FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

DESARROLLO DE UN PLAN DE MITIGACIÓN DE RIESGOS DE LA INFORMACIÓN APLICADO AL ÁREA DE OPERACIONES DE UNA EMPRESA PETROLERA SIGUIENDO LA METODOLOGÍA NIST SP 800-30

AUTOR

CRISTHIAN EDUARDO ALMEIDA GARCES

AÑO

2020

FACULTAD DE INGENIERIA Y CIENCIAS APLICADAS

DESARROLLO DE UN PLAN DE MITIGACIÓN DE RIESGOS DE LA INFORMACIÓN APLICADO AL ÁREA DE OPERACIONES DE UNA EMPRESA PETROLERA SIGUIENDO LA METODOLOGÍA NIST SP 800-30

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Sistemas de Computación e Informática

Profesor Guía

Mgt. Eddy Mauricio Armas Pallasco

Autor

Cristhian Eduardo Almeida Garces

Año

2020

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido el trabajo, Desarrollo de un plan de mitigación de riesgos de la información aplicado al área de operaciones de una empresa petrolera siguiendo la metodología NIST SP 800-30, a través de reuniones periódicas con el estudiante Cristhian Eduardo Almeida Garces, en el semestre 202010, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Eddy Mauricio Armas Pallasco

Magister en Gerencia de Sistemas y TI

CC: 1711715803

DECLARACIÓN DEL PROFESOR CORRECTOR

"Declaro haber revisado este trabajo, Desarrollo de un plan de mitigación de riesgos de la información aplicado al área de operaciones de una empresa petrolera siguiendo la metodología NIST SP 800-30, del Cristhian Eduardo Almeida Garces, en el semestre 202010, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Verónica Fernanda Falconi Ausay

Magister en Ciencias de la Computación y Comercio Electrónico

CC:050239527-0

DECLARACIÓN DE AUDITORIA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Cristhian Eduardo Almeida Garces

CC: 1726831926

tías Neyner y Ligia por su apoyo incondicional.

AGRADECIMIENTOS

Agradezco a mi familia, amigos y profesores por apoyarme en toda esta travesía universitaria, en especial a mis tías Neyner y Ligia por su apoyo incondicional.

DEDICATORIA

Este trabajo está dedicado tanto a mi Padre como a mi Madre por siempre darme lo mejor y a mi hermana Katherine por ser siempre un apoyo incondicional.

Resumen

Las empresas manejan una gran cantidad de información, la cual muchas veces es considerada activo más importante, por lo cual resguardarla de la mejor manera debe ser una de sus prioridades. Pero no todas las empresas toman las medidas necesarias para hacerlo. Por lo que es muy importante contar con una metodología para el análisis de riesgo como es la NIST 800-30 que ayuda a las empresas a la mitigación de riesgos. Utilizando el método de NIST SP 800-30 se detectaron las diferentes amenazas y vulnerabilidades del Área de Operaciones de una empresa Petrolera y de esa manera determinar el riesgo de cada vulnerabilidad del Área de Operaciones. Por último, se propone un plan para definir las recomendaciones de control para minimizar los riesgos contra la información de la Petrolera.

Abstract

Companies handle a large amount of information, which is often considered the most important asset, so safeguarding it in the best way should be one of your priorities. But not all companies take the necessary steps to do. So, it is very important to have a methodology for risk analysis such as NIST 800-30 that helps companies to mitigate risks. Using the NIST SP 800-30 method, the different threats and vulnerabilities of the Operations Area of an Oil company were detected and, in that way, to determine the risk of each vulnerability of the Operations Area. Finally, a plan is proposed to define the control recommendations to minimize the risks against the information of the Oil Company.

ÍNDICE

1. INTRODUCCION

1.1 Descripción del problema

En la actualidad el uso de la tecnología para las Petroleras se ha vuelto algo muy importante, ya que con él paso del tiempo tanto software como hardware han ido mejorando, y debido a esto nos ayudan a manejar de mejor manera los datos, pero de igual manera dicha información puede estar en peligro ya sea por ataques informáticos, robos de información o ya sea por agentes naturales. Este tipo de empresas petroleras se caracteriza por obtener y manejar una gran cantidad de datos sensibles, debido a que la pérdida de estos puede generar una interrupción en el proceso productivo, por lo que siempre está latente el riesgo de que ocurra un problema con dicha información y muchas veces uno de los problemas más comunes es la falta de concienciación de las personas en la seguridad de la información.

El análisis de riesgo realizado en este proyecto puede ser propuesto para una petrolera donde su matriz se encuentra ubicada en Quito y con un campo de perforación en Pinto, lo que vamos a realizar será un análisis del riesgo, y dar a conocer las diferentes vulnerabilidades en las que se puede encontrar la información del área de operaciones que incluye un grupo de trabajo que se llama geología como se puede ver en la figura 1.

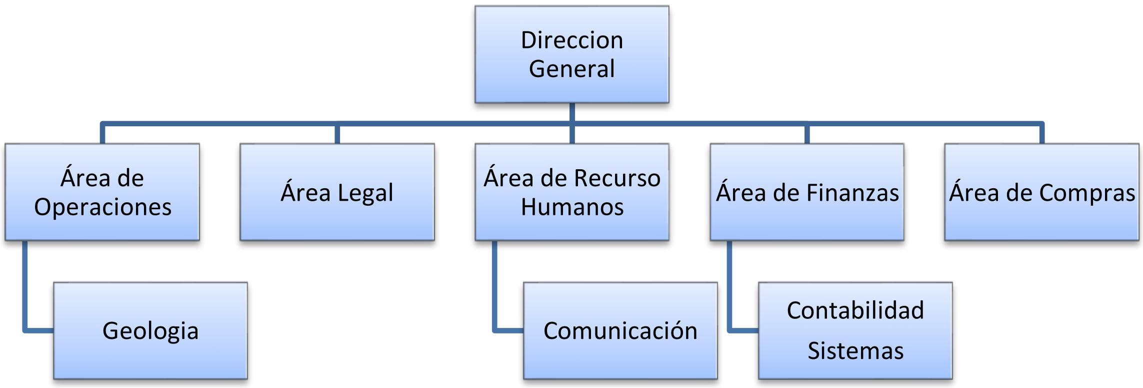

Figura 1. Esquema de división de áreas.

La cual es la parte más importante del área de operaciones, ya que el grupo de geología procesa un volumen alto de datos e información de la petrolera muchas veces con archivos que contienen datos incluso desde la creación de la petrolera.

Para la extracción exitosa de un campo petrolero se genera todo un proceso desde el inicio hasta el final que consta de 4 pasos generales, que van desde la exploración de los campos hasta la entrega o movilización del producto.

Exploración. – La búsqueda de petróleo requiere conocimientos de geología, geofísica y petrofísica, ya que el petróleo se encuentra en ciertos tipos de estructuras geológicas, que se encuentran bajo diferentes terrenos y en distintos climas como lo podemos ver en la Figura 2 en la parte inferior.

Figura 2. Estructuras Geológicas.

Adaptado de Vix, s.f

Por lo que se debe se recolectar gran cantidad de información con diferentes tipos de prospecciones geofísicas, y de esta forma se hacen mediciones con el fin de obtener una imagen exacta de las formaciones del subsuelo y de esta forma poder proveer de diferentes modelos que nos ayudan a predecir en que área se podría encontrar petróleo, y así proponer áreas de perforación para la gerencia, esperando la aprobación (Kraus, 2012, p. 9).

Perforación de Pozos. – Después del análisis de los datos geológicos y de las prospecciones geofísicas. El proceso de perforación comienza con el armado de una torre como la visualizada en la figura 3.

Figura 3. Torre de Perforación.

Adaptado de San Antonio, s.f.

Muchas veces pueden ser torres móviles para perforaciones en donde lo que se requiere es explorar o probar, como también pueden torres fijas para perforaciones definitivas o pozos de descubrimiento que son cuando ya se descubrió un yacimiento de petróleo, para lo cual se tendrá que decidir el mejor método de hacerlo, ya que no hay una única manera de hacerlo y todo dependerá del análisis de datos previo, existen varias formas de perforación como puede ser perforación por percusión que es la más antigua o la más común que es la perforación rotativa(Kraus, 2012, p. 10), en esta fase se siguen adquiriendo datos para su continuo análisis.

Extracción o Producción. – Procedimiento de poner en marcha un pozo de producción, y una vez perforado hasta la profundidad necesaria para hallar petróleo, el siguiente paso es la extracción de este, que se lleva a cabo por desplazamiento, agua o gas. Al comenzar la perforación el petróleo se encuentra bajo presión, esta misma presión hace que el petróleo salga naturalmente (Kraus, 2012, p. 11), pero según se vaya extrayendo petróleo del pozo, esta presión natural va disminuyendo, por lo que se aplican métodos de recuperación, como pueden ser inyección de gas o de agua como se puede ver en la Figura 4.

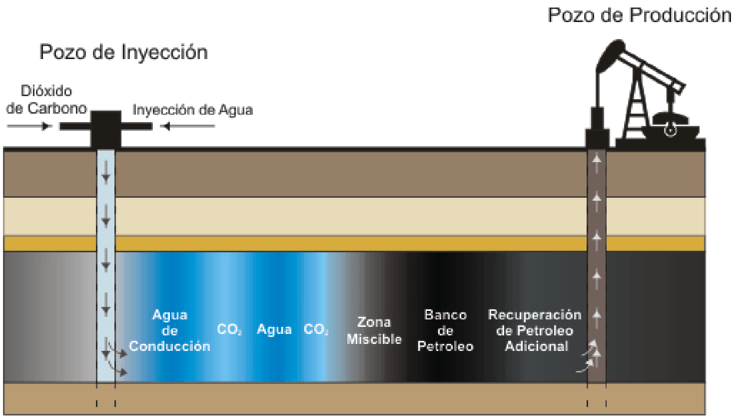

Figura 4: Recuperación Asistida con Inyección del agua.

Adaptado de Textos Científicos. 2005

Movilización. – El último paso es el transporte del petróleo, ya que comúnmente los pozos se suelen hallar en zonas alejadas como pueden ser desiertos, selvas o incluso bajo el mar, por ende, el transporte de petróleo se vuelve un aspecto importante de la industria petrolera, por lo que, al momento de extraer y almacenar el petróleo, el siguiente paso es transportarlo y la forma de hacerlo es mediante tubería hasta la zona costera donde se entrega al mejor postor.

Por lo que la primera parte de este gran proceso se tiene que realizar de la mejor manera para que de esta forma la información requerida por la gerencia sea la más acertada y de esta manera tomar las mejores decisiones en las siguientes partes del proceso y si en uno de estos procesos llegara a pasar un problema con la información, ya que en cada una de estas partes se sigue registrando información importante sobre los pozos y su mantenimiento, por ende esta información debe ser cuidada de la mejor manera, ya que ha pasado casos con archivos que no son encontrados o que han estado corruptos y no han sido respaldados de alguna forma y esto puede ocasionar un efecto en cadena y hacer que la producción descienda o hasta el punto de parar la producción. A todo esto, no hay una documentación o plan oficial de la manera adecuada de salvaguardar la información de los diferentes riesgos o que esté relacionado con la seguridad de la información (Hugo S, 2019).

1.2 Antecedentes

La empresa Petrolera, que tuvo su inicio en el año 2001 con su matriz en Quito y su campo de perforación en Pindo, y prontamente a ser poseedor de otro campo de perforación, actualmente la organización cuenta con 38 personas de planta en la Matriz de Quito y otras 30 en campo Pindo, es una pequeña petrolera a comparación de otra pero con un gran potencial de expansión en los próximos años con futuras perforaciones en el Oriente, por lo que se requiere un servicio de contingencia y recuperación de la información. La información de la organización se encuentra en servidores físicos y virtuales que se encuentran 5 en la Matriz de Quito en los cuales se encuentra toda la información de su campo Pindo.

Gran parte de esta información que se encuentra en estos servidores es de correos electrónicos de todos los usuarios de la empresa como también información importante del área de operaciones, esta área es conformada por 10 personas de las cuales se dividen en dos partes, el grupo de geología y operaciones como tal, esta área maneja toda la información de la organización como son: datos de excavación de los pozos, datos de próximas excavaciones de pozos, datos de extracción de barriles de petróleo, presupuestos en base al petróleo extraído, etc. Muchas veces esta información son archivos que yacen desde el 2001, año en el que se creó la petrolera y se comenzó con el proceso para la primera perforación y extracción de petróleo. Por lo que si esta información se pierde la organización pudiera perder mucha productividad y hasta parar por completo su trabajo, ya que esta información se almacena en los servidores propios de la empresa, a diferencia de otras áreas como compras o finanzas que tiene su información en un ERP que almacena la información en la nube la cual es mucho más segura a riesgos tangibles de la empresa por lo cual esta información que se encuentra en los servidores se puede encontrar en riesgo.

Por lo que, ya que se maneja mucha información delicada en dichas organizaciones, es necesario aplicar un servicio de contingencia y recuperación de la información para la empresa, por lo que se debe realizar estudios de los riesgos de la empresa y de esta manera poder prever cualquier problema y si es el caso recuperar la información en el caso de perdida, y de esta manera tener la mejor solución para la misma,

Para este proyecto de propuesta nos guiaremos con la ayuda de la metodología NIST SP 800-30 (Stoneburner, 2002). La cual nos proveerá con diferentes métodos que nos ayudaran a evaluar a la organización y encontrar la mejor estrategia para la mitigación de riesgos en la Petrolera.

1.3 Alcance

Para la organización es de gran importancia la información que se genera dentro de la empresa y por ende también la que se almacena dentro y fuera de la empresa, por lo que buscaremos una estrategia donde se pueda evaluar las diferentes amenazas y vulnerabilidades que puedan existir en los servidores físicos o los diferentes equipos que guardan información dentro de la empresa donde se encuentra esta importante información del área de operaciones que están en riesgo por varios factores y pudiera ser perdida por completo, también se determinara los riesgos y el impacto que podría tener la empresa si algún problema ya sea de bajo impacto o de gran impacto ocurriera, por lo que se buscara de igual forma una manera para resolver dichos problemas. Por lo que se armará una propuesta para la empresa y proveer de un entregable donde se especifique todo el proceso e información necesaria para dar solución a su problema, y así de esta manera cuidar la integridad de la información con la ayuda de la metodología NIST SP 800-30 la cual nos dará las directrices para lograr este objetivo (Stoneburner, 2002).

