezada C., 2006, q)**.**

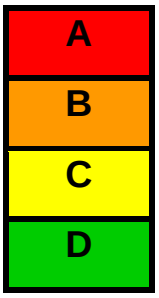
Acontecimiento	Frecuencia	Clasificación
Insignificante	Sin probabilidad de que ocurra	0
Muy Bajo	2-3 veces cada 5 años	1
Bajo	< = una vez por año	2
Medio	< = una vez cada 6 meses	3
Alto	< = una vez por mes	4
Muy Alto	= > una vez por mes	5
Extremo	= > una vez por día	6

En otro contexto similar, dentro de la disciplina de Seguridad de Procesos en la Industria Química, existe matriz de riesgos creada por el Center for Chemical Process Safety (CCPS) del American Institute for Chemical Engineers (AIChE), que para esta tesis se adaptará y posteriormente en la sección 4.1.7 se explicará la manera en que será utilizada.

		Frecuencia / Probabilidad del evento			
		Improbable	Posible	Ocasional	Frecuente
Gravedad de las consecuencias	Catastrófico	**C**	**B**	**A**	**A**
	Mayor	**D**	**C**	**B**	**A**
	Critico	**D**	**D**	**C**	**B**
	Importante	**D**	**D**	**D**	**C**

En la matriz anterior existen cuatro categorías de riesgo que funcionan como un indicador de posibles acciones a realizar dependiendo cual ocurra:

Categorías de riesgos



- Inaceptable – Atención inmediata, alta prioridad.
- Indeseable – Introducir medidas de control con prioridad media.
- Aceptable con controles – Verificar las medidas de control existentes.
- Aceptable como está – No requiere medidas de control.

En cuanto a las categorías de Frecuencia / Probabilidad del evento, también serán definidas en la sección 4.1.7 como parte de la metodología adaptada del análisis de riesgos propuesta en esta tesis.

2.5.3. Objetivos del análisis de riesgos

De acuerdo con López, M. J. y Quezada C. (2006, q), algunos objetivos esenciales de los análisis de riesgos son:

- Identificar, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un recurso a una amenaza determinada.
- Determinar que combinación de medidas de seguridad proporcionan un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones en seguridad de la información.
- Enfocar recursos y esfuerzos en la protección de los activos.

2.5.4. Tipos de controles para el análisis de riesgos

En la sección 2.4 ya se realizó la definición de un control, para tener un panorama adecuado al momento de elegir los controles adicionales después de haber realizado el análisis de riesgo, es útil conocer que existen diversos tipos de controles, cada uno con metas particulares. A continuación y de acuerdo a la clasificación de López, M. J. y Quezada C. (2006, r), existen cuatro tipos de controles principales:

- Controles disuasivos: reducen la posibilidad de un ataque deliberado.
- Controles preventivos: protegen vulnerabilidades y hacen que un ataque fracase o reduzca su impacto.
- Controles correctivos: reducen el efecto de un ataque.
- Controles detectores: descubren ataques y disparan controles preventivos o correctivos.

2.5.5. Pasos para el análisis de riesgos

Con todos los antecedentes señalados previamente, ahora es posible comprender los pasos que se llevan a cabo en un análisis de riesgo. Es recomendable que un análisis de riesgos siempre indique: niveles actuales de riesgo, las consecuencias probables y las acciones posteriores para contrarrestar los riesgos residuales altos. Para la que la metodología resulte útil, siempre se debe buscar el lograr: balance al momento de mitigar un impacto en lo referente al costo, medir la efectividad real de los controles del lugar y ofrecer una serie de recomendaciones de valía y que realmente sirvan para corregir o minimizar los riesgos identificados.

En concordancia con lo sostenido por López, M. J. y Quezada C. (2006, s) a continuación se describen los pasos para realizar un análisis de riesgos informáticos:

1. Identificación y evaluación de los activos: el primer paso es identificar y asignar un valor a los activos que necesitan protección. El valor de estos es un factor significante en la toma de decisiones para realizar cambios operacionales o incrementar la protección de los mismos. Su valor radica frecuentemente en su costo, sensibilidad, misión crítica o la combinación de algunas o todas las propiedades mencionadas.
2. Identificación de las amenazas correspondientes: el segundo paso consiste en identificar y examinar (describir) las amenazas que afecten a los activos, para determinar cuál sería la pérdida si estas últimas se presentaran.
3. Identificación y descripción de las vulnerabilidades: el nivel de riesgo se determina analizando la relación entre las amenazas y las vulnerabilidades. Un riesgo existe cuando una amenaza tiene una vulnerabilidad correspondiente asociada.
4. Determinación del impacto de la ocurrencia de una amenaza: cuando la explotación de una amenaza ocurre, los activos sufren cierto impacto, este paso consiste en determinar la magnitud de ese impacto.
5. Controles del lugar: La identificación de los controles es parte del proceso de recolección de datos para cualquier proceso de análisis de riesgos.
6. Determinación de los riesgos residuales (conclusiones): siempre existirán riesgos residuales, por lo que se debe determinar cuando estos son aceptables o no, en este paso se decide esa situación sobre estos riesgos.
7. Identificación de los controles adicionales (recomendaciones): Una vez determinados los riesgos residuales, lo siguiente es identificar la forma más efectiva y menos costosa para reducirlos a un nivel aceptable.

8. Preparación de un informe del análisis de riesgo: Son las conclusiones y el reporte final del proceso de evaluación de riesgos, que contiene en general la identificación de riesgos residuales y su evaluación, el resultado sobre la efectividad de los controles actuales. Lo cual permite comenzar con la selección necesaria de los controles adicionales.

Es importante mencionar que para cuatro de los incisos mencionados de la metodología anterior (determinación del impacto de la ocurrencia de una amenaza, controles del lugar, determinación de los riesgos residuales e identificación de los controles adicionales); en otro contexto similar, para la disciplina de Seguridad de Procesos en la industria química, en la en la Metodología AVS*,* existe una parte llamada *cuantificación de los riesgos*; la cual tiene la ventaja de llevar a cabo los cuatro pasos mencionados de manera cuasi simultánea, la forma para realizar esta parte de la metodología es la siguiente (CCPS, 2003):

1. Realizar una matriz que contenga cinco columnas y tantas filas como se requiera.
2. La primera columna contendrá la descripción de la relación de la amenaza con su respectiva vulnerabilidad.
3. La segunda columna deberá subdividirse en otras 3 columnas que contengan: un índice de impacto del acontecimiento, un índice de frecuencia de ocurrencia del acontecimiento (determinado en base a escalas definidas en la misma metodología AVS) y también un índice de riesgo (que se obtiene de la matriz de riesgos creada por el CCPS del AIChE, mencionada en la sección 2.5.2). Estos índices deben ser calculados sin considerar ningún control de seguridad aunque existan.
4. La tercera columna deberá contener el tipo de controles con los que se cuenta para proteger a los activos de interés.

5. La cuarta columna se construye de manera análoga a la columna definida en el inciso c, y se recalculan el impacto y los índices definidos, pero ahora si tomando en cuenta los controles existentes.
6. Finalmente en la quinta columna; en base a los resultados obtenidos, y refiriéndose a la matriz de riesgos del CCPS para ver la categoría de riesgo, se realiza o no la propuesta de controles adicionales (recomendaciones).

A continuación en la tabla 4, se muestra un ejemplo de una posible matriz conformada de acuerdo con lo descrito por una de las partes de la metodología *cuantificación de los riesgos*.

Tabla 4. Ejemplo de una matriz construida para una parte de la Metodología AVS (cuantificación de los riesgos) (CCPS, 2003)**.**

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E-R+H-PSPPA	4	4	A	Correctivo:	3	1	B	
E-R+H-PSIS	3	4	B	Detector:	3	1	C	
E-R+H-PNA	4	2	C	Disuasivo:	4	1	D	
E-R+H-PD	4	1	D	Preventivo:	3	1	D	

El ejemplo anterior, es el tipo de tabla que se ocupará en la sección 5.8 para realizar la cuantificación del riesgo.

CAPÍTULO 3

FUNDAMENTOS DE CRIPTOGRAFÍA

En este capítulo se tratan algunos fundamentos de criptografía, no se honda mucho en la cuestión de la historia o la evolución de la criptografía, más bien se explican conceptos, de criptografía simétrica y asimétrica, así como algunos de los algoritmos que se emplean de cada una de ellas.

La criptografía es una herramienta útil cuando se desea tener seguridad informática; la criptografía también puede entenderse como un medio para proveer los tres servicios de seguridad comprendidos en la triada de seguridad para un sistema (Granados, G., 2006).

Es un hecho que la criptografía es capaz de garantizar algunos de los servicios de seguridad mencionados, pero también es preciso saber cómo emplearla. Para que esto sea posible se deben entender correctamente los conceptos básicos que preceden a los sistemas criptográficos actuales. Por mencionar algunos de los conceptos incluidos en esta afirmación se tienen: el concepto de criptografía, su clasificación, el funcionamiento básico de sistemas de cifrado, entre otros (Granados, G., 2006).

3.1. Conceptos básicos de criptografía

Criptografía: Del sentido etimológico es un concepto que proviene del griego: *Kriptos*, *(*ocultar) y Graphos*,* (escritura), es decir, ocultar la escritura. Aunque en un sentido más amplio podría ser: aplicar alguna técnica para hacer confuso un mensaje. En su clasificación dentro de las ciencias, la criptografía proviene de una rama de las matemáticas llamada Criptología (Aguillón, E., 2012).

Por lo tanto, la criptografía es la ciencia encargada diseñar y crear funciones o dispositivos, capaces de transformar mensajes sin cifrar, a mensajes ilegibles para cualquier persona que no tenga la llave correspondiente.

Como contraparte; el criptoanálisis es una ciencia que estudia los métodos que se utilizan para, a partir de uno o varios mensajes cifrados, recuperar los mensajes en claro (mensajes originales, sin cifrar) en ausencia de la(s) llave(s) y/o encontrar la llave o llaves con las que fueron cifrados dichos mensajes (Aguillón, E., 2012).

De estas definiciones el siguiente nivel lógico para definir seria: un sistema de cifrado. Este último es aquel sistema que permite al emisor y receptor contar con cierta información confidencial. El emisor proporciona el mensaje original (mensaje en claro) para que el algoritmo de cifrado mediante un determinado procedimiento auxiliado por una clave cifre o transforme dicho mensaje en un mensaje cifrado (criptograma) que se envía por un canal público. El receptor que conoce la clave, transforma ese criptograma en el texto original con ayuda de un algoritmo de descifrado (Granados, G., 2006).

Existen varias formas de clasificar a los sistemas de cifrado, sin embargo, por cuestiones de facilidad y brevedad, se toma la clasificación que permite clasificarlos en dos rubros (Aguillón, E., 2012):

- Sistema de cifrado serial (también llamado continuo, en flujo o secuencial): en este tipo de sistemas el texto original es cifrado carácter por carácter.
- Sistema de cifrado por bloque: en este tipo de sistemas el texto original es dividido en grupos de caracteres (bloques) para ser cifrado.

3.2. Clasificación de la criptografía

La criptografía se puede clasificar históricamente en dos: La criptografía clásica y la criptografía moderna. La criptografía clásica es aquella que se utilizó desde antes de la época actual hasta la mitad del siglo XX. Posteriormente, la criptografía moderna se inició después de tres hechos: el primero fue la publicación de la *Teoría de la Información*, por Shannon. El segundo fue la aparición del estándar del sistema de cifrado DES (Data Encryption Standard) en 1974 y el tercero fue un estudio realizado por Whitfield, Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifrado, denominado cifrado de llave pública en 1976. Para esta tesis, se hará uso de la criptografía moderna, que a su vez, se puede clasificar en dos grandes grupos: la criptografía de llave secreta o simétrica y la criptografía de llave pública o asimétrica (Granados, G., 2006).

3.2.1 Criptografía simétrica

La criptografía simétrica, o de clave secreta, utiliza algún método matemático llamado sistema de cifrado para cifrar y descifrar un mensaje utilizando únicamente una llave secreta. Este tipo de criptografía sólo utiliza una llave para cifrar y descifrar, este tipo de llave conocida como secreta se debe de compartir entre las personas que se desea que vean los mensajes. Con este tipo de criptografía es posible proveer el servicio de confidencialidad porque únicamente quien posea la llave secreta será capaz de ver el mensaje (Granados, G., 2006).

Algunas de las principales características de estos sistemas son (Aguillón, E., 2012):

- La clave es la misma para cifrar que para descifrar un mensaje, por lo que sólo el emisor y el receptor deben conocerla.
- Se basan en operaciones matemáticas sencillas, por ello son fácilmente implementados en hardware.
- Debido a su simplicidad matemática son capaces de cifrar grandes cantidades de datos en poco tiempo.

Algunos de los problemas de la criptografía simétrica es el compartir la llave secreta, la administración de tales acciones, el continuar garantizando la confidencialidad e integridad de la llave, entre otros similares (Aguillón, E., 2012). Este tipo de criptografía tiene varios algoritmos representativos, sin embargo, para fines de esta tesis, solo se utilizará uno de ellos; el algoritmo de cifrado AES.

AES surge a finales del 2001 a partir de un concurso, también es conocido como el algoritmo Rijndael, ganó su nombre por las siglas en ingles de la oración: Estándar Avanzado de Cifrado (Advanced Encryption Standard). Algunas de las características de este algoritmo son las siguientes (Granados, G., 2006):

- Opera sobre bloques de datos de 128 bits para cifrar y la clave que utiliza puede ser de 128, 192 o 256 bits
- El número de rondas que realiza depende del tamaño de la clave; en cualquier caso, el criptograma siempre tiene la longitud de 128 bits.
- Aseguran la confidencialidad, pero no asegura la integridad de la información.

Para cifrar mensajes de mayor tamaño se usan diferentes modos de operación, estos modos de cifrado son:

- ECB (Electronic Codebook) libro de códigos electrónico.
- CBC (Cipher-Block Chaining) cifrado en bloque encadenado.
- OFB (Output Feedback) cifrado realimentado.
- CFB (Cipher Feedback) salida realimentada.

3.2.2 Criptografía asimétrica

La criptografía asimétrica o de clave pública, tiene la característica primordial de que en ella se cifra o descifra con una llave pública y en el otro lado con una privada. Cabe mencionar que para este tipo de criptografía lo que se cifra con una llave se puede descifrar con la otra llave (Granados, G., 2006).

Algunas de las principales características de estos sistemas son (Aguillón, E., 2012):

- Se utiliza una clave para cifrar y otra para descifrar. El emisor emplea la clave pública del receptor para cifrar el mensaje, éste último lo descifra con su clave privada.
- Se basan en operaciones matemáticas complejas.
- Se ejecutan de 100 a 1000 veces más lento que los algoritmos simétricos.

Este tipo de criptografía tiene varios algoritmos representativos, sin embargo, para fines de esta tesis, solo se utilizará uno de ellos; la función Hash MD5.

Funciones Hash: lo que una función Hash realiza, es que a partir de un documento de tamaño N bits, la función entrega una cadena de M bits. No hay límite para el tamaño de N, pero M siempre es de tamaño constante de acuerdo con el algoritmo usado, normalmente es de 128 o 256 bits. Una de las características de este tipo de funciones es que son unidireccionales, es decir, que debe ser imposible a partir del resumen del documento encontrar el mensaje original. También deben cumplir la propiedad de dispersión, lo que significa que si se cambia al menos un bit del documento, su resumen debe de cambiar la mitad de sus bits aproximadamente. El *Algoritmo de Resumen del Mensaje 5* (Message-Digest Algorithm 5), es un ejemplo de función Hash. MD5 fue desarrollado por Ron Rivest en 1992 en el MIT, entre las aplicaciones más recurrentes están la autenticación en el protocolo SSL y la firma digital en PGP. MD5 procesa mensajes de cualquier longitud (longitud variable) y procesa bloques uniformes de 512 bits a la vez, hasta concluir con el mensaje total a fin de entregar a la salida un bloque "resumen" de 128 bits (longitud fija) (Granados, G., 2006).

CAPÍTULO 4

PROPUESTA DE METODOLOGÍA PARA ANÁLISIS DE RIESGOS

En este capítulo se realiza la proposición y adaptación de una metodología de análisis de riesgos informáticos cualitativa sobre el proceso de distribución de la QITDraw, con la cual se pretende identificar y evaluar los riesgos de seguridad que existen actualmente.

4.1. Proposición de una metodología adaptada de análisis de riesgos cualitativo

A continuación y de acuerdo con lo planteado en los tres capítulos anteriores, se proponen los siguientes pasos para estructurar y adaptar una metodología de análisis de riesgos cualitativa, que posteriormente en el capítulo 5 será aplicada sobre el problema definido en esta tesis.

4.1.1. Identificación y evaluación de los activos

En este paso se *identificaran formalmente los activos de interés* por el autor de la tesis junto con el jefe del grupo de soporte técnico, el del grupo de desarrollo y el director de proyectos del CEASP^{4}A (López, M. J. y Quezada C., 2006, e).

Lo anterior debido a que *un análisis de riesgo siempre debe ser realizado por varios expertos de diversas áreas de la compañía con la finalidad de integrar un grupo multidisciplinario*, no solo para identificar las vulnerabilidades de seguridad, sino también para emitir los últimos juicios de valor al momento de realizar las recomendaciones sobre los nuevos controles de seguridad (CCPS, 2003).

Para la evaluación de los activos se consideran dos características principales; el valor del activo para los dueños así como la consideración del grado de atractivo del mismo para los intrusos. La clasificación de los valores y el grado de atractivo de los activos se establece en la *tabla 5*. (CCPS, 2003). Cabe señalar que las ponderaciones de grado de atractivo pueden no siempre coincidir con el valor que dan los dueños del activo a la hora de calificar ambas cualidades, estos valores son meramente de referencia.

Tabla 5. Valor y grado de atractivo de los activos.

Activos Identificados	Valor Del Activo	Grado de Atractivo
Activo 1	Bajo	Nada atractivo
Activo 2	Medio	Parcialmente Atractivo
Activo 3	Alto	Atractivo
Activo 4	Muy Alto	Muy Atractivo

4.1.2. Establecimiento de las premisas para el análisis de riesgos

Antes de comenzar con la identificación de amenazas y sus fuentes, en este paso se establecerá información previa sobre el proceso de distribución de la herramienta. Esto comprende la definición de los escenarios de distribución de la herramienta, lo que en ellos acontece, la descripción propia del proceso de distribución de la herramienta y los diferentes tipos de personal que se relacionan con éste, con la finalidad de facilitar la clasificación y organización de la información.