Esta propuesta se aplicará primeramente al área de operaciones ya que es la más crítica de la empresa, si la propuesta es exitosa se ampliará a las otras áreas como son las de Legal y Recursos Humanos, pero que en esta ocasión no estarán contempladas al igual que compras, ya que ellos se manejan únicamente con el sistema de ERP (Tic.Portal. 2019).

1.4 Justificación

Gracias a la aplicación de esta propuesta se espera primeramente dar a conocer a la empresa Petrolera sobre las diferentes amenazas que pueden estar latentes dentro de la organización, como también dar a conocer una solución para la situación en la que se encuentra comprometida su información ya que es información bastante delicada y si se llega a comprometer la organización pudiera tener una gran recaída, por lo que esta solución debe de garantizar la integridad de la información de la empresa ante cualquier altercado que pudiera ocurrir y de no ocurrir siempre estar prevenidos ante cualquier emergencia. Ya que no solo se trata de proponer una solución si no también dar a conocer y crear conciencia de las diferentes amenazas y vulnerabilidades que las empresas de este nivel se encuentran todo el tiempo por la gran cantidad de ingresos que obtienen. Si llegara a ocurrir un problema en alguno de los procesos en la que los datos son procesados ya sea un problema de perdida de información, robo de información o por causas naturales debe haber un plan para salvaguardar la información o de caso contrario la producción pudiera disminuir o hasta para completamente ya que esta información está directamente relacionada con la explotación del petróleo.

Por lo que es de gran importancia tener un marco claro de la situación en la que se encuentra la empresa y de esta manera poder ayudarla con la propuesta que se va a realizar y salvaguardar los intereses de la empresa, y la mejor forma de hacerlo es cuidar de su información y que siempre se encuentre segura y disponible.

1.5 Objetivo General

Desarrollar un plan de mitigación de riesgos de la información aplicado al área de Operaciones de una empresa Petrolera siguiendo la metodología NIST SP 800-30.

1.5.1 Objetivos específicos

- Definir los principales activos tecnológicos en los que está involucrado la información que forma parte del modelo de negocio del área de operaciones de la empresa Petrolera.

- Identificar las principales amenazas que puedan afectar a los activos previamente considerados, pudiendo afectar la integridad, disponibilidad y confiabilidad de la información que estos almacenan.

- Definir las recomendaciones de control para minimizar los riesgos contra la información de la Petrolera.

2. MARCO TEORICO

En este capítulo vamos a describir los principales conceptos aplicados en nuestro proyecto de análisis de riesgo.

2.1 Petróleo

En la siguiente sección vamos a describir todos los conceptos necesarios para entender que es el petróleo y el proceso que se debe llegar hacer para su extracción.

2.1.1 Que es el Petróleo?

Es un líquido de origen natural que está compuesto principalmente de una mezcla de hidrocarburos y diversos compuestos orgánicos, por lo general se lo encuentra debajo de la superficie de la Tierra y mediante perforación de pozos se lo logra extraer, el petróleo se crea de manera similar al carbón. Cuando los animales o las plantas que vivieron en el agua mueren, sus restos se depositan al fondo de estanques, océanos, etc. Y es ahí cuando esos restos después de millones de años se comienzan a transformar en diferentes elementos en este caso petróleo. Pero a diferencia del carbón que requiere millones de años para ser creado, el petróleo tan solo necesita un millón de años (Ambientum, 2019).

2.1.2 Localización

Al ser un compuesto líquido, su presencia no se encuentra normalmente en el lugar en el que se generó, tiende a moverse de forma vertical o lateral, y de esta forma se filtra mediante la porosidad de las rocas, muchas de estas veces son distancias bastante largas, hasta poder encontrar una salida a la superficie los cual es bastante complicado sin la intervención humana, en el caso que llegara a pasar, puede evaporarse o hasta oxidarse al momento de hacer contacto con el aire, y si llegara a pasar el petróleo podría desaparecer, o puede ocurrir que encuentre una roca no porosa que impida su salida, en cuyo caso hablamos de un yacimiento (Aguirre, 2007).

2.1.3 Tipos de petróleo

El petróleo está compuesto por una gran cantidad de compuestos químicos, los cuales se diferencian por su volatilidad. Al exponer al petróleo a altas temperaturas algunos de los compuestos más ligeros se evaporan.

Por lo que dependerá del punto de ebullición del petróleo para saber qué tipo es. Se usan las curvas de destilación TBP para diferenciar los tipos de petróleos y de esta manera poder definir los rendimientos que se pudieran obtener de los productos por separación directa (Aguirre, 2007).

2.2 Exploración

Para encontrar las zonas donde se hallan yacimientos de petróleo no existe una formula exacta, por lo que es necesario la realización de una gran cantidad de trabajos previos para el estudio del terreno, La exploración está compuesta de 5 fases las cuales no ayudan a la planificación de la perforación como podemos visualizar en la Figura 2 (NousGroup, 2014, p 24).

La fase de exploración significa iniciar toda la planificación de las perforaciones.

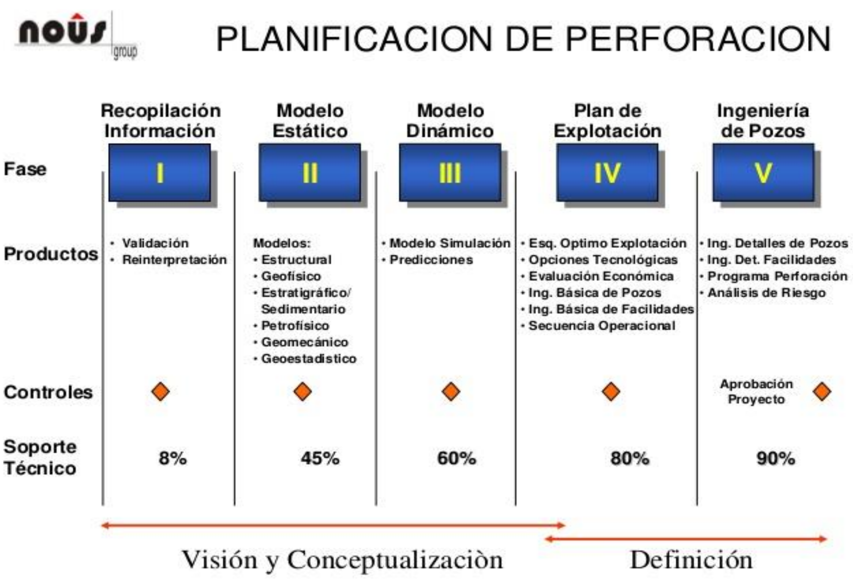

Figura. 5. Fases de planificación de perforación.

Adaptado de NousGroup, 2014, p. 24

2.2.1 Recopilación de Información

Comienza con la información topográfica de la zona la cual se realiza con una prospección sísmica la cual son cálculos que nos ayudan a lograr una evaluación exacta de las formaciones del subsuelo (Kraus, 2012, p. 8), este proceso se puede entender de mejor manera con la Figura 3 en la parte inferior.

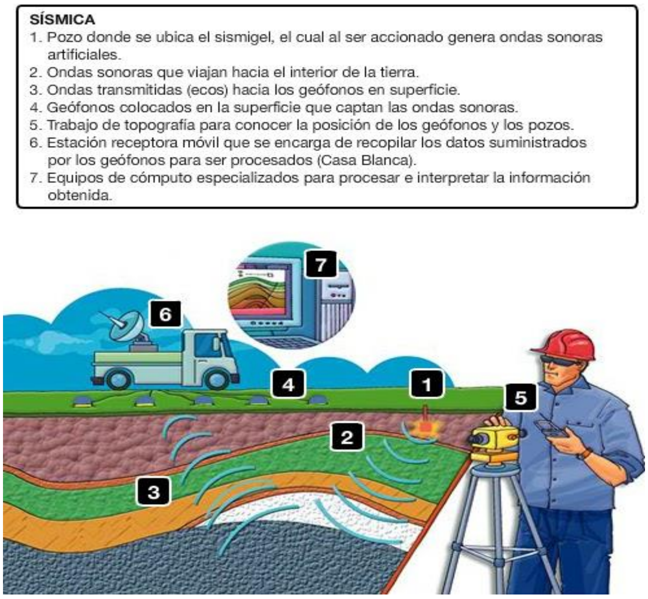

Figura. 6. Recopilación de información.

Adaptado de E.E Hydrocarbons Company. 2012

Estas ondas que son recibidas llegan a equipos especiales de cómputo que van dibujando el interior de la tierra de esta forma, se adquiere datos cartográficos, archivos vectoriales, imágenes tipo tif entre otras, lo que implica un volumen importante de información que debe ser manejado también por software especializado. Además, que se hace un análisis de datos de los ripios ya sean de previas perforaciones o de la zona donde se quiere hacer el siguiente pozo, los ripios son las muestras o las rocas que se van adquiriendo durante el proceso para la perforación.

2.2.2 Modelo Estático

En esta fase podemos encontrar a los encargados de la petrofísica qué son los que analizan las partes físicas de la roca mediante datos de registros eléctricos de perforación lo cual se logra con la ayuda de sondeos eléctricos verticales, que nos permiten conocer a través de la resistividad de los materiales sus propiedades físicas de la roca cómo son saturación de agua o contenido de petróleo, en esta misma fase también podemos encontrar al personal geofísica que analiza toda la parte del subsuelo mediante información sísmica previamente adquirida, con esta información en conjunto con petrofísica se realiza un modelo estático y gracias a esto se propone nuevos pozos para la petrolera. (Hugo S, 2019).

2.2.3 Modelo Dinámico

Los encargados son los reservorista y yacimientos, ellos arman este modelo con todos los datos que son enviados desde el campo y con aporte de la información del personal de petrofísica y geofísica, de esta manera generan un modelo dinámico y con el cual comenzar hacer predicciones, ya que no hay un método preciso para asegurar la presencia de petróleo a menos que se perfore, por ende estas predicciones son extremadamente importantes ya que pueden ser como cantidad de petróleo que se podría encontrar o como cantidad de barriles por día, de igual manera esto gracias a sistemas informáticos especializados (Hugo S, 2019)..

2.2.4 Plan de Explotación e Ingeniería de Pozos

Las siguientes dos fases son un poco más gerenciales ya que se enfocan más a lo económico, ya que se elige que tipos de pozos se perforarían o la tecnología con la que se va a perforar y de qué forma se lo hará, como también temas de facilidades que son el personal que se encargan de permisos de construcción de vial ya que muchas veces no existen vías para trasladar toda la maquinaria donde se realizara el nuevo pozo. Todo este proceso es necesario para llegar a realizar la perforación y saber cómo extraer el petróleo de la mejor forma ya que no hay una única manera de hacerlo todo dependerá de la tecnología y forma que decidan los técnicos (Aguirre, 2007, p. 18).

2.3 Perforación de pozos

No obstante, en un principio se usaba la técnica de percusión, cuando los pozos petroleros estaban a poca profundidad, este método desde mediados del siglo XX dio un paso al costado para que entrara el método de rotación, ya que se ha determinado que la mayor parte de petróleo se encuentra a profundidades de 900 y 5000 metros, pero hay casos de pozos que llegan a los 8000 metros (Aguirre, 2007, p. 19).

2.3.1 Métodos de Perforación

Como ya se ha dicho antes con el paso del tiempo se han creado nuevas formas para la perforación de pozos, cada uno de estos métodos dependerá de la profundidad del yacimiento y el análisis de las capas del subsuelo de la tierra, ya que si el pozo no se encuentra a mucha profundidad se podría utilizar el método de percusión, ya que el método de perforación rotativa es económicamente mucho más alto que el método de perforación por percusión, como también existe el método de perforación direccional que es usado básicamente cuando no se puede ingresar al yacimiento de forma vertical por lo que todo dependerá de los análisis de la información previa en la etapa de exploración (Kraus, 2012, p.10).

Por lo que aquí podemos ver los diferentes métodos de perforación:

- Perforación por percusión
- Perforación rotativa
- Perforación roto percutante
- Electro perforación
- Perforación direccional

2.3.2 Operaciones de perforación

Al momento de realizar la perforación de los pozos a ciertos procesos que se deben de realizar a la par de la perforación para que se continua y no ocurra problemas durante su ejecución estas son las siguiente.

Técnicas de perforación. – La plataforma de perforación ayuda de base para que el personal de perforación pueda acoplar las diferentes secciones de la tubería de perforación según vaya aumentando la profundidad. Cuando hay que extraer la barrena ya sea por algún problema, el tubo de perforación debe ser extraído por completo, separando cada una de las partes y hasta llegar a la barrena y de esta forma poder cambiarla, y hay que tener mucha atención que la columna de perforación no se disgregue ya que puede caer al hoyo y ocasionar muchos problemas.

Lodo de Perforación. – Es un líquido compuesto por petróleo y arcilla, el cual se inyecta desde el tanque de mezcla hasta la barrena y después asciende a la superficie desde el exterior de la tubería, este lodo de perforación nos ayuda básicamente a refrigerar y lubricar la barrena, de igual forma al momento que sale nos ayuda a expulsar fragmentos de roca triturada (Kraus, 2012, p. 11).

Revestimiento. – Para revestir el agujero del pozo se usa una tubería de acero especial. Se utiliza para que no ocurra derrumbes de las paredes del agujero, como también para proteger y que no penetren tierra, rocas, agua salda y otros contaminantes (Kraus, 2012, p. 11).

2.4 Extracción o Producción

Los antecedentes de antiguos pozos nos permiten afirmar que comúnmente un yacimiento de petróleo solo se es aprovechado entre un 25% a un 50% de su capacidad total.

El petróleo tiende a estar acompañado por gas. Ambos por la profundidad en la que se encuentran, están sometidas a altas presiones, al llegar la barrena de perforación y rompe la roca impermeable provoca que la presión baje y provoca que el gas se expanda y el petróleo deja de tener un obstáculo de la roca impermeable, y esto permite que el petróleo suba a la superficie (Aguirre, 2007, p. 20).