4.1.3. Identificación de amenazas y sus fuentes

En este paso se identificarán las amenazas y sus correspondientes fuentes que afectan a los activos *de interés* en base a la información recopilada durante el establecimiento de las premisas para el análisis de riesgos, y tomando la *clasificación general de amenazas* (López, M. J. y Quezada C., 2006, j). Debido a los objetivos y alcances de esta tesis; las siguientes fuentes de amenaza no se consideran dentro del análisis de riesgo ni en ningún otro punto del trabajo desarrollado: *errores de hardware, errores de la red, y desastres*.

4.1.4. Identificación y clasificación de vulnerabilidades

En este paso se identificarán, clasificarán y describirán las vulnerabilidades que afectan a los activos *a proteger*, tomando la *clasificación general de vulnerabilidades* (López, M. J. y Quezada C., 2006, k). Debido a los objetivos y alcances de esta tesis; los siguientes tipos de tipos de vulnerabilidades no se consideran dentro del análisis de riesgo ni en ningún otro punto del trabajo desarrollado: *vulnerabilidades de hardware, vulnerabilidades de red, ni desastres naturales*.

4.1.5. Relación de Amenazas y Vulnerabilidades

En este paso se realizará la relación (cruce) de las amenazas con las vulnerabilidades de los activos para determinar los casos de estudio, esta relación se realiza tomando una determinada amenaza y relacionándola con su vulnerabilidad correspondiente (CCPS, 2003).

4.1.6. Relación de Amenazas y Vulnerabilidades Consideradas

En este paso se realizará una agrupación de las relaciones de amenaza-vulnerabilidades que sean consideradas en el apartado 5.6, para ello se utilizará una matriz de tres columnas que contenga en cada una de ellas: el nombre del escenario, las abreviaturas concatenadas con un signo de "+" para denotar la relación y el nombre de la misma, que será la combinación del nombre de la amenaza con el de sus vulnerabilidades mediante alguna palabra lógica. Un ejemplo de la notación anterior se presenta en la tabla 6.

Tabla 6. Ejemplo de una matriz de relación de amenazas y vulnerabilidades.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	Amenaza + Tipo de Vulnerabilidad-Vulnerabilidad	Nombre de la amenaza, palabra conector, nombre de la vulnerabilidad
	ATI-L+S-EIV	Administradores de T.I. de PEMEX Refinación ladrones **que aprovechan** los errores Inesperados en validaciones para la QITDraw distribuida en PEMEX Refinación

4.1.7. Cuantificación de los riesgos

En este paso se realizará la determinación del impacto de ocurrencia de las amenazas, el análisis de los controles del lugar, la determinación de los riesgos residuales y las recomendaciones. Es decir, la evaluación de que ocurran las amenazas y las vulnerabilidades asociadas (ISO/IEC 27001:2005); para ello se tomarán los pasos descritos en la sección 2.5.5.

Sin embargo, las escalas definidas en la sección 2.5.2 no se emplearán como se muestran en la referencia, en su lugar se utilizarán escalas de elaboración propia que se definen en las tablas 7, 8 y 9. Las anteriores están basadas en: las escalas de riesgo, las del impacto de acontecimiento y las de frecuencia de ocurrencia de un acontecimiento, definidas por López, M. J. y Quezada C. (2006, q)**.** También se emplea la matriz de riesgos construida y sugerida por CCPS del AIChE, para la cual se tomará el índice del impacto por acontecimiento y se multiplica por el de la frecuencia de ocurrencia. El resultado se ajustará según las ponderaciones que resulten, y de esta manera se observará en qué categoría de riesgo se encuentra cada activo, independientemente de los controles que existan (CCPS, 2003).

Tabla 7. Escala de riesgo ajustada para los activos de la QITDraw

Categoría de riesgo		Clasificación
Aceptable como está – No requiere medidas de control	D	1 – 4
Aceptable con controles – Verificar las medidas de control existentes	C	5 – 8
Indeseable – Introducir medidas de control con prioridad media	B	9 – 12
Inaceptable – Atención Inmediata, alta prioridad	A	13 – 16

Para la tabla 7, la clasificación utilizada de índices, es del número 1 hasta el 16 debido a que la matriz de la sección 2.5.2 es simétrica, por lo tanto, con el objetivo de calcular la categoría de riesgo de una forma equitativa, se usan índices del número 1 al 4 para el impacto del acontecimiento (tabla 8) así como para la frecuencia / probabilidad de ocurrencia de los acontecimientos (tabla 9). Cabe recordar que la categoría de riesgo se calcula con la formula mencionada en la sección 2.5 (fórmula para determinar el riesgo total).

Tabla 8. Impacto del acontecimiento para los activos de la QITDraw

Daño del acontecimiento	Grado del daño	Clasificación
Importante	No se requiere esfuerzo extra para reparar, se lograron recrear por completo las plantillas, los bloques están intactos y el código fuente también.	1
Critico	Se lograron recrear por completo las plantillas, se copiaron por completo los bloques, y se lograron sobrepasar algunos controles de seguridad que permiten un funcionamiento parcial de la herramienta. El código fuente está intacto. Se puede solucionar el problema con un esfuerzo extra	2
Mayor	Se lograron recrear por completo las plantillas, se copiaron por completo los bloques, y se lograron sobrepasar algunos controles de seguridad que permiten un funcionamiento casi completo de la herramienta. El código fuente continua intacto. Se puede solucionar el problema pero con un esfuerzo extra, considerable	3
Catastrófico	Compromiso total de los activos, las plantillas, los bloques y el código fuente fueron totalmente robados. No existe solución.	4
Para conocer cuáles son los activos que conforman a la QITDraw y una mejor comprensión de esta tabla, se sugiere consultar la sección 5.1 de este trabajo.		

Tabla 9. Frecuencia / Probabilidad de Ocurrencia de acontecimientos para los activos de la QITDraw

Acontecimiento	Frecuencia / Probabilidad	Clasificación
Insignificante	Improbable	1
Bajo	Posible	2
Medio	Ocasional	3
Alto	Frecuente	4

4.1.8. Preparación del informe para el análisis de riesgos

El último paso de la metodología adaptada, consistirá en preparar un informe conciso sobre lo realizado. El informe deberá contener tres elementos indispensables que se mencionan a continuación.

1. Las relaciones Amenaza-Vulnerabilidades que implican un riesgo: Solo se excluirán aquellas que tengan una categoría de riesgo “D” (Aceptable como está), las demás deberán ser documentadas sin excepción.
2. El resultado sobre la efectividad de los controles actuales sobre las relaciones de Amenaza-Vulnerabilidades de riesgos.
3. A partir de estas dos partes del informe; se realizará e implementa la propuesta de mejora correspondiente.

CAPÍTULO 5

APLICACIÓN DEL ANÁLISIS DE RIESGOS

En este capítulo se aplicará una metodología adaptada de un análisis de riesgos cualitativo, propuesta y detallada en el capítulo 4. La metodología comienza con la identificación de los activos que se requieren proteger con respecto al proceso de distribución de la QITDraw. Con base en los resultados de este procedimiento, en el capítulo 6 se realizará, implementará y presentará la propuesta de mejora para los mecanismos de seguridad empleados en la distribución de la herramienta de dibujo previamente mencionada.

5.1. Identificación y evaluación de los activos

Como se mencionó en la introducción de esta tesis, el valor de la **QITDraw** radica en su capacidad para aumentar la eficiencia cerca de un 300% en el proceso de dibujo con AutoCAD®, de diagramas técnicos de tuberías y equipos utilizados para inspección técnica en PEMEX Refinación.

A continuación, se realizará la Identificación, evaluación y descripción de los activos de interés (que conforman la QITDraw); identificados formalmente por el autor de la tesis junto con el jefe del grupo de soporte técnico, el del grupo de desarrollo y el director de proyectos del CEASP^{4}A.

Se considera el primer activo a proteger el **código fuente de los comandos** utilizados por la QITDraw, debido a que toda la funcionalidad que posee la herramienta está basada en él. Este código fuente está conformado por una serie de procedimientos, métodos y técnicas de programación estructurada y orientada a objetos que interactúan con el API de AutoCAD®, lo cual le permite a la herramienta realizar alguna de las varias tareas posibles y específicas de una manera automatizada.

Varios de los comandos de la QITDraw requieren de elementos de dibujo predefinidos para funcionar correctamente; a estos elementos se les conoce como **bloques**, accesorios que también forman parte de la herramienta y no solo tienen la utilidad de complementar la funcionalidad de algunos de los comandos de la herramienta de dibujo, igualmente son requeridos en el proceso de homologación de diagramas técnicos; lo cual es posible porque los diagramas elaborados a partir de ellos se pueden manejar e interpretar adecuadamente en cualquier instancia de PEMEX Refinación por tratarse de elementos estándar de dibujo. Por lo tanto, los bloques se consideran un activo más a proteger.

Otro elemento de la QITDraw son las **plantillas**; las cuales son archivos de dibujo con extensión de archivo “dwt” que contienen configuraciones de diseño, geometría predeterminada, cuadros de rotulación y algunos bloques predefinidos. Una plantilla es utilizada como la base para un nuevo dibujo en el formato de archivos de AutoCAD® (cuya extensión es también la mencionada anteriormente). Toda la información que contienen las plantillas (por ejemplo, capas predefinidas), es necesaria para el funcionamiento correcto de algunos comandos de la herramienta de dibujo, por ello también son consideradas como otro activo más.

El código fuente de los comandos, los bloques y las plantillas representan los tres activos de interés que fueron identificados para protegerse, el siguiente paso consiste en evaluar su importancia de forma cualitativa. Luego de ello, se establecerán ciertas premisas necesarias para poder continuar llevando a cabo la metodología propuesta de un análisis de riesgos cualitativo de los mecanismos de seguridad para la distribución de la QITDraw. A continuación en la tabla 10, se establece el valor y grado de atractivo de los activos que forman parte de la herramienta de dibujo.

Tabla 10. Evaluación cualitativa de los activos que conforman la QITDraw.

Nombre del activo	Valor del activo (Para el CEASP^{4}A)	Grado de atractivo (Para externos)
Código fuente de los comandos	Muy alto	Muy atractivo
Bloques	Muy alto	Parcialmente atractivo
Plantillas	Muy alto	Parcialmente atractivo

Los tres activos identificados se consideran igualmente significativos para el CEASP^{4}A porque en conjunto representan un desarrollo tecnológico innovador que ha sido capaz de solventar dos puntos de mejora importantes para PEMEX Refinación: aumentar la eficiencia en el proceso de dibujo de diagramas técnicos para su constante actualización y la homologación de los mismos. Lo anterior se ha traducido en nuevos proyectos de colaboración académico-industrial que representan beneficios económicos directos para la UNAM así como una buena reputación para la misma. El grado de atractivo del código fuente de los comandos se considerará muy alto porque; si algún agente de amenaza (perpetrador o atacante) lograra la obtención parcial o total del mismo, tendría la base necesaria para desarrollar otras herramientas capaces aprovechar el mismo nicho de negocios, ya sea dentro de PEMEX Refinación u otras compañías.

En cuanto a los bloques y las plantillas; tienen un diseño enfocado específicamente a la problemática y necesidades de PEMEX Refinación, por lo que no son adecuadas para alguna otra compañía. Estos últimos dos activos mencionados se distribuyen de manera no controlada y con carácter público, con el objetivo de contar con la disponibilidad de ambos siempre y así apoyar el proceso de homologación previamente mencionado. También ocurre que el contenido de estos dos activos es fácilmente replicable por cualquier persona que posea conocimientos básicos de AutoCAD® y tenga acceso a los mismos. Por tal razón se considera que estos activos solo son parcialmente atractivos para algún atacante, en comparación con el código fuente.

5.2. Premisas para el análisis de riesgos cualitativo

Para facilitar la organización de la información sobre las premisas y el proceso de distribución de la herramienta, se proponen y describen una serie de ámbitos (tres escenarios) representativos de los casos reales y lo que en ellos ocurre al momento de distribuir y utilizar la QITDraw.

5.2.1. Definición de los escenarios donde se distribuye la QITDraw

A continuación en la tabla 11, se proponen tres escenarios:

Tabla 11. Escenarios propuestos para la distribución de la QITDraw.

Nombre del escenario	Abreviatura del escenario
PEMEX Refinación	PR
CEASP^{4}A UNAM	CU
Contratistas Externos	CE

PR: Escenario que contempla las instalaciones de PEMEX Refinación donde la herramienta de dibujo es distribuida y utilizada, así como los equipos de cómputo de escritorio y portátiles necesarios para lo anterior. En este escenario se considera también el siguiente personal.

CU: Escenario que contempla las instalaciones del CEASP^{4}A ubicadas dentro del instituto de ingeniería de la UNAM; en el ala norte del cuarto piso de la Torre de Ingeniería (TI), donde la QITDraw es distribuida y utilizada, así como los equipos de cómputo de escritorio y portátiles necesarios para lo anterior.

CE: Escenario del cual se desconocen varias características pero se sabe qué; dentro del mismo laboran firmas de ingeniería contratadas por PEMEX Refinación como apoyo para los trabajos requeridos en sus instalaciones, entre ellos está el dibujo de diagramas técnicos.

5.2.2. El proceso de distribución de la QITDraw

En la tabla 12 de este apartado se realiza una descripción general de cómo ocurre el proceso de distribución de la herramienta de dibujo, quien lo lleva a cabo y a quienes va dirigido; solo se emplea y organiza la información considerada necesaria para utilizar con la metodología propuesta del análisis de riesgos cualitativo.

Tabla 12. Descripción del proceso de distribución para la QITDraw.

Escenario	Descripción del proceso de distribución para cada escenario
PR	La QITDraw se entrega por personal de soporte técnico del CEASP^{4}A a los Administradores de T.I. en cada centro de trabajo de PEMEX Refinación, quienes a su vez instalan (de forma remota) la QITDraw en los equipos de cómputo (de escritorio y portátiles) del personal correspondiente que utilizará la herramienta en los centros de trabajo. Se debe mencionar que la herramienta tiene cierto periodo de validez que después de concluir, evita que esta se siga utilizando, la medida se implementó por cuestiones de actualización más que de seguridad.
CU	La QITDraw se instala en cada uno de los equipos de cómputo de escritorio y portátil del CEASP^{4}A por personal de soporte técnico del mismo; equipos que son utilizados por los empleados del grupo. Es importante mencionar que la herramienta tiene cierto periodo de validez que después de concluir, evita que esta se siga utilizando, la medida se implementó por cuestiones de actualización más que de seguridad.
CE	Se otorga una memoria USB a cada contratista (como parte del material de un curso previo impartido por la UNAM, siempre que este haya sido aprobado), la cual contiene a la QITDraw y es necesario conectar y ejecutar Autodesk® AutoCAD® 2008 o posterior en equipo de cómputo en el que la herramienta se desee utilizar. Tanto los comandos como los bloques de la QITDraw son leídos desde la USB, por ello, su desconexión implicaría mal funcionamiento.

Para concluir este apartado, en la tabla 13 se presentan los diferentes tipos de personal que se relacionan de alguna forma con el proceso de distribución y la utilización de la QITDraw. Cada tipo de personal cuenta con un perfil que influirá en mayor o menor medida en el proceso de distribución y utilización de la herramienta de dibujo, por ello, en siguiente apartado (5.2.3) se detallará el perfil de cada uno de ellos.

Tabla 13. Tipos y dependencia del personal relacionado con la distribución y el uso de la QITDraw.

Escenarios	Tipos de personal	Dependencia del personal
PR	Administradores de T.I. de PEMEX Refinación	Departamento de T.I. PEMEX Refinación
	Ingenieros del área de seguridad	Subdirección de Auditoría de Seguridad Industrial y Protección Ambiental de PEMEX Refinación (SASIPA)
	Dibujantes	Departamento de dibujo de PEMEX Refinación
	Ayudantes de ingeniero	Trabajadores sindicalizados de PEMEX Refinación
CU	Personal de soporte técnico del CEASP^{4}A	Grupo de soporte técnico del CEASP4A
	Coordinadores del CEASP^{4}A	Grupo de coordinadores del CEASP^{4}A
	Residentes del CEASP^{4}A	Grupo de residentes del CEASP^{4}A
	Empleados del CEASP^{4}A	Grupo de empleados de confianza del CEASP^{4}A
CE	Contratistas Externos	Firmas de ingeniería contratadas por PEMEX Refinación como apoyo para los trabajos requeridos en sus instalaciones

5.2.3. Perfil del personal de los tres escenarios

El perfil del personal de los tres escenarios definidos (PEMEX Refinación, el CEASP^{4}A y los contratistas externos) se describe en las tablas de esta sección sin considerar la forma de ataque. Posteriormente, la información de los mismos será considerada en la sección 5.5 de la metodología adaptada del análisis de riesgos cualitativo.

Para todos los casos de ex empleados establecidos en cada tipo de personal de las tablas del **Anexo 1**; se considerarán las mismas características descritas en la sección 2.2.1 para los mismos.

Tabla 14. Perfiles del personal de PEMEX Refinación.

Atacantes	Perfil
Administradores de T.I. de PEMEX Refinación **ATI-PR**	Personal con conocimiento especializado en programación, redes de datos, seguridad de la información, administración de equipos de cómputo y servidores, ocupan cargos técnicos con acceso completo a los equipos de cómputo y a los activos que se desean proteger. Firmaron acuerdos de confidencialidad, su rango de edad es desde los 30 hasta los 45 años, los puestos que ocupan son de confianza.
Ingenieros del área de seguridad **IAS-PR**	Personal con conocimiento especializado en procesos químicos y en el área de seguridad de los mismos, conocimientos básicos en el área de computación, tienen permisos de lectura y acceso limitado sobre los equipos de cómputo que pueden utilizar y los activos a proteger. Firmaron acuerdos de confidencialidad, su rango de edad es desde los 25 hasta los 50 años, los puestos que ocupan son una plaza de trabajo.
Dibujantes **D-PR**	Personal con conocimientos en dibujo técnico encargado de realizar parte del proceso de dibujo de diagramas técnicos, conocimientos intermedios en el área de computación y en manejo de software CAD, tienen permisos de lectura y acceso limitado sobre los equipos de cómputo que pueden utilizar y los activos a proteger. No firmaron acuerdos de confidencialidad, su rango de edad es desde los 25 hasta los 50 años, los puestos que ocupan son una plaza de trabajo.
Ayudantes de ingeniero **AI-PR**	Personal encargado de auxiliar a los ingenieros de área de seguridad en diversas tareas, entre ellas se encuentra la de dibujar diagramas técnicos, tienen conocimientos intermedios en el área de computación, algunos de ellos cuentan con carreras técnicas y no con licenciatura en ingeniería, tienen permisos de lectura y acceso limitado sobre los equipos de cómputo que pueden utilizar y los activos a proteger. No firmaron acuerdos de confidencialidad, su rango de edad es desde los 25 hasta los 50 años, los puestos que ocupan son una plaza de trabajo.