2.4.1 Producción y conservación de petróleo

La producción de petróleo se produce básicamente por el desplazamiento de agua o gas. Cuando comienza la perforación casi todo el petróleo está a presión. Esta presión naturalmente disminuye a medida que se extrae el petróleo durante las tres fases siguientes (Kraus, 2012, p. 11).

Primera fase. – llamada de producción emergente, el flujo lo controla la presión natural del yacimiento.

Segunda fase. – La cual se realiza inyectando diferentes sustancias a presión en el yacimiento cuando se ha acabado la presión natural

Tercera Fase. - denominada de agotamiento y es cuando los pozos solo producen intermitentemente.

2.4.2 Métodos de recuperación

Muchas veces la productividad de los yacimientos puede mejorar con el uso de diferentes formas de recuperación cuando la presión a disminuido como se habló anteriormente, pero varias veces todo dependerá del pozo y saber que método usar, y muchas veces de esta forma generar una acción química que ayude, en ciertos casos se puede hasta llegar a usar dos métodos de recuperación para generar la presión artificial, como los siguientes (Kraus, 2012, p. 12).

- Acidificación
- Fracturación
- Inyección de agua
- Inyección de fuego
- Inyección de vapor

En esta etapa se debe registrar las cantidades de petróleo que se extraer, para que de esta forma tener un balance y mantener un equilibrio ya que si se fuerza al pozo este se podría apagar y si eso sucede ningún tipo de método de recuperación puede volver hacer que el pozo se active.

2.5 Movilización

Los pozos petrolíferos se hallan en lugares muy alejados, por lo que se necesita un transporte eficaz para el mismo, pero algunos de entonces significan una gran inversión como son los oleoductos o barcos.

En la antigüedad el petróleo se refinaba cerca del lugar de producción. A medida que fue incrementando la demanda, se consideró que era más factible transportar el petróleo crudo a las refinerías que se encontraban en los países donde más se lo consumía (Aguirre, 2007, p. 26).

2.5.1 Medios de transporte

A pesar de que todos los medios de transporte son buenos para transportar este producto, ya sea el mar, la carretera, el ferrocarril o la tubería, el petróleo crudo utiliza sobre todo dos medios de transporte masivo que son el oleoducto y los petroleros de gran capacidad.

Oleoducto

Un oleoducto son un conjunto de instalaciones que ayudan a transportar por tuberías los productos petrolíferos líquidos, en bruto o refinado.

Un oleoducto se basa no tan solo en las tuberías, sino también las diferentes instalaciones para su explotación como son: depósito de almacenamiento, estaciones de bombeo, equipos de limpieza, conexiones y distribuidores, control medio ambiental, etc. (Aguirre, 2007, p.27).

Las tuberías de los oleoductos tienen un diámetro que oscila entre 10 centímetros y un metro. Ayudan a comunicar a los depósitos donde se almacena el crudo desde de los campos de extracción hacia los depósitos costeros o directamente con los depósitos de las refinerías.

Petroleros

En la actualidad los barcos petroleros son los más grandes navíos de transporte que existen. Son enormes depósitos flotantes que pueden llegar a medir más 300 metros de largo y llegar a pesar hasta las 250.000 toneladas. (Aguirre, 2007, p.29).

El petrolero la forma más económica de transportar petróleo a grandes distancias y tiene la gran ventaja, la cual es su característica de división de su espacio interior en cisternas individuales, lo que permite separar los diferentes tipos de petróleo o sus productos derivados. (Aguirre, 2007, p. 30).

2.5.2 Actividades de los contratistas

Las compañías de prospección y producción de petróleo suelen utilizar los servicios de contratistas para que ayuden con algunos de los siguientes servicios de soporte necesarios para perforar y poner en explotación campos productores (Kraus, 2012, p. 11).

- **Preparación del emplazamiento:** rampas, puentes, construcción de carreteras, etc.
- **Montaje e instalación:** energía y servicios, equipo de perforación, tanques y oleoducto, alojamiento, etc.
- **Mantenimiento y reparación:** mantenimiento preventivo de equipos de perforación y producción, vehículos, etc.
- **Ingeniería y trabajos técnicos:** pruebas y análisis, servicios informáticos, laboratorios, almacenamiento y manipulación de explosivos, etc.
- **Servicios externos:** alcantarillado y recogida de basura, radio y televisión, teléfono.

Algunos de estos servicios en conjunto son los que ayudan a la construcción de la tubería de oleoducto para el transporte eficaz del petróleo crudo (Kraus, 2012, p. 13). Por lo que el tema de las actividades de los contratistas va de la mano con la movilización en una petrolera.

A continuación, se mostrará la Figura 6 la cual nos engloba todo el proceso.

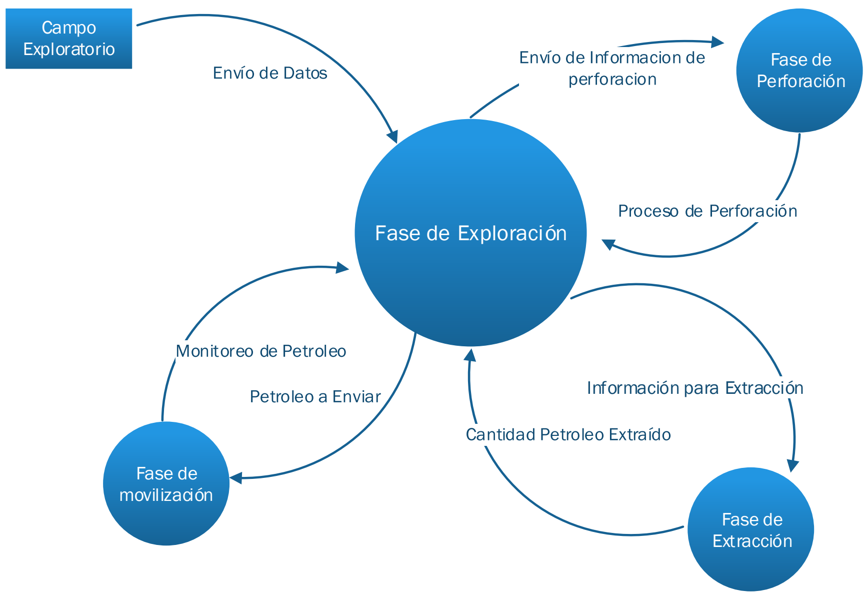

Figura. 8. Diagrama general de las fases del área de operaciones.

2.6 Seguridad Informática

La importancia de la seguridad informática es cada vez más grande en los usuarios de las empresas, ya que deben de ser conscientes de que el funcionamiento correcto de sus sistemas dependerá en gran medida en protegerlos.

Para tener una mejor idea y concisa de lo que es la seguridad informática se citara el siguiente concepto que menciona:

> “La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una

organización seas utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.” (Costas, 2014, p. 19)

2.6.1 Importancia de la información

La información es el activo más importante para cualquier empresa. La información es el conjunto de datos que da razón de ser a una empresa, los datos que la definen, datos con los que trabaja, que, si llegaran a manos inadecuadas, pueden llevar a la ruina

Este concepto se puede dividir en dos partes los cuales son: seguridad de la información y seguridad informática (Escriva, 2013, p. 7).

Seguridad de la información. – es un conjunto de medidas y procedimientos tanto humanos como técnicos, que nos ayudan a proteger la integridad, confidencialidad y disponibilidad de la información

Seguridad informática. – es una parte de la seguridad de la información que ayuda a proteger la información que utiliza la una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida.

2.6.2 Activos en la seguridad informática

Los activos informáticos son recursos del sistema necesarios para que la organización llegue a los objetivos planeados, esto quiere decir todo aquello que tenga valor y que debe ser protegido frente a cualquier problema. Por lo que podemos decir que consideramos como activo: los trabajadores, el software, los datos, los archivos, el hardware, las telecomunicaciones, etc.

Entonces la seguridad informática tiene como objetivo proteger dichos activos, por lo que el primer paso es identificarlos para proponer los métodos necesarios para su protección y analizar la relevancia de estos, ya que no tiene sentido invertir miles de dólares en un activo que no es importante para el negocio. (Escriva, 2013, p. 8).

Por lo que desde la informática podemos definir que los principales activos en una empresa son:

Software. – Programas o cualquier tipo de aplicación que use la organización para su buen funcionamiento

Información. – Cualquier elemento de datos que este almacenado en algún soporte como puede ser: libros, documentos, datos de los empleados, etc.

Físicos. – Infraestructura tecnológica que se utiliza para procesar, almacenar o administrar la información de la empresa para su correcto funcionamiento

Personal de la organización. – Que maneje la estructura tecnológica y de comunicación para la utilización de la información.

2.6.3 Vulnerabilidades

En la actualidad en las organizaciones es muy común que esté presente el hecho de las vulnerabilidades

Según (Escriva, 2013), en la seguridad informática se considera como vulnerabilidad a cualquier debilidad de un activo de poder ocasionar problemas al correcto funcionamiento del sistema informático. Ya sea, no utilizar ningún tipo de protección contra fallos eléctricos o no tener mecanismos de protección contra ataques informáticos, como antivirus o firewall, etc.

2.6.4 Amenaza

Una amenaza puede ser cualquier entidad o circunstancia que atente contra el correcto funcionamiento de un sistema informático, aunque hay algunas amenazas que pueden afectar involuntariamente a los sistemas de información, por ejemplo, un desastre natural.

Citando a (Costas, 2014), las amenazas pueden ser provocadas por tres diferentes razones y pueden ser por:

- Personas. – Personal de la empresa, Exempleados, Hackers, Crackers o Intruso Remunerados
- Amenazas lógicas. – Herramientas de seguridad, Software incorrecto, Puertas traseras, Caballos de troya, Virus, Gusanos, etc.
- Amenazas físicas. – Robos, Sabotaje, Cortes de suministros eléctricos, Condiciones atmosféricas adversas, catástrofes naturales, etc.

2.6.5 Riesgos

Existen diversas definiciones para definir el termino riesgo, pero entre una de ella se destaca al de la UNE-71504:2008, que no indica lo siguiente:

> “Un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.”

Por ende, el riesgo es una medida de la probabilidad de que se materialice una amenaza.

Cuando se hace un análisis de riesgos se debe tener presente los activos que hay que proteger, sus vulnerabilidades y amenazas, así como la posibilidad de que estas se produzcan. Los resultados del análisis de riesgos nos permitirán recomendar qué medidas se deberán tomar para conocer, prevenir, impedir, reducir o controlar los riesgos anteriormente identificados y de esta manera poder reducir sus posibles daños (Escriva, 2013, p. 11).

2.7 Metodología NIST SP 800-30

Es una metodología que fue desarrollado por el Instituto Nacional de Estándares y Tecnología. La NIST SP 800-30 nos ayuda a la gestión de riesgos, que se orienta a los procesos mediante un buen análisis y gestión de riesgos.

La gestión de riesgos juega un papel importante en la protección de los activos de la organización. Gracias a la gestión de riesgos se puede identificar de mejor manera los activos más importantes en la seguridad de los sistemas de información, como también las amenazas que puedan afectarles, de igual forma identificar las diferentes vulnerabilidades de cada uno de los activos y calcular el riesgo en el que se puedan encontrar.

Citando a (Stoneburner, 2002, p. 9), la metodología NIST SP 800-30 está conformada por los siguientes pasos:

- La caracterización del sistema
- Identificación de amenazas
- Identificación de vulnerabilidades
- Análisis de control
- Determinación de probabilidad
- Análisis de impacto
- Determinación del riesgo
- Recomendaciones de control
- Documentación de resultados

En los primero siete pasos se realiza todo el análisis de riesgo pertinente y en los dos últimos pasos se realiza la verificación y validación de los resultados.

2.7.1 Porque NIST SP 800-30?

NIST SP 800-3 nos ayuda a analizar la seguridad de la infraestructura en la que residen los datos. En esta metodología los riesgos organizacionales o los requisitos comerciales no son una forma para medir el riesgo, como sucede con otra metodología como la ISO 27005 u Octave, por lo que la NISTSP 800-30 está enfocada al análisis de riesgo de la información de la empresa. (Shanthamurthy, s.f.), a continuación, se realizará una comparación con otras dos metodologías para fundamentar la elección de la metodología.

Tabla 1

Comparación de Metodologías

NIST SP 80030	CRAMM	MAGERIT
1.- Su modelo si involucra vulnerabilidades	1.- Su modelo si involucra vulnerabilidades.	1.- En su modelo no involucra vulnerabilidades .
2.- La guía provee herramientas para la valoración y mitigación de riesgos 3.- Lista de controles recomendados	2.- El resultado del análisis es la tabla de valorización de riesgos sobre los activos, se requiere complementar con otra metodología para la mitigación de los riesgos o lista de controles recomendados.	2.- La metodología provee las herramientas necesarias para la valoración y mitigación de riesgos 3.- Lista de controles recomendados
4.-Certificada internacionalmente	3.-Certificada internacionalmente	3.- Solo se puede aplicar a nivel nacional ósea solo en España, no está certificada internacionalmente

3. IMPLEMENTACION

En este capítulo se realizó la aplicación del proyecto con la Metodología NIST SP 800-30 en la petrolera siguiendo los siguientes 9 pasos como se ve en la figura 6 y que fueron descritos previamente.

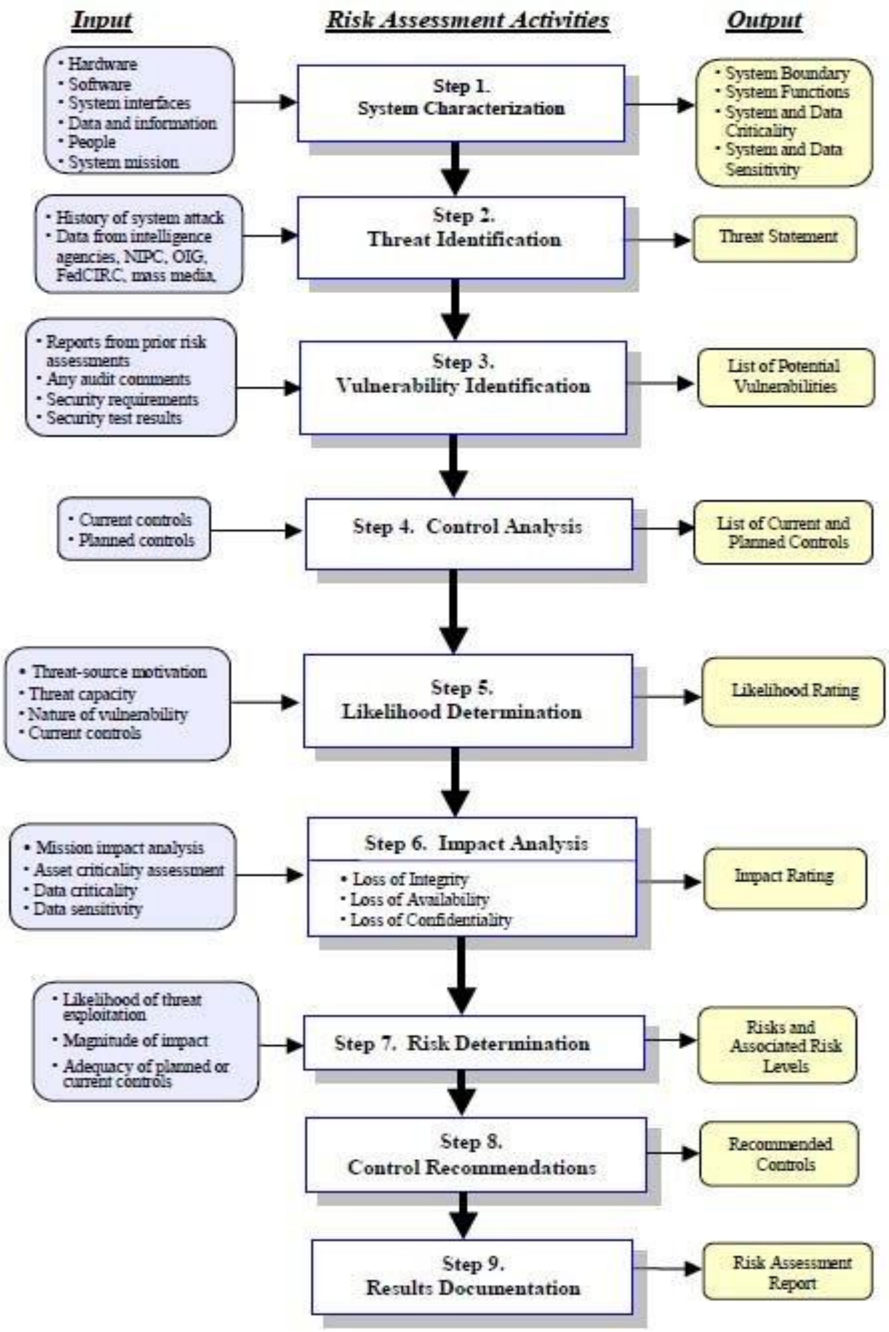

Figura 9. Metodología NIST SP 800-30.

Adaptado de Stoneburner, 2002

3.1 Caracterización de sistema

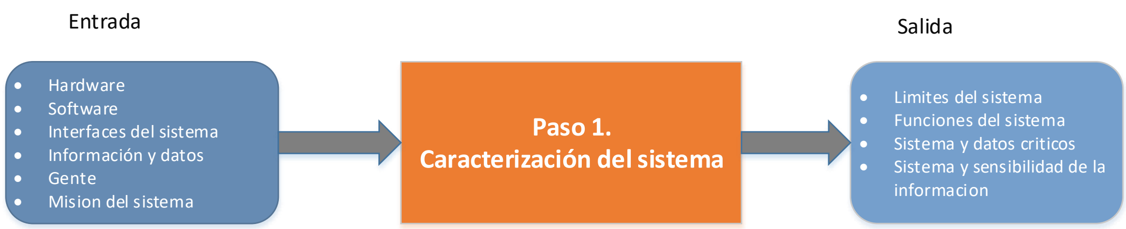

Figura 10. Caracterización de sistema.

Adaptado de Stoneburner, 2002

En este primer paso se identificarán todos los activos informáticos y aplicaciones, el cual es identificado mediante los recursos e información que lo componen. Para lograr la caracterización del sistema según (Stoneburner, 2002) se necesita describir el sistema bajo los siguientes puntos que son:

- Hardware
- Software
- Datos e información
- Personas que usan el sistema y dan soporte
- Los procesos que se realizan en el área de operaciones
- Sistema y datos críticos
- Sistema y datos sensibles

Esta información se puede recolectar de 4 diferentes formas como ya se había explicado previamente, en el caso de la Petrolera el método de recopilación de información que se uso es:

Gracias al método de recopilación de información pudimos llegar a la siguiente caracterización del sistema como se ve a continuación en la tabla

Tabla 2

Caracterización del sistema

CARACTERIZACION DEL SISTEMA
Límites del sistema
El área de operaciones de la Petrolera se compone de: - **Hardware** (Servidores, Workstation de Geólogos, Computadores de usuarios, Plotter, Storage, Routers, Switch) - **Software** (Office 2016, Petrel de Geofísica, Petrel de Reservorio, TechLog, DesicionSpace) - **Equipos Electrónicos** (Microscopios, Sensores de campo) - **Seguridad Informática** (Antivirus y Firewall) - **Personas** (Operadores, Técnicos, Directivos, Geólogos, Petroleros)
Funciones del sistema
- Recopilación de datos de campos de perforación - Creación de modelos para proponer nuevos campos perforación - Creación de modelos para la predicción de petróleo a extraerse - Proceso continuo de información de los diferentes yacimientos - Monitoreo de Almacenamiento y Entrega de petróleo
Sistema y datos críticos
El sistema Petrel es un sistema de gran importancia ya que ahí es donde se hacen los modelos estáticos y dinámico los cuales son archivos que contienen un gran volumen de información y de los cuales salen datos importantes como: - Predicciones de nuevos pozos petroleros - Barriles de petróleo que puede tener el pozo perforado - Como se encuentra la producción del pozo - Duración aproximada del pozo
Sistemas y sensibilidad de la información

-La gran mayoría de la información del Área de operaciones no se encuentra respaldada y solo se encuentra guardada en los mismos computadores de los usuarios por lo que es un problema.

3.1.1 Especificación de los límites del sistema

A continuación, se documenta las diferentes características que tienen los activos informativos y sus funciones.

Hardware

Servidor Backup. – Básicamente contiene los respaldos del personal de la empresa y por ende del área de operaciones, pero no contiene un respaldo completo como tal, es parcial ya que la mayoría de información es de office y no de los sistemas de información especializados que usan los geólogos ya que son muchas veces muy pesados.

Servidor de Archivos. – Este servidor se encarga de almacenar la documentación de las diferentes áreas, esto ayuda al intercambio de información entre el personal, en el área de operaciones y en las demás es útil ya que el personal puede tener presente siempre la información relacionada con su área.

Servidor de Antivirus. – Este servidor ayuda a brindar el servicio de antivirus a los computadores de todo el personal de la petrolera, mediante la utilización de Kaspersky.

Active Directory. – Este servidor nos ayuda a la administración de todo el personal incluido el personal de campo de la petrolera, como también nos ayuda con los equipos y recursos.

Workstation. – Son equipos de alto poder de procesamiento que son entregados únicamente al grupo de geólogos del área de operaciones en los cuales se genera y almacena gran parte de la información del proceso de extracción de petróleo, su valor puede pasar hasta los 10 mil dólares por equipo, el grupo de geólogos tienes 3 Workstation en la actualidad.

Computadores. – Son los equipos utilizados por el resto del área de operaciones son de gama mucho más baja, ya que ellos hacen labores un poco más administrativas y no necesitan tanto procesamiento del computador, pero de igual forma guardan gran parte de su información en el mismo equipo, de esta clase de equipos podemos encontrar 8 equipos que conforman al área de operaciones exclusivamente.

Plotter. – Este dispositivo de impresión ayuda al área de operaciones cuando se necesita imprimir mapas con diferentes características para su presentación, debe ser un plotter ya que los mapas deben visualizarse de correcta forma porque tienes muchos detalles en cada uno de ellos.

Storage. – Mucha de la información del área de operación también se encuentra guardada en diferentes dispositivos de almacenamiento ya sean Cd's o discos duros externos, ya que muchas veces cuando se necesita enviar información los archivos son muy pesados y se necesita de Cd's para hacerlos.

Software

Office 2016. – Es el encargado de brindar todos los programas de ofimática necesarios para la realización de presentaciones o reportes, momento de proponer un nuevo pozo a la directiva de manera más formal y detallada.

DesicionSpace. – Es un software que ayuda al análisis de la información cartográfica de la zona, archivos vectoriales entre otros, también sirve para el análisis de datos de los ripios de perforación que se van adquiriendo antes o durante el proceso de perforación.

TechLog. – Es un software que ayuda al análisis de las propiedades físicas de la roca, mediante datos de registros eléctricos que se adquieren durante el proceso de perforación de un pozo, con dichos datos se analiza las propiedades de la roca como son: permeabilidad, porosidad, saturación de agua, contenido de petróleo, etc.

Petrel Geofísica. – Este software ayuda a la creación de un modelo estático con el análisis de toda la parte del subsuelo mediante información sísmica, gracias a esto se puede proponer nuevos pozos para la petrolera

Petrel Reservorio. – Es el software encargado de la creación de los modelos dinámicos que detectan y evalúan los elementos que afectan el comportamiento de un yacimiento, con el aporte de la información de petrofísica y el modelo estático previamente realizado, y de esta forma poder realizar un modelo final.

Equipos Electrónicos

Microscopios. – En el área de geología se lo utiliza para la examinación de muestras de suelo de campo para su respectivo análisis.

Sensores de campo. – Estos ayudan a la recolección de información de campo durante todas las etapas del proceso de extracción de petróleo, los son enviado periódicamente a la matriz al grupo de geólogos para su respectivo análisis.

Seguridad Informática

Antivirus y Firewall. – Como ya se indicó anteriormente tenemos un servidor de antivirus que provee el servicio a todo el personal de la petrolera, pero también el mismo Antivirus Kaspersky hace de firewall, por lo que el firewall predeterminado de Windows esta desactivado para no ocasionar inconvenientes.

3.1.2 Activos Críticos

Una vez se haya especificado los diferentes activos, se realizó una clasificación de los activos por su nivel de impacto a la organización para esto nos ayudaremos con una valoración de dimensiones que se divide en disponibilidad, integridad y confidencialidad, y después generar criterios de valoración como veremos continuación.

3.1.2.1 Dimensiones de Valoración.

Cuando hablamos de dimensiones de la valoración debemos tener en cuenta la disponibilidad, integridad y confidencialidad que son características que hacen valioso a un activo por lo que Magerit nos indica las siguientes dimensiones ya que en la metodología NIST SP 800-30 no se establecen dimensiones como tal.

[D]Disponibilidad. – Los activos tienen un nivel alto desde el punto de vista de la disponibilidad cuando una amenaza afecta a su disponibilidad, y las consecuencias serían graves, y de igual manera un activo carece de valor cuando puede estar no disponible frecuentemente o durante largos periodos de tiempos sin causar mayores problemas, la pregunta más importante aquí es: ¿Qué importancia tendría que el activo no estuviera disponible?

[I]Integridad. – Los datos o información reciben una alta valoración en cuanto a integridad cuando su alteración voluntaria o intencionada podría causar daños a la organización, también puede pasar que los datos tienen un valor poco apreciable y su alteración no supone preocupación alguna. Una pregunta importante aquí es: ¿Qué importancia tendría que los datos fueran modificados sin un control?

[C]Confidencialidad. - Desde el punto de vista de la confidencialidad los datos reciben una alta valoración cuando su revelación causa graves daños a la organización. O por lo contrario los datos tienen un valor bajo cuando su revelación no supone ningún riesgo, por una pregunta importante es este caso es: ¿Qué importancia tendría que los datos fueran conocidos por personas no autorizadas? (Magerit, 2012, p 15).

3.1.2.2 Criterios de valoración.

Una vez tenemos claras las dimensiones de valoración para nuestros activos debemos seguir con los criterios de valoración, en este caso se usará la valoración de baja, media y alta, ya que en la metodología NIST SP 800-30 se utiliza la misma valoración por lo que será una forma más conveniente de hacerlo y no ocurra confusiones en las valoraciones.

La siguiente tabla nos ayudará a tener más claro los criterios de valoración que se tiene con los activos.

Tabla 3

Criterios de valoración.

Valoración	Criterio de Valoración
[A] Alto	Daño grave, probablemente ocasionaría un paro en la producción del Área de Operaciones
[M] Medio	Daño importante, probablemente impediría la operación efectiva del Área de operaciones
[B] Bajo	Daño menor, probablemente genere molestias en el Área de operaciones.

Tomada de Magerit, 2012

Una vez realizada la tabla de los criterios de valoración se procedió a realizar la valoración de los activos en los que está involucrada el Área de Operaciones, para la cual nos guiaremos con una valoración de criticidad realizada por el Mintic que nos ayuda con una guía para la gestión y clasificación de los activos de información, esta guía nos ayuda a evaluar la criticidad de los activos mediante su confidencialidad, integridad y disponibilidad, valores que son igualmente usados en la metodología NIST-SP 800-30, por ende se pudiese usar para generar el nivel de criticidad del activo.

Según el (Mintic, 2016, p 7), nos das los siguientes cálculos para determinar el valor del activo de acuerdo con la clasificación de la información.

- Alta. - Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (disponibilidad, integridad o confidencialidad) es Alta.
- Media. – Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (disponibilidad, integridad o confidencialidad) o al menos una de ellas es de nivel medio.

- Baja. – Activos de información en los cuales la clasificación de la información en todas sus propiedades (disponibilidad, integridad o confidencialidad) es baja.

Basado en los cálculos previamente visto podemos realizar la siguiente Tabla que veremos a continuación.