Tabla 15. Perfiles del personal del CEASP^{4}A.

Atacantes	Perfil
Personal de soporte técnico del CEASP^{4}A **PST-CU**	Personal con licenciatura en ingeniería química, tienen conocimiento especializado en programación, redes de datos, seguridad de la información, administración de equipos de cómputo, bases de datos y servidores, ocupan cargos técnicos con acceso completo a los equipos de cómputo y a los activos que se desean proteger. Firmaron acuerdos de confidencialidad, su rango de edad es desde los 24 hasta los 40 años, los puestos que ocupan son de confianza.
Coordinadores del CEASP^{4}A **C-CU**	Personal con licenciatura en ingeniería química, tienen conocimientos básicos en el área de computación, tienen permisos de lectura y escritura sobre los equipos de cómputo que pueden utilizar (equipos de cómputo portátiles) y los activos a proteger. Firmaron acuerdos de confidencialidad, su rango de edad es desde los 28 hasta los 45 años, los puestos que ocupan son de confianza.
Residentes del CEASP^{4}A **R-CU**	Personal con licenciatura en ingeniería química, tienen conocimientos básicos en el área de computación, tienen permisos de lectura y escritura sobre los equipos de cómputo que pueden utilizar (equipos de cómputo portátiles) y los activos a proteger. Firmaron acuerdos de confidencialidad, su rango de edad es desde los 25 hasta los 30 años, los puestos que ocupan son de confianza.
Empleados del CEASP^{4}A **E-CU**	Personal con licenciatura en ingeniería química, tienen conocimientos básicos en el área de computación, tienen permisos de lectura y acceso limitado sobre los equipos de cómputo que pueden utilizar y los activos a proteger. Firmaron acuerdos de confidencialidad, su rango de edad es desde los 25 hasta los 30 años, los puestos que ocupan son de confianza.

Tabla 16. Perfiles de los contratistas externos.

Atacantes	Perfil
Contratistas externos **CE**	Personal del que se desconocen sus conocimientos, sus habilidades o su área de trabajo, poseen una USB que contiene a los activos a proteger, solo tienen permisos de lectura sobre los anteriores, son contratados por PEMEX Refinación de manera interina para apoyar trabajos específicos de dibujo de diagramas técnicos, no se sabe si firman acuerdos de confidencialidad, su rango de edad se desconoce, los puestos que ocupan son de confianza.

Tabla 17. Perfiles de los intrusos remunerados por PEMEX Refinación, el CEASP^{4}A o los contratistas externos.

Atacantes	Perfil
Cracker remunerados por: PEMEX Refinación **C-PR** El CEASP^{4}A **C-CU** Contratistas Externos **C-CE**	Personas capaces de irrumpir en sistemas de manera ilegal por: alguna ganancia personal (como una remuneración por parte de PEMEX Refinación, el CEASP^{4}A o los Contratistas Externos), vandalismo, alardear que son los mejores, etc. Algunos posen gran habilidad (incluso para crear sus propias herramientas para vulnerar la seguridad), tienen entrenamiento extensivo en manejo de redes, conocimientos muy avanzados en programación, manejo y administración de bases de datos, entre otros. Sin embargo son los menos, la mayoría utiliza herramientas prefabricadas y su habilidad esta sobrestimada, hacen lo que pueden para cubrir las huellas de sus actos ilegales y no entienden el verdadero funcionamiento del software. A pesar de sus limitaciones la mayoría son muy capaces técnicamente, también son conocidos como los Hackers Black Hats.
Hackers Grey Hat remunerados por: PEMEX Refinación **HGH-PR** El CEASP^{4}A **HGH-CU** Contratistas Externos **HGH-CE**	Personas cuya conducta oscila entre lo legal e ilegal respecto a la incursión a sistemas, saben encontrar vulnerabilidades de seguridad y repórtalas pero también pueden ocultarlas para su propio beneficio o para el de PEMEX Refinación, el CEASP^{4}A o los Contratistas Externos. Cuando estas personas realizan un ataque son prácticamente indistinguibles de los Crackers. Saben crear herramientas avanzadas para probar la seguridad de diversos sistemas, su ética es ambigua y muchas veces sirven a quien mejor los remunera o les ofrece algo que ellos necesitan.

5.3. Identificación de amenazas y sus fuentes

Se presentan en el **Anexo 1** las tablas A1.1, A1.2, A1.3 y A1.4, que enlistan las fuentes y los agentes de amenaza (atacantes o perpetradores), así como el tipo de personal del que derivan y su abreviatura para referenciarlos.

5.4. Identificación y clasificación de vulnerabilidades

Se presentan en el **Anexo 2** las tablas A2.1, A2.2 Y A2.3, que organizan y clasifican a los tipos a las vulnerabilidades para los activos a proteger.

5.4.1. Descripción de las vulnerabilidades

Análogo a la definición de perfiles del personal de los tres escenarios realizada en la sección **5.2.3**, en las tablas de este apartado se realizará una descripción de cada una de las clasificaciones de vulnerabilidades para los escenarios definidos. En lo referente a las vulnerabilidades físicas de los casos PR y CU, se tomará como entorno físico el tipo de equipos de cómputo (de escritorio y portátiles) en los que se distribuye y utiliza la QITDraw.

Tabla 18. Vulnerabilidades físicas para PEMEX Refinación.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
F-AECE-PR	Equipos de cómputo de escritorio que tienen instalada la QITDraw, ubicados dentro de las instalaciones en los diversos centros de trabajo de PEMEX Refinación. Son utilizados por más de una persona.
F-AECP-PR	Equipos de cómputo portátiles que tienen instalada la QITDraw, ubicados dentro de las instalaciones en los diversos centros de trabajo de PEMEX Refinación. Están asignados y son utilizados por una sola persona con cargos medios y superiores.
En ambos casos, los dos tipos de equipos de cómputo están sujetos a permisos administrados por reglas de un Dominio llamado PEMEX, constituido a partir de servidores tipo Windows, los cuales son gestionados por el Departamento de T.I. de PEMEX Refinación. En cuanto a los usuarios; cada uno tiene asociado un nombre y una contraseña, información que es administrada por el dominio y a su vez requerida para acceder al mismo mediante equipos de computo unidos a él. Es importante mencionar que los usuarios no tienen permisos de administrador sobre los equipos de cómputo, el software instalado en ellos o el dominio.	

Tabla 19. Vulnerabilidades de software para PEMEX Refinación.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
S-EPC-PR	Errores de programación en los mecanismos de validación utilizados para la distribución de la QITDraw en PEMEX Refinación, que facilitan el acceso a los activos de la herramienta y permite a los atacantes comprometer alguno o los tres servicios de seguridad (que conforman la triada de seguridad) para la última.
S-EIV-PR	Errores que ocurren súbitamente con la validación en la distribución de la QITDraw durante su funcionamiento ordinario, que permiten a los atacantes comprometer alguno o los tres servicios de seguridad (que conforman la triada de seguridad) de la herramienta y la hacen menos confiable dentro de las instalaciones de PEMEX Refinación.

Tabla 20. Vulnerabilidades humanas para PEMEX Refinación.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
H-PSPPA-PR	Personas que fueron contratadas en PEMEX Refinación sin haber aprobado las pruebas correspondientes indicadoras de que poseen los conocimientos, las aptitudes y las actitudes necesarias para estar en el puesto de trabajo que tienen asignado. Lo cual propicia la materialización de un ataque contra los activos a proteger dentro de PEMEX Refinación por parte de los atacantes.
H-PSIS-PR	Personas que laboran dentro de las instalaciones de PEMEX Refinación, tienen alguna relación con el proceso de distribución y uso de la QITDraw, y son susceptibles a ser engañados o manipulados.
H-PNA-PR	Personas no contratadas por PEMEX Refinación que logran acceder a sus instalaciones de manera no autorizada y logran acceder a los equipos de cómputo que cuentan con la QITDraw.
H-PD-PR	Personas que laboran dentro de las instalaciones de PEMEX Refinación que tiene alguna relación con el proceso de distribución y uso de la QITDraw y de forma inconsciente dan pauta a la materialización de un ataque contra los activos a proteger dentro de PEMEX Refinación por parte de los perpetradores.

Tabla 21. Vulnerabilidades físicas para el CEASP^{4}A.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
F-AECE-CU	Equipos de cómputo de escritorio, se encuentran ubicados en el 4to Piso de la Torre de Ingeniería (instalaciones utilizadas por el CEASP^{4}A). Son utilizados por más de una persona.
F-AECP-CU	Equipos de cómputo portátiles, se encuentran ubicados en el 4to Piso de la Torre de Ingeniería (instalaciones utilizadas por el CEASP^{4}A). Son utilizadas por más de una persona; en la torre de ingeniería, en centros de trabajo de Pemex refinación, y otros lugares como: hoteles, hogares de los empleados, etc.
En ambos casos, los equipos de cómputo están sujetos a permisos administrados por reglas de un Dominio llamado CEASP^{4}A, constituido a partir de servidores tipo Windows, los cuales son gestionados por el Departamento de T.I. del CEASP^{4}A. En lo referente a los usuarios; cada uno tiene asociado un nombre y también una contraseña, información que es administrada por el dominio y también es requerida para acceder al mismo mediante equipos de computo unidos a él. Es importante mencionar que los usuarios **no** tienen permisos de administrador sobre los equipos de cómputo el software instalado en ellos o el dominio, a excepción de personal de desarrollo, soporte y coordinadores del CEASP^{4}A.	

Tabla 22. Vulnerabilidades de software para el CEASP^{4}A.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
S-EPC-CU	Errores de programación en los mecanismos de validación utilizados para la distribución de la QITDraw en el CEASP^{4}A, que facilitan el acceso a los activos de la herramienta y permite a los atacantes comprometer alguno o los tres servicios de seguridad (que conforman la triada de seguridad) para la última.
S-EIV-CU	Errores que ocurren súbitamente con la validación en la distribución de la QITDraw durante su funcionamiento ordinario, que permiten a los atacantes comprometer alguno o los tres servicios de seguridad (que conforman la triada de seguridad) de la herramienta y la hacen menos confiable dentro de las instalaciones del CEASP^{4}A.

Tabla 23. Vulnerabilidades humanas para el CEASP^{4}A.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
H-PSPPA-CU	Personas que fueron contratadas en CEASP^{4}A sin haber aprobado las pruebas correspondientes indicadoras de que poseen los conocimientos, las aptitudes y las actitudes necesarias para estar en el puesto de trabajo que tienen asignado. Lo cual propicia la materialización de un ataque contra los activos a proteger dentro de CEASP^{4}A por parte de los atacantes.
H-PSIS-CU	Personas que laboran dentro de las instalaciones de CEASP^{4}A, tienen alguna relación con el proceso de distribución y uso de la QITDraw, y son susceptibles a ser engañados o manipulados.
H-PNA-CU	Personas no contratadas por CEASP^{4}A que logran acceder a sus instalaciones de manera no autorizada y logran acceder a los equipos de cómputo que cuentan con la QITDraw.
H-PD-CU	Personas que laboran dentro de las instalaciones de CEASP^{4}A que tiene alguna relación con el proceso de distribución y uso de la QITDraw y de forma inconsciente dan pauta a la materialización de un ataque contra los activos a proteger dentro de CEASP^{4}A por parte de los perpetradores.

Tabla 24. Vulnerabilidades físicas para los contratistas externos.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
F-AUCQ-CE	Equipos de cómputo que disponen de puertos USB. Son utilizados de manera foránea a PEMEX Refinación y al CEASP^{4}A por más de una persona, con el único requisito de tener la correspondiente memoria USB (que se asigna c cada persona y contiene a la QITDraw), conectada todo el tiempo al equipo de cómputo donde se utiliza. Los equipos de computo que se utilizan habitualmente no están sujetos a ningún dominio, reglas o permisos controlados; la única limitante que asumen es la de tener conectada permanentemente al equipo de computo la memoria USB asignada a cada contratista para utilizar la QITDraw, el resto del hardware u otros alcances del mismo son desconocidos.

Tabla 25. Vulnerabilidades de software para los contratistas externos.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
S-EPC-CE	Errores de programación en los mecanismos de validación utilizados en las memorias USB para la distribución de la QITDraw con los contratistas externos, que facilitan el acceso a los activos de la herramienta y permite a los atacantes comprometer alguno o los tres servicios de seguridad (que conforman la triada de seguridad) para la última.
S-EIV-CE	Errores que ocurren súbitamente con la validación en la distribución de la QITDraw durante su funcionamiento ordinario, que permiten a los atacantes comprometer alguno o los tres servicios de seguridad (que conforman la triada de seguridad) de la herramienta y la hacen menos confiable.

Tabla 26. Vulnerabilidades humanas para los contratistas externos.

Clasificaciones de vulnerabilidades	Descripción de las vulnerabilidades
H-D-CE	Personas que laboran para firmas de ingeniería externas a PEMEX Refinación o al CEASP^{4}A que tiene alguna relación con el proceso de uso de la QITDraw y de forma inconsciente dan pauta a la materialización de un ataque contra los activos a proteger dentro de CEASP^{4}A por parte de los perpetradores.
H-PSPPAPR-CE **H-PSPPACU-CE**	Personas que fueron contratadas en PEMEX Refinación o el CEASP^{4}A (según corresponda la abreviatura), sin haber aprobado las pruebas correspondientes indicadoras de que poseen los conocimientos, las aptitudes y las actitudes necesarias para estar en el puesto de trabajo que tienen asignado. Lo cual propicia la materialización de un ataque contra los activos a proteger por parte de los atacantes dentro de PEMEX Refinación por parte de los atacantes.
H-PSISPR-CE **H-PSISCU-CE**	Personas que laboran dentro de las instalaciones de PEMEX Refinación o el CEASP^{4}A (según corresponda la abreviatura), tienen alguna relación con el proceso de distribución y uso de la QITDraw, y son susceptibles a ser engañados o manipulados por los atacantes.

5.5. Relación de amenazas y vulnerabilidades

Al efectuar la relación entre amenazas y vulnerabilidades para determinar el nivel de riesgo, el número de relaciones generadas para analizar es extenso. Aunque estrictamente cada una de ellas debería ser estudiada a detalle; debido a los objetivos y alcances de esta tesis, se realizarán varias consideraciones que evitarán un análisis exhaustivo sobre los niveles de riesgo existentes para las relaciones amenaza-vulnerabilidad, pero se dejarán abiertas las posibilidades de trabajo futuro sobre esta tesis. Para las consideraciones y el proceso de eliminación de relaciones, se utiliza la información establecida desde la sección 5.2 hasta la 5.4.1.

5.5.1. Consideraciones para la evaluación de riesgos en los tres escenarios

En esta sección se establecerán consideraciones generales aplicables a todos los casos presentes en el análisis de riesgo. Estas consideraciones (y aquellas mostradas en las secciones siguientes) se realizan con el objetivo de disminuir el número de casos a analizar y han sido aceptadas en acuerdo con el jefe del grupo de soporte técnico, el del grupo de desarrollo y el director de proyectos del CEASP^{4}A; personal con el que posteriormente se realizará el análisis formal de los casos que no sean descartados por estas consideraciones:

- Las amenazas *manipuladores* y *ex empleados* cuya fuente de amenaza es de tipo humana solo serán relacionadas con las vulnerabilidades de tipo humanas para cualquier tipo de personal en todos los escenarios.

- La amenaza *ex empleando* de cualquier tipo de personal, no tendrán acceso a los activos a proteger, por lo que las vulnerabilidades de tipo físico y de software no se consideran para esta relación, solo las vulnerabilidades de tipo humano.
- La amenaza "saboteadores" de cualquier tipo de personal no se toma en cuenta, debido a que el acto de sabotear los activos se vería reflejado de manera negativa para el mismo personal que decidiera llevarlo a cabo, independientemente de que sea factible o no.
- La amenaza "intrusos remunerados" no se toma en cuenta para PEMEX Refinación ni tampoco para el CEASP^{4}A; por considerarlo un caso improbable de presentarse, no así para el escenario contratistas externos.

5.5.2. Consideraciones para la evaluación de riesgos en PEMEX Refinación

En esta sección se establecerán conjeturas para descartar relaciones amenaza-vulnerabilidad que competen al escenario PEMEX Refinación.

- Las vulnerabilidades de tipo físicas y de software no se considerarán para las amenazas que surgen a partir de los siguientes tipos de personal: Ingenieros del Área de Seguridad, dibujantes y ayudantes de ingeniero debido a su perfil, por los conocimientos poseídos en el área de computación y al tipo de permisos que tienen sobre los activos a proteger y los equipos de cómputo.
- La amenaza "negligentes" para el personal: Administradores de T.I. de PEMEX Refinación y los ingenieros del área de seguridad no se toma en cuenta, debido a que es un puesto muy estricto en cuanto al reclutamiento y al perfil psicológico requerido para laborar en el.

5.5.3. Consideraciones para la evaluación de riesgos en el CEASP^{4}A

En esta sección se establecerán conjeturas para descartar relaciones amenaza-vulnerabilidad que competen al escenario CEASP^{4}A UNAM.

- No se toma en cuenta ningún tipo de amenaza derivada del personal de soporte técnico del CEASP^{4}A ni tampoco se considera algún tipo de vulnerabilidad, se considerará a este personal como el más confiable, con ética profesional y un perfil psicológico adecuado.
- Las vulnerabilidades de software no se considerarán para las amenazas que surgen a partir de los: coordinadores, residentes y empleados del CEASP^{4}A, debido a su perfil, por los conocimientos poseídos en el área de computación.
- La amenaza “negligentes” para el personal: Coordinadores del CEASP^{4}A y residentes del CEASP^{4}A no se toma en cuenta, debido a que es un puesto estricto en cuanto al reclutamiento y al perfil psicológico requerido para laborar en el.
- Las vulnerabilidades de tipo físicas no se considerarán para las amenazas que surgen a partir de los empleados del CEASP^{4}A, debido al tipo de permisos que tienen sobre los activos a proteger y los equipos de cómputo.

5.5.4. Consideraciones para la evaluación de riesgos para los contratistas externos

En esta sección no se establecerán conjeturas, se tomarán todos los casos.

5.6. Cruce de amenazas y vulnerabilidades

Tomando las consideraciones mencionas desde la sección 5.5.1 hasta la 5.5.4, se procede a efectuar el cruce de amenazas y vulnerabilidades.

Tabla 27. Relación de vulnerabilidades para la amenaza ATI-L-PR.

Relación de vulnerabilidades para la amenaza *A*dministradores de T.I. de PEMEX Refinación ladrones		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
ATI-L-PR	F-AECE-PR	NO
ATI-L-PR	F-AECP-PR	NO
ATI-L-PR	**S-EPC-PR**	**SÍ**
ATI-L-PR	**S-EIV-PR**	**SÍ**
Justificación: Solo se consideran dos de los cruces debido a que el personal no necesita de los equipos de cómputo para realizar el ataque.		

Tabla 28. Relación de vulnerabilidades para la amenaza ATI-F-PR.

Relación de vulnerabilidades para la amenaza Administradores de T.I. de PEMEX Refinación fraudulentos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
ATI-F-PR	**F-AECE-PR**	**SÍ**
ATI-F-PR	**F-AECP-PR**	**SÍ**
ATI-F-PR	**S-EPC-PR**	**SÍ**
ATI-F-PR	**S-EIV-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: En esta relación no hay consideraciones especiales, se toman todos los casos.		

Tabla 29. Relación de vulnerabilidades para la amenaza ATI-M-PR.

Relación de vulnerabilidades para la amenaza Administradores de T.I. de PEMEX Refinación manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
ATI-M-PR	H-PSPPA-PR	NO
ATI-M-PR	H-PSIS-PR	NO
ATI-M-PR	H-PNA-PR	NO
ATI-M-PR	H-PD-PR	NO
Justificación sobre esta relación de amenaza-vulnerabilidades: Esta relación se descarta por completo, debido a que este tipo de personal no necesita manipular a nadie para obtener acceso a la distribución de los activos a proteger.		

Tabla 30. Relación de vulnerabilidades para la amenaza E-ATI-PR.

Relación de vulnerabilidades para la amenaza Ex administradores de T.I. de PEMEX Refinación manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-ATI-PR	**H-PSPPA-PR**	**SÍ**
E-ATI-PR	**H-PSIS-PR**	**SÍ**
E-ATI-PR	**H-PNA-PR**	**SÍ**
E-ATI-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 31. Relación de vulnerabilidades para la amenaza IAS-M-PR.

Relación de vulnerabilidades para la amenaza Ingenieros del área de seguridad manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
IAS-M-PR	**H-PSPPA-PR**	**SÍ**
IAS-M-PR	**H-PSIS-PR**	**SÍ**
IAS-M-PR	**H-PNA-PR**	**SÍ**
IAS-M-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 32. Relación de vulnerabilidades para la amenaza E-IAS-PR.

Relación de vulnerabilidades para la amenaza Ex ingenieros del área de seguridad		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-IAS-PR	**H-PSPPA-PR**	**SÍ**
E-IAS-PR	**H-PSIS-PR**	**SÍ**
E-IAS-PR	**H-PNA-PR**	**SÍ**
E-IAS-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 33. Relación de vulnerabilidades para la amenaza D-M-PR.

Relación de vulnerabilidades para la amenaza Dibujantes manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
D-M-PR	**H-PSPPA-PR**	**SÍ**
D-M-PR	**H-PSIS-PR**	**SÍ**
D-M-PR	**H-PNA-PR**	**SÍ**
D-M-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 34. Relación de vulnerabilidades para la amenaza E-D-PR.

Relación de vulnerabilidades para la amenaza Ex dibujantes		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-D-PR	**H-PSPPA-PR**	**SÍ**
E-D-PR	**H-PSIS-PR**	**SÍ**
E-D-PR	**H-PNA-PR**	**SÍ**
E-D-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 35. Relación de vulnerabilidades para la amenaza AI-M-PR.

Relación de vulnerabilidades para la amenaza Ayudantes de ingeniero manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
AI-M-PR	**H-PSPPA-PR**	**SÍ**
AI-M-PR	**H-PSIS-PR**	**SÍ**
AI-M-PR	**H-PNA-PR**	**SÍ**
AI-M-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 36. Relación de vulnerabilidades para la amenaza E-AI-PR.

Relación de vulnerabilidades para la amenaza Ex ayudantes de ingeniero		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-AI-PR	**H-PSPPA-PR**	**SÍ**
E-AI-PR	**H-PSIS-PR**	**SÍ**
E-AI-PR	**H-PNA-PR**	**SÍ**
E-AI-PR	**H-PD-PR**	**SÍ**
Justificación sobre esta relación de amenaza-vulnerabilidades: Misma justificación que en la tabla 28.		

Tabla 37. Relación de vulnerabilidades para la amenaza C-L-CU.

Relación de vulnerabilidades para la amenaza Coordinadores del CEASP[4]A ladrones		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
C-L-CU	F-AECE-CU	NO
C-L-CU	**F-AECP-CU**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: En esta relación solo se considera uno de los cruces debido a que el personal no tiene permisos de acceso administrativos sobre los equipos de cómputo de escritorio.		

Tabla 38. Relación de vulnerabilidades para la amenaza C-F-CU.

Relación de vulnerabilidades para la amenaza Coordinadores del CEASP^{4}A fraudulentos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
C-F-CU	F-AECE-CU	NO
C-F-CU	F-AECP-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: En esta relación no se considera ningún cruce debido a que el personal no tiene los permisos administrativos requeridos sobre los equipos de cómputo necesarios para realizar el proceso de distribución de los activos. Por ello se descarta esta relación		

Tabla 39. Relación de vulnerabilidades para la amenaza C-M-CU.

Relación de vulnerabilidades para la amenaza Coordinadores del CEASP^{4}A manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
C-M-CU	H-PSPPA-CU	NO
C-M-CU	H-PSIS-CU	NO
C-M-CU	H-PNA-CU	NO
C-M-CU	H-PD-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: En esta relación no se considera ningún cruce porque el personal necesitaría manipular al personal de soporte técnico para lograr su objetivo, el cual no está considerado en ningún momento. Por lo que esta relación también se descarta.		

Tabla 40. Relación de vulnerabilidades para la amenaza E-C-CU.

Relación de vulnerabilidades para la amenaza Ex coordinadores del CEASP^{4}A		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-C-CU	H-PSPPA-CU	NO
E-C-CU	H-PSIS-CU	NO
E-C-CU	H-PNA-CU	NO
E-C-CU	H-PD-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: En el CEASP^{4}A existen tres coordinadores, los cuales siguen conservando su puesto de trabajo, esta amenaza no existe, se descarta por completo la relación.		

Tabla 41. Relación de vulnerabilidades para la amenaza R-L-CU.

Relación de vulnerabilidades para la amenaza Residentes del CEASP[4]A ladrones		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
R-L-CU	**F-AECE-CU**	**SÍ**
R-L-CU	**F-AECP-CU**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 42. Relación de vulnerabilidades para la amenaza R-F-CU.

Relación de vulnerabilidades para la amenaza Residentes del CEASP[4]A fraudulentos		
Amenaza	Vulnerabilidad	Consideración de las acepciones para la relación
R-F-CU	F-AECE-CU	NO
R-F-CU	F-AECP-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 38.		

Tabla 43. Relación de vulnerabilidades para la amenaza R-M-CU.

Relación de vulnerabilidades para la amenaza Residentes del CEASP[4]A manipuladores		
Amenaza	Vulnerabilidad	Consideración de las acepciones para la relación
R-M-CU	H-PSPPA-PR	NO
R-M-CU	H-PSIS-PR	NO
R-M-CU	H-PNA-PR	NO
R-M-CU	H-PD-PR	NO
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 39.		

Tabla 44. Relación de vulnerabilidades para la amenaza E-R-CU.

Relación de vulnerabilidades para la amenaza Ex residentes del CEASP[4]A		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-R-CU	**H-PSPPA-CU**	**SÍ**
E-R-CU	**H-PSIS-CU**	**SÍ**
E-R-CU	**H-PNA-CU**	**SÍ**
E-R-CU	**H-PD-CU**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28		

Tabla 45. Relación de vulnerabilidades para la amenaza E-L-CU.

Relación de vulnerabilidades para la amenaza Empleados del CEASP[4]A ladrones		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-L-CU	F-AECE-CU	NO
E-L-CU	F-AECP-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: En esta relación no se considera ningún cruce porque el personal no tiene los permisos necesarios sobre los activos a proteger. Por lo tanto, esta relación se descarta.		

Tabla 46. Relación de vulnerabilidades para la amenaza E-F-CU.

Relación de vulnerabilidades para la amenaza Empleados del CEASP[4]A fraudulentos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-F-CU	F-AECE-CU	NO
E-F-CU	F-AECP-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 38.		

Tabla 47. Relación de vulnerabilidades para la amenaza E-N-CU.

Relación de vulnerabilidades para la amenaza Empleados del CEASP[4]A negligentes		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-N-CU	F-AECE-CU	NO
E-N-CU	F-AECP-CU	NO
Justificación sobre la relación de amenaza-vulnerabilidades: En esta relación no se considera ningún cruce porque el personal no tiene los permisos necesarios sobre los activos a proteger, y no sería posible que su negligencia causara algún daño considerable a los mismos. Por lo tanto, esta relación se descarta.		

Tabla 48. Relación de vulnerabilidades para la amenaza E-M-CU.

Relación de vulnerabilidades para la amenaza Empleados del CEASP[4]A manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-M-CU	H-PSPPA-PR	NO
E-M-CU	H-PSIS-PR	NO
E-M-CU	H-PNA-PR	NO
E-M-CU	H-PD-PR	NO
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 39.		

Tabla 49. Relación de vulnerabilidades para la amenaza E-E-CU.

Relación de vulnerabilidades para la amenaza Ex empleados del CEASP[4]A		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-E-CU	**H-PSPPA-CU**	**SÍ**
E-E-CU	**H-PSIS-CU**	**SÍ**
E-E-CU	**H-PNA-CU**	**SÍ**
E-E-CU	**H-PD-CU**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 50. Relación de vulnerabilidades para la amenaza L-CE.

Relación de vulnerabilidades para la amenaza Contratistas externos ladrones		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
L-CE	**F-AUCQ-CE**	**SÍ**
L-CE	**S-EPC-CE**	**SÍ**
L-CE	**S-EIV-PR**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 51. Relación de vulnerabilidades para la amenaza F-CE.

Relación de vulnerabilidades para la amenaza Contratistas externos fraudulentos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
F-CE	**F-AUCQ-CE**	**SÍ**
F-CE	**S-EPC-CE**	**SÍ**
F-CE	**S-EIV-PR**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 52. Relación de vulnerabilidades para la amenaza S-CE.

Relación de vulnerabilidades para la amenaza Contratistas externos saboteadores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
S-CE	**F-AUCQ-CE**	**SÍ**
S-CE	**S-EPC-CE**	**SÍ**
S-CE	**S-EIV-PR**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 53. Relación de vulnerabilidades para la amenaza N-CE.

Relación de vulnerabilidades para la amenaza Contratistas externos negligentes		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
N-CE	**F-AUCQ-CE**	**SÍ**
N-CE	**S-EPC-CE**	**SÍ**
N-CE	**S-EIV-PR**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 54. Relación de vulnerabilidades para la amenaza M-CE.

Relación de Vulnerabilidades para la amenaza Contratistas externos manipuladores		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
M-CE	**H-D-CE**	**SÍ**
M-CE	**H-PSPPAPR-CE**	**SÍ**
M-CE	**H-PSPPACU-CE**	**SÍ**
M-CE	**H-PSISPR-CE**	**SÍ**
M-CE	**H-PSISCU-CE**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 55. Relación de vulnerabilidades para la amenaza E-CE.

Relación de vulnerabilidades para la amenaza Ex contratistas externos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
E-CE	**H-D-CE**	**SÍ**
E-CE	**H-PSPPAPR-CE**	**SÍ**
E-CE	**H-PSPPACU-CE**	**SÍ**
E-CE	**H-PSISPR-CE**	**SÍ**
E-CE	**H-PSISCU-CE**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 56. Relación de vulnerabilidades para la amenaza C-CE.

Relación de vulnerabilidades para la amenaza Crackers dispuestos a dañar por los contratistas externos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
C-CE	**F-AUCQ-CE**	**SÍ**
C-CE	**S-EPC-CE**	**SÍ**
C-CE	**S-EIV-PR**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 57. Relación de vulnerabilidades para la amenaza HGH-CE.

Relación de vulnerabilidades para la amenaza Hackers Gray Hat dispuestos a dañar por los Contratistas Externos		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
HGH-CE	**F-AUCQ-CE**	**SÍ**
HGH-CE	**S-EPC-CE**	**SÍ**
HGH-CE	**S-EIV-PR**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 58. Relación de vulnerabilidades para la amenaza PTL-DME.

Relación de vulnerabilidades para la amenaza Diseño mal elaborado de los mecanismos de validación para los tres escenarios		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
PTL-DME	**S-EPC-PR**	**SÍ**
PTL-DME	**S-EIV-PR**	**SÍ**
PTL-DME	**S-EPC-CU**	**SÍ**
PTL-DME	**S-EIV-CU**	**SÍ**
PTL-DME	**S-EPC-CE**	**SÍ**
PTL-DME	**S-EIV-CE**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

Tabla 59. Relación de vulnerabilidades para la amenaza PTL-DMI.

Relación de Vulnerabilidades para la amenaza Diseño mal implementado de los mecanismos de validación para los tres escenarios		
Amenaza	Vulnerabilidad	Consideración de la relación para este trabajo
PTL-DMI	**S-EPC-PR**	**SÍ**
PTL-DMI	**S-EIV-PR**	**SÍ**
PTL-DMI	**S-EPC-CU**	**SÍ**
PTL-DMI	**S-EIV-CU**	**SÍ**
PTL-DMI	**S-EPC-CE**	**SÍ**
PTL-DMI	**S-EIV-CE**	**SÍ**
Justificación sobre la relación de amenaza-vulnerabilidades: Misma consideración que en la tabla 28.		

5.7. Relación de amenazas y vulnerabilidades consideradas

En este paso se realizará una agrupación y se clasificarán las relaciones de amenaza-vulnerabilidades consideradas del apartado 5.6, tal y como se describe en el apartado 4.1.6.

Tabla 60. Relación 01 considerada para el análisis de riesgos: ATI-L + S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	ATI-L+S-EPC	Administradores de T.I. de PEMEX Refinación ladrones que aprovechan los errores de programación en el código fuente de la QITDraw distribuida en PEMEX Refinación
	ATI-L+S-EIV	Administradores de T.I. de PEMEX Refinación ladrones que aprovechan los errores Inesperados en validaciones para la QITDraw distribuida en PEMEX Refinación

Tabla 61. Relación 02 considerada para el análisis de riesgos: ATI-F + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	ATI-F+F-AECE	Administradores de T.I. de PEMEX Refinación fraudulentos con acceso a los equipos de computo de escritorio en PEMEX Refinación que contienen a la herramienta
	ATI-F+F-AECP	Administradores de T.I. de PEMEX Refinación fraudulentos con acceso a los equipos de computo portátiles en PEMEX Refinación que contienen a la herramienta
	ATI-F+S-EPC	Administradores de T.I. de PEMEX Refinación fraudulentos que aprovechan los errores de programación en el código fuente de la QITDraw distribuida en PEMEX Refinación
	ATI-F+S-EIV	Administradores de T.I. de PEMEX Refinación fraudulentos que aprovechan los errores Inesperados en validaciones para la QITDraw distribuida en PEMEX Refinación

Tabla 62. Relación 03 considerada para el análisis de riesgos: E-ATI + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	E-ATI+H-PSPPA	Ex administradores de T.I. de PEMEX Refinación que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	E-ATI+H-PSIS	Ex administradores de T.I. de PEMEX Refinación que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	E-ATI+H-PNA	Ex administradores de T.I. de PEMEX Refinación que aprovechan a personal no autorizado en PEMEX Refinación
	E-ATI+H-PD	Ex administradores de T.I. de PEMEX Refinación que aprovechan a personal descuidado en PEMEX Refinación

Tabla 63. Relación 04 considerada para el análisis de riesgos: IAS-M + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	IAS-M+H-PSPPA	Ingenieros del área de seguridad manipuladores que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	IAS-M+H-PSIS	Ingenieros del área de seguridad manipuladores que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	IAS-M+H-PNA	Ingenieros del área de seguridad manipuladores que aprovechan a personal no autorizado en PEMEX Refinación
	IAS-M+H-PD	Ingenieros del área de seguridad manipuladores que aprovechan a personal descuidado en PEMEX Refinación

Tabla 64. Relación 05 considerada para el análisis de riesgos: E-IAS + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	E-IAS+H-PSPPA	Ex ingenieros del área de seguridad que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	E-IAS+H-PSIS	Ex ingenieros del área de seguridad que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	E-IAS+H-PNA	Ex ingenieros del área de seguridad que aprovechan a personal no autorizado en PEMEX Refinación
	E-IAS+H-PD	Ex ingenieros del área de seguridad que aprovechan a personal descuidado en PEMEX Refinación

Tabla 65. Relación 06 considerada para el análisis de riesgos: D-M + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	D-M+H-PSPPA	Dibujantes manipuladores que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	D-M+H-PSIS	Dibujantes manipuladores que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	D-M+H-PNA	Dibujantes manipuladores que aprovechan a personal no autorizado en PEMEX Refinación
	D-M+H-PD	Dibujantes manipuladores que aprovechan a personal descuidado en PEMEX Refinación

Tabla 66. Relación 07 considerada para el análisis de riesgos: E-D + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	E-D+H-PSPPA	Ex dibujantes que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	E-D+H-PSIS	Ex dibujantes que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	E-D+H-PNA	Ex dibujantes que aprovechan a personal no autorizado en PEMEX Refinación
	E-D+H-PD	Ex dibujantes que aprovechan a personal descuidado en PEMEX Refinación