Tabla 4

Criticidad de los activos

Equipo	[D]	[I]	[C]	Nivel Activo Critico	Detalle
Servidor de Archivos	M	M	M	Medio	Intercambio de información entre el personal
Servidor de Backup	M	M	M	Medio	Respaldo de la información del personal
Servidor de Antivirus	M	M	M	Medio	Gestión de Antivirus en la organización
Estación de Trabajo 1	A	A	B	Alto	Utilización del software TechLog
Estación de Trabajo 2	A	A	B	Alto	Utilización del software Petrel Geofísica
Estación de Trabajo 3	A	A	B	Alto	Utilización del software Petrel de Reservorio
Computadores Personales 1	M	M	B	Medio	Utilizado en el área de geología con el software DecisionSpace

Equipo	[D]	[I]	[C]	Nivel Activo Critico	Detalle
Computadores Personales 2	M	M	B	Medio	Computador ubicado en campo uso para operadores.
Computadores Personales 3	M	M	B	Medio	Personal de operaciones que lleva el balance económico del petróleo extraído durante los años.
Computadores Personales 4	M	M	B	Medio	Gerencia de operaciones
Computadores Personales 5	M	M	B	Medio	Labores Administrativas de Facilidades
Computadores Personales 6	M	M	B	Medio	Labores Administrativas de Ambiente
Computadores Personales 7	M	M	B	Medio	Labores Administrativas de Operaciones
Router Matriz 1	A	B	B	Alto	Ubicado en la Matriz, Control de red
Router Campo 2	A	B	B	Alto	Ubicado en Campo, Control de Red
Switch Matriz1	M	B	B	Medio	Ubicado en la Matriz, Conecta puntos de red de

Equipo	[D]	[I]	[C]	Nivel Activo Critico	Detalle
					las diferentes áreas
Switch Campo 2	M	B	B	Medio	Ubicado en campo, Conecta puntos de red de los diferentes equipos.
Plotter	B	B	B	Bajo	Impresión de mapas geográficos.
Storage	A	M	M	Alto	Dispositivos de almacenamiento externos.

3.2 Identificación de Amenazas

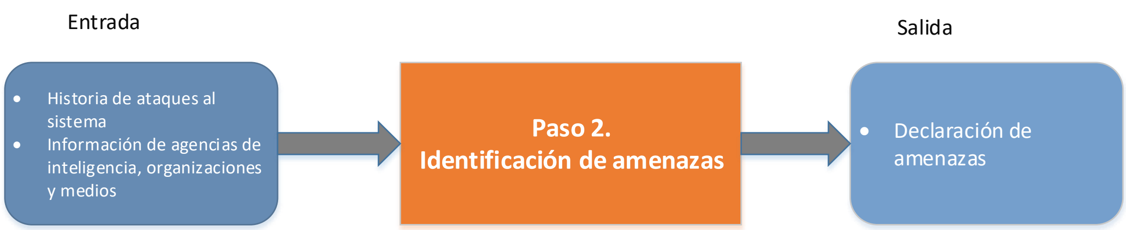

Figura 11. Identificación de Amenazas.

Adaptado de Stoneburner, 2002

Una amenaza es un acontecimiento que puede pasar sobre un activo informático, el cual puede ser causado por una fuente natural, humana o ambientales. Una fuente de amenaza no representa un riesgo si es que no hay una vulnerabilidad latente.

El objetivo en este paso es identificar las posibles amenazas que puedan desarrollarse sobre los activos informáticos que se están evaluando, para esto pueden utilizarse registros previos de ataques o problemas en el sistema, como también información de agencias de inteligencia o de organizaciones que se centran en este tema.

Para identificar las siguientes amenazas se tomará en cuenta ataques o problemas en el sistema que hayan ocurrido previamente y además la tabla # que nos proporciona (Stoneburner, 2012).

Tabla 5

Identificación de Amenazas.

IDENTIFICACION DE AMENAZAS	
Tipo de Amenaza	Fuente de la Amenaza
Amenaza Humana	• Hackers, Crackers • Espionaje Industrial • Personal Insatisfecho • Robo de Información • Perdida de Información
Amenaza Naturales	• Inundaciones • Terremotos • Tormentas Eléctricas
Amenaza Tecnológicas	• Interrupción del servicio de internet • Problemas con Activos Informáticos
Amenaza Infraestructura	• Humedad • Variación o Corte Eléctrico • Incendios

Tomada de Stoneburner, 2012

Una vez hecha la identificación de las posibles amenazas se realizó el listado de las posibles motivaciones y consecuencias de estas.

Tabla 6

Amenaza Humana

Fuente de la Amenaza	**Motivación**	**Acciones de Amenazas**
Hackers, Crackers	Desafío, Ego, Rebeldía	Sabotaje de los sistemas de información, Ingeniería Social, Manipulación de la información de la Organización, Robo de información.
Espionaje Industrial	Ventaja competitiva, Espionaje Económico	Intrusión a la información personal de la organización, Ingeniería Social, Robo de Información.
Personal Insatisfecho	Problemas en la empresa, Venganza	Borrado de información de la organización, daños a los activos informáticos de la empresa, sustracción de información sensible.
Robo de Información	Extorción, Ganancia monetaria, Venganza	Perdida de información sensible para la organización, Extorción a la organización.

Fuente de la Amenaza	Motivación	Acciones de Amenazas
Perdida de información	Errores no intencionales, Descuidos	Pérdida de Productividad para la organización, Retraso en entrega de proyectos

Tabla 7

Amenaza Naturales

Fuente de la Amenaza	Motivación	Acciones de Amenazas
Inundaciones	Causas Naturales	Daños a los activos informáticos de la organización, Problemas al personal de la organización.
Terremotos	Causas Naturales	Daños a los activos informáticos de la organización, Problemas al personal de la organización.
Tormenta Eléctrica	Causas Naturales	Daños a los activos informáticos, Fallas eléctricas o cortes de energía.

Tabla 8

Amenaza Tecnológicas

Fuente de la Amenaza	**Motivación**	**Acciones de Amenazas**
Interrupción del servicio de internet	Problemas de Infraestructura	Problemas de comunicación y transferencia de datos entre el campo petrolero y la Matriz
Problemas con Activos Informáticos	Falta de Mantenimiento	El personal no podrá trabajar adecuadamente en sus labores asignada, Falta de producción.

Tabla 9

Amenaza Infraestructura

Fuente de la Amenaza	**Motivación**	**Acciones de Amenazas**
Humedad	Falta de Mantenimiento	Daños a los activos informáticos.
Variación o Corte Eléctrico	Problemas de Infraestructura	Daños parciales o permanente a los activos informáticos.
Incendios	Falta de medida adecuada de seguridad	Daños parciales o permanente a los activos informáticos, Problemas al personal de la Organización.

3.3 Identificación de Vulnerabilidades

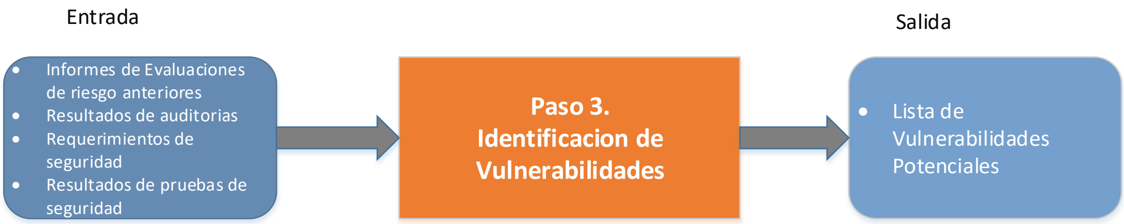

Figura 12. Identificación de Vulnerabilidades.

Adaptado de Stoneburner, 2002

Después de la realización de la identificación de las amenazas se procedió a realizar la identificación de las vulnerabilidades en las que está implicada el área de operaciones de la petrolera.

Como entradas de información general en este paso se debe tener en cuenta informes de evaluaciones de riesgo anteriores, resultados de auditoria, requerimientos de seguridad y resultados de pruebas de seguridad, los métodos más recomendados según (Stonesburner, 2012) son: el uso de fuentes de vulnerabilidades, pruebas de seguridad del sistema y el desarrollo de un checklist de requerimientos de seguridad los cuales fueron explicados a detalle en el capítulo anterior.

Para el área de operaciones se utilizó entrevistas y revisión de documentación, los resultados fueron los siguientes.

Tabla 10

Identificación de vulnerabilidades

Código	Vulnerabilidades	Fuente de la Amenaza	Acción de la Amenaza
VU1	Falta de control de los datos que se descargan de la red	Hackers, Crackers, Perdida Información	Los archivos o datos que se descarga el personal de operaciones no siempre son de fuentes

Código	Vulnerabilidades	Fuente de la Amenaza	Acción de la Amenaza
			seguras, y personas no autorizadas pueden aprovecharse de aquello.
VU2	Uso de contraseñas débiles en computadores	Usuarios no autorizados, Perdida de Información, Robo de Información	Puede generar el ingreso de personas no autorizadas a la información del computador con facilidad mediante ingeniería social
VU3	Inventario incompleto de hardware y software	Perdida de Información, Robo de Información, Problemas con Activos Informáticos	No llevar un inventario de los activos informáticos puede generar problemas a la organización.
VU4	Falta de actualización de Antivirus en algunos computadores	Hackers, Crackers, Perdida Información, Usuarios no autorizados, Robo de Información	Si no se encuentra correctamente actualizado el antivirus el computador pudiera ser vulnerado.
VU5	No hay capacitaciones sobre seguridad informática a los empleados	Hackers, Crackers	Sin capacitaciones de seguridad informática el personal pudiera ser víctima de ingeniería social.

Código	Vulnerabilidades	Fuente de la Amenaza	Acción de la Amenaza
VU6	No existen respaldos formales de la información del software Petrel y demás software de Geología	Perdida de información, Robo de información	En el caso que ocurra un accidente en los computadores gran parte de la información contenida se perdería
VU7	Los puertos USB no se encuentran bloqueados en computadores	Robo de Información, Perdida de información, Personal Insatisfecho.	Mediante un dispositivo USB se podría realizar ingeniería social y robar fácil mente información de cualquier computador.
VU8	Falta de mantenimiento en Equipos de computo	Problemas con Activos Informáticos	El personal no podrá trabajar adecuadamente.
VU9	Daño en Equipos electrónicos de campo	Problemas con Activos Informáticos, Tormenta Eléctrica, Terremoto, Inundaciones, Incendios.	Son dispositivos que muchas veces se encuentran a la intemperie y pueden recibir daño de factores externos
VU10	Infección de virus y malware en computadores del área de operaciones	Hackers, Crackers, Perdida de Información.	Infectar la máquina de usuario mediante diferentes técnicas de ingeniería social y producir daño en los activos computadores

Código	Vulnerabilidades	Fuente de la Amenaza	Acción de la Amenaza
VU11	Se terceriza el mantenimiento de activos informáticos como servidores y computadores	Filtrado de Información, Robo de Información.	Durante el mantenimiento el personal externo de la empresa puede extraer información de la empresa.

3.4 Análisis de controles

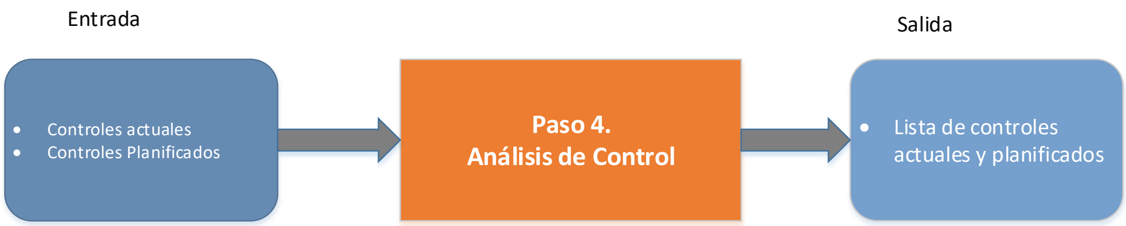

Figura 13. Análisis de control.

Adaptado de Stoneburner, 2002

Una vez se haya terminado con la identificación de las potenciales vulnerabilidades, el siguiente paso que se realizo es el de análisis de control en el cual según (Stoneburner, 2012) el objetivo es analizar los controles que se han implementado o que están planificados por la organización para minimizar o eliminar la probabilidad de que una amenaza explote una vulnerabilidad del sistema.

Los controles además hay que clasificarlos según su método ya sea técnico o no técnicos, como también según su categoría como puede ser preventivos o detectivos.

De igual manera para adquirir esta información se realizó mediante la entrevista con el personal de operaciones como también con el área de sistemas, para tener claro los diferentes controles.

El resultado del control de análisis es el siguiente:

Tabla 11

Controles Actuales o Planeados

Código	Controles	Actual / Planeado	Método	Categoría
CO1	Uso de aspersores en caso de incendios	Actual	No técnico	Preventivo
CO2	Protocolo de evacuación en caso de terremotos o erupción volcánica	Actual	No técnico	Preventivo
CO3	Políticas de autentificación de usuarios	Actual	Técnico	Preventivo
CO4	La contraseña de cada computador es personal del usuario y no debe de ser divulgada.	Actual	No técnico	Preventivo
CO5	Prohibido el uso de programas o recursos que no tengan licencia o autorización del área de sistemas	Actual	Técnico	Preventivo
CO6	Si se desea la instalación de un software, es necesario enviar un correo al área de sistemas para solicitarlo.	Planeada	Técnico	Preventivo
CO7	Prohibido el uso de servicios en la nube como Dropbox,	Planeada	Técnico	Preventivo

Código	Controles	Actual / Planeado	Método	Categoría
	One Drive, etc., sin previa autorización.			
CO8	En el caso del mal funcionamiento de un equipo se debe informar al área de sistemas.	Actual	Técnico	Preventivo
CO9	Prohibido el acceso a música, servicios de streaming o videos por internet ya que afecta a la calidad del servicio.	Actual	Técnico	Preventivo
CO10	Cada área tendrá un espacio designado para información en los servidores.	Actual	Técnico	Preventivo
CO11	Si el personal de un área requiere más espacio en los servidores deberá requerir permiso a gerencia.	Actual	Técnico	Preventivo
CO12	Los activos informáticos deberán estar identificados y asignados a un usuario en específico.	Actual	Técnico	Detectivo
CO13	Cada usuario es responsable del equipo que se le haya asignado.	Actual	Técnico	Preventivo
CO14	Gestión de Antivirus por el área de sistemas.	Actual	Técnico	Detectivo
CO15	Comunicados de seguridad informática por parte del área de sistemas.	Actual	No técnico	Preventivo

Visualizando la tabla en la parte superior podemos ver varios controles que se aplican, pero no todos los controles son respetados muchas veces por lo que se producen problemas en el área de Operaciones.