Tabla 67. Relación 08 considerada para el análisis de riesgos: AI-M + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	AI-M+H-PSPPA	Ayudantes de ingeniero manipuladores que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	AI-M+H-PSIS	Ayudantes de ingeniero manipuladores que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	AI-M+H-PNA	Ayudantes de ingeniero manipuladores que aprovechan a personal no autorizado en PEMEX Refinación
	AI-M+H-PD	Ayudantes de ingeniero manipuladores que aprovechan a personal descuidado en PEMEX Refinación

Tabla 68. Relación 09 considerada para el análisis de riesgos: E-AI + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR	E-AI+H-PSPPA	Ex ayudantes de ingeniero que aprovechan a personal sin perfil psicológico adecuado en Pemex Refinación
	E-AI+H-PSIS	Ex ayudantes de ingeniero que aprovechan a personal susceptible a ingeniería social en Pemex Refinación
	E-AI+H-PNA	Ex ayudantes de ingeniero que aprovechan a personal no autorizado en PEMEX Refinación
	E-AI+H-PD	Ex ayudantes de ingeniero que aprovechan a personal descuidado en PEMEX Refinación

Tabla 69. Relación 10 considerada para el análisis de riesgos: C-L + F.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CU	C-L+F-AECP	Coordinadores del CEASP^{4}A ladrones con acceso a los equipos de computo portátiles en el CEASP^{4}A que contienen a la herramienta

Tabla 70. Relación 11 considerada para el análisis de riesgos: R-L + F.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CU	R-L+F-AECP	Residentes del CEASP^{4}A ladrones con acceso a los equipos de computo portátiles en el CEASP^{4}A que contienen a la herramienta

Tabla 71. Relación 12 considerada para el análisis de riesgos: E-R + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CU	E-R+H-PSPPA	Ex residentes del CEASP^{4}A que aprovechan a personal sin perfil psicológico adecuado en el CEASP^{4}A
	E-R+H-PSIS	Ex residentes del CEASP^{4}A que aprovechan a personal susceptible a ingeniería social en el CEASP^{4}A
	E-R+H-PNA	Ex residentes del CEASP^{4}A que aprovechan a personal no autorizado en el CEASP^{4}A
	E-R+H-PD	Ex residentes del CEASP^{4}A que aprovechan a personal descuidado en el CEASP^{4}A

Tabla 72. Relación 13 considerada para el análisis de riesgos: E-E + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CU	E-E+H-PSPPA	Ex empleados del CEASP^{4}A que aprovechan a personal sin perfil psicológico adecuado en el CEASP^{4}A
	E-E+H-PSIS	Ex empleados del CEASP^{4}A que aprovechan a personal susceptible a ingeniería social en el CEASP^{4}A
	E-E+H-PNA	Ex empleados del CEASP^{4}A que aprovechan a personal no autorizado en el CEASP^{4}A
	E-E+H-PD	Ex empleados del CEASP^{4}A que aprovechan a personal descuidado en el CEASP^{4}A

Tabla 73. Relación 14 considerada para el análisis de riesgos: L + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	L+F-AUCQ	Contratistas externos ladrones con a las USB que contienen a la QITDraw que se distribuye para cada uno de ellos
	L+S-EPC	Contratistas externos ladrones que aprovechan los errores de programación en el código fuente de la QITDraw distribuida para cada uno de ellos
	L+S-EIV	Contratistas externos ladrones que aprovechan los errores Inesperados en validaciones para la QITDraw distribuida para cada uno de ellos

Tabla 74. Relación 15 considerada para el análisis de riesgos: F + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	F+F-AUCQ	Contratistas externos fraudulentos con a las USB que contienen a la QITDraw que se distribuye para cada uno de ellos
	F+S-EPC	Contratistas externos fraudulentos que aprovechan los errores de programación en el código fuente de la QITDraw distribuida para cada uno de ellos
	F+S-EIV	Contratistas externos fraudulentos que aprovechan los errores Inesperados en validaciones para la QITDraw distribuida para cada uno de ellos

Tabla 75. Relación 16 considerada para el análisis de riesgos: S + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	S+F-AUCQ	Contratistas externos saboteadores con a las USB que contienen a la QITDraw que se distribuye para cada uno de ellos
	S+S-EPC	Contratistas externos saboteadores que aprovechan los errores de programación en el código fuente de la QITDraw distribuida para cada uno de ellos
	S+S-EIV	Contratistas externos saboteadores que aprovechan los errores Inesperados en validaciones para la QITDraw distribuida para cada uno de ellos

Tabla 76. Relación 17 considerada para el análisis de riesgos: N + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	N+F-AUCQ	Contratistas externos negligentes con las USB que contienen a la QITDraw que se distribuye para cada uno de ellos
	N+S-EPC	Contratistas externos negligentes que aprovechan los errores de programación en el código fuente de la QITDraw distribuida para cada uno de ellos
	N+S-EIV	Contratistas externos negligentes que aprovechan los errores Inesperados en validaciones para la QITDraw distribuida para cada uno de ellos

Tabla 77. Relación 18 considerada para el análisis de riesgos: M + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	M+H-D-CE	Contratistas externos manipuladores que aprovechan a compañeros contratistas externos descuidados
	M+H-PSPPAPR M+H-PSPPACU	Contratistas externos manipuladores que aprovechan a personal sin perfil psicológico adecuado de PEMEX Refinación o del CEASP[4]A
	M+H-PSISPR M+H-PSISCU	Contratistas externos manipuladores que aprovechan a personal susceptible a ingeniería social de PEMEX Refinación o del CEASP[4]A

Tabla 78. Relación 19 considerada para el análisis de riesgos: E + H.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	E+H-D-CE	Ex contratistas externos manipuladores que aprovechan a compañeros contratistas externos descuidados
	E+H-PSPPAPR E+H-PSPPACU	Ex contratistas externos manipuladores que aprovechan a personal sin perfil psicológico adecuado de PEMEX Refinación o del CEASP^{4}A
	E+H-PSISPR E+H-PSISCU	Ex contratistas externos manipuladores que aprovechan a personal susceptible a ingeniería social de PEMEX Refinación o del CEASP^{4}A

Tabla 79. Relación 20 considerada para el análisis de riesgos: C + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	C+F-AUCQ	Crackers dispuestos a dañar por los contratistas externos las USB que contienen a la QITDraw que se distribuye para cada uno de ellos
	C+S-EPC	Crackers dispuestos a dañar por los contratistas externos aprovechando los errores de programación en el código fuente de la QITDraw distribuida para cada uno de ellos
	C+S-EIV	Crackers dispuestos a dañar por los contratistas externos aprovechando los errores Inesperados en validaciones para la QITDraw distribuida para cada uno de ellos

Tabla 80. Relación 21 considerada para el análisis de riesgos: HGH + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
CE	HGH+F-AUCQ	Hackers Gray Hat dispuestos a dañar por los contratistas externos las USB que contienen a la QITDraw que se distribuye para cada uno de ellos
	HGH+S-EPC	Hackers Gray Hat dispuestos a dañar por los contratistas externos aprovechando los errores de programación en el código fuente de la QITDraw distribuida para cada uno de ellos
	HGH+S-EIV	Hackers Gray Hat dispuestos a dañar por los contratistas externos aprovechando los errores Inesperados en validaciones para la QITDraw distribuida para cada uno de ellos

Tabla 81. Relación 22 considerada para el análisis de riesgos: HGH + F, S.

Escenario	Abreviatura de las relaciones consideradas	Nombre de la relación
PR, CU, CE	PTL-DME+EPC	Diseño mal elaborado de los mecanismos de validación que podrían generar errores de programación en el código fuente de la QITDraw distribuida en los tres escenarios
	PTL-DME+EIV	Diseño mal elaborado de los mecanismos de validación que podrían generar errores inesperados en validaciones para la QITDraw distribuida en los tres escenarios
	PTL-DMI+EPC	Diseño mal implementado de los mecanismos de validación que podrían generar errores de programación en el código fuente de la QITDraw distribuida en los tres escenarios
	PTL-DMI+EPC	Diseño mal implementado de los mecanismos de validación que podrían generar errores inesperados en validaciones para la QITDraw distribuida en los tres escenarios

5.8. Cuantificación de los riesgos

En esta sección se realiza la determinación del impacto de ocurrencia de las amenazas, con base al análisis de los controles del lugar, la determinación de los riesgos residuales y las recomendaciones en caso de ser necesarias.

De la tabla 82 a la tabla 103 se utilizarán las siguientes abreviaturas:

I = Impacto del acontecimiento.

Fr = Frecuencia / Probabilidad del acontecimiento.

CR = Categoría del Riesgo.

Tabla 82. Cuantificación de riesgos para la relación 01: ATI-L + S en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
ATI-L+S-EPC	4	3	**B**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	4	3	**B**	Introducir medidas de control con Prioridad Media.
ATI-L+S-EIV	4	3	**B**		4	3	**B**	Introducir medidas de control con Prioridad Media.

Tabla 83. Cuantificación de riesgos para la relación 02: ATI-F + F, S en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
ATI-F+F-AECE	3	2	C	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	2	2	D	No se consideran necesarios controles adicionales
ATI-F+F-AECP	3	2	C		2	2	D	No se consideran necesarios controles adicionales
ATI-F+S-EPC	3	2	C		2	2	D	No se consideran necesarios controles adicionales
ATI-F+S-EIV	3	2	C		2	2	D	No se consideran necesarios controles adicionales

Tabla 84. Cuantificación de riesgos para la relación 03: E-ATI + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E-ATI+H-PSPPA	4	1	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	3	1	D	No se consideran necesarios controles adicionales
E-ATI+H-PSIS	4	1	C		3	1	D	No se consideran necesarios controles adicionales
E-ATI+H-PNA	4	1	D		3	1	D	No se consideran necesarios controles adicionales
E-ATI+H-PD	3	1	D		3	1	D	No se consideran necesarios controles adicionales

Tabla 85. Cuantificación de riesgos para la relación 04: IAS-M + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
IAS-M+H-PSPPA	4	2	C	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	3	1	D	No se consideran necesarios controles adicionales
IAS-M+H-PSIS	4	2	C		4	1	D	No se consideran necesarios controles adicionales
IAS-M+H-PNA	4	2	C		4	1	D	No se consideran necesarios controles adicionales
IAS-M+H-PD	3	1	D		2	1	D	No se consideran necesarios controles adicionales

Tabla 86. Cuantificación de riesgos para la relación 05: E-IAS + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E-IAS+H-PSPPA	4	2	C	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	2	2	D	No se consideran necesarios controles adicionales
E-IAS+H-PSIS	2	4	C		1	4	D	No se consideran necesarios controles adicionales
E-IAS+H-PNA	4	2	C		2	2	D	No se consideran necesarios controles adicionales
E-IAS+H-PD	2	4	C		1	4	D	No se consideran necesarios controles adicionales

Tabla 87. Cuantificación de riesgos para la relación 06: D-M + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
D-M+H-PSPPA	4	1	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	3	0	D	No se consideran necesarios controles adicionales
D-M+H-PSIS	4	2	C		3	1	D	No se consideran necesarios controles adicionales
D-M+H-PNA	4	2	C		3	1	D	No se consideran necesarios controles adicionales
D-M+H-PD	3	1	D		2	0	D	No se consideran necesarios controles adicionales

Tabla 88. Cuantificación de riesgos para la relación 07: E-D + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	F	CR	
E-D+H-PSPPA	3	0	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	1	0	D	No se consideran necesarios controles adicionales
E-D+H-PSIS	3	1	C		1	1	D	No se consideran necesarios controles adicionales
E-D+H-PNA	3	1	C		1	1	D	No se consideran necesarios controles adicionales
E-D+H-PD	2	0	D		0	0	D	No se consideran necesarios controles adicionales

Tabla 89. Cuantificación de riesgos para la relación 08: AI-M + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
AI-M+H-PSPPA	2	1	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	1	1	D	No se consideran necesarios controles adicionales
AI-M+H-PSIS	2	2	D		1	2	D	No se consideran necesarios controles adicionales
AI-M+H-PNA	3	2	C		2	2	D	No se consideran necesarios controles adicionales
AI-M+H-PD	2	1	D		1	1	D	No se consideran necesarios controles adicionales

Tabla 90. Cuantificación de riesgos para la relación 09: E-AI + H en el escenario PR.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E-AI+H-PSPPA	1	2	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	1	1	D	No se consideran necesarios controles adicionales
E-AI+H-PSIS	1	3	D		1	2	D	No se consideran necesarios controles adicionales
E-AI+H-PNA	2	3	C		2	2	D	No se consideran necesarios controles adicionales
E-AI+H-PD	1	2	D		1	1	D	No se consideran necesarios controles adicionales

Tabla 91. Cuantificación de riesgos para la relación 10: C-L + F en el escenario CU.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
C-L+F-AECP	3	2	**C**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio CEASP^{4}A.	3	1	**D**	No se consideran necesarios controles adicionales

Tabla 92. Cuantificación de riesgos para la relación 11: R-L + F en el escenario CU.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
R-L+F-AECE	3	2	**C**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	3	1	**D**	No se consideran necesarios controles adicionales.

Tabla 93. Cuantificación de riesgos para la relación 12: E-R + H en el escenario CU.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E-R+H-PSPPA	4	1	**D**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	3	1	**D**	No se consideran necesarios controles adicionales
E-R+H-PSIS	4	1	**D**		3	1	**D**	No se consideran necesarios controles adicionales
E-R+H-PNA	4	1	**D**		3	1	**D**	No se consideran necesarios controles adicionales
E-R+H-PD	4	1	**D**		3	1	**D**	No se consideran necesarios controles adicionales

Tabla 94. Cuantificación de riesgos para la relación 13: E-E + H en el escenario CU.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E-E+H-PSPPA	1	3	**D**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	1	2	D	No se consideran necesarios controles adicionales
E-E+H-PSIS	1	3	**D**		1	2	D	No se consideran necesarios controles adicionales
E-E+H-PNA	1	3	**D**		1	2	D	No se consideran necesarios controles adicionales
E-E+H-PD	1	3	**D**		1	2	D	No se consideran necesarios controles adicionales

Tabla 95. Cuantificación de riesgos para la relación 14: L + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
L+F-AUCQ	4	2	**C**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	4	1	**D**	No se consideran necesarios controles adicionales
L+S-EPC	3	2	**C**		3	1	**D**	No se consideran necesarios controles adicionales
L+S-EIV	3	2	**C**		3	1	**D**	No se consideran necesarios controles adicionales

Tabla 96. Cuantificación de riesgos para la relación 15: F + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
F+F-AUCQ	3	2	**C**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	3	1	**D**	No se consideran necesarios controles adicionales
F+S-EPC	3	2	**C**		2	1	**D**	No se consideran necesarios controles adicionales
F+S-EIV	3	2	**C**		2	1	**D**	No se consideran necesarios controles adicionales

Tabla 97. Cuantificación de riesgos para la relación 16: S + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
S+F-AUCQ	2	2	**D**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	2	1	**D**	No se consideran necesarios controles adicionales
S+S-EPC	2	2	**D**		2	1	**D**	No se consideran necesarios controles adicionales
S+S-EIV	2	2	**D**		2	1	**D**	No se consideran necesarios controles adicionales

Tabla 98. Cuantificación de riesgos para la relación 17: N + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
N+F-AUCQ	1	3	**D**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	1	2	**D**	No se consideran necesarios controles adicionales
N+S-EPC	1	3	**D**		1	2	**D**	No se consideran necesarios controles adicionales
N+S-EIV	1	3	**D**		1	2	**D**	No se consideran necesarios controles adicionales

Tabla 99. Cuantificación de riesgos para la relación 18: M + H en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
M+H-D-CE	2	2	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	2	0	D	No se consideran necesarios controles adicionales
M+H-PSPPAPR	2	3	C		2	1	D	No se consideran necesarios controles adicionales
M+H-PSPPACU	2	4	C		2	2	D	No se consideran necesarios controles adicionales
M+H-PSISPR	2	3	C		2	1	D	No se consideran necesarios controles adicionales
M+H-PSISCU	1	4	D		1	2	D	No se consideran necesarios controles adicionales

Tabla 100. Cuantificación de riesgos para la relación 19: E + H en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
E+H-PSPPAPR	1	1	D	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	1	0	D	No se consideran necesarios controles adicionales
E+H-PSISPR	2	2	D		2	1	D	No se consideran necesarios controles adicionales
E+H-PSPPACU	2	2	D		2	1	D	No se consideran necesarios controles adicionales
E+H-PSISCU	2	2	D		2	1	D	No se consideran necesarios controles adicionales
E+H-CED	2	2	D		2	1	D	No se consideran necesarios controles adicionales

Tabla 101. Cuantificación de riesgos para la relación 20: C + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
C+F-AUCQ	4	3	**B**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	4	3	**B**	Introducir medidas de control con Prioridad Media.
C+S-EPC	4	3	**B**		4	3	**B**	Introducir medidas de control con Prioridad Media.
C+S-EIV	4	3	**B**		4	3	**B**	Introducir medidas de control con Prioridad Media.

Tabla 102. Cuantificación de riesgos para la relación 21: HGH + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
HGH+F-AUCQ	4	3	**B**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	4	3	**B**	Introducir medidas de control con Prioridad Media.
HGH+S-EPC	4	3	**B**		4	3	**B**	Introducir medidas de control con Prioridad Media.
HGH+S-EIV	4	3	**B**		4	3	**B**	Introducir medidas de control con Prioridad Media.

Tabla 103. Cuantificación de riesgos para la relación 22: HGH + F, S en el escenario CE.

Relación de amenaza - vulnerabilidad	Evaluación del riesgo inicial (sin controles)			Controles	Evaluación del riesgo residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
PTL-DME + H-PVMDOACC	4	2	**C**	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	4	1	**D**	No se consideran necesarios controles adicionales
PTL-DMI + H-PVMDOACC	4	2	**C**		4	1	**D**	No se consideran necesarios controles adicionales

5.9. Preparación del informe para el análisis de riesgos

Las relaciones Amenaza-Vulnerabilidades de mayor riesgo fueron las siguientes:

Tabla 104. Relación de Amenaza-Vulnerabilidades de mayor riesgo.