3.5 Determinación de la probabilidad

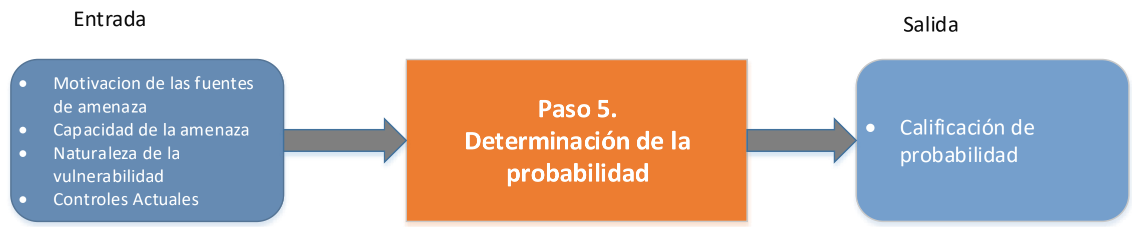

Figura 14. Determinación de probabilidad.

Adaptado de Stoneburner, 2002

En este paso se realizó una calificación de la probabilidad de que una posible vulnerabilidad pueda ser explotada por una fuente de amenaza determinada en el área de operaciones, donde deben de ser considerados los siguientes puntos que son:

- Motivación y capacidad del origen de la amenaza.
- Naturaleza de la vulnerabilidad.
- Existencia y eficacia de los controles actuales.

Para esto ya se realizó un análisis previo de amenazas, vulnerabilidades y controles, y de esta forma poder realizar la calificación de la probabilidad, la cual se determina con tres niveles que son alto, medio, bajo como visualizaremos en el siguiente cuadro propuesto por (StoneBurner, 2012).

Tabla 12

Definición de niveles de probabilidad.

Nivel de Probabilidad	Definición de Probabilidad
Alto	La fuente de amenaza está fuertemente motivada y los controles existentes para prevenir que la vulnerabilidad sea explotada son ineficientes.
Medio	La fuente de amenaza está motivada y los controles implantados pueden prevenir que la vulnerabilidad sea explotada
Bajo	La fuente de amenaza carece de motivación o capacidad y los controles actuales pueden impedir significativamente que la vulnerabilidad sea explotada.

Tomada de Stoneburner, 2012.

Realizado el análisis previo y junto a la tabla descrita anteriormente se pudo realizar una descripción de cada vulnerabilidad y determinar su probabilidad de ocurrencia.

Probabilidad de las Vulnerabilidades

VU1. Falta de control de los datos que se descargan de la red

Están presentes las diferentes amenazas como hackers o crackers ya que los usuarios del grupo de geología tienen acceso a mucho contenido de internet a diferencia del resto del área de operaciones ya que muchas veces necesitan buscar información extra en el internet y esto puede ser una puerta para las potenciales amenazas, existen controles actuales como son el control CO7 y CO9 para estos casos, pero no siempre se aplican al grupo de geología por lo que la probabilidad de que ocurra es: Alta.

VU2. Uso de contraseñas débiles en computadores

La fuente de amenaza carece de motivación ya que la principal razón podrían ser usuarios no autorizados, pero la seguridad para ingresar a las instalaciones es bastante rígida además que existen controles como son los CO3 y CO4 que nos ayudan a este problema por lo que la posibilidad que ocurra es: Baja.

VU3. Inventario incompleto de hardware y software

La amenaza en este caso está motivada a ocurrir ya que siempre está presente el que se pierda información o robo de información si no se lleva adecuadamente un inventario en este caso el de Hardware y Software, existen controles como son el CO12 y CO13 que nos ayudan a este problema pero que no siempre se lo hace ya sea por diferentes razones el área de sistemas, por lo que la probabilidad de que ocurra es: Media.

VU4. Falta de actualización de Antivirus en algunos computadores

En este caso una amenaza humana como puede ser un hacker o cracker puede estar presente ya que a veces no todos los equipos se encuentran con el antivirus actualizado, existen el control CO14 que ayuda a que esto no suceda, pero se ha dado casos que se pasado por alto, por lo que la probabilidad de que ocurra es: Media.

VU5. No hay capacitaciones sobre seguridad informática a los empleados

La amenaza en este caso está presente ya que cualquier usuario puede ser víctima de un ataque informático en su estación de trabajo si no tienen las capacitaciones correctas en este tema, pero gracias a los controles CO15, CO9 y CO14 ayuda en este caso, por lo que la probabilidad de que ocurra es: Baja.

VU6. Falta de respaldos formales de la información del software Petrel y demás software de Geología

La amenaza de pérdida de información está altamente presente ya que no existen respaldos formales de dichos archivos por lo que la pérdida de uno de ellos puede ser un problema, y los controles CO10 y CO11 no satisfacen dicha vulnerabilidad por lo que la probabilidad de que ocurra es: Alta.

VU7. Los puertos USB no se encuentran bloqueados en computadores

La amenaza se encuentra presente, un usuario no autorizado con un dispositivo USB podría sustraer información de un computador del área de operaciones, sin embargo, es poco probable que sea un usuario de la misma empresa, pero existe la probabilidad que lo realice una persona externa ya que entran y salen de las instalaciones constantemente, no existe un control actual para bloqueo de puertos USB por lo que la probabilidad de que ocurra es: Media.

VU8. Falta de mantenimiento en Equipos de computo

La amenaza de tener problemas con los activos informáticos del área de operaciones se encuentra presente ya que no existe un control actual o una rutina de mantenimiento de los equipos, tan solo en el caso de que el equipo comience a dar un mal funcionamiento se lo revisa por lo que la probabilidad a que ocurra es: Media.

VU9. Daño en Equipos electrónicos de campo

Existe la probabilidad de que una amenaza natural pueda dañar los equipos electrónicos de campos ya que muchas veces estos se los utiliza en la intemperie, existen controles actuales como el CO13 que pueden ayudar en estos casos a que los equipos sean mejor manejados por lo que la probabilidad a que ocurra es: Baja.

VU10. Infección de virus y malware en computadores del área de operaciones

La amenaza está altamente presente ya que muchos usuarios del área de operaciones tienen permisos extendidos para navegar por internet y descargar información del mismo por lo que hay una alta probabilidad de que un equipo pueda infectarse por un virus, pero existen controles que pueden ayudar a esto como son los CO7, CO9 y CO14, pero a pesar de eso habido casos que los virus ingresan a los equipos, por lo que la probabilidad de ocurrencia es: Baja.

VU11. Se terceriza el mantenimiento de activos informáticos como servidores y computadores

Existe la probabilidad de que una amenaza humana como filtrado de información o robo de información esté presente en esta vulnerabilidad ya que, como se terceriza el mantenimiento muchas veces se llevan los equipos y pueden aprovechar para hacerlo, pero en tal caso la empresa de mantenimiento perdería confianza por lo que no es tan probable, además que se firma un contrato de confidencialidad muchas veces, no existen controles actuales para esta vulnerabilidad, pero se la clasificó como: Bajo.

A continuación, se podrá visualizar de mejor manera el nivel de probabilidad asignado a cada vulnerabilidad en la siguiente Tabla.

Tabla 13

Nivel de Probabilidad

Código	**Vulnerabilidades**	**Nivel de Probabilidad**
VU1	Falta de control de los datos que se descargan de la red	Alta
VU2	Uso de contraseñas débiles en computadores	Baja
VU3	Inventario incompleto de hardware y software	Medio
VU4	Falta de actualización de Antivirus en algunos computadores	Medio

Código	Vulnerabilidades	Nivel de Probabilidad
VU5	No hay capacitaciones sobre seguridad informática a los empleados	Baja
VU6	Falta de respaldos formales de la información del software Petrel y demás software de Geología	Alto
VU7	Los puertos USB no se encuentran bloqueados en computadores	Media
VU8	Falta de mantenimiento en Equipos de computo	Media
VU9	Daño en Equipos electrónicos de campo	Baja
VU10	Infección de virus y malware en computadores del área de operaciones	Baja
VU11	Se terceriza el mantenimiento de activos informáticos como servidores y computadores	Baja.

3.6 Análisis de Impacto

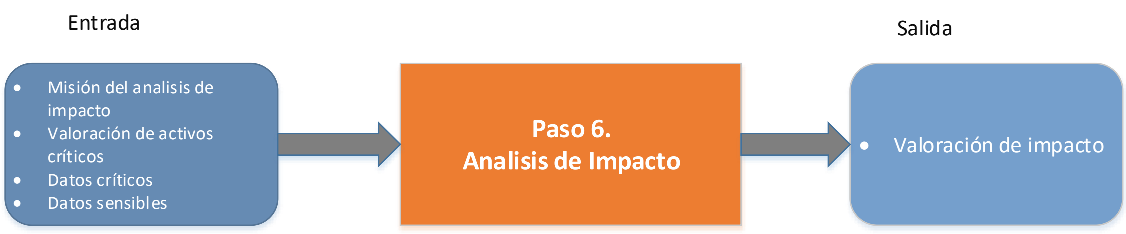

Figura 15. Análisis de Impacto.

Adaptado de Stoneburner, 2002

En este paso el objetivo es determinar el impacto negativo que ocurriría al ejecutarse exitosamente una amenaza en una vulnerabilidad, por lo que se tomara en cuenta valoración de activos la cual se realizó previamente en el paso 3.1.2, datos críticos y datos sensible.

El análisis de impacto puede se basa principalmente en los tres objetivos de seguridad que son integridad, disponibilidad y confidencialidad. A continuación, se describirán brevemente estos objetivos de seguridad y el impacto si estos no son cumplidos:

- **Pérdida de integridad:** Esto quiere decir que la información sea protegida de modificación no autorizadas. La integridad es perdida en el área de operaciones si hay cambios no autorizados en los diferentes archivos o datos que genera dicha área, más aún en el grupo de geología los cuales manejan información delicada y puede generar problemas si es modificada ya sea intencional o accidentalmente.
- **Pérdida de disponibilidad:** Si la información del área de operaciones no está disponible para sus usuarios, entonces las operaciones de la Petrolera pueden estar afectadas.
- **Pérdida de confidencialidad:** Esto se trata sobre protección de la información de no ser divulgada por personas no autorizadas, ya que muchas veces la información puede usarse para sacar ventaja de otras organizaciones (Stoneburner, 2002, p. 22),

De acuerdo con Stoneburner (2002) el impacto se describe solamente de una manera cualitativa como se puede visualizar en la Tabla de la parte inferior.

Tabla 14

Definición de Impacto.

Magnitud de Impacto	Definición de Impacto
Alta	La vulnerabilidad ejercida (1) puede dar lugar a la pérdida muy costosa de los principales activos o recursos

Magnitud de Impacto	Definición de Impacto
	tangibles; (2) puede violar, dañar o impedir significativamente la misión, reputación o interés de una organización; o (3) puede resultar en muerte humana o lesiones graves
Media	La vulnerabilidad ejercida (1) puede dar lugar a la costosa pérdida de activos o recursos tangibles; (2) puede violar, dañar o impedir la misión, reputación o interés de una organización; o (3) puede resultar en lesiones humanas
Baja	La vulnerabilidad ejercida (1) puede resultar en la pérdida de algunos activos o recursos tangibles o (2) puede afectar notablemente a la misión, reputación o interés.

Tomada de Stoneburner, 2012.

Una vez establecido los parámetros con los que se va a evaluar dichas vulnerabilidades se procede a la valoración de estas, como se visualiza a continuación.

Impacto de las vulnerabilidades

VU1. Falta de control de los datos que se descargan de la red

La magnitud de impacto se la puede considerar Media ya que si ingresa un virus lo suficientemente fuerte puede causar la perdida de algún activo importante o recurso tangible del área de operaciones.

VU2. Uso de contraseñas débiles en computadores

De igual manera la magnitud de impacto de esta vulnerabilidad se la puede considerar Baja ya que en el peor de los casos pudiera causar problemas de perdida de activos o recursos tangibles.

VU3. Inventario incompleto de hardware y software

La magnitud de impacto de esta vulnerabilidad pudiera considerarse Medio ya que, como el inventario se encuentra incompleto los activos pueden perderse y más aún activos como discos duros externos que son la única fuente de respaldo de los sistemas de información que usan los geólogos y los cuales ya se ha indicado que se trata de información delicada, por ende, hasta ocasionar problema significativo en la operabilidad de la Petrolera.

VU4. Falta de actualización de Antivirus en algunos computadores

La falta de actualización del Antivirus en ciertos computadores puede considerarse como magnitud Baja ya que, aunque no esté completamente actualizado sigue protegiendo de todas maneras al computador de la mayoría de las infecciones de virus.

VU5. No hay capacitaciones sobre seguridad informática a los empleados

La falta de capacitaciones en el tema de la seguridad informática podríamos asignarle una magnitud de impacto Medio, muchos usuarios ignoran los correos sobre noticias de seguridad por lo que siguen siendo susceptible a diferentes ataques de ingeniería social o de virus en el computador, lo cual podría llegar a ser un problema a cuando a perdidas costosas de activos o también a un problema de reputación o interés de la empresa.

VU6. Falta de respaldos formales de la información del software Petrel y demás software de Geología

La magnitud de impacto para esta vulnerabilidad es Alta ya que puede ocasionar perdidas muy costosas de los principales activos del área de operaciones como son la información que se encuentran en las estaciones de trabajo del grupo de geología, si llegara a ocurrir un accidente esa información se podría perder y el esfuerzo humano para generarla es bastante grande y, por ende, podría dañar o impedir significativamente la operabilidad de la Petrolera.