Escenario	Relación de amenaza-vulnerabilidad	Categoría de riesgo (CR)	Significado de CR	Controles actuales	Efectividad de los controles actuales
PR	ATI-L+S-EPC	**B**	Indeseable: Introducir medidas de control con prioridad media	**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno. **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con el dominio PEMEX.	Los controles no son efectivos para cubrir los casos de amenaza y el riesgo residual es muy elevado. Se requieren controles adicionales que mitiguen y manejen adecuadamente los riesgos.
	ATI-L+S-EIV				
CE	C+F-AUCQ			**Correctivo:** La licencia tiene vigencia. **Detector:** Ninguno **Disuasivo:** La QITDraw tiene actualizaciones regulares. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	
	C+S-EPC				
	C+S-EIV				
	HGH+F-AUCQ				
	HGH+S-EPC				
	HGH+S-EIV				

Notas adicionales: Es trascendental puntualizar que el escenario CU (CEASP^{4}A), no presentó ningún riesgo significativo con ninguna de las relaciones amenaza-vulnerabilidad que se evaluaron para el mismo.

CAPÍTULO 6

PROPUESTA DE MEJORA

De acuerdo con los resultados de la sección 5.9, existen 8 relaciones de amenaza-vulnerabilidad que presentan un riesgo indeseable que podría afectar a los activos a proteger en el proceso de distribución de la QITDraw. Los controles implementados actualmente son efectivos en todas las otras relaciones para un funcionamiento seguro de la QITDraw, sin embargo, cuando amenazas de tipo humano cuyo perfil comparte la característica común de: tener un conocimiento extenso en diversas áreas de la computación, los mecanismos de seguridad actualmente implementados resultan ser inefectivos.

Por ello, lo primero que se buscará con la creación de la propuesta de mejora es la determinación de los controles adecuados para manejar los riesgos para las relaciones de amenaza-vulnerabilidad presentadas en la sección 5.9. Después, se revisara si estos nuevos mecanismos son adecuados para también proporcionar los tres servicios de seguridad que conforman la triada de la seguridad; en caso de que la respuesta sea afirmativa, la propuesta de mejora concluirá en ese momento, de lo contrario, se continuará con la construcción de la misma hasta que los tres servicios de seguridad sean proporcionados para la el proceso de distribución de los activos de interés.

En términos prácticos, el servicio contra el que los ocho atacantes de la sección 5.9 podrían atentar, es el de confidencialidad. Para todas las relaciones de amenaza-vulnerabilidad, la categoría de riesgo concluida resulto ser “B”. Sin embargo, es congruente suponer que el no implementar controles de inmediato, cualquiera de estos cruces podría elevarse a una categoría “A”, ya que cabe recordar que este es un análisis de riesgos únicamente enfocado al proceso de distribución de la herramienta.

El código fuente de los comandos de la QITDraw, están contenidos en un archivo con extensión DLL, archivo que es el núcleo de la herramienta y el cual dentro de AutoCAD debe ser cargado con el comando “netload” para crear la herramienta de dibujo (como un Add-on) dentro del el software mencionado. Cuando la herramienta es cargada, simultáneamente, es una ocasión en la que los mecanismos de seguridad actúan para validar la herramienta. En base a la decisión de los controles de seguridad, la paleta de herramientas puede ser generada o no. Los mecanismos de seguridad implementados en la carga de la herramienta son ejecutados también en varias rutinas del funcionamiento de la QITDraw, esto proporciona protección contra posibles ataques a los escudos dado que sería necesario localizar estas rutinas para poder ejecutar este tipo de ataque.

Por cuestiones legales y de confidencialidad con el CEASP[4]A, no es posible profundizar mucho en el tema del funcionamiento de la herramienta, en cómo están constituidos los comandos o nombres exactos de las partes que conforman la librería. Pero si es posible tratar el tema en términos de funciones genéricas, lo cual se considera suficiente para explicar cómo se implementa y actúa la propuesta de mejora.

Como ya se mencionó, la paleta de herramientas se genera y es posible ocuparla, a partir de un resultado de validación dependiendo del escenario en donde se esté ejecutando la herramienta. El modulo del código del archivo DLL que se encarga de ejecutar los controles de seguridad (de aquí en adelante llamado el “Modulo de Validación”) es donde están implementados los mecanismos de seguridad actuales y también donde se implementarán los controles adiciones que se establezcan en la propuesta de mejora, en conjunto con otras acciones y recomendaciones en caso de que sean requeridas para manejar los riesgos de las ocho relaciones de amenaza-vulnerabilidad de la sección 5.9, así como para cumplir los objetivos de esta tesis.

6.1. Propuesta de mejora para el manejo de los riesgos: ofuscación del código fuente

No se considera que los métodos de validación para el escenario PEMEX Refinación o CEASP^{4}A sean inadecuados, el problema surge cuando atacantes con el perfil apropiado decidan hacer un ataque debajo del escudo (es decir, atacar al "Modulo de Validación" antes de que ejecute los controles correspondientes). Con esto, no importaría incluso que la validación ocurra en varios puntos, ya no sería eficaz debido al tipo de ataque. El ataque mencionado sería logrado sin mayor dificultad por los atacantes mencionados con solo descompilar (traducir código o información de bajo nivel de abstracción a un lenguaje medio o de mayor abstracción con la intención de obtener una forma de código fuente lo más cercana posible a la forma original del mismo). La QITDraw, no cuenta con algún mecanismo de protección para este tipo de ataque, por lo que el primer mecanismo de seguridad (control) que se estipula para la propuesta de mejor es: Ofuscación de código (M86 Security., 2012).

La ofuscación de código se refiere a encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar, en el área de desarrollo de software se refiere a realizar un acto deliberado y no destructivo para hacer que el código fuente de algún programa sea difícil de comprender para un humano. El código ofuscado es un código fuente que se ha sido complicado específicamente para ocultar su funcionalidad y mantener su confidencialidad (haciéndolo confuso). Lo anterior, complica la ingeniería inversa (el obtener información o un diseño a partir del producto final) y el descompilado del código fuente mencionado (Oleksiy, G., 2012).

Aunque existe una gran variedad de herramientas que se encargan de realizar ofuscación de código fuente (experimentales, desarrolladas por profesionales, por académicos, productos comerciales, gratuitos, de código libre, etc.), para la propuesta de mejora se utilizará “Eazfuscator.NET” para realizar el manejo de riesgos de los casos expuestos en la sección 5.9 de esta tesis (Oleksiy, G., 2012). Algunas de las razones principales por las que se decidió utilizar esta herramienta son:

- El objetivo principal del proyecto que se encarga de realizar la herramienta Eazfuscator.NET (Ofrecer el servicio de confidencialidad para proteger propiedad intelectual) coincide en parte con una parte del segundo objetivo de esta tesis.
- Eazfuscator.NET está desarrollado .NET Framework y soporta su integración a proyectos desarrollados en la misma tecnología sin importar la versión del mismo (2.0, 3.0, 3.5 and 4.0).
- Su utilización no requiere ningún conocimiento previo sobre ofuscación, basta con seguir la documentación del sitio web del proyecto.

Al implementar esta medida de control, la propiedad intelectual del código fuente quedaría protegida a un nivel apropiado. Es un hecho que existen herramientas para hacer el proceso de inverso a los ofuscadores de código (desofuscadores), sin embargo, el código generado por el proceso de desofuscación a una librería previamente ofuscada resulta en código en el cual las los nombres de las clases, así como sus métodos y propiedades, son sustituidos por nombres genéricos como “Clase1” ó “Rutina1”.

Implementado ofuscación en el código fuente sería posible manejar adecuadamente todos los riesgos que indicaban los resultados de la sección 5.9, sin embargo, el segundo objetivo específico de esta tesis solo está cubierto parcialmente; aun falta proporcionar los tres servicios que conforman la triada de seguridad (se considera que el servicio de confidencialidad solo se está proporcionando parcialmente y existen oportunidades de mejora sobre los controles actuales de seguridad en el proceso de distribución para el escenario Contratistas externos).

6.2. Propuesta de mejora para el servicio de confidencialidad: uso de AES

La QITDraw tiene controles preventivos, para esta sección de la propuesta de mejora se pondrá particular atención en el control preventivo encargado de validar la herramienta con la memoria USB otorgada a cada contratista externo. Este control validar la QITDraw contra el identificador de hardware (hardware id) que trae grabado la memoria USB como un dato único (número de serie). El diseño actual de esta validación ha funcionado adecuadamente, evitando el duplicado de la QITDraw hasta el momento, pero tiene una implementación que podría mejorarse. Para lograr lo anterior y concluir con la proporción del servicio de confidencialidad para la herramienta, se fortalecerá el mecanismo que se encarga de ofrecer este servicio. Para lo cual, se propone sustituir el actual algoritmo de validación de ese control de seguridad (un algoritmo de cifrado simétrico no estándar), por el algoritmo Rijndael (AES). En el **Apéndice 2** de esta tesis se presenta una posible implementación de una clase capaz de manejar el cifrado y descifrado de datos mediante este algoritmo. El empleo del anterior, se profundizará más en la siguiente sección de la propuesta de mejora, ya que aparte de sustituir al algoritmo implementado actualmente, forma parte de todo un esquema de licencia que se va a proponer para el siguiente servicio de seguridad.

6.3. Propuesta de mejora para el servicio de integridad: uso de MD5

Debido al análisis que se realizó para los controles para la distribución de la herramienta, se puede concluir que no existe ningún control encargado de proporcionar el servicio de integridad al proceso de distribución de la QITDraw. Por ello, se propone la utilización de un control preventivo adicional que proporcione este servicio.

Se considera adecuado proponer el uso de la función Hash unidireccional MD5, en el **Apéndice 3 y 4** de esta tesis, se presenta una posible implementación de una clase capaz de manejar el cifrado asimétrico mencionado y un método para comprobación de integridad de archivos. La manera en que se propone utilizar esta función se detallará posteriormente en la sección 6.5.

6.4. Propuesta de mejora para el servicio de disponibilidad: uso de licencia y fecha de validez

Para el servicio de disponibilidad existe una situación particular: la QITDraw tiene implementado un control correctivo, es decir, la licencia para usar la herramienta tiene cierta vigencia, medida que se implemento inicialmente por cuestiones de actualización del software, más que por seguridad. Por ello, se propone aprovechar las oportunidades de mejora de este control de seguridad, en el **Apéndice 5** se presenta una clase que muestra una posible mejora de la implementación del mecanismo de seguridad mencionado.

También se propone una refactorización del código fuente del “Modulo de Validación” de la QITDraw, para que sea posible administrar, mantener y modificar este último en cualquier momento que sea necesario para el proceso de distribución de la herramienta.

Para implementar la propuesta de mejora, se modificará el “Modulo de Validación” de la QITDraw y se programará un generador de licencias en formato de archivo XML (metalenguaje extensible de etiquetas), utilizando las clases desarrolladas en el **Apéndice 2, 3, 4 y 5**; para lo anterior, en el **Apéndice 6** se presenta el código fuente de un programa que sería capaz de brindar esta solución. La licencia generada se copiará en la USB correspondiente, será única y validará la QITDraw antes de ejecutarse. El proceso de validación, la lógica del diseño de este esquema y la forma en la que se aplican los controles de seguridad se describen en los apartados posteriores.

6.5. Diseño de la implementación de la propuesta de mejora

El generador de licencias XML, operará con las correspondientes funciones de cifrado designadas (Hash, MD5, AES así como la función del manejo de la fecha de validación). La licencia que se genera contendrá la siguiente información:

- El nombre de la firma de ingeniería a la que se le otorgo la USB con la QITDraw cifrada con AES.
- El identificador de Hardware de cada USB con la QITDraw cifrado con AES.
- El password del usuario cifrado con MD5.
- La fecha de expiración de la licencia.

La información anterior, será utilizada también para generar el propio MD5 del archivo de licencia, mismo dato que se encontrará en el código fuente, y será el primer paso que realizará el “Modulo de Validación” modificado, validar la integridad del archivo de licencia XML, lo que provocará que cualquier alteración que pudiera ocurrir sobre este último, la invalidación inmediata del resto del proceso de validación (los otros datos ni siquiera serían revisados).

Lo siguiente que se validará, es el dato cifrado del nombre de la compañía, se decidió cifrar esta información con criptografía simétrica porque se considera que en algún momento podría requerirse descifrar la información para saber a qué compañía se le otorgo la USB (por cuestiones de control internas), y también se decidió colocar este dato en la licencia para complicar en mayor grado su estructura, así como, las posibilidades de éxito para los ataques al servicio de integridad. La forma en que se valida el dato mencionado es la siguiente: el dato es leído de la licencia, se descifra en tiempo real con AES y se compara con un dato sin cifrar en el código fuente.

Para el próximo paso de validación, se utilizará el dato más importante de la licencia, prácticamente, el dato que vincula y hace única a la QITDraw para cada USB generada: el identificador de hardware de la USB, cifrado. Para el control anterior de seguridad, este dato se encontraba solamente en el código fuente en claro, y se directamente con el identificador de hardware de la USB. Con la implementación de la propuesta de mejora, se pretende descifrar los datos de la licencia y compararlos en tiempo real de ejecución con el valor del compilado para cada USB, con la finalidad de hacer más robusto los métodos de validación.

Lo siguiente que se lee y valida del archivo de licencia, es el dato que contiene el password de usuario, el penúltimo paso antes de crear la paleta de herramientas; esta contraseña de cada usuario se encuentra cifrado con MD5, para este mecanismo de seguridad, se propone hacer un hash en tiempo real del password que el usuario ingrese para validarse, leer el dato del password cifrado del archivo de licencia y compararlos en tiempo real.

El último paso de validación es la fecha de expiración de la licencia de la QITDraw, es decir, el periodo en el que la herramienta estará disponible para utilizarse. Este dato se encuentra en claro en la licencia y se lee de la misma, dependiendo si la fecha del sistema alcanzo o no a esta ultima la licencia se valida o no. Cualquier intento de cambiar la fecha de la maquina en la que se ejecuta la herramienta o cuando expiró la fecha de la herramienta, se registra de inmediato en el registro del sistema en la sección del programa de AutoCAD, haciendo muy complicado el pasar este control de seguridad.

Estos controles de seguridad, concluyen la propuesta de mejora para la implementación de los mecanismos de seguridad para la distribución de la QITDraw, el siguiente paso, es verificar la propuesta de mejora.

6.6. Verificación de la propuesta de mejora

En base a los controles implementados de la propuesta de mejora y los casos encontrados:

Tabla 105. Verificación de la propuesta de mejora.

Relación de Amenaza - Vulnerabilidad	Evaluación del Riesgo Inicial (sin controles)			Controles	Evaluación del riesgo Residual (con controles)			Recomendaciones (controles adicionales)
	I	Fr	CR		I	Fr	CR	
ATI-L+S-EPC	4	3	**B**	**Correctivo:** La licencia tiene vigencia (control optimizado). **Detector:** Verificador de datos de integridad de la licencia y varios datos **Disuasivo:** La QITDraw tiene actualizaciones regulares y ofuscación de código implementada. **Preventivo:** Validación de la herramienta con la memoria USB otorgada a cada contratista.	1	3	**D**	No se consideran necesarios controles adicionales
ATI-L+S-EIV	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales
C+F-AUCQ	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales
C+S-EPC	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales
C+S-EIV	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales
HGH+F-AUCQ	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales
HGH+S-EPC	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales
HGH+S-EIV	4	3	**B**		1	3	**D**	No se consideran necesarios controles adicionales

Los controles implementados de acuerdo a la propuesta de mejora, son capaces de manejar los riesgos, y por lo tanto, hacer que la distribución de la herramienta para todos los casos analizados, sea segura.

CONCLUSIONES

Se propuso, adaptó e implementó una metodología de análisis de riesgos informáticos al proceso de distribución de la QITDraw que fue capaz de permitir la identificación y evaluación de los riesgos de de seguridad que existían antes de implementar las propuesta de mejor que se construyó.

Aunque se utilizaron conceptos de otra disciplina (estudio de riesgos para la seguridad de procesos en la Industria Química) para construir una propuesta de una metodología adaptada de análisis de riesgos informáticos, se logró demostrar que en realidad fue posible complementar a una metodología con la otra, tomando las similitudes de ambas y luego adaptándolas de forma lógica y sistemática. Dando como resultado una metodología hibrida que es resulto útil para cumplir los objetivos especificas de esta tesis.

Los resultados obtenidos en el análisis de riesgos demuestran que los mecanismos de seguridad que tenía establecidos para su distribución la QITDraw antes de que la propuesta de mejora fuera implementada, no eran suficientes ni totalmente efectivos para evitar ataques en el proceso de distribución de la herramienta de dibujo, ni tampoco ofrecían cabalmente los servicios de seguridad de confidencialidad y disponibilidad, mientras que el servicio de integridad no era ofrecido de ninguna forma.

Se verificó que la propuesta de mejora construida (con base en los resultados obtenidos en el análisis de riesgos informáticos cualitativo y referencias extraídas de normatividad internacional para la seguridad de la información), implementada (para los mecanismos de seguridad informática en la distribución de la herramienta QITDraw) y presentada en este trabajo de tesis fue capaz de manejar los riesgos existentes y proporcionar los tres servicios que conforman la triada de la seguridad (confidencialidad, integridad y disponibilidad):

- Confidencialidad: Se proporcionó este servicio de seguridad a la QITDraw; el cual permite resguardar la propiedad intelectual de la herramienta, la protección contra: copia, modificación, desensamblado, descompilado y similares.
- La integridad: Se proporcionó este servicio de seguridad a la QITDraw; el cual permite que la integridad del archivo de licencia de la QITDraw permanezca intacto en su contenido, es decir, sin ninguna modificación, independientemente del escenario en el que se encuentre o del periodo de tiempo para el que fue autorizada a ejecutarse de manera válida, de lo contrario, al realizar cualquier modificación sobre esto último, la utilización de la herramienta quedaría invalidada en ese instante.
- Disponibilidad: Se proporcionó este servicio de seguridad a la QITDraw, el cual permite que la herramienta se pueda utilizar durante el periodo de validez establecido por el CEASP^{4}A para ejecutarse. También se refactorizó el código fuente del “Modulo de Validación” de la QITDraw, lo que permite administrar, mantener y modificar este último en cualquier momento que sea necesario para hacer cualquier adaptación del proceso de distribución de la herramienta.

La ofuscación de código junto con el uso de criptografía simétrica y asimétrica resultaron ser herramientas con las que se pueden proporcionar los servicios que conforman la triada de la seguridad.

Se puede concluir también de acuerdo con los resultados del análisis de riesgos que la fuente amenaza humana es la que genera más riesgos en el esquema de seguridad.