VU7. Los puertos USB no se encuentran bloqueados en computadores

No tener un control de bloqueo de los puertos USB podría ocasionar problemas de perdida de información de los computadores de los usuarios, ya que un visitante sin ningún problema podría colocar la USB sin que se dé cuenta y robar información importante con ingeniería social por lo que la magnitud de impacto es: Medio

VU8. Falta de mantenimiento en Equipos de computo

La falta de mantenimiento preventivo en los diferentes equipos del área de operaciones puede causar perdidas muy costosas de los principales activos del área, y por lo tanto impedir significativamente las operaciones de la Petrolera, por lo que la magnitud de impacto es: Alto

VU9. Daño en Equipos electrónicos de campo

Un problema con los equipos electrónicos de campo podría causar una repercusión significativa para la operabilidad de la Petrolera ya que dichos equipos generan datos que son enviados a diario a la Matriz con los cuales se hacen los modelos estáticos y dinámicos, la magnitud de impacto seria: Alto

VU10. Infección de virus y malware en computadores del área de operaciones

La infección de virus o malware en los equipos de cómputo, más aún en las estaciones de trabajo, podría causar perdidas muy costosas de activos o recursos tangibles ya que hay se encuentra la mayoría de información del área de operaciones, al igual que las mismas estaciones de trabajo tienen costos muy elevados y si se dañaran podrían impedir significativamente las operaciones diarias, la magnitud de impacto es: Alto

VU11. Se terceriza el mantenimiento de activos informáticos como servidores y computadores

La pérdida de confidencialidad por parte de una empresa tercerizada para la realización de mantenimiento de los diferentes equipos del área de operaciones podría generar perdidas para la empresa ya que dicha información puede venderse a la competencia y sacar ventaja, y a la misma vez perdidas de reputación de la organización, por lo que la magnitud de impacto es: Medio

Una vez realizada la descripción de la magnitud de impacto en las vulnerabilidades, se generó la tabla de magnitudes impacto como se puede visualizar en la parte inferior.

Tabla 15

Magnitud de Impacto

Código	**Vulnerabilidades**	**Magnitud de Impacto**
VU1	Falta de control de los datos que se descargan de la red	Medio
VU2	Uso de contraseñas débiles en computadores	Bajo
VU3	Inventario incompleto de hardware y software	Medio
VU4	Falta de actualización de Antivirus en algunos computadores	Baja
VU5	No hay capacitaciones sobre seguridad informática a los empleados	Medio
VU6	Falta de respaldos formales de la información del software Petrel y demás software de Geología	Alto
VU7	Los puertos USB no se encuentran bloqueados en computadores	Medio
VU8	Falta de mantenimiento en Equipos de computo	Alto

Código	Vulnerabilidades	Magnitud de Impacto
VU9	Daño en Equipos electrónicos de campo	Alto
VU10	Infección de virus y malware en computadores del área de operaciones	Alto
VU11	Se terceriza el mantenimiento de activos informáticos como servidores y computadores	Media

3.7 Determinación del riesgo

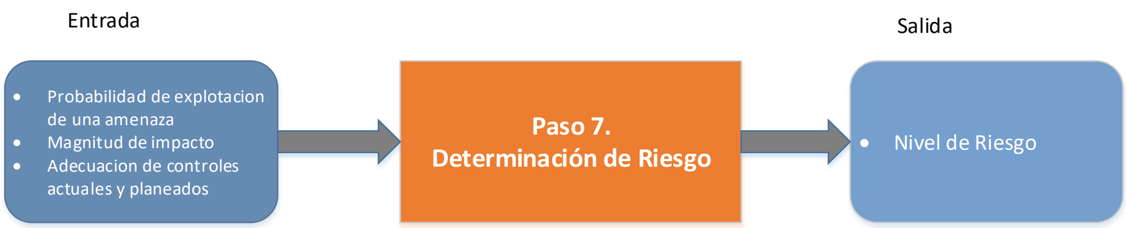

Figura 16. Determinación de Riesgo.

Adaptado de Stoneburner, 2002

El objetivo de este paso es valorar el nivel de riesgo en el que se encuentra el área de operaciones. Para la determinación de riesgos según Stoneburner (2002) debemos tener en cuenta los siguientes puntos:

- Probabilidad de una amenaza.
- Magnitud de Impacto.
- Los controles actuales y planeados.

Dichos puntos ya se analizaron previamente por lo que ahora debemos realizar la multiplicación de los valores asignados a la probabilidad de la amenaza y a la magnitud de impacto. Dichos valores se pueden visualizar en la siguiente Tabla.

Tabla 16

Cálculo del riesgo.

Probabilidad	Impacto		
	Baja (10)	Media (50)	Alta (100)
Alta (1.0)	Baja 10 x 1.0 = 10	Media 50 x 1.0 = 50	Alta 100 x 1.0 = 100
Media (0.5)	Baja 10 x 0.5 = 5	Media 50 x 0.5 = 25	Media 100 x 0.5 = 50
Baja (0.1)	Baja 10 x 0.1 = 1	Baja 50 x 0.1 = 5	Baja 100 x 0.1 = 10

Tomada de Stoneburner, 2012.

Con nuestra tabla para ayudarnos con el cálculo del riesgo procederemos a realizarla, cabe recalcar que si el riesgo es demasiado bajo no hay que descartarlo en todo caso hay que aceptar el riesgo o tratarlo.

Nuestra tabla de determinación de riesgo quedaría de la siguiente manera como se puede visualizar en la Tabla 17

Tabla 17

Determinación del riesgo

Cód.	Vulnerabilidades	Amenaza	Prob	Imp	Riesgo	Control
RI1	VU1. Falta de control de los datos que se descargan de la red	Hackers, Crackers, Perdida Información	Alta	Medio	Medio	CO7: Prohibido el uso de servicios en la nube como Dropbox, One Drive, etc., sin previa autorización CO9: Prohibido el acceso a música, servicios de streaming o videos por internet ya que afecta a la calidad del servicio
RI2	VU2. Uso de contraseñas débiles en computadores	Usuarios no autorizados, Perdida de Información, Robo de Información	Baja	Bajo	Bajo	CO3: Políticas de autentificación de usuarios CO4: La contraseña de cada computador es personal del usuario y no debe de ser divulgada

RI3	VU3. Inventario incompleto de hardware y software	Perdida de Información, Robo de Información, Problemas con Activos Informáticos	Media	Medio	Media	CO12: Los activos informáticos deberán estar identificados y asignados a un usuario en especifico CO13: Cada usuario es responsable del equipo que se le haya asignado
RI4	VU4. Falta de actualización de Antivirus en algunos computadores	Hackers, Crackers, Perdida Información, Usuarios no autorizados, Robo de Información	Medio	Bajo	Bajo	CO14: Gestión de Antivirus por el área de sistemas

RI5	VU5. No hay capacitaciones sobre seguridad informática a los empleados	Hackers, Crackers	Medio	Baja	Baja	CO9: Prohibido el uso de programas o recursos que no tengan licencia o autorización del área de sistemas CO14: Gestión de Antivirus por el área de sistemas CO15: Comunicados de seguridad informática por parte del área de sistemas
RI6	VU6. Falta de respaldos formales de la información del software Petrel y demás software de Geología	Perdida de información, Robo de información	Alto	Alto	Alto	CO10: Cada área de tendrá un espacio designado de espacio para información en los servidores CO11: Si el personal de un área requiere más espacio en los servidores deberá requerir permiso a gerencia.

RI7	VU7. Los puertos USB no se encuentran bloqueados en computadores	Robo de Información, Perdida de información, Personal Insatisfecho.	Medio	Medio	Medio	No existe
RI8	VU8. Falta de mantenimiento en Equipos de computo	Problemas con Activos Informáticos	Medio	Alta	Medio	No existe
RI9	VU9. Daño en Equipos electrónicos de campo	Problemas con Activos Informáticos, Tormenta Eléctrica, Terremoto, Inundaciones, Incendios.	Baja	Alta	Bajo	CO13: Cada usuario es responsable del equipo que se le haya asignado

RI10	VU10. Infección de virus y malware en computadores del área de operaciones	Hackers, Crackers, Perdida de Información.	Baja	Alto	Bajo	CO7: Prohibido el uso de servicios en la nube como Dropbox, One Drive, etc., sin previa autorización CO9: Prohibido el acceso a música, servicios de streaming o videos por internet ya que afecta a la calidad del servicio CO14: Gestión de Antivirus por el área de sistemas
RI11	VU11. Se terceriza el mantenimiento de activos informáticos como servidores y computadores	Filtrado de Información, Robo de Información.	Baja.	Medio	Bajo	No existe

El mapa de calor de riesgo que se muestra a continuación permite visualizar la determinación del riesgo de manera simplificada.

Tabla 18

Mapa de calor del riesgo

		Impacto		
		Baja	**Media**	**Alta**
Probabilidad	**Alta**		1	6
	Media	4	7 3	8
	Bajo	2	5 11	9 10

1. Falta de control de los datos que se descargan de la red
2. Uso de contraseñas débiles en computadores
3. Inventario incompleto de hardware y software
4. Falta de actualización de Antivirus en algunos computadores
5. No hay capacitaciones sobre seguridad informática a los empleados
6. Falta de respaldos formales de la información del
7. Los puertos USB no se encuentran bloqueados en computadores
8. Falta de mantenimiento en Equipos de computo
9. Daño en Equipos electrónicos de campo
10. Infección de virus y malware en computadores del área de operaciones
11. Se terceriza el mantenimiento de activos informáticos como servidores y computadores

4. RESULTADOS DEFINITIVOS

En este capítulo lo que se realiza es disminuir el nivel de riesgo implementando diferentes controles, muchas veces no todos los controles serán implementados ya que estos dependerán de cada organización.

4.1 Recomendaciones de control

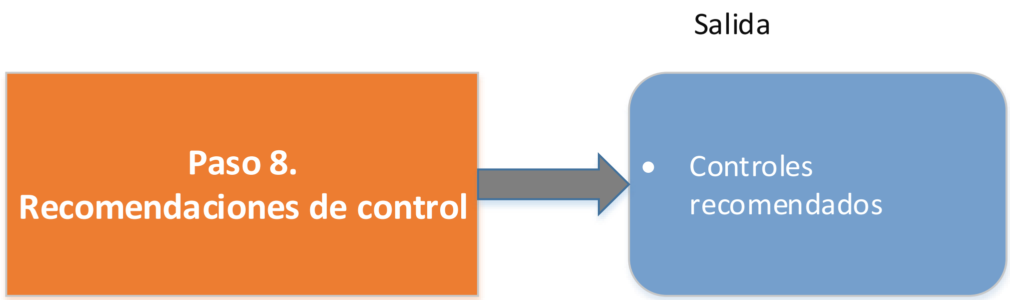

Figura 17. Recomendaciones de control.

Adaptado de Stoneburner, 2002

El objetivo de un control recomendado es reducir el riesgo en este caso en el Área de Operaciones y sus datos a un nivel aceptable, ya que la eliminación de todo el riesgo es casi imposible, por lo que se debe implementar los controles más adecuados.

4.1.1 Ranking de Riesgos

El primer paso en esta etapa es priorizar las acciones realizando un ranking de los riesgos previamente analizado y de esta forma saber cuáles son los riesgos que necesitan prioridad Alta y Media, los riesgos de nivel Bajo en este caso serán aceptados, más no descartados, siempre hay que tener presente el riesgo aun cuando sea demasiado bajo.

El ranking de los riesgos se puede visualizar en la siguiente Tabla.

Tabla 19

Ranking de riesgos

RANKING DE RIESGOS DEL AREA DE OPERACIONES		
Ranking	Riesgo	Valor de Riesgo
1	RI6. Falta de respaldos formales de la información del software Petrel y demás software de Geología.	Alto
2	RI8. Falta de mantenimiento en Equipos de cómputo.	Medio
3	RI1. Falta de control de los datos que se descargan de la red.	Medio
4	RI3. Inventario incompleto de hardware y software.	Medio
5	RI7. Los puertos USB no se encuentran bloqueados en computadores.	Medio

4.1.2 Controles Recomendados

Una vez establecido el ranking de los riesgos se conocerá cuáles son los que se debe tratar con más urgencia, y de esta manera recomendar opciones de control basados en la viabilidad y efectividad para los diferentes riesgos, por lo que se realizará una lista de posibles controles.

Tabla 20

Controles Recomendados

Lista de Controles Recomendados				
Cod	Control Recomendado	Riesgo	Viabilidad	Efectividad
CR1	Contratación de un backup online a medida de la empresa.	Falta de respaldos formales de la información del software Petrel y demás software de Geología	SI	SI
CR2	Realización de un cronograma para mantenimiento preventivo	Falta de mantenimiento en Equipos de computo	SI	SI
CR3	Cancelación de permisos especiales al grupo de geología	Falta de control de los datos que se descargan de la red	SI	SI
CR4	Implementar una aplicación para la gestión de activos e inventario.	Inventario incompleto de hardware y software	SI	SI
CR5	Instalación de software para bloqueo de puertos USB.	Los puertos USB no se encuentran bloqueados en computadores	SI	SI

CR1. - Contratación de un backup en la nube a medida de la empresa

Es una opción cómoda y segura para las empresas, la información se almacena automáticamente cada día y es encriptada, cosa que no sucede con servicios de empresas extranjeras como Google drive y Dropbox, por lo que lo vuelve viable y de la misma forma efectivo. Y de esta forma tendremos un respaldo ordenado de cada persona.

CR2. - Realización de un cronograma para mantenimiento preventivo

Es un control efectivo, con una correcta organización del Departamento de Sistemas se puede lograr y de esta manera prevenir daños más grandes en los equipos informáticos, por el lado de la viabilidad talvez es un poco más complicado por la falta de personal en el área de Sistemas, se puede considerar contratar un pasante.

CR3. - Cancelación de permisos especiales al grupo de geología

Es un control que se puede aplicar con facilidad, normalmente las otras áreas de la Petrolera no tienen estos permisos especiales que tienen el grupo de geología, por tal razón debido al uso inadecuado es viable aplicar.