TRABAJO FUTURO

- Realizar el análisis de riesgos, no solo para el proceso de distribución de la herramienta, sino también para los otros ámbitos que implica la ingeniera de software.
- Consultar aun más normatividad de la misma familia ISO/IEC 27000 o de alguna otra, con el fin de mejorar las metodologías que aquí se proponen.
- Verificar también de manera más exhaustiva la propuesta de mejora realizada en este trabajo con una mayor cantidad de pruebas, simulaciones de más escenarios, ataques controlados y con condiciones determinadas, para verificar si en realidad los controles adicionales establecidos son capaces de manejar convenientemente los riesgos.
- Proporcionar los seis servicios de seguridad a la herramienta QITDraw, ya que en esta propuesta de mejora, se proporcionan solo tres (los que conforman la triada de la seguridad).
- Realizar análisis de riesgos, sin consideraciones para la evaluación de los riesgos que permitan descartar relaciones de amenaza-vulnerabilidad, es decir, realizarlo exhaustivamente para todos los casos generados y que existan.
- Definir con más exactitud los perfiles de las personas de los escenarios planteados; y sin considerar relaciones de confianza que permitan descartar personal.
- Considerar las cinco fuentes de amenaza y los seis tipos de vulnerabilidades definidas por López, M. J. y Quezada C. (2006, j) cuando se realice un análisis de riesgos.

GLOSARIO

- Acts of God: amenazas que surgen de las fuerzas naturales (actos de dios), conocidas así por tratarse de eventualidades que están fuera del control humano.
- Add-Ons: extensiones o complementos, aplicaciones capaces de aportar nuevas funciones a productos de software más complejos.
- API: Interface de Programación para Aplicaciones (Application Programming Interface), es una es una fuente de código basado en la especificación destinada a ser utilizada como una interfaz de componentes de software para comunicarse entre sí.
- Backdoors: se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado, sin conocimiento por parte del usuario.
- CEASP^{4}A: Centro de Estudios para la Administración de la Seguridad de los Procesos Petroquímicos, Poliméricos y la Protección Ambiental), el cual es un grupo de trabajo perteneciente a la Facultad de Química de la UNAM. Fundado en 1997, con el único objetivo fundamental de lograr desarrollos tecnológicos y soluciones aplicables en el área de seguridad para los procesos en la industria química.
- Crackers (hackers black hat): persona que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño, son atacantes poco habituales pero extremadamente peligrosos, con grandes conocimientos y experiencia en computación.
- Hacker: Es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.
- Hacker gray hat: Tienen habilidades equiparables a las de un cracker, así como una ética ambigua en lo referente al acceso a información y sistemas para los cuales no tienen la autorización correspondiente.
- Hardware: Conjunto de los componentes que integran la parte material de una computadora.
- ISO: Es la Organización Internacional para la estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales.
- Malware: Término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento.
- Metodología AVS: Metodología de Análisis de Vulnerabilidades De Seguridad (Security Vulnerability Analysis Methodology, SVA Methodology).
- Plug-in(s): del idioma inglés “acoplable”, concepto que se utiliza también para designar a los Add-Ons.

- PHVA : Planificar, Hacer, Verificar, Actuar; metodología nombrada en base al acrónimo en el idioma inglés: *Plan, Do, Check, Act*, (PDCA), también llamado “Ciclo de Deming”.
- POO: Programación Orientada a Objetos; paradigma (esquema formal) que representa un cambio de perspectiva con respecto a la programación estándar por procedimientos (estructurada).
- QITDraw: Es una barra (o paleta) de herramientas diseñada para dibujar diagramas técnicos y funcionar con AutoCAD® versión 2006 o posterior, dirigida principalmente a personas sin experiencia previa para realizar este tipo de diagramas con el programa de Autodesk® AutoCAD®.
- Servidor espejo: Es un sitio web que contiene una réplica exacta de otro. Estas réplicas u espejos se suelen crear para facilitar descargas grandes y facilitar el acceso a la información aun cuando haya fallos en el servicio del servidor principal.
- SGSI: Sistema de Gestión de la Seguridad de la Información basado en la metodología PHVA; se encarga de establecer los requerimientos y especificaciones de un SGSI.
- T.I.: Tecnología de la información (del idioma inglés, Information Technology, IT).
- UPS: “Uninterruptible Power Supply”; fuente de energía ininterrumpida, es una fuente de suministro eléctrico que posee una batería con el fin de seguir suministrando energía a un dispositivo en el caso de interrupción eléctrica.

BIBLIOGRAFÍA Y MESOGRAFÍA

- Aguillón, E. (2012). *Fundamentos de Criptografía*: Laboratorio de Redes y Seguridad. Proyectos. Criptografía. [Fecha de consulta: 01 de febrero de 2012]. Disponible en: <http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/>

- Andrade, J. (2011). *Preguntas Frecuentes en Seguridad en Cómputo*: UNAM-CERT. Equipo de Respuesta a Incidentes. [Fecha de consulta: 01 de enero de 2012]. Disponible en: <http://www.seguridad.unam.mx/documento/?id=14#Diferencia>.

- Autodesk®. (2010). *Overview of the AutoCAD .NET API*: AutoCAD .NET Developer's Guide. Introduction. Overview of the AutoCAD .NET API. [Fecha de consulta: 29 de noviembre de 2011]. Disponible en: <http://docs.autodesk.com/ACD/2010/ENU/AutoCAD%20.NET%20Developer%27s%20Guide/index.html?url=WS73099cc142f48755-5c83e7b1120018de8c0-23fe.htm,topicNumber=d0e79>.

- Autodesk®. (2012). *AutoCAD*: Developer Center. Products & Technologies. [Fecha de consulta: 21 de octubre de 2011]. Disponible en: <http://usa.autodesk.com/adsk/servlet/index?id=1911627&siteID=123112>.

- Bozdoc, M. (2003). *The History of CAD: Introducing CAD*: MB Solutions. Resources and information for professionals designers. [Fecha de consulta: 7 de octubre de 2011]. Disponible en: <http://www.mbdesign.net/mbinfo/CAD-Intro.htm>.

- British Standards Institution. (2012). BSI Fast Facts: The BSI Group. About BSI. [Fecha de consulta: 15 de diciembre de 2011]. Disponible en: <http://www.bsigroup.com/en/About-BSI/News-Room/BSI-Fast-Facts2/>.

- CCPS (Center for Chemical Process Safety). (1992). Guidelines for Hazard Evaluation Procedures. New York: the American Institute of Chemical Engineers (AIChE). Páginas consultadas: 198-219.

- CCPS (Center for Chemical Process Safety). (2003). Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. New York: the American Institute of Chemical Engineers (AIChE). Páginas consultadas: 9-48.

- Computerworld. (2011). *Perfil psicológico de ladrones de datos empresariales*: International Data Group (IDG), Communications, S. A. U. [Fecha de consulta: 22 de noviembre de 2011]. Disponible en: <http://www.idg.es/computerworld/Los-empleados-que-roban-documentos-confidenciales-/seccion-mercado/noticia-116861>.

- Granados, G. (2006). *Introducción a la criptografía*: Revista Digital Universitaria. Volumen 7. Número 7. [Fecha de consulta: 08 de enero de 2012]. Páginas consultadas: 2-16. Disponible en: <http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf>.

- Gómez, A. (2011). *Enciclopedia de la Seguridad Informática*, (2da ed.). México: Alfaomega. Páginas consultadas: a) 85, b) 201.

- González, L. (2009). *AutoCAD 2010, de la pantalla a la realidad*, (1ra ed.). México: Guías Inmediatas de Computación (GIC). Páginas consultadas: 1-14

- ISO/IEC 27001:2005 - Information security management systems - Requirements.

- ISO/IEC 27002:2005 - Code of practice for information security management.

- López, M. J. y Quezada C. (2006). *Fundamentos de Seguridad Informática*, (1ra ed.). México: UNAM, Facultad de Ingeniería. Páginas consultadas: a) 155-170, b) b) 115-126, c) 2, d) 1, e) 3, f) 155, g) 4, h) 5, i) 63-64, j) 91-99, k) 100-105, l) 100-103 m) 107, n) 116, o) 157, p) 116-125, q) 155-158, r) 159-161, s) 167.

- M86 Security. (2012). *Code Obfuscation*: M86 Security Labs. Resources. [Fecha de consulta: 22 de enero de 2012]. Disponible en: <http://www.m86security.com/labs/code-obfuscation.asp>.

- Microsoft® Corporation. (2012). *Programación orientada a objetos*: Microsoft Developer Network Platforms Library®. Programar en Visual FoxPro®. Programación orientada a objetos. [Fecha de consulta: 10 de enero de 2012]. Disponible en: <http://msdn.microsoft.com/es-es/library/cc450502%28v=vs.71%29.aspx>.

- O'Connell, P. (2002). *The CEO as Thief: A Psychological Profile*: Bloomberg L.P. BusinessWeek. BusinessWeek Magazine. [Fecha de consulta: 7 de noviembre de 2011]. Disponible en: <http://www.businessweek.com/magazine/content/02_51/b3813012.htm>.

- Oleksiy, G. (2012). *What is Eazfuscator.NET?*: Projects. Eazfuscator. [Fecha de consulta: 02 de marzo de 2012]. Disponible en: <http://www.foss.kharkov.ua/g1/projects/eazfuscator/dotnet/Default.aspx>.

- Sandoval, E. (2011). *Ingeniería Social: Corrompiendo la mente humana*: Revista .Seguridad. Defensa Digital. Número 10. [Fecha de consulta: 15 de enero de 2012]. Páginas consultadas: 23-28. Disponible en: <http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Revista%20.Seguridad_10.pdf>.

- Segura, J. (2005). *Curso de Java: Introducción*. Genomic Science Center – UNAM. Laboratory of Computational Genomics. [Fecha de consulta: 21 de enero de 2012]. Disponible en: <http://tikal.cifn.unam.mx/~jsegura/LCGII/java1.htm>.

- Symantec® Corporation. (2011). *Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall*: Press Release. [Fecha de consulta: 02 de febrero de 2012]. Disponible en: <https://symantec-corporation.com/servlet/formlink/f?kPugHuQUTYY&ACTIVITYCODE=129753&inid=GL_NA_WP_BehavioralRiskIndicatorsOfIpTheft_DLP_Press_Release_dai81510_cta56681_aid129753>.

- TechTarget. (2003). The difference between hackers and crackers. Topics. InformIT. Technology-Specific. IT Media and Events. [Fecha de consulta: 15 de febrero de 2012]. Disponible en: <http://searchenterprisedesktop.techtarget.com/tip/The-difference-between-hackers-and-crackers>.

- WebFinance Inc. (2012). *Secure System*: BusinessDictionary.com. [Fecha de consulta: 4 de febrero de 2012]. Disponible en: <http://www.businessdictionary.com/definition/secure-system.html>.

ANEXOS

Anexo 1

En las tablas de este anexo se utilizarán abreviaturas consideradas útiles para manejo y claridad en la información. Éstas serán construidas en base a las letras iniciales de cada tipo de personal, la primera letra del tipo de atacantes considerados la abreviatura del escenario al que pertenezcan, un ejemplo sería el siguiente:

Para la abreviatura: **ATI-L-PR**

ATI	L	PR
Debida al tipo del personal con el que se está tratando	Debido al tipo de atacante	Escenario del que se están clasificando las amenazas
ATI: Administradores de T.I.	**L**: Ladrones	**PR**: PEMEX Refinación

Tabla A1.1. Identificación de amenazas y sus fuentes para el escenario PR.

Tipos de personal	Fuente de amenaza	Amenazas	Abreviatura
Administradores de T.I. de PEMEX Refinación	Humana	Administradores de T.I. de PEMEX Refinación ladrones	ATI-L-PR
		Administradores de T.I. de PEMEX Refinación fraudulentos	ATI-F-PR
		Administradores de T.I. de PEMEX Refinación saboteadores	ATI-S-PR
		Administradores de T.I. de PEMEX Refinación negligentes	ATI-N-PR
		Administradores de T.I. de PEMEX Refinación manipuladores	ATI-M-PR
		Ex administradores de T.I. de PEMEX Refinación	E-ATI-PR
Ingenieros del Área de Seguridad	Humana	Ingenieros del área de seguridad ladrones	IAS-L-PR
		Ingenieros del área de seguridad fraudulentos	IAS-F-PR
		Ingenieros del área de seguridad saboteadores	IAS-S-PR
		Ingenieros del área de seguridad negligentes	IAS-N-PR
		Ingenieros del área de seguridad manipuladores	IAS-M-PR
		Ex ingenieros del área de seguridad	E-IAS-PR
Dibujantes	Humana	Dibujantes ladrones	D-L-PR
		Dibujantes fraudulentos	D-F-PR
		Dibujantes saboteadores	D-S-PR
		Dibujantes negligentes	D-N-PR
		Dibujantes manipuladores	D-M-PR
		Ex dibujantes	E-D-PR
Ayudantes de Ingeniero	Humana	Ayudantes de ingeniero ladrones	AI-L-PR
		Ayudantes de ingeniero fraudulentos	AI-F-PR
		Ayudantes de ingeniero saboteadores	AI-S-PR
		Ayudantes de ingeniero negligentes	AI-N-PR
		Ayudantes de ingeniero manipuladores	AI-M-PR
		Ex ayudantes de ingeniero	E-AI-PR
Intrusos remunerados por PEMEX Refinación	Humana	Crackers dispuestos a dañar en PEMEX Refinación	C-PR
		Hackers Gray Hat dispuestos a dañar en PEMEX Refinación	HGH-PR

Tabla A1.2. Identificación de amenazas y sus fuentes para el escenario CU.

Tipos de personal	Fuente de amenaza	Amenazas	Abreviatura
Personal de soporte técnico del CEASP^{4}A	Humana	Personal de soporte técnico del CEASP^{4}A ladrones	PST-L-CU
		Personal de soporte técnico del CEASP^{4}A fraudulentos	PST-F-CU
		Personal de soporte técnico del CEASP^{4}A saboteadores	PST-S-CU
		Personal de soporte técnico del CEASP^{4}A negligentes	PST-N-CU
		Personal de soporte técnico del CEASP^{4}A manipuladores	PST-M-CU
		Ex personal de soporte técnico del CEASP^{4}A	E-PST-CU
Coordinadores del CEASP^{4}A	Humana	Coordinadores del CEASP^{4}A ladrones	C-L-CU
		Coordinadores del CEASP^{4}A fraudulentos	C-F-CU
		Coordinadores del CEASP^{4}A saboteadores	C-S-CU
		Coordinadores del CEASP^{4}A negligentes	C-N-CU
		Coordinadores del CEASP^{4}A manipuladores	C-M-CU
		Ex coordinadores del CEASP^{4}A	E-C-CU
Residentes del CEASP^{4}A	Humana	Residentes del CEASP^{4}A ladrones	R-L-CU
		Residentes del CEASP^{4}A fraudulentos	R-F-CU
		Residentes del CEASP^{4}A saboteadores	R-S-CU
		Residentes del CEASP^{4}A negligentes	R-N-CU
		Residentes del CEASP^{4}A manipuladores	R-M-CU
		Ex residentes del CEASP^{4}A	E-R-CU
Empleados del CEASP^{4}A	Humana	Empleados del CEASP^{4}A ladrones	E-L-CU
		Empleados del CEASP^{4}A fraudulentos	E-F-CU
		Empleados del CEASP^{4}A saboteadores	E-S-CU
		Empleados del CEASP^{4}A negligentes	E-N-CU
		Empleados del CEASP^{4}A manipuladores	E-M-CU
		Ex empleados del CEASP^{4}A	E-E-CU
Intrusos remunerados por el CEASP^{4}A	Humana	Crackers dispuestos a dañar en el CEASP^{4}A	C-CU
		Hackers Gray Hat dispuestos a dañar en el CEASP^{4}A	HGH-CU

Tabla A1.3. Identificación de amenazas y sus fuentes para el escenario CE.

Tipos de personal	Fuente de amenaza	Amenazas	Abreviatura
Contratistas externos	Humana	Contratistas externos ladrones	L-CE
		Contratistas externos fraudulentos	F-CE
		Contratistas externos saboteadores	S-CE
		Contratistas externos negligentes	N-CE
		Contratistas externos manipuladores	M-CE
		Ex contratistas externos	E-CE
Intrusos remunerados por contratistas externos	Humana	Crackers dispuestos a dañar por los contratistas externos	C-CE
		Hackers Gray Hat dispuestos a dañar por los CE	HGH-CE

Tabla A1.4. Identificación de amenazas y sus fuentes que son comunes para los escenarios: PR, CU y CE.

Tipo de amenaza	Fuente de amenaza	Amenazas	Abreviatura
Lógico	Problemas de Tipo Lógico	Diseño mal elaborado de los mecanismos de validación	PTL-DME
		Diseño mal implementado de los mecanismos de validación	PTL-DMI

Anexo 2

En las tablas de este anexo se utilizarán abreviaturas consideradas útiles para manejo y claridad en la información. Estas serán construidas en base a la letra inicial de cada tipo de vulnerabilidad, las letras iniciales de la clasificación de la vulnerabilidad y la abreviatura del escenario al que pertenezcan, un ejemplo sería:

Para la abreviatura: **H-PSPPA-PR**:

H	PSPPA	PR
Debida al tipo de vulnerabilidad con la que se está tratando	Debido a la clasificación de vulnerabilidad	Escenario del que se están clasificando las vulnerabilidades
H: Humana	**PSPPA**: Personal Sin Perfil Psicológico Adecuado	**PR**: PEMEX Refinación

Tabla A2.1. Identificación de vulnerabilidades y sus tipos para el escenario PR.

Tipo de vulnerabilidad	Clasificación de la vulnerabilidad	Abreviatura
Física	Acceso a los equipos de computo de escritorio en PEMEX Refinación que contienen a la herramienta	F-AECE-PR
	Acceso a los equipos de computo portátiles en PEMEX Refinación que contienen a la herramienta	F-AECP-PR
De Software	Errores de programación en el código fuente de la QITDraw distribuida en PEMEX Refinación	S-EPC-PR
	Errores Inesperados en validaciones para la QITDraw distribuida en PEMEX Refinación	S-EIV-PR
Humana	Personal sin perfil psicológico adecuado en PEMEX Refinación	H-PSPPA-PR
	Personal susceptible a ingeniería social en PEMEX Refinación	H-PSIS-PR
	Personal no autorizado en PEMEX Refinación	H-PNA-PR
	Personal descuidado en PEMEX Refinación	H-PD-PR

Tabla A2.2. Identificación de vulnerabilidades y sus tipos para el escenario CU.