CR4. - Implementar una aplicación para la gestión de activos e inventario

Ayudaría a tener un control mucho más seguro del inventario, no solo del área de Operaciones sino también de la Petrolera en general, sería algo mucho más fácil de controlar a diferencia de hojas físicas o confusos archivos de Excel por lo que sería efectivo su aplicación en la petrolera, por la viabilidad un sistema de inventario es algo bastante común por lo que no habría mucho problema.

CR5. – Instalación de software para bloqueo de puertos USB

Es una solución efectiva y viable, se puede encontrar diferentes tipos de software free, se necesita de una contraseña para desbloquear, la misma que se solicita al Departamento de Sistemas.

Estos cinco controles recomendados cumplen con las dos características de viabilidad y efectividad, los cuales nos ayudaran con la mitigación de los riesgos, y mejor aún son controles que pueden ser aplicados con un poco de organización y ayuda del área de sistemas, muchas veces los controles recomendados son muy complejos y por lo tanto no son muy atractivos para la gerencia de las empresas.

4.1.3 Análisis de Costo de los Controles Recomendados

Una de las partes importantes en este proceso es el costo de la implementación de estos controles recomendados en la petrolera y el impacto que tendría en la misma los cuales se explicaran a continuación.

CR1. - Contratación de un backup en la nube a medida de la empresa

Como comienzo para este control se puede comenzar con las tres estaciones de trabajo del grupo de geólogos donde la información es más delicada, el costo de un backup en la nube por persona redondea los 70 dólares y con la posibilidad de aumentar la capacidad, por lo tanto un costo redondeado sería de unos 210 dólares, al año el costo sería de 2200 dólares, un precio relativamente bajo por tener asegurada la información más delicada del área de operaciones, el impacto de este control seria medio, el riesgo disminuiría considerablemente ya que ayuda directamente al problema.

CR2. - Realización de un cronograma para mantenimiento preventivo

Este es un control que por sí mismo no tiene un costo directo, pero si se lo quiere cumplir se deberá incluir una persona más al equipo de sistemas, lo que sí es un costo adicional de unos $1.500 que es un impacto bajo, pero lo importante de esto es que esta contratación no solo ayudara en este control sino también para los demás controles ya que el departamento de sistemas de conforma solo de dos personas y tan solo 1 se encarga de todo lo que es redes, seguridad, help desk, etc. Esto ayudaría a equilibrar el trabajo y que siempre se esté pendiente de los diferentes problemas es un costo de impacto medio.

CR3. - Cancelación de permisos especiales al grupo de geología

Es un control que se puede aplicar sin costo alguno y por ende tendrá un impacto bajo, y seria de ayuda a la seguridad de la información ya que la mayoría de los casos de ingresos de virus es en el grupo de geología por lo tanto es necesario este control, en caso especial se podrá habilitar permisos para descarga de información de la nube ya que algunas veces reciben información externa por ese recurso, pero los permisos serán temporales mas no permanentes como antes.

CR4. - Implementar una aplicación para la gestión de activos e inventario

Este es uno de los controles más costosos ya que mandar a desarrollar una aplicación para la gestión de los activos e inventario podría llegar a valorarse entre los $5000 y el impacto podría considerarse medio, pero considerando la falta de organización en el inventario y bodega durante todos estos años esta puede ser la mejor opción.

CR5. – Instalación de software para bloqueo de puertos USB

Este control no tiene un costo económico ya que este software muchas veces no tiene costo y son fáciles de instalar, además son fáciles administrar para el personal de sistemas, por lo que el impacto es bajo y solo tendría veneficios directos a la seguridad de la información.

La información anteriormente explicada se resumirá en la siguiente tabla.

Tabla 21

Análisis de Costo

ANALISIS DE COSTO				
Cod	Control Recomendado	Impacto de Implementación	Costo Aproximado	Impacto de no Implementar
CR1	Contratación de un backup online a medida de la empresa.	Medio	2200	Alto
CR2	Realización de un cronograma para mantenimiento preventivo	Bajo	1500	Medio
CR3	Cancelación de permisos especiales al grupo de geología	Bajo	0	Medio
CR4	Implementar una aplicación para la gestión de activos e inventario	Medio	5000	Medio
CR5	Instalación de software para bloqueo de puertos USB	Bajo	0	Medio

Una vez se tenga un análisis de los costos y de su impacto se deberá asignar a los responsables que ayudarán a aplicar estos controles, los cuales son el departamento de sistemas y por lo tanto el área de finanzas, donde básicamente son tres personas las que toman las decisiones de esta índole, el gerente del área de finanzas y el personal de sistemas que se dividen en la responsable de la seguridad y redes de comunicación, y el encargado de bases de datos, por lo cual la asignación de los controles es de la siguiente manera como vemos en la tabla de la parte inferior.

Tabla 22

Asignación de responsabilidades

Asignación de Responsabilidades				
Cod	Control Recomendado	Áreas	Asignados	Tiempo Implementación
CR1	Contratación de un backup online a medida de la empresa.	Área de Finanzas y Departamento de Sistemas	-Gerente de Finanzas -Responsable de Base de datos	2 a 4 semanas
CR2	Realización de un cronograma para mantenimiento preventivo	Departamento de Sistemas	-Responsable de Seguridad y redes de comunicación	1 a 2 semanas
CR3	Cancelación de permisos especiales al grupo de geología	Departamento de Sistemas	-Responsable de Seguridad y redes de comunicación	Implementación inmediata

Asignación de Responsabilidades				
Cod	Control Recomendado	Áreas	Asignados	Tiempo Implementación
CR4	Implementar una aplicación para la gestión de activos e inventario	Área de Finanzas y Departamento de Sistemas	-Gerente de Finanzas -Responsable de Base de datos -Responsable de Seguridad y redes de comunicación	4 a 5 meses ya que se debe desarrollar la aplicación
CR5	Instalación de software para bloqueo de puertos USB	Departamento de Sistemas	-Responsable de Seguridad y redes de comunicación	1 semana

Una vez hecho el análisis de los controles recomendados, los cuales se usarán para la mitigación de los riesgos se procederá con la documentación de los resultados la cual normalmente se presenta a la alta gerencia para la toma de futuras decisiones.

4.2 Documentación de Resultados

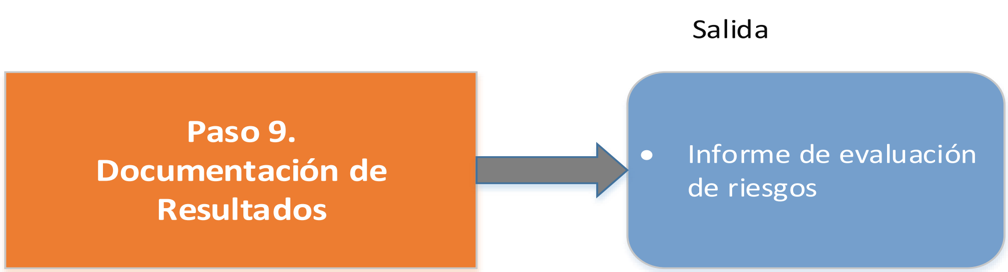

Figura 18. Documentación de resultados.

Adaptado de Stoneburner, 2002

En este paso se realizará el informe de evaluación de riesgos en el cual se describe las amenazas y vulnerabilidades, como también los riesgos y las recomendaciones para la implementación del control y realizar la mitigación de los riesgos.

Informe de la valoración de riesgos y estrategias de mitigación de riesgos de la información en el Área de Operaciones basado en la Metodología NIST SP 800-30.

Resumen

I) Objetivo

Informar a la Gerencia de los resultados obtenidos durante la valoración de los riesgos y estrategias de mitigación de riesgos de la información en el Área de Operaciones.

II) Antecedentes

La Petrolera actualmente cuenta con varias áreas de trabajo para su correcto funcionamiento, una de las más importantes es el área de operaciones en la cual se encuentra el grupo de geología, el cual maneja información importante para la Petrolera y la cual no ha sido respaldada para su seguridad, lo cual ha producido incidentes de pérdida de información. Por esta razón es necesario que la gerencia entienda los problemas que se han encontrado y de esta manera proponer una solución para reducir el riesgo de pérdida información importante para la Petrolera.

III) Resultados

Después de la realización de un análisis con la metodología NIST SP 800-30, se obtuvieron los siguientes resultados que se resumen en: 13 posibles amenazas, 11 vulnerabilidades, 11 riesgos resultantes, de los cuales 6 tienen un riesgo bajo y fueron aceptados más no desechados, se definen 5 riesgos para los cuales se propone 5 controles para ayudar a la mitigación de riesgo que se encuentran en la parte superior en el apartado 4.1.2 controles recomendados. De igual forma se debe destacar el punto 4.1.3 que nos indica el análisis de costos de los controles recomendados, y nos ayuda a saber que controles son factibles de aplicar, cabe mencionar que el control CR4 tiene el costo más alto que es de $5000 pero es un gasto de una sola vez, puede parecer ser alto pero por la seguridad de los activos informáticos y su información es algo necesario después de todos estos años de desorganización con dicho tema, de igual manera el tema de la falta de respaldos de la información del grupo de geología es un tema a tener en cuenta ya que por $2200 se puede resguardar la información y no tener perdida de archivos de años de antigüedad y los se siguen usando hasta ahora, lo cual significaría años de trabajo perdido.

IV) Conclusión

Con los resultados obtenidos se espera la aceptación del plan de mitigación de riesgos de la información con los controles propuestos y de esta manera mejorar la gestión de la seguridad en el Área de Operaciones de la Petrolera.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El resultado de la combinación de la metodología NIST SP 800-30 en conjunto con la guía para la gestión y clasificación de activos de información del Mintic nos ayudó a identificar los principales activos tecnológicos donde se encuentra la información más importante del Área de Operaciones de una manera más acertada.

Los principales activos tecnológicos definidos fueron las estaciones de trabajo del grupo de geólogos que tienen la mayor criticidad, y son los activos que están más relacionados con el riesgo RI6 que está catalogado como Alto y por ende se debe dar prioridad al momento de implementar los controles recomendados.

Las amenazas de tipo humano como también tecnológicas son las que más afectan a la disponibilidad, integridad y confidencialidad de los activos críticos del Área de Operaciones de la Petrolera.

Una vez realizado el análisis de los controles recomendados es necesario integrar una persona más al Departamento de Sistemas, para que de esta forma se reparta el trabajo de la administración de los usuarios y sistemas de mejor manera, Los controles que están al alcance de poder ser aplicados en la Petrolera, ya que dos de ellos no tendrían costo en aplicarlos y los otros tres controles tienen costo, pero no uno demasiado elevado si estamos hablando de una Petrolera.

5.2 Recomendaciones

Al momento de realizar un análisis de riesgo es necesario tener una comunicación abierta con los usuarios y con el departamento de sistemas, para que la obtención de la información sea eficaz y fácil de obtener.

Tomar en consideración el tipo de organización a la que se realiza el análisis de riesgo para determinar sus limitaciones y comprobar si la empresa está en condiciones de adoptar un control ya sea por el impacto al usuario o por la parte económica.

Es importante que se realicen reuniones o capacitaciones sobre la seguridad de la información en la empresa con la finalidad de identificar las amenazas a las que pueden estar expuestas.

Se recomienda que la gerencia aplique uno o varios de los controles recomendados, para así cumplir con el plan de la mitigación de los riesgos de la información del área de operación, y de esta manera minimizar los riesgos al nivel más bajo posible.

REFERENCIAS

Ambientum. (2016). El Petróleo. Recuperado el 20 de octubre de 2019, de https://www.ambientum.com/enciclopedia_medioambiental/energia/el_petroleo.asp.

Eduardo Aguirre. (2007). El Petróleo: Una visión sencilla de nuestra industria petrolera. Recuperado el 24 de octubre de 2019, de https://ebookcentral.proquest.com/lib/udlasp/reader.action?docID=3173507

E.E Hydrocarbons. (2012). Desarrollo temático Hidrocarburos. Recuperado el 15 de octubre de 2019, de http://eehydrocarbonscompany.blogspot.com/

EliteForm. (2018). Método de análisis de riesgos NIST SP 800-30. Recuperado el 06 de julio de 2019, de http://elite-formacion.blogspot.com/2018/04/metodo-de-analisis-de-risgos-nist-sp.html

Ester Chicano. (2014). Auditoria de seguridad informática. Recuperado el 22 de noviembre de 2019, de https://ebookcentral.proquest.com/lib/udlasp/reader.action?docID=4184005

Ever Arrieta. (2017). Método inductivo y deductivo. Recuperado el 08 de julio de 2019, de https://www.lifeder.com/metodo-inductivo-deductivo/

Gary Stoneburner, Alice G y Alexis F. (2002). Risk Management guide for information technology systems. Recuperado el 28 de mayo de 2019, de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

Gema E, Rosa R y David R. (2013). Seguridad Informática. Recuperado el 14 de noviembre de 2019, de https://ebookcentral.proquest.com/lib/udlasp/reader.action?docID=3217398

José Molina. (2000). Seguridad de la información criptología. Recuperado el 14 de noviembre de 2019, de https://ebookcentral.proquest.com/lib/udlasp/reader.action?docID=3155970

Magerti. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado el 10 de diciembre de 2019, de https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

María Estela. (2019). Método inductivo. Recuperado el 08 de julio de 2019, de https://concepto.de/metodo-inductivo/

Mintic. (2016). Guía para la gestión y clasificación de Activos Informáticos. Recuperado el 10 de diciembre de 2019, de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Richard S. Kraus. (2012). 75- Petróleo: Prospección y perforación. Recuperado el 20 de octubre de 2019, de https://ebookcentral.proquest.com/lib/udlasp/reader.action?docID=3204062

Tic.Portal. (2019). Sistemas ERP. Recuperado el 29 de mayo de 2019, de https://www.ticportal.es/temas/enterprise-resource-planning/que-es-sistema-erp

Textos Científicos. (2005). Recuperación asistida de petróleo. Recuperado 28 de octubre de 2019, de https://www.textoscientificos.com/petroleo/recuperacion