Tipo de vulnerabilidad	Clasificación de la vulnerabilidad	Abreviatura
Física	Acceso a los equipos de computo de escritorio en el CEASP^{4}A que contienen a la herramienta	F-AECE-CU
	Acceso a los equipos de computo portátiles en el CEASP^{4}A que contienen a la herramienta	F-AECP-CU
De Software	Errores de programación en el código fuente de la QITDraw distribuida en el CEASP^{4}A	S-EPC-CU
	Errores Inesperados en validaciones para la QITDraw distribuida en el CEASP^{4}A	S-EIV-CU
Humana	Personal sin perfil psicológico adecuado en el CEASP^{4}A	H-PSPPA-CU
	Personal susceptible a ingeniería social en el CEASP^{4}A	H-PSIS-CU
	Personal no Autorizado en el CEASP^{4}A	H-PNA-CU
	Personal descuidado en el CEASP^{4}A	H-PD-CU

Tabla A2.3. Identificación de vulnerabilidades y sus tipos para el escenario CE.

Tipo de vulnerabilidad	Clasificación de la vulnerabilidad	Abreviatura
Física	Acceso a las USB que contienen a la QITDraw que se distribuye para cada uno de los contratistas externos	F-AUCQ-CE
De Software	Errores de programación en el código fuente de la QITDraw distribuida para los contratistas externos	S-EPC-CE
	Errores Inesperados en validaciones para la QITDraw distribuida para los contratistas externos	S-EIV-CE
Humana	Contratistas externos descuidados	H-D-CE
	Personal sin perfil psicológico adecuado de PEMEX Refinación	H-PSPPAPR-CE
	Personal sin perfil psicológico adecuado del CEASP^{4}A	H-PSPPACU-CE
	Personal susceptible a ingeniería social de PEMEX Refinación	H-PSISPR-CE
	Personal susceptible a ingeniería social del CEASP^{4}A	H-PSISCU-CE

APÉNDICES

Apéndice 1

```
Option Strict Off
Option Explicit On
Option Compare Binary

Imports Autodesk.AutoCAD.Runtime
Imports Autodesk.AutoCAD.EditorInput
Imports System.IO

Public Class UserCommands


    <CommandMethod("Botón_número_uno", CommandFlags.Session)> _
Public Sub ButtonNumberOneSubRoutine()
        MsgBox("Ejecutando comando 'Mi_primer_comando_en_AutoCAD'")
    End Sub

    <CommandMethod("Botón_número_dos", CommandFlags.Session)> _
Public Sub ButtonNumberTwoSubRoutine ()
        MsgBox("Ejecutando comando 'Otro_botón_que_ejecuta_ventana'")
    End Sub

    <CommandMethod("Botón_Información", CommandFlags.Session)> _
Public Sub AboutInfo()
        MsgBox("Ejecutando comando 'Ventana_que_muestra_información'")
    End Sub


End Class
```

Apéndice 2

```
Friend Class AESEncryptionAndDecryptionFunctions
Friend Shared Function AES_Encryption(ByVal InputToEncrypt As String,
ByVal PasswordForEncryptionWithAES As String) As String
            Dim AES As New RijndaelManaged
            Dim byteGenerator As New
Rfc2898DeriveBytes(PasswordForEncryptionWithAES,
Convert.FromBase64String(salt))
            AES.Key = byteGenerator.GetBytes(32)
            AES.Mode = CipherMode.ECB
            Dim DESEncrypter As ICryptoTransform = AES.CreateEncryptor
            Dim Buffer As Byte() =
ASCIIEncoding.ASCII.GetBytes(InputToEncrypt)
            Dim ResultsFromTheAESEncryption =
Convert.ToBase64String(DESEncrypter.TransformFinalBlock(Buffer, 0,
Buffer.Length))
            Return ResultsFromTheAESEncryption
End Function
Friend Shared Function AES_Decryption(ByVal InputToDecrypt As String,
ByVal PasswordForDencryptionWithAES As String) As String
            Dim AES As New RijndaelManaged
            Dim byteGenerator As New
Rfc2898DeriveBytes(PasswordForDencryptionWithAES,
Convert.FromBase64String(salt))
            AES.Key = byteGenerator.GetBytes(32)
            AES.Mode = CipherMode.ECB
            Dim DESDecrypter As ICryptoTransform = AES.CreateDecryptor
            Dim Buffer As Byte() =
Convert.FromBase64String(InputToDecrypt)
            Dim ResultsFromTheAESDecryption =
ASCIIEncoding.ASCII.GetString(DESDecrypter.TransformFinalBlock(Buffer, 0,
Buffer.Length))
            Return ResultsFromTheAESDecryption
        End Function
    End Class
```

Apéndice 3

```
Friend Shared Function MD5_Encryption(ByVal InputToEncrypt As String) As
String
      Dim MD5 As New MD5CryptoServiceProvider()
      Dim EncodignObjetForInputToEncrypt As New UnicodeEncoding()
      Dim ByteArrayRetriever() As Byte =
      EncodignObjetForInputToEncrypt.GetBytes(InputToEncrypt)
      Dim ByteEncoderForMD5() As Byte =
      MD5.ComputeHash(ByteArrayRetriever)
      Dim ResultsFromTheMD5Ecryption =
      Convert.ToBase64String(ByteEncoderForMD5)
      Return ResultsFromTheMD5Ecryption
End Function
```

Apéndice 4

```
Friend Shared Function MD5_LicenseIntegrityVerification() As String
      ValidationModule.FindConectedUSBs()
      'Se leen los datos del archivo de licencia en la USB
      correspondiente en forma de bytes
      Dim XMLLicenseToAnalyzeAndValidate() As Byte =
      System.IO.File.ReadAllBytes(ValidationModule.USBPath & "\" &
      ValidationModule.XMLFileName)
      'Se crea el nuevo objeto MD5
      Dim MD5 As New MD5CryptoServiceProvider()
      Dim EncodingObjectForStandardizeTheInputContent As New
      UnicodeEncoding()
      Dim TheXMLFileHashInFormOfBytes() As Byte =
      MD5.ComputeHash(XMLLicenseToAnalyzeAndValidate)
      Dim ResultsFromTheHashFunction =
      Convert.ToBase64String(TheXMLFileHashInFormOfBytes)
      Return ResultsFromTheHashFunction
End Function
```

Apéndice 5

```
Friend Shared Function CheckDateStatus() As Integer
If Date.Now >= LicenseExpirationDate And My.Settings.StillValid = ""
Then My.Settings.StillValid = "False"
     My.Settings.Save()
MsgBox("La licencia de QITDraw PLT 2012 ha expirado, necesita adquirir
una nueva licencia.") Return 0
End If

If Date.Now >= LicenseExpirationDate And My.Settings.StillValid = "False"
Then MsgBox("La licencia de QITDraw PLT 2012 ha expirado, necesita
adquirir una nueva licencia.") Return 1
End If

If Date.Now <= LicenseExpirationDate And My.Settings.StillValid = "False"
Then MsgBox("La fecha del equipo se ha intentado alterar, la licencia se
suprimirá.") Return 2
End If
End Function

Friend Shared Function CheckValidityLicensePeriod() As Boolean
      My.Settings.ExpirationDate = LicenseExpirationDate
      CheckDateStatus()
If My.Settings.StillValid = "" Then
      Return True
Else
      Return False
End If
End Function
```

Apéndice 6

```
Imports System.IO
Imports System.Management
Imports System.Security.Cryptography
Imports System.Text
Imports System.Windows.Forms
Imports System.Xml


Public Class Form1
    Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
    End Sub


    'FIRMA: "ceasp4a.FQ-UNAM"
    'Public Class QITDraw2011USBLicenseGenerator
    Private _expirationDate As Nullable(Of Date)
    Private _encryptedCompanyName As String
    Private _encryptedUSBKey As String
    Private _hashedpassword As String

    Private Sub Button1EncryptedCompanyNameGenerator_Click(ByVal sender
As System.Object, ByVal e As System.EventArgs) Handles
Button1EncryptedCompanyNameGenerator.Click
        EncrypCompanyName()
    End Sub

    Private Sub EncrypCompanyName()
        Dim CompanyNameCatcher As String =
TextBox1CompanyNameUnencrypted.Text
        'Solo un password aleatorio extraido de un RANDOM GUID, con la
función: Dim GeneratedGUID As String = Guid.NewGuid.ToString
        Dim PasswordForEncryptCompanyName = "2d4ec2a0-cea2-4420-a703-
c3db6e549cb5"
        Dim PasswordForDecryptCompanyName = "2d4ec2a0-cea2-4420-a703-
c3db6e549cb5"
        Me.TextBox2EncryptedCompanyName.Text =
AESEncryptionFunctions.AES_Encryption(Me.TextBox1CompanyNameUnencrypted.T
ext, PasswordForEncryptCompanyName)
        Me.TextBox1.Text =
AESEncryptionFunctions.AES_Decryption(TextBox2EncryptedCompanyName.Text,
PasswordForDecryptCompanyName)
        _encryptedCompanyName = TextBox2EncryptedCompanyName.Text
    End Sub


    Private Sub Button2USBKeysListGenerator_Click_1(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
Button2USBKeysListGenerator.Click
        GenerateUSBList()
    End Sub
```

```
    Private Sub GenerateUSBList()
        'Solo un password aleatorio extraido de un RANDOM GUID, con la
función: Dim GeneratedGUID As String = Guid.NewGuid.ToString
        Dim PasswordForEncryptUSBHardwareID = "a01a4b7b-8545-457b-8d10-
86287e41f0c0"
        Dim PasswordForDecryptUSBHardwareID = "a01a4b7b-8545-457b-8d10-
86287e41f0c0"
        Me.TextBox3USBKeysList.DataSource = CreateTheDeviceList()
        Me.TextBox4EncryptedUSBKey.Text =
AESEncryptionFunctions.AES_Encryption(TextBox3USBKeysList.SelectedValue.T
oString.Substring(4), PasswordForEncryptUSBHardwareID)
        Me.TextBox5DencryptedUSBKey.Text =
AESEncryptionFunctions.AES_Decryption(TextBox4EncryptedUSBKey.Text,
PasswordForDecryptUSBHardwareID)
        _encryptedUSBKey = Me.TextBox4EncryptedUSBKey.Text
    End Sub

    Private Sub UserPasswdButton_Click(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles UserPasswdButton.Click
        Dim GeneratedRandomPassword As String =
RandomPasswordGenerator(4, True)
        Me.TextBox6UserPasswd.Text = GeneratedRandomPassword
        Me.TextBox6UserPasswdMD5.Text =
MD5EncryptionFunctions.MD5_Encryption(GeneratedRandomPassword)
        _hashedpassword = Me.TextBox6UserPasswdMD5.Text
    End Sub

    Private Sub CreateXMLButton_Click(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles CreateXMLButton.Click
        Me.ResultsForXMLFile.Text = CretaXMLFileText()
        XMLFileCreator()
    End Sub

    'Esta funcion captura los IDs de HARDWARE de las USBs conectadas al
equipo de cómputo
    Private Function GetUSBsPluggedSerialNumber() As Dictionary(Of
String, String)
        Dim USBSerialNumbers As New Dictionary(Of String, String)
        For Each aDriveInfo In My.Computer.FileSystem.Drives
            If aDriveInfo.DriveType = DriveType.Removable Then
                Dim DriveLetter = aDriveInfo.RootDirectory.FullName
                Dim LogicalDisk = New
ManagementObject("Win32_LogicalDisk.DeviceID='" &
DriveLetter.TrimEnd("\"c) & "'")
                For Each DiskPartition As ManagementObject In
LogicalDisk.GetRelated("Win32_DiskPartition")
                    For Each DiskDrive In
DiskPartition.GetRelated("Win32_DiskDrive")
                        Dim DeviceID = DiskDrive("PnPDeviceID").ToString
                        If Not DeviceID.StartsWith("USBSTOR") Then
Continue For
                        Dim DeviceIDParts =
DeviceID.Split("\&".ToCharArray)

USBSerialNumbers.Add(DeviceIDParts(DeviceIDParts.Length - 2),
DriveLetter)
                    Next
```

```
                Next
            End If
        Next
        Return USBSerialNumbers
    End Function

    'Con los IDs de HARDWARE de las USBs, esta funcion crea la lista de
datos de diccionario (LETRA DE UNIDAD + HW-ID)
    Private Function CreateTheDeviceList() As IList(Of String)
        Dim USBIDsList As New List(Of String)
        ' USBIDsList = New List(Of String)
        'Creando un nuevo diccionario de cadenas de UNIDADES-USB | USB-
IDs
        Dim USBDictionary As New Dictionary(Of String,
String)(GetUSBsPluggedSerialNumber)
        Dim aUSBKey As String
        For Each aUSBKey In GetUSBsPluggedSerialNumber.Keys
            USBIDsList.Add(String.Format("{0} {1}",
USBDictionary(aUSBKey), aUSBKey))
        Next
        Return USBIDsList
    End Function

    'Esta funcion crea un passwrod aleatorio
    Private Function RandomPasswordGenerator(ByVal PasswdSize As Integer,
ByVal LowerCase As Boolean) As String
        Dim PasswdBuilder As New StringBuilder()
        Dim RandomPass As New Random()
        Dim Character As Char
        Dim Index As Integer
        For Index = 0 To PasswdSize - 1
            Character = Convert.ToChar(Convert.ToInt32((26 *
RandomPass.NextDouble() + 65)))
            PasswdBuilder.Append(Character)
        Next
        If LowerCase Then
            Return PasswdBuilder.ToString().ToLower()
        End If
        Return PasswdBuilder.ToString()
    End Function

    Private Sub ExpirationDatePicker_ValueChanged(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
ExpirationDatePicker.ValueChanged
        Dim DefinedExpirationDate As Nullable(Of Date)
        DefinedExpirationDate = ExpirationDatePicker.Value
        _expirationDate = DefinedExpirationDate
    End Sub

    Private Function CretaXMLFileText() As String
        Dim BuilderOfXMLText As New StringBuilder()
        'BuilderOfXMLText.AppendLine("<?xml version="1.0" encoding="UTF-
8"?>")
        BuilderOfXMLText.AppendLine("<xml>")

BuilderOfXMLText.AppendLine(String.Format("<CompanyName>{0}</CompanyName>
", _encryptedCompanyName))
```

```
        BuilderOfXMLText.AppendLine(String.Format("<USB>{0}</USB>",
_encryptedUSBKey))
        BuilderOfXMLText.AppendLine(String.Format("<Pass>{0}</Pass>",
_hashedpassword))

BuilderOfXMLText.AppendLine(String.Format("<ExpirationDate>{0}</Expiratio
nDate>", _expirationDate))
        BuilderOfXMLText.AppendLine("</xml>")
        Return BuilderOfXMLText.ToString
    End Function


    Public Function CreateEncryptionKeyPair() As List(Of String)
        Using rsa As New RSACryptoServiceProvider
            Dim result As New List(Of String)
            result.Add(rsa.ToXmlString(True))
            result.Add(rsa.ToXmlString(False))

            Return result
        End Using
    End Function

    'Esta subrutina se encarga de crear el archivo XML y permite
nombrarlo y
    'guardarlo en la ubicación deseada
    Private Sub XMLFileCreator()
        Dim saveFileDialog As New SaveFileDialog()
        saveFileDialog.Filter = "Archivos XML (*.xml)|*.xml"
        saveFileDialog.RestoreDirectory = True
        If saveFileDialog.ShowDialog() = DialogResult.OK Then
            Dim objWriter As New
System.IO.StreamWriter(saveFileDialog.FileName)
            objWriter.Write(ResultsForXMLFile.Text)
            objWriter.Close()
        End If
    End Sub


End Class
Public Class AESEncryptionFunctions
    'Salt generado apartir de un SALT aleatorio
    'Dim byteGenerator As New Rfc2898DeriveBytes(pass, New Byte() {12,
23, 34, 45, 56, 67, 34, 23, 34, 45})
    Private Shared salt = "OWkGer5u/b7Pn0k8QinVvWHu4sNm3nLA1XqV/ueqlIk="
    Public Shared Function AES_Encryption(ByVal InputToEncrypt As String,
ByVal PasswordForEncryptionInAES As String) As String
        Dim AES As New RijndaelManaged
        Dim byteGenerator As New
Rfc2898DeriveBytes(PasswordForEncryptionInAES,
Convert.FromBase64String(salt))
        AES.Key = byteGenerator.GetBytes(32)
        AES.Mode = CipherMode.ECB
        Dim DESEncrypter As ICryptoTransform = AES.CreateEncryptor
        Dim Buffer As Byte() =
ASCIIEncoding.ASCII.GetBytes(InputToEncrypt)
```

```
        Dim ResultsFromTheAESEncryption =
Convert.ToBase64String(DESEncrypter.TransformFinalBlock(Buffer, 0,
Buffer.Length))
        Return ResultsFromTheAESEncryption
    End Function
    Public Shared Function AES_Decryption(ByVal InputToDecrypt As String,
ByVal PasswordForDencryptionInAES As String) As String
        Dim AES As New RijndaelManaged
        Dim byteGenerator As New
Rfc2898DeriveBytes(PasswordForDencryptionInAES,
Convert.FromBase64String(salt))
        AES.Key = byteGenerator.GetBytes(32)
        AES.Mode = CipherMode.ECB
        Dim DESDecrypter As ICryptoTransform = AES.CreateDecryptor
        Dim Buffer As Byte() = Convert.FromBase64String(InputToDecrypt)
        Dim ResultsFromTheAESDecryption =
ASCIIEncoding.ASCII.GetString(DESDecrypter.TransformFinalBlock(Buffer, 0,
Buffer.Length))
        Return ResultsFromTheAESDecryption
    End Function
End Class
Public Class MD5EncryptionFunctions
    Public Shared Function MD5_Encryption(ByVal InputToEncrypt As String)
As String
        Dim MD5 As New MD5CryptoServiceProvider()
        Dim EncodignObjetForInputToEncrypt As New UnicodeEncoding()
        Dim ByteArrayRetriever() As Byte =
EncodignObjetForInputToEncrypt.GetBytes(InputToEncrypt)
        Dim ByteEncoderForMD5() As Byte =
MD5.ComputeHash(ByteArrayRetriever)
        Dim ResultsFromTheMD5Ecryption =
Convert.ToBase64String(ByteEncoderForMD5)
        Return ResultsFromTheMD5Ecryption
    End Function
End Class
